Dual-PTZ Camera Web 5.0

User Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

Foreword

General

This manual introduces the functions and operations of the Dual-PTZ Camera (hereinafter 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 in death 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.
ESD	Electrostatic Sensitive Devices. Indicates a device that is sensitive to electrostatic discharge.
ELECTRIC SHOCK	Indicates dangerous high voltage. Take care to avoid coming into contact with electricity.
LASER RADIATION	Indicates a laser radiation hazard. Take care to avoid exposure to a laser beam.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	November 2024

Privacy Protection Notice

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

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

Table of Contents

Foreword I
1 Overview 1
1.1 Introduction 1
1.2 Functions 1
1.2.1 Basic functions 1
1.2.2 AI Functions 2
2 Configuration Flow 4
3 Device Initialization 5
4 Setting 8
4.1 Device Login 8
4.2 Local 11
4.3 Camera 12
4.3.1 Setting Image Parameters 12
4.3.2 Setting Splicing Parameters 26
4.3.3 Setting Encode Parameters 26
4.3.4 Audio 38
4.4 Network 41
4.4.1 TCP/IP 41
4.4.2 Port 43
4.4.3 PPPoE 45
4.4.4 DDNS 46
4.4.5 Email 47
4.4.6 UPnP 50
4.4.7 SNMP 50
4.4.8 Bonjour 53
4.4.9 Multicast 54
4.4.10 Register 55
4.4.11 QoS 56
4.4.12 Platform Access 56
4.4.13 Basic Service 59
4.5 PTZ 61
4.5.1 Configuring Presets 61
4.5.2 Configuring Tour 62
4.5.3 Configuring Scan 63
4.5.4 Configuring Pattern 64
4.5.5 Configuring Pan 64
4.5.6 Configuring PTZ Speed 65

4.5.7 Configuring Idle Motion....66
4.5.8 Configuring PowerUp....66
4.5.9 Configuring PTZ Rotation Limit....67
4.5.10 Configuring Scheduled Task....68
4.5.11 Configuring PTZ Maintenance....69
4.5.12 Configuring Protocol....69
4.6 Event....70
4.6.1 Setting Alarm Linkage....70
4.6.2 Setting Exception....77
4.6.3 Setting Video Detection....80
4.6.4 Setting Audio Detection....84
4.6.5 Setting Smart Motion....85
4.6.6 Setting Upload....86
4.7 Storage....87
4.8 System....87
4.8.1 General....88
4.8.2 Account....90
4.8.3 Peripheral Management....97
5 Live....99
5.1 Live Page....99
5.2 Configuring Encoding....100
5.3 Live View Function Bar....100
5.4 Window Adjustment Bar....101
5.4.1 Adjustment....101
5.4.2 PTZ Control....102
5.4.3 PTZ Function....103
5.4.4 Image Adjustment....104
5.4.5 Peripheral Management....105
5.5 Display Mode....105
6 Record....108
6.1 Playback....108
6.1.1 Playing Back Video....108
6.1.2 Clipping Video....110
6.1.3 Downloading Video....111
6.2 Setting Record Control....112
6.3 Setting Record Plan....113
6.4 Storage....115
6.4.1 Local Storage....116
6.4.2 Network Storage....117
7 Picture....120

7.1 Playback 120
7.1.1 Playing Back Picture 120
7.1.2 Downloading Picture 121
7.2 Setting Snapshot Parameters 123
7.3 Setting Snapshot Plan 124
7.4 Snapshot by Location 125
7.5 Storage 126
7.5.1 Local Storage 127
7.5.2 Network Storage 127
8 AI 130
8.1 Configuring Smart Plan 130
8.2 Configuring Face Detection 130
8.2.1 Configuring Face Detection Rules 131
8.2.2 Viewing Face Detection Results 133
8.3 Configuring IVS 134
8.3.1 Global Configuration 134
8.3.2 Rule Configuration 138
8.4 Panoramic Linkage 143
8.4.1 Linkage Track 143
8.4.2 Main/sub Calibration 145
9 Security 147
9.1 Security Status 147
9.2 System Service 148
9.2.1 802.1x 148
9.2.2 HTTPS 149
9.3 Attack Defense 150
9.3.1 Firewall 150
9.3.2 Account Lockout 151
9.3.3 Anti-DoS Attack 152
9.4 CA Certificate 153
9.4.1 Installing Device Certificate 153
9.4.2 Installing Trusted CA Certificate 156
9.5 A/V Encryption 156
9.6 Security Warning 157
10 Maintenance Center 159
10.1 One-click Diagnosis 159
10.2 System Information 160
10.2.1 Viewing Version Information 160
10.2.2 Viewing Online User 160
10.2.3 Viewing Legal Information 160

10.3 Log Information....160
10.3.1 Viewing Local Log....161
10.3.2 Setting Remote Log....162
10.4 Manager....162
10.4.1 Requirements....162
10.4.2 Maintenance....162
10.4.3 Import/Export....163
10.4.4 Default....164
10.5 Update....164
10.6 Advanced Maintenance....165
10.6.1 Export....165
10.6.2 Packet Capture....166
10.6.3 Run Log....166
11 App Center....167
11.1 Application Overview....167
11.2 Application....167
Appendix 1 Security Commitment and Recommendation....169

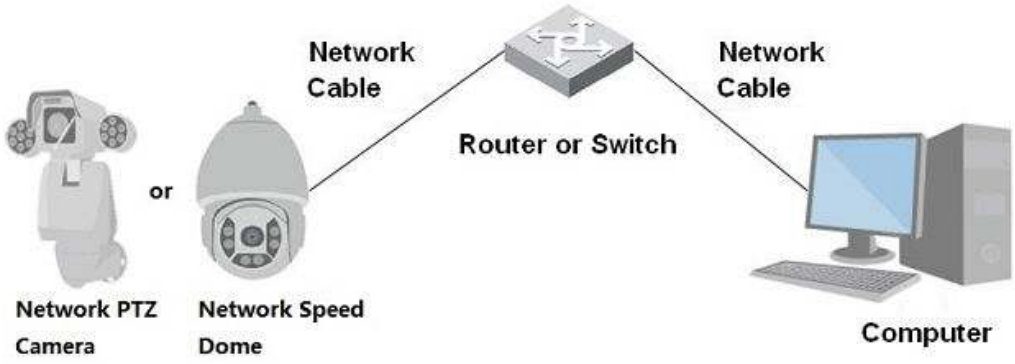
1 Overview

1.1 Introduction

The Camera is a combination of traditional camera and network technology. Users can remotely connect to the Camera through the network for configuration and management.

Before accessing the PTZ Camera through the network, you need its IP address, which can be searched for by ConfigTool.

Figure 1-1 Connected through network router or switch



1.2 Functions

Functions might be different depending on the model.

1.2.1 Basic functions

Real-time Monitoring

- Live view.
- When watching the live view, you can enable audio, and talk to people in the monitoring area to quickly process exceptions.
- Adjust the image to the proper position by PTZ.
- Take a snapshot or three snapshots of the exceptional monitoring image for subsequent viewing and processing.
- Record the monitoring image with exceptions for subsequent viewing and processing.
- Configure coding parameters, and adjust live view.

Recording

- Auto recording as scheduled.
- Play back recorded videos and images.
- Download recorded videos and images.
- Link recordings when alarms are triggered.

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 Functions

Alarm

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

Video Detection

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

Audio Detection

- Detects 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.

Panorama Linkage

Panorama camera serves as the main camera to view panoramic images. Detail camera serves as the subordinate camera to view detailed images.

IVS

- Supports 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.

Face Recognition

- Detects 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.

Video Metadata

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

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 snapshots.

Exception Processing

- SD card error detection, network exception detection and tampering detection.
- When SD card error or tampering alarm is triggered, the system performs linkages such as alarm output and email sending.
- When a network exception is detected, the system performs linkages such as video recording and alarm output.

2 Configuration Flow

Configure the Camera as needed.

Figure 2-1 Configuration flow

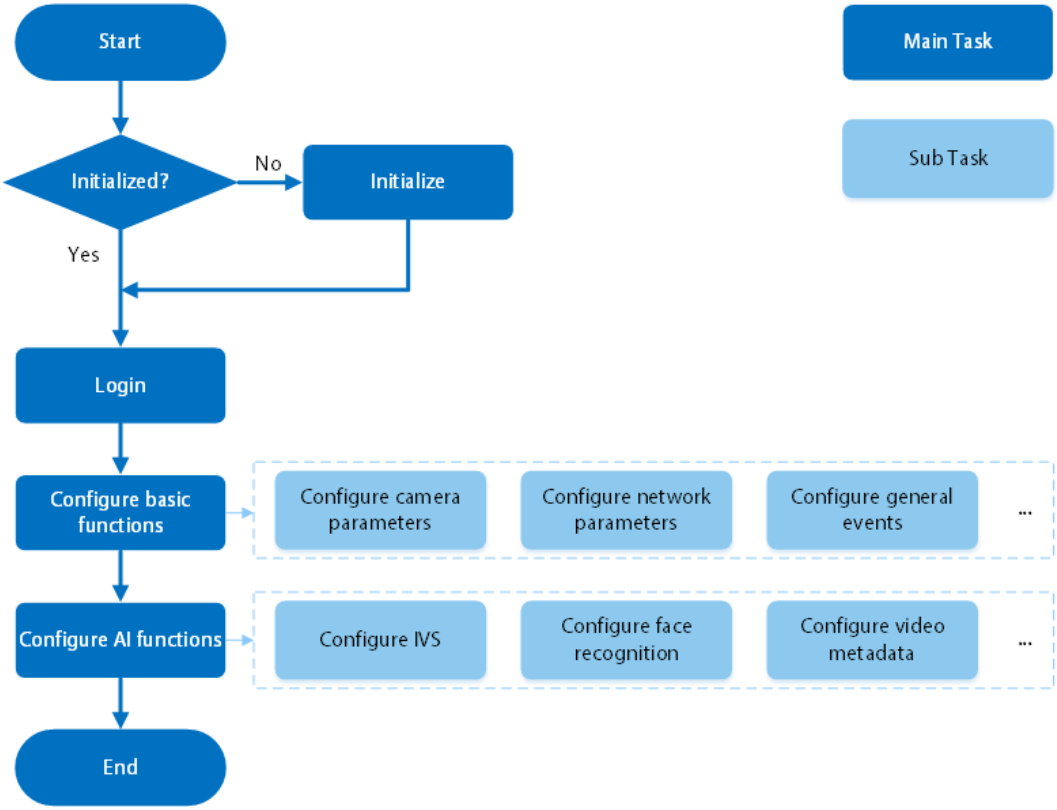


Table 2-1 Flow description

Configuration	Description	Reference
Login	Open the browser and enter the IP address to log in to the webpage. The camera IP address is 192.168.1.108 by default.	"4.1 Device Login"
Initialization	Initialize the Camera when you use it for the first time.	"3 Device Initialization"
Configure basic functions	Configure camera parameters, network parameters, general events and more.	"4 Setting"
Configure AI functions	Configure detection rules for AI events.	"8 AI"

3 Device Initialization

Background Information

Device initialization is required for the first-time use. This manual is focused on the operation on the webpage. You can also initialize the Camera through ConfigTool, NVR (Network Video Recorder), or platforms such as DSS Pro.

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

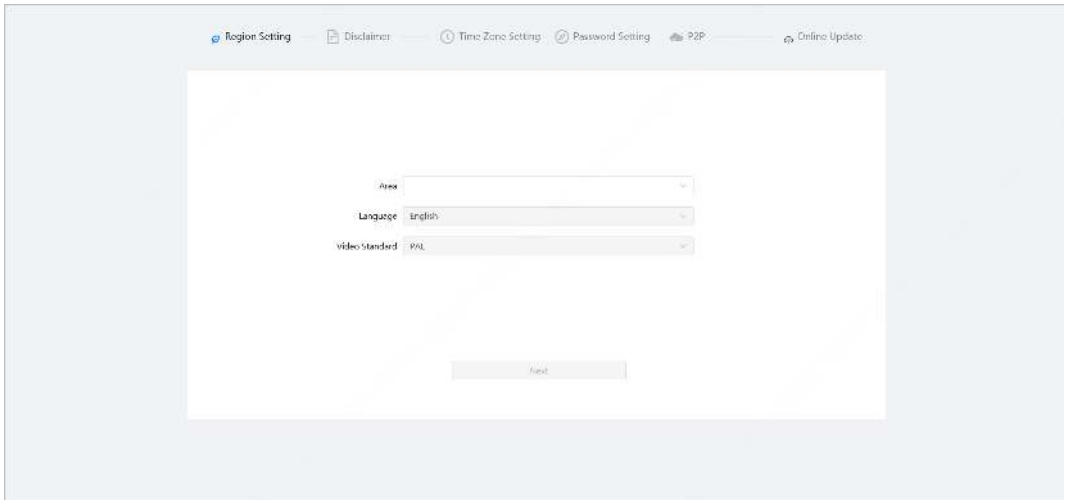
Procedure

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

The IP is 192.168.1.108 by default.

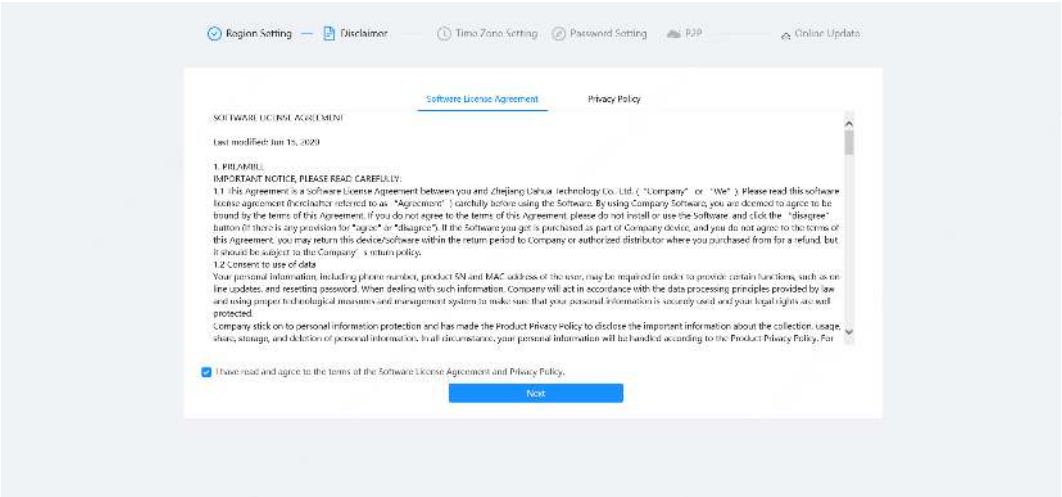
Step 2 Select the area, language, and video standard according to the actual situation, and then click **Next**.

Figure 3-1 Region setting



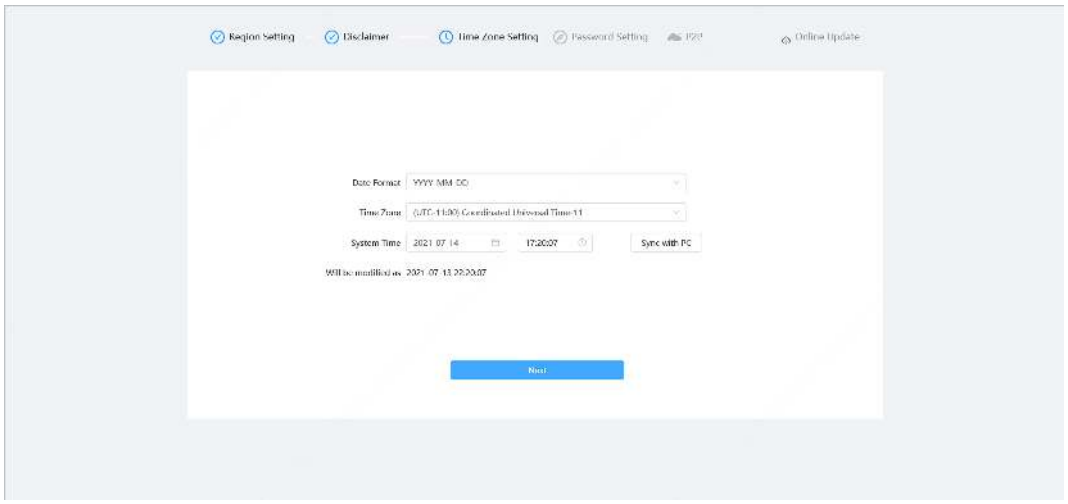
Step 3 Select the **I have read and agree to the terms of the Software License Agreement and Privacy Policy** checkbox, and then click **Next**.

Figure 3-2 Disclaimer



Step 4 Configure the time parameters, and then click **Next**.

Figure 3-3 Time zone setting



Step 5 Set the password for admin account.

Figure 3-4 Password setting

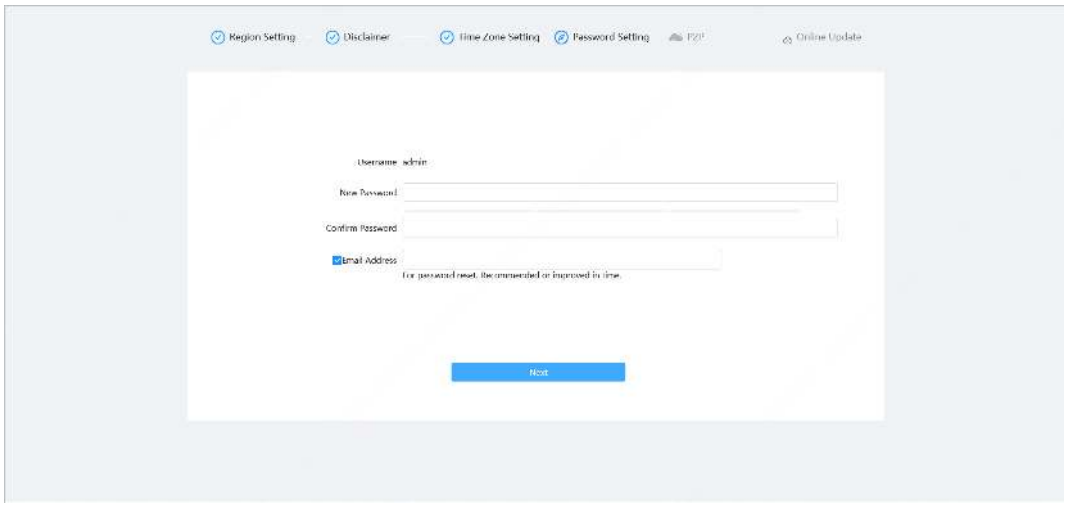
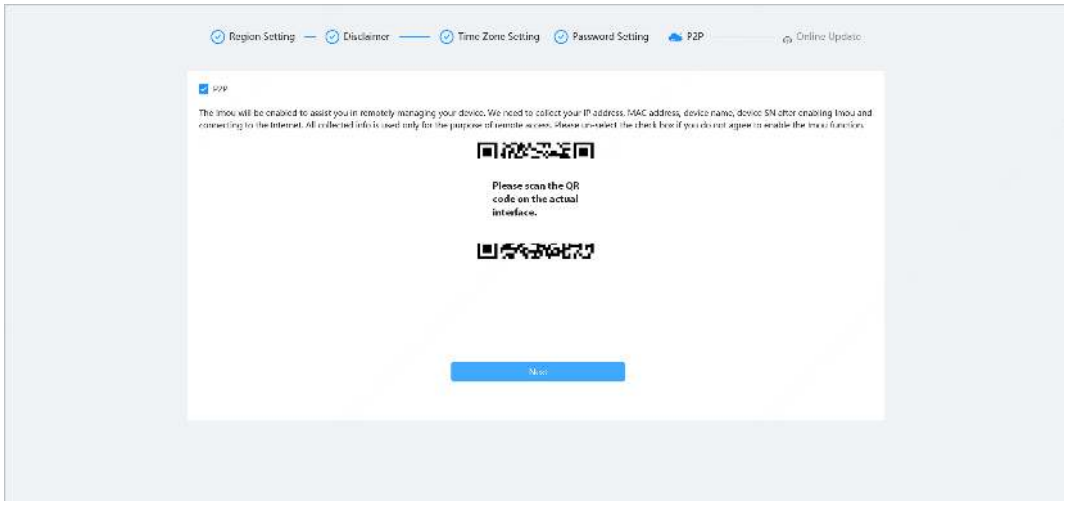


Table 3-1 Description of password configuration

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 email address.

Step 6 Click **Next** , and the **P2P** page is displayed.

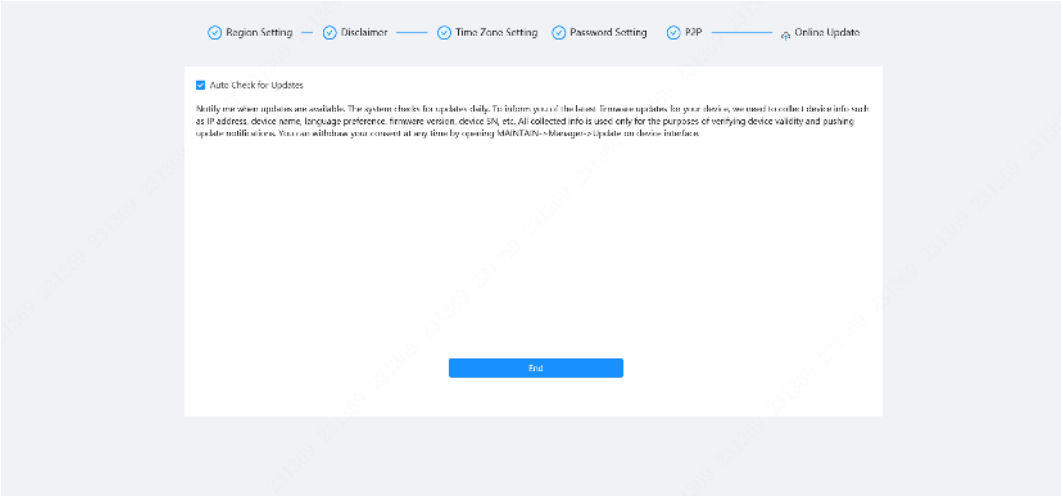
Figure 3-5 P2P



Step 7 Click **Next** , and the **Online Update** page is displayed.

Click **End** to complete initialization.

Figure 3-6 Online update



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 1 as 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 webpage through a browser.

Prerequisites

- You need to initialize the Camera before logging in to the webpage. For details, see"3 Device Initialization".
- When logging in to the webpage, keep the IP of the computer and the IP of the Camera on the same network.

Procedure

Step 1 Open the browser, enter the device IP address (192.168.1.108 by default) in the address box, and then press **Enter**.

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. For details, see "4.8.2.2 Resetting Password".

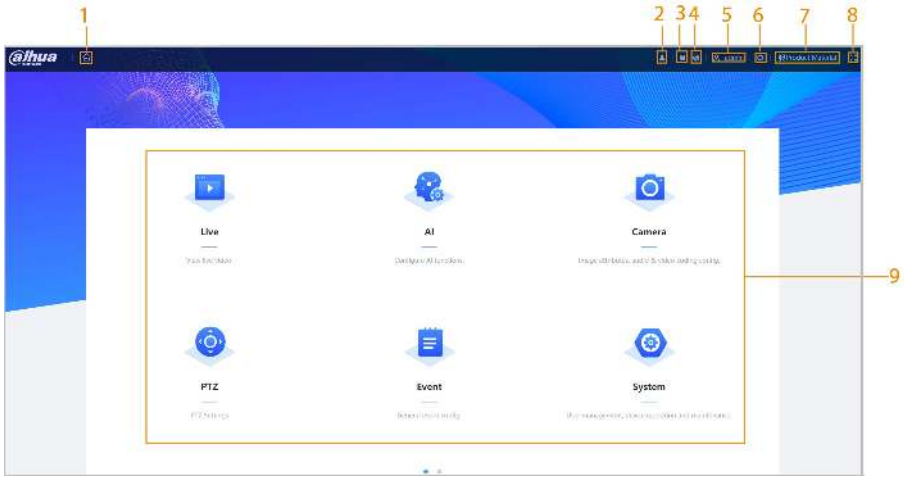
Figure 4-1 Login

Step 3 Click **Login**.

The **Live** page is displayed. For details, see "5.1 Live Page".

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

Figure 4-2 Main page



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

Table 4-1 Description of main page

No.	Button	Description
1		Display the main page.
2		Subscribe to alarm. For details, see "4.6.1.3.2 Subscribing Alarm Information".
3		Set the skin.
4		Set the language.
5	admin	• Click and select **Restart**, and the camera restarts. • Click and select **Logout** to go back to the login page.
6		Configure the basic parameters. For details, see "4 Setting".
7	Product Material	Scan the QR code to obtain the product material.
8		• Click the button to enter full screen mode. • Click to exit full screen mode.
9	Main Page	The main page includes the following modules. Click on the bottom of the page to switch between multiple interfaces. • 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: Configuring PTZ functions. • Event: Configure alarm linkage parameters of general events. • System: Configure basic system parameters, manage users and peripherals, maintain and upgrade the system. • Security: Check the device security status and set security functions. • Record: Configure record functions, play back or download recorded videos. When playing back multi-channel recordings, you can choose channel No. to play back. • Picture: Configure picture functions, play back or download image files. When playing back multi-channel images, you can choose channel No. to play back.

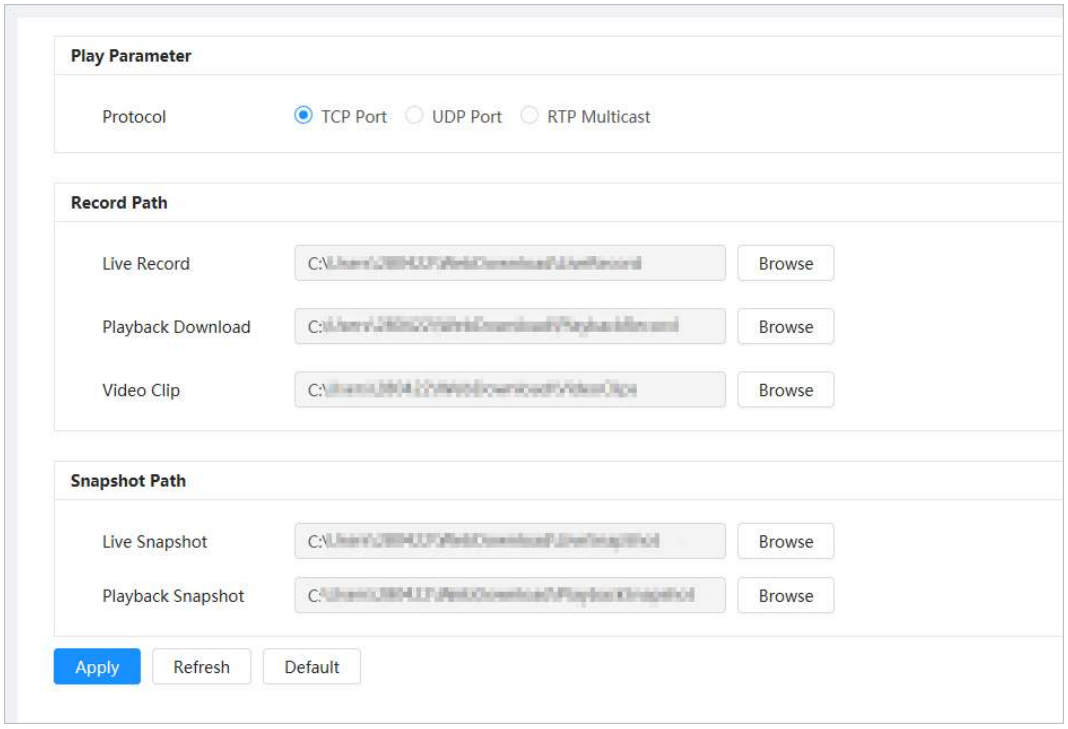
4.2 Local

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**.

Figure 4-3 Local



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. For details, see "4.4.9 Multicast".

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

Table 4-2 Description of local parameter

Parameter	Description
Protocol	You can select the network transmission protocol, and the options are **TCP** , **UDP** and **Multicast**. Before selecting **Multicast** , make sure that you have set the **Multicast** parameters.

Parameter	Description	
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. 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**.

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 Setting Image Parameters

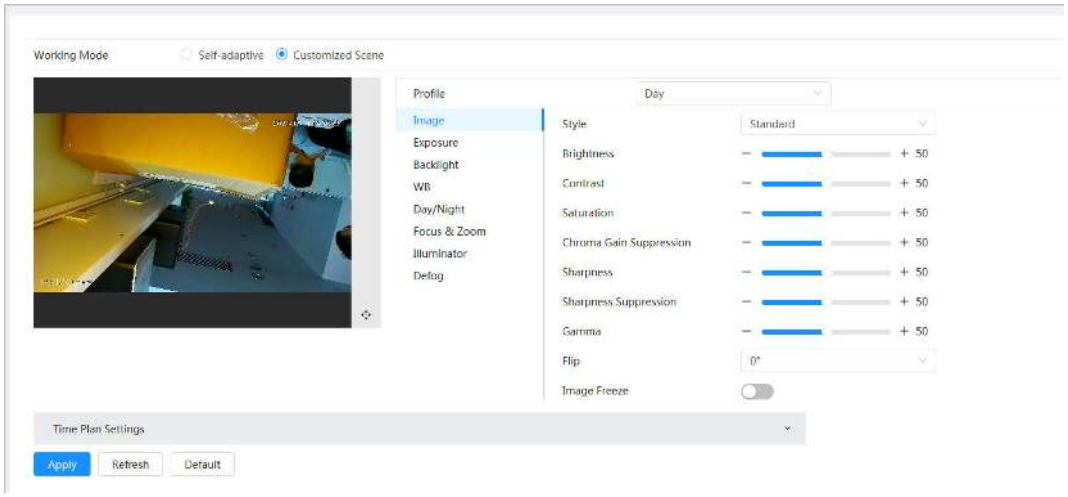
Configure image parameters according to the actual situation, including image, exposure, backlight, white balance, Day/Night, and more.

4.3.1.1 Page Layout

Configure camera parameters to improve the scene 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, front light, to set and view the configuration parameters and effects under the corresponding type, including image, exposure, backlight.

Figure 4-4 Camera conditions (common camera)



4.3.1.2 Configuring Operating Mode

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

Procedure

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 Step 5 .
- Customized scene: camera monitors according to the settings of the profile type at different times.

  If you select **Customized scene**, go straight to Step 3 .

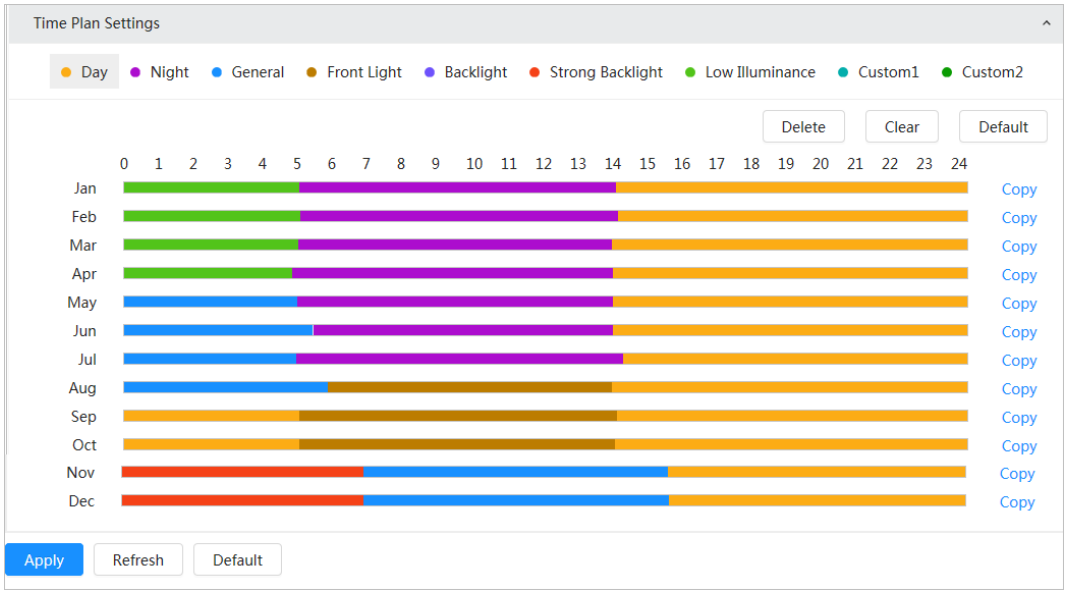
Step 3 Select configuration file type.

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

Step 4 Set time plans.

Support setting daily schedule by month.

Figure 4-5 Time plan settings



1. Click **Time Plan Settings** or to open time plan.
2. Click to configure file type, for example **general** , left-drag on the timeline to set the time period 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. Please click **Delete** or **Clear** before you start setting time period.
3. (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 Picture

You can configure picture parameters as needed. The actual parameters of the camera can be adjusted here.

Procedure

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 4-6 Picture

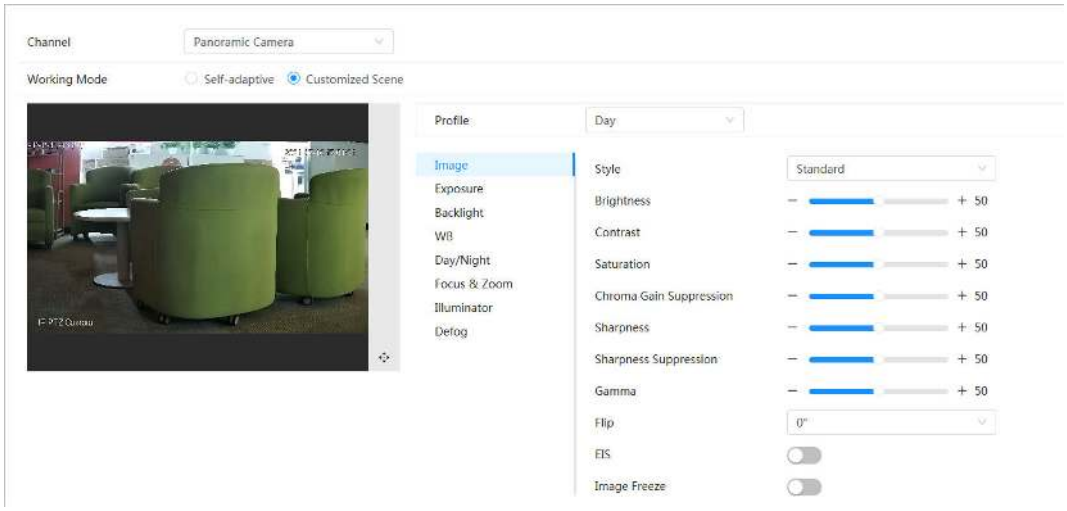


Table 4-3 Description of picture parameters

Parameter	Description
Style	Select the picture style from soft, standard and vivid. ● Standard: Default image style, displays the actual color of the image. ● Soft: The hue of the image is weaker than the actual one, and contrast is smaller. ● Vivid: The image is more vivid than the actual one.
Brightness	Change the overall brightness of the picture. The higher the value is, the brighter the picture will be, and the weaker its darker. The picture might be hazy if the value is configured too high.
Contrast	Changes the contrast of the picture. The higher the value is, the greater the contrast will be between bright and dark areas. If the value is too big, the dark area will be too dark and the bright area will more vulnerable to overexposure. The picture might be hazy if the value is set too small.
Saturation	Makes the color stronger or lighter. The higher the value is, the deeper the color will be, and the weaker the light. Saturation value does not change image brightness.
Chroma Gain Suppression	Reduces the image color and prevents it from being too strong. The higher the value, the stronger the effect. This parameter takes effect only when the Camera is in an environment with low luminance.
Sharpness	Changes the sharpness of picture edges. The higher the value is, the clearer the picture edges will be. If the value is too big, image noise is more likely to appear.

Parameter	Description
Sharpness Suppression	Change the sharpness NCT level of the Camera. The bigger the value, the stronger the sharpness CNT. This parameter takes effect only when the Camera is in an environment with low luminance.
Gamma	Changes the picture brightness and contrast in a non-linear way. The higher the value is, the brighter the picture will be, and the weaker the darkness.
Flip	Change the display direction of the image. ● Normal: The normal display of the image. ● Reflection: The image flips up and down. This function is available on select models.
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. This function is available on select models.

Step 3 Click **Apply**.

4.3.1.4 Exposure

Background Information

Configure iris and shutter to improve image clarity.

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

Procedure

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 4-7 Exposure

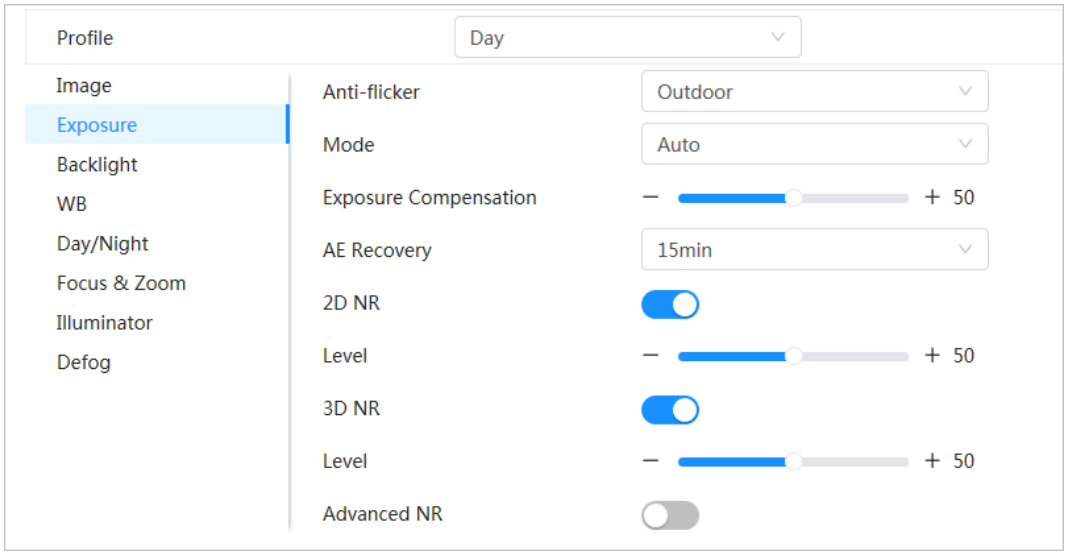


Table 4-4 Description of exposure parameters

Parameter	Description
Anti-flicker	You can select **50Hz** , **60Hz**, or **Outdoor** from the list. ● **50Hz** : When the electric supply is 50 Hz, the system adjusts the exposure according to ambient light automatically to ensure that stripes do not appear. ● **60Hz** : When the electric supply is 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**, **Iris Priority**. Different devices support different exposure modes.
Mode	Set the exposure modes. You can select **Auto** , **Manual**, **Iris Priority**, **Shutter Priority** 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 adjust the shutter value. If the image brightness is not 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 Device automatically adjusts the aperture and gain according to the scene brightness. ● **Gain Priority** : Gain value and exposure compensation value can be adjusted manually.
Gain	If you select **Gain Priority** or **Manual**, you can set gain range to automatically increase the gain of the device when the illumination is low, thus obtaining a clear image.

Parameter	Description
Shutter	Set the effective exposure time. The smaller the value, the shorter the exposure time.
Shutter range	If you select **Shutter Priority** or **Manual**, and select **Shutter** as **Custom**, you can 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 pictures by expending the automatic exposure time effectively reduces image noise, but pictures 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. This function is available on select models.
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-domain and space-domain based on the video filter method.
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. The value ranges from 0 to 100.

Some models do not support advanced noise reduction, time domain grade, or space domain grade.

Step 3 Click **Apply**.

4.3.1.5 Backlight

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

Procedure

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 4-8 Backlight mode

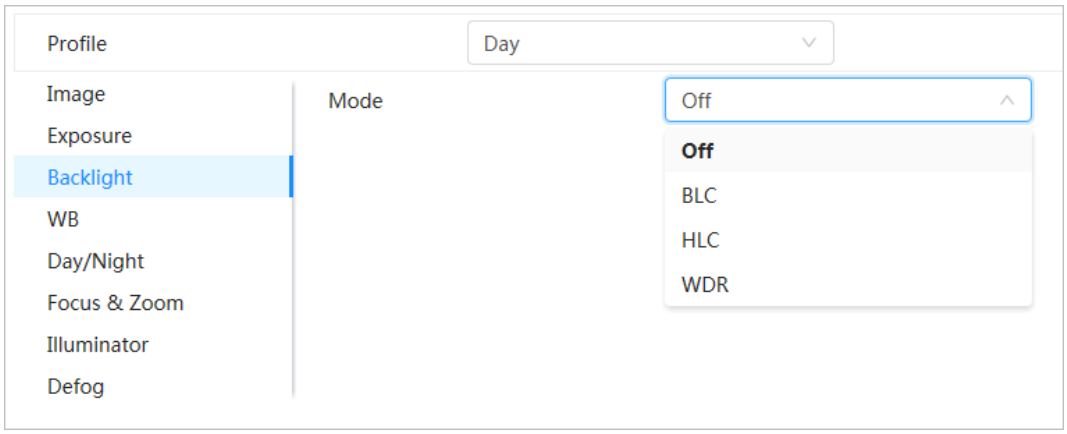


Table 4-5 Description of backlight parameters

Parameter	Description
BLC	Enable BLC, the camera can get a clearer image of the dark areas on the target when shooting against light. You can select default mode or customized mode. ● When in default mode, the system adjusts exposure according to ambient lighting conditions automatically to ensure the clarity of the darkest area. ● When in customized mode, the system auto adjusts exposure only to the set area according to ambient lighting conditions to ensure the image of the set area is at its ideal brightness.
WDR	The system dims bright areas and compensates for dark areas to ensure the clarity of all areas. The higher the value is, the stronger the darkness will 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 a toll station or parking lot), the camera will dim strong lights, and reduce the size of Halo zone to lower the brightness of the whole image, so that the 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

WB function makes the image color display precisely as it is. When in WB mode, white objects are displayed in a white color depending on the environment.

Procedure

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 the white balance mode.

Figure 4-9 White balance

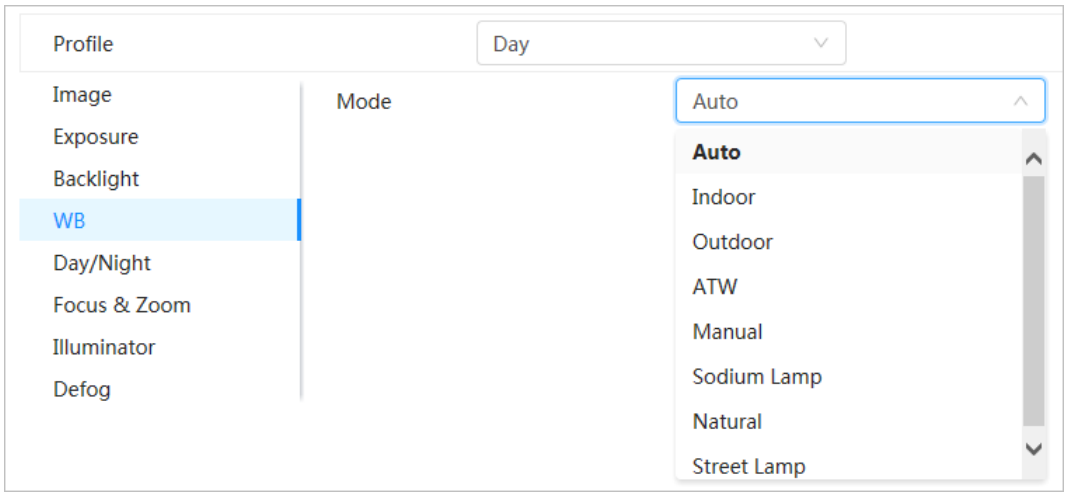


Table 4-6 Description of white balance parameters

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 to ensure 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 to ensure color precision.
Street Lamp	The system compensates WB to outdoor night scenes to ensure color precision.

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-white mode according to the actual condition.

Procedure

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 4-10 Day/Night mode

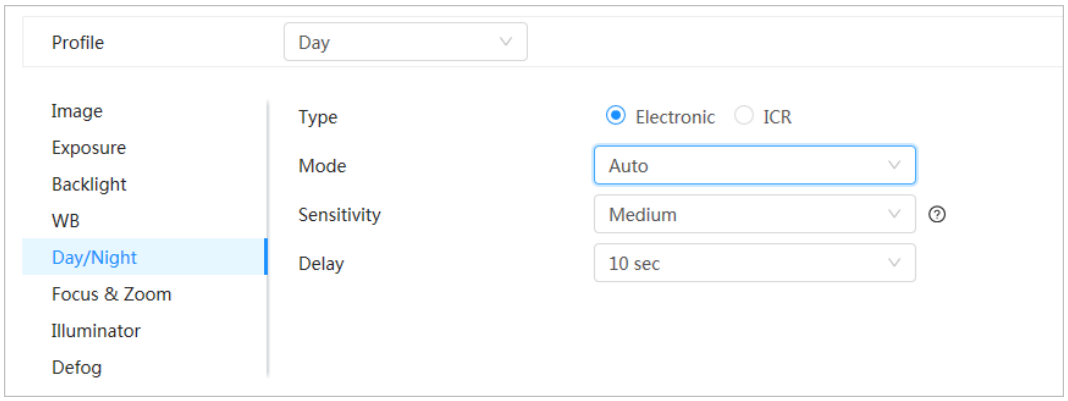


Table 4-7 Description of Day/Night mode parameters

Parameter	Description
Type	Select the type from **Electronic** and **ICR**.
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-Switch 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 can configure camera sensitivity when switching between color and black-and-white mode. The higher the sensitivity, the easier it is for the switch to be 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-white mode. 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.

Procedure

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 then configure focus & zoom parameters.

Figure 4-11 Focus & Zoom

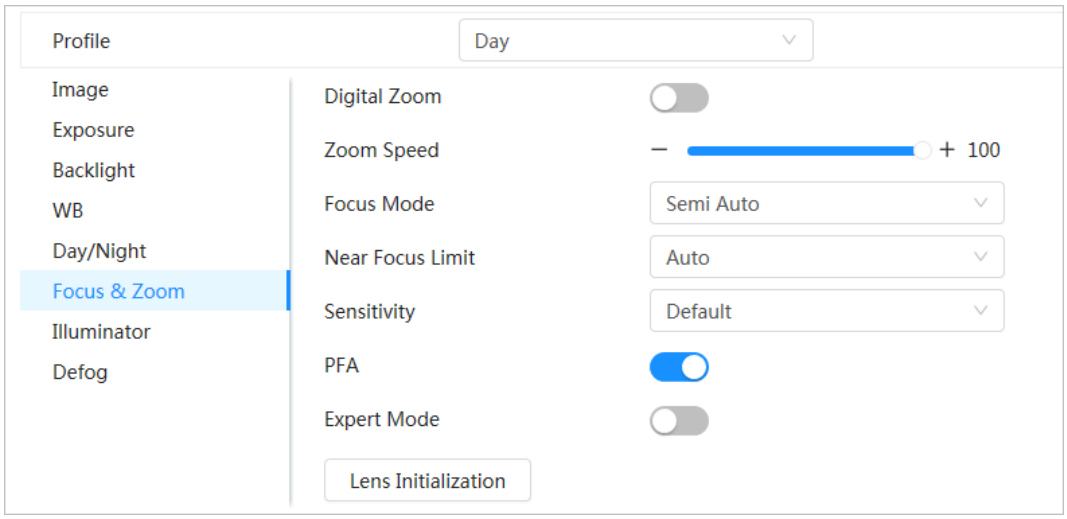


Table 4-8 Description of focus & zoom parameters

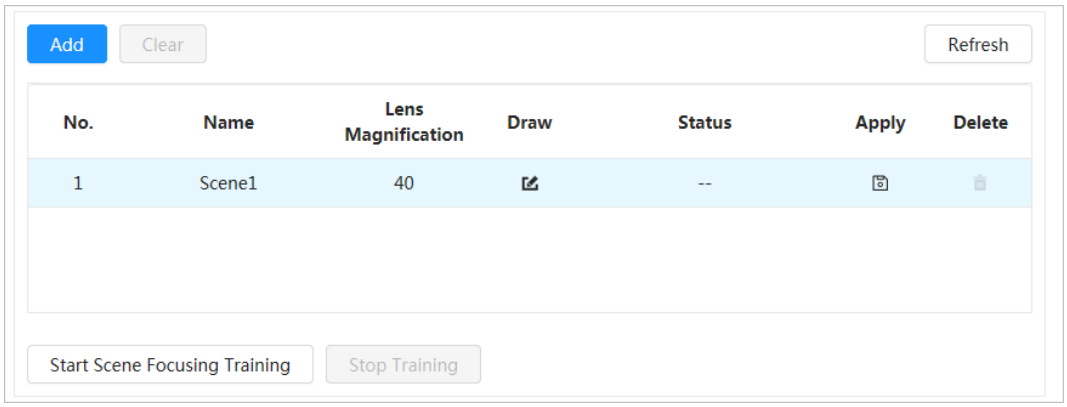
Parameter	Description
Digital Zoom	Click to enable digital zoom function. You can use the digital zoom to continue zooming operation even if the optical zoom is at its maximum value.
Zoom Speed	Adjust the zoom speed of the camera. The larger the value, the faster the zoom speed.
Focus Mode	Set focus mode. ● **Auto** : Once there is any movement or change of an object on the 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**. It will also focus automatically when a preset change or PTZ switch is detected. ● **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.

Parameter	Description
Sensitivity	Trigger the focusing sensitivity of the camera. The higher the sensitivity, the easier to trigger focus.
PFA	Enable **PFA**. When moving the picture, the camera automatically focuses for a clear picture..
Expert Mode	Enable **Expert mode**. Train the camera to rotate and focus on the specified route.
Lens Initialization	Click this button, and the lens will be initialized automatically. The lens will be extended to calibrate the zoom and focus.

Step 3 (Optional) Configure expert mode.

1. Enable **Expert mode** , click **Add** to add a new scene.

Figure 4-12 Expert Mode



2. Click to adjust the video screen and draw the training region on the screen.

   Only supports closed model area (triangle and polygons above).
3. Double-click **Lens Magnification** to set focus magnification.
4. Click **Apply** to save settings.
5. Click **Start Scene Focusing Training**.

   The scene rotates and automatically focuses to the specified position. After the training is complete, the scene status is displayed as **Complete**.

Step 4 Click **Apply**.

4.3.1.9 Illuminator

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

Procedure

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 4-13 Illuminator

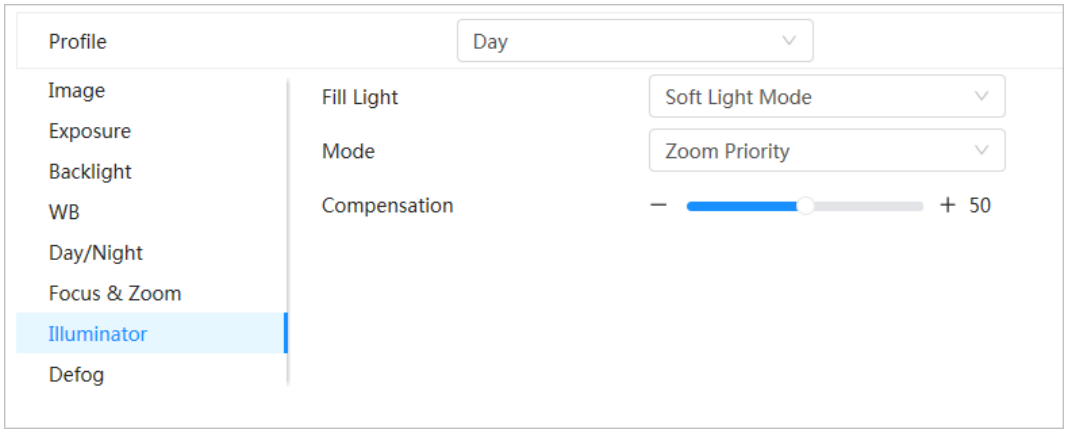


Table 4-9 Description of illuminator parameters

Parameter		Description
Fill Light		When the Camera is equipped with illuminator, it supports setting illumination mode for illuminator, including **IR Mode** , **White Light Mode**, **Soft Light Mode**, and **Smart Illumination**. ● **IR Mode** : Enable the IR illuminator, and the white light is disabled. You can only capture black and white images after enabling this function. ● **White Light Mode** : Enable the white light, and the IR illuminator is disabled. You can capture clear scene image after enabling this function. ● **Soft Light Mode** : Enable both IR illuminator and white light at the same time, and adjust the brightness of the two illuminators to get clear images. ● **Smart Illumination** : This function is mainly used at night. Smart illumination applies IR mode in most situations. When an event occurs (perimeter, motion detection and human detection), the camera automatically switches to white light mode to link image capturing and video recording under the full color mode. The white light turns off when the event stops, and then the mode switches to IR mode according to the ambient brightness. The status of the illuminator mainly depends on time and environment. If the smart illumination is triggered at night and the event continues during the day, the illuminator configured for the daytime will be turned off.
Mode	Manual	Adjust the brightness of illuminator manually, and then the system will illuminate the image accordingly.

Parameter		Description
	Auto	The system adjusts the illuminator intensity according to the 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 required to turn off the illuminator. ● Brightness upper limit: If the filling light is too bright, the 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.
	SmartIR	The system adjusts the illumination intensity according to the ambient lighting condition. Only IR illuminator supports the smart IR mode.
	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 the low beam lights. ● When the focus reaches certain wide angle, the system will not turn on high beam light in order to avoid over-exposure in short distance. Some devices support setting the sensitivity of the illuminator.
	Off	Illuminator is off.
Illuminator Delay		The duration of the illuminator. When selecting **Smart Illumination** in the drop-down list next to **Fill Light**, you need to set **Illuminator Delay**.

Step 3 Click **Apply**.

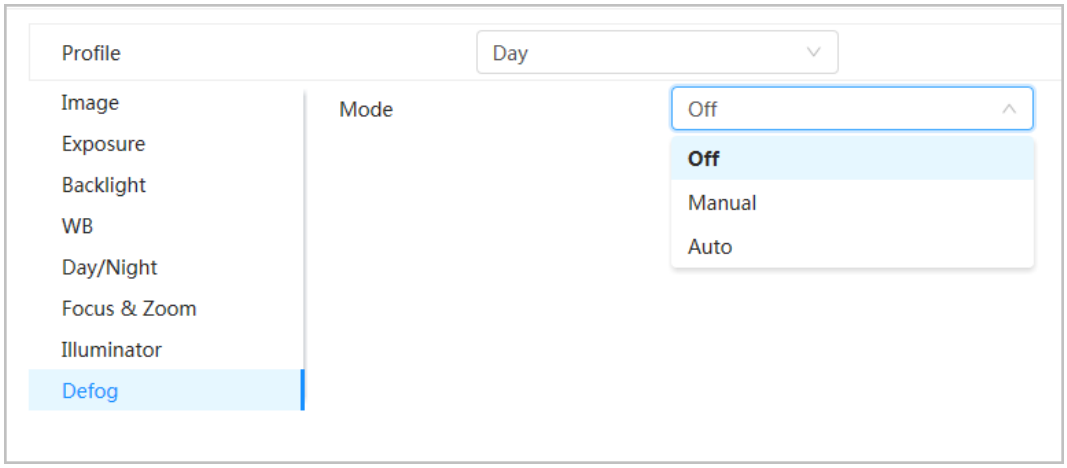
4.3.1.10 Defog

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

Procedure

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

Figure 4-14 Defog



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

Table 4-10 Description of defog parameters

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

Step 3 Click **Apply**.

4.3.2 Setting Splicing Parameters

If the splicing effect of the panoramic image is not desirable, you can use this function to automatically optimize it.

Procedure

Step 1 Click on the upper-right corner of the page, and then select **Camera** > **Splicing**.

Step 2 Click **Start**, and then the Camera starts splicing lenses.

Please wait patiently. After the splicing completes, the image is displayed.

Repeat this step until the image meets your requirements.

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

4.3.3 Setting Encode Parameters

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

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

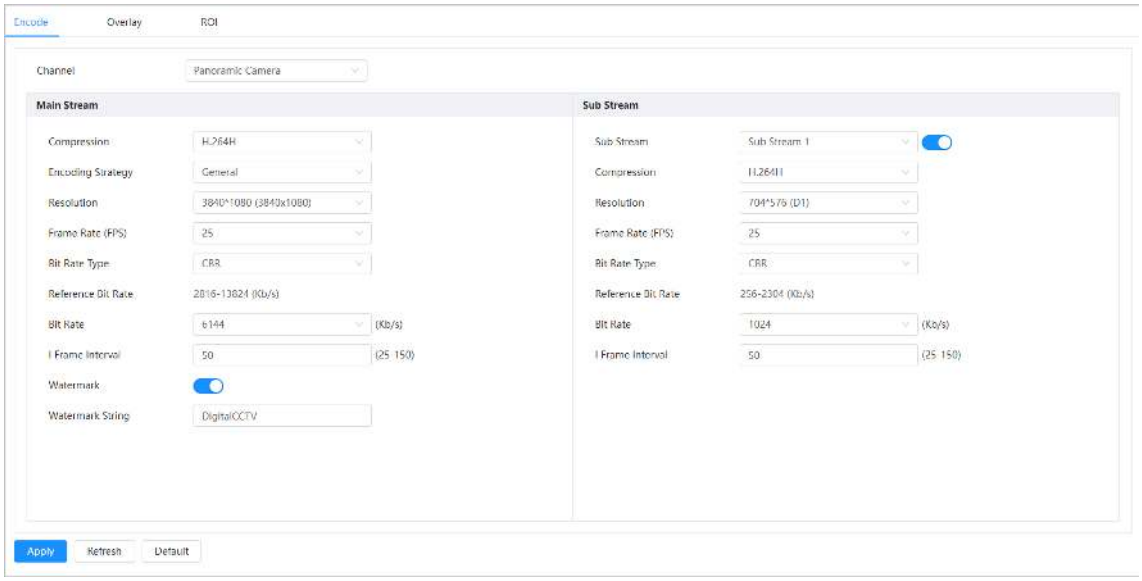
4.3.3.1 Encode

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

Procedure

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

Figure 4-15 Encode



Step 2 Configure encode parameters.

Table 4-11 Description of encode parameters

Parameter	Description
Sub Stream	Click to enable sub stream, it is enabled by default. You can enable multiple sub streams simultaneously.
Compression	Select encode mode. • **H.264** : it includes **H.264B** (baseline profile encode mode), **H.264** (main profile encode mode) and **H.264H** (high profile encode mode). Under the same image quality, the bandwidth of the three decreases in turn • **H.265** : Main profile encode mode. Compared with H.264, it requires smaller bandwidth. • **MJPEG** : When under this mode, the image requires high bit rate value to ensure clarity, you are recommended to set the **Bit Rate** value to the biggest value in the **Reference Bit Rate**.

Parameter	Description
Encoding Strategy	Select the encoding strategy. When you enabling smart codec, it can improve video compressibility and save storage space. After smart codec is enabled, the device would stop supporting the third bit stream, ROI and smart event detection.
Output Mode	You can select from **Single Stream** or **Flex Stream**.
Resolution	The resolution of the video. The higher the value is, the clearer the image will be, but the bigger the required bandwidth will be.
Frame Rate (FPS)	The number of frame in one second of video. The higher the value is, the clearer and smoother the video will be.
Bit Rate Type	The bit rate control type during video data transmission. You can select bit rate type from: ● **CBR** (Constant Bit Rate): The bit rate changes a little and keeps close to the defined bit rate value. ● **VBR** (Variable Bit Rate): The bit rate changes as monitoring scene changes. The **Bit Rate Type** can only be set as **CBR** when **Encode Mode** is set as **MJPEG**.
Quality	This parameter can be configured only when the **Bit Rate Type** is set as **VBR**. The better the quality is, but the bigger the required bandwidth will be.
Reference Bit Rate	The most suitable bit rate value range recommended to user according to the defined resolution and frame rate.
Max Bit Rate	This parameter can be configured only when the **Bit Rate Type** is set as **VBR**. You can select the value of the **Max Bit Rate** according to the **Reference Bit Rate** value. The bit rate then changes as monitoring scene changes, but the max bit rate keeps close to the defined value.
Bit Rate	This parameter can be configured only when the **Bit Rate Type** is set as **CBR**. Select bit rate value in the list according to actual condition.
I Frame Interval	The number of P frames between two I frames, and the **I Frame Interval** range changes as **FPS** changes. It is recommended to set **I Frame Interval** twice as big as **FPS**.

Parameter	Description
SVC	Scaled video coding, is able to encode a high quality video bit stream that contains one or more subset bit streams. When sending stream, to improve fluency, the system will quit some data of related lays according to the network status. ● 1: The default value, which means that there is no layered coding. ● 2, 3 and 4: The lay number that the video stream is packed.
Watermark	You can verify the watermark to check if the video has been tampered.
Watermark String	

Step 3 Click **Apply**.

4.3.3.2 Overlay

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

4.3.3.2.1 Privacy Masking

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

Procedure

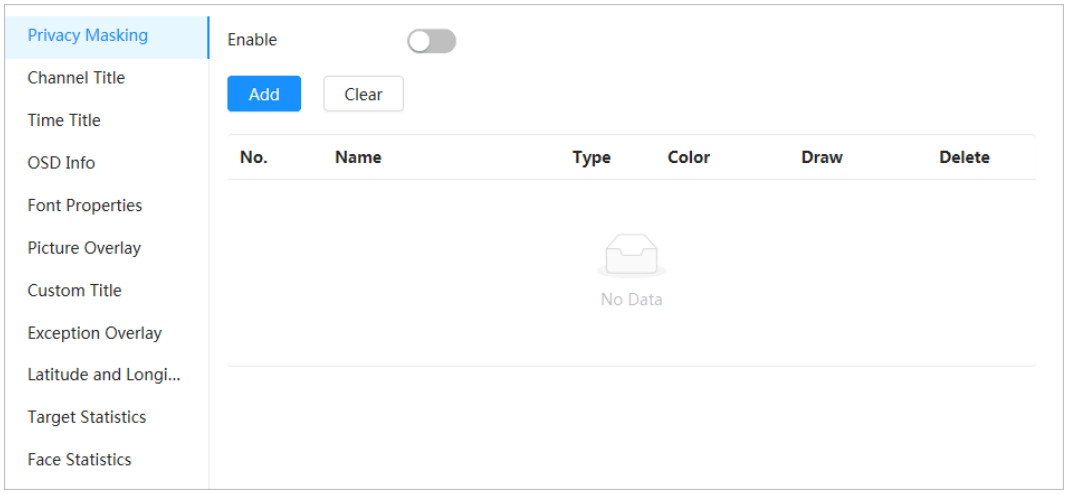
Step 1 Select > **Camera** > **Encode** > **Privacy Masking**.

Step 2 Select **Enable**.

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

- You can drag 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 to delete the corresponding block.

Figure 4-16 Privacy masking



Step 4 Adjust block size to protect the privacy.

Step 5 Click **Apply**.

4.3.3.2.2 Channel Title

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

Procedure

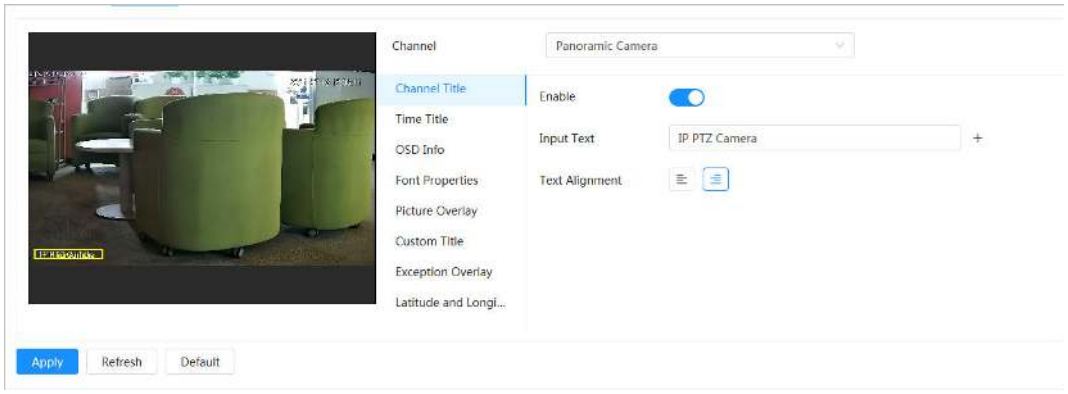
Step 1 Select > **Camera** > **Encode** > **Overlay** > **Channel Title**.

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 4-17 Channel title



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

Step 5 Click **Apply**.

4.3.3.2.3 Time Title

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

Procedure

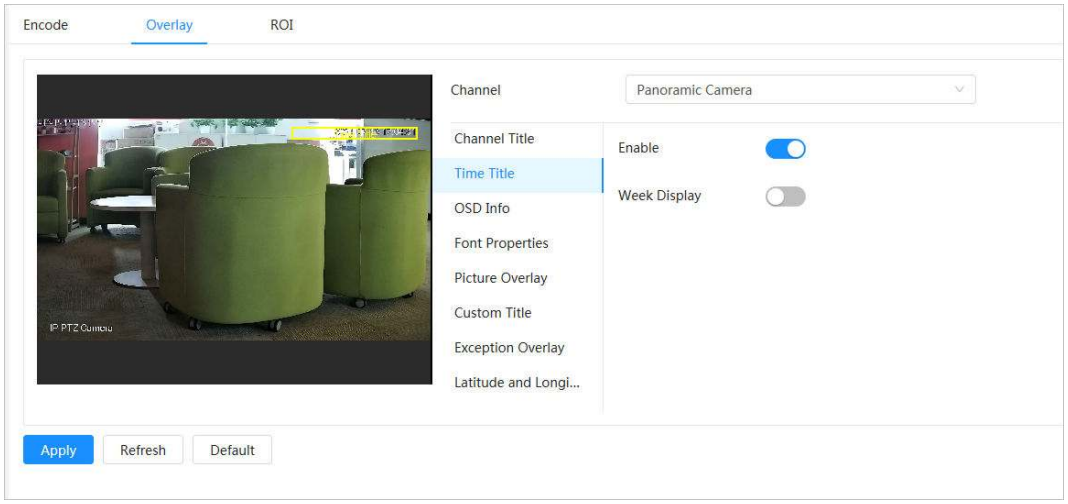
Step 1 Select > **Camera** > **Encode** > **Overlay** > **Time Title**.

Step 2 Select **Enable**.

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

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

Figure 4-18 Time title



Step 5 Click **Apply**.

4.3.3.2.4 Location

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

Procedure

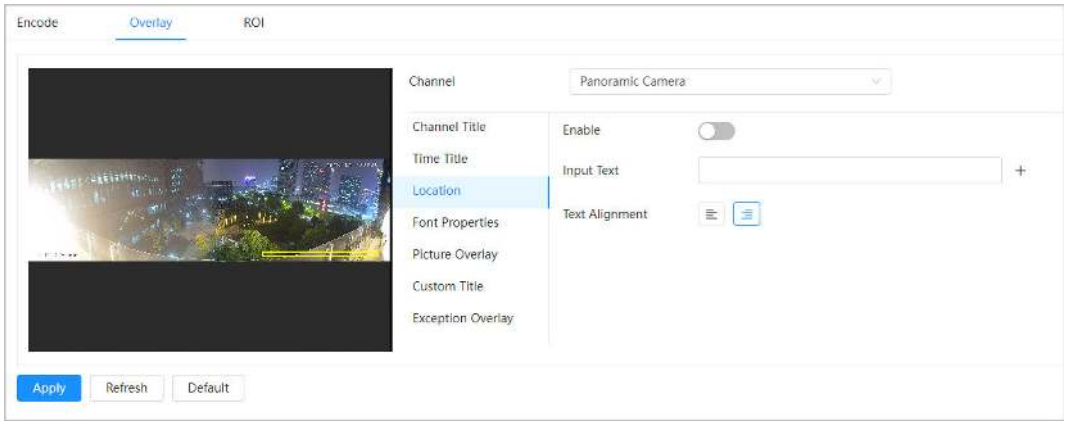
Step 1 Select > **Camera** > **Encode** > **Overlay** > **Location**.

Step 2 Select **Enable**.

Step 3 Configure location information, and then select the text alignment.

Click **+** to add the location, and you can add 13 lines at most.

Figure 4-19 Location



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

Step 5 Click **Apply**.

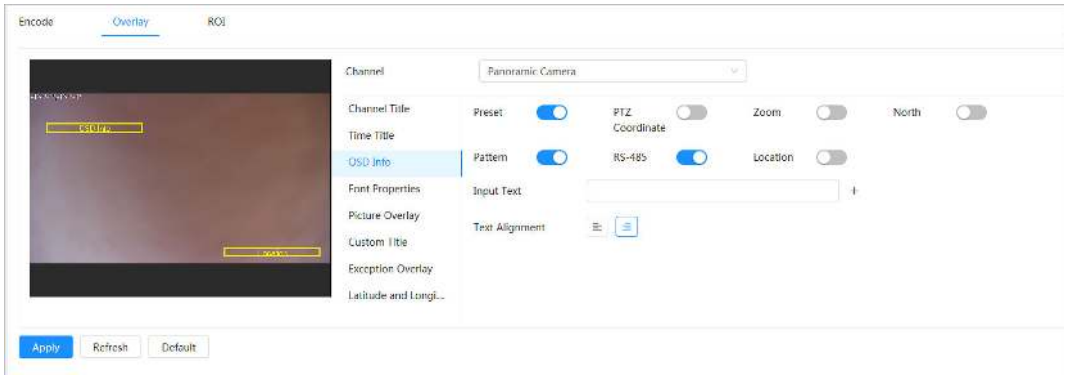
4.3.3.2.5 OSD Info

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.

Procedure

Step 1 Select > **Camera** > **Encode** > **Overlay** > **OSD Info**.

Figure 4-20 OSD info



Step 2 Configure OSD Information.

Table 4-12 Description of OSD information parameter

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

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

Step 4 Click **Apply**.

4.3.3.2.6 Font Properties

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

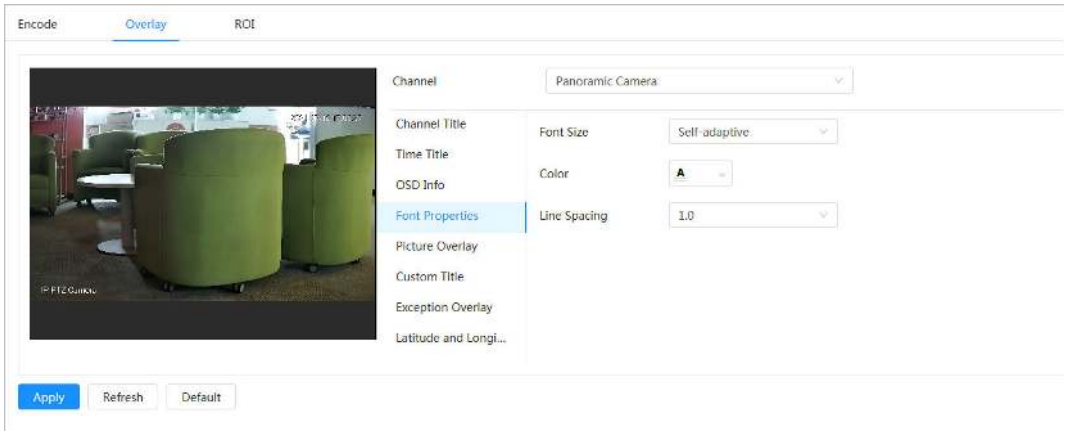
Procedure

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 4-21 Font properties



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

After saving the settings, the font properties in the video image change color and size accordingly.

4.3.3.2.7 Picture Overlay

Background Information

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

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

Procedure

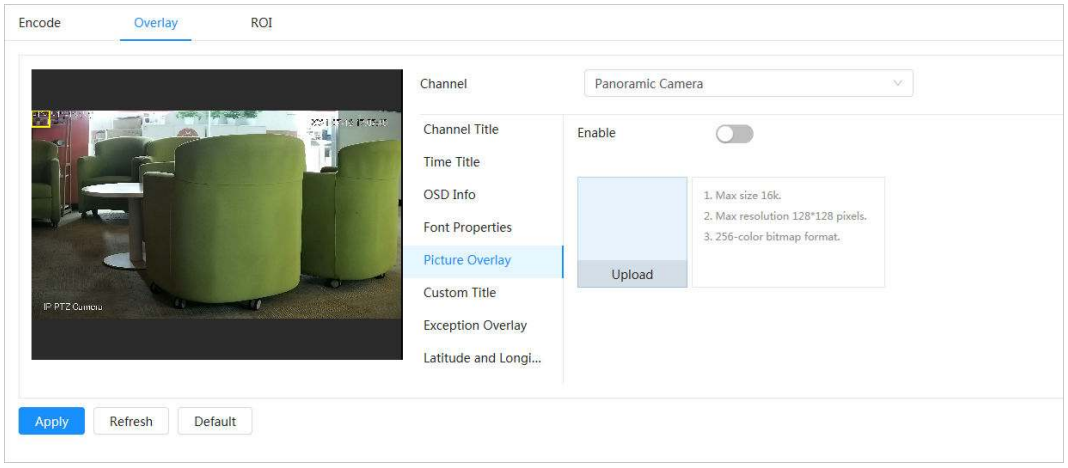
Step 1 Select > **Camera** > **Encode** > **Overlay** > **Picture Overlay**.

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

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

The picture show in the **Picture Preview**.

Figure 4-22 Picture overlay



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

Step 5 Click **Apply**.

4.3.3.2.8 Custom Title

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

Procedure

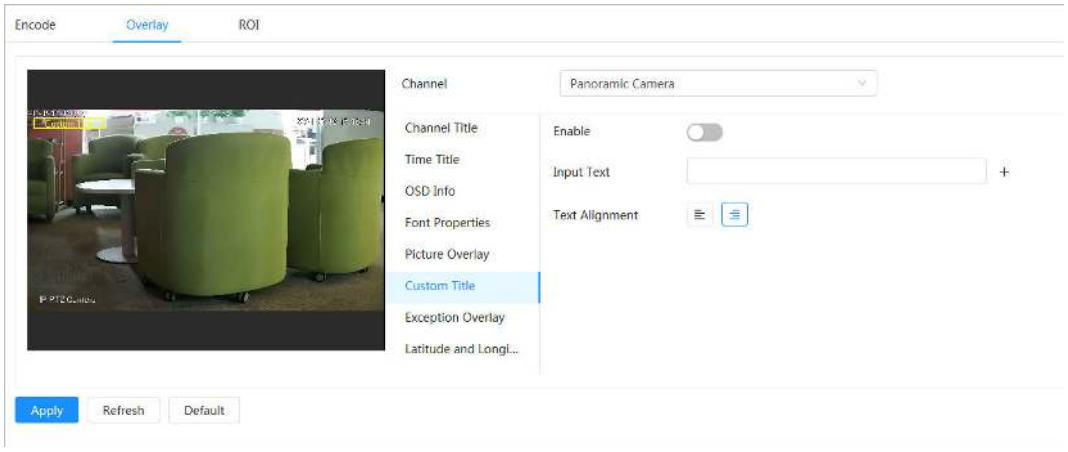
Step 1 Select > **Camera** > **Encode** > **Overlay** > **Custom Title**.

Step 2 Select **Enable**.

Step 3 Configure custom overlay and then select the text align.

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

Figure 4-23 Custom title



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

Step 5 Click **Apply**.

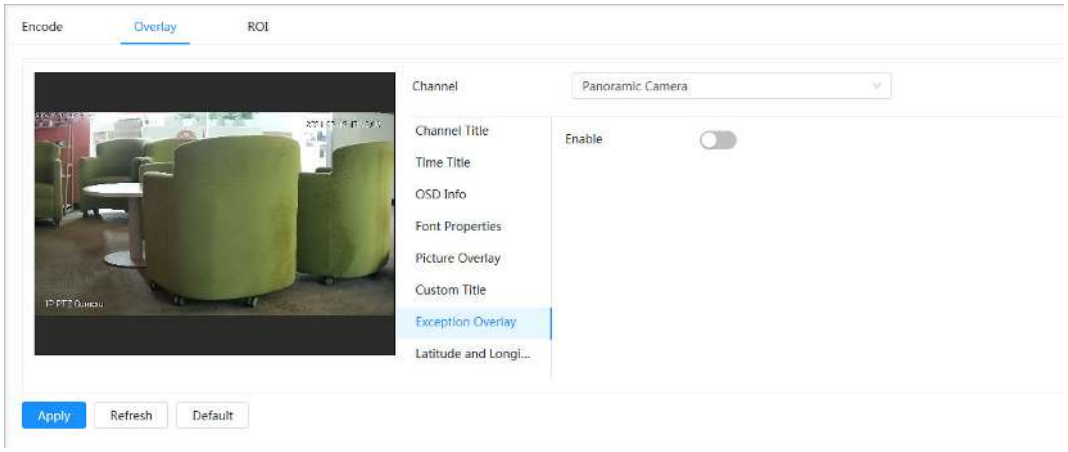
4.3.3.2.9 Exception Overlay

You can enable this function to display the overlaid abnormal information of the cameras in the video image.

Procedure

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

Figure 4-24 Exception overlay



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

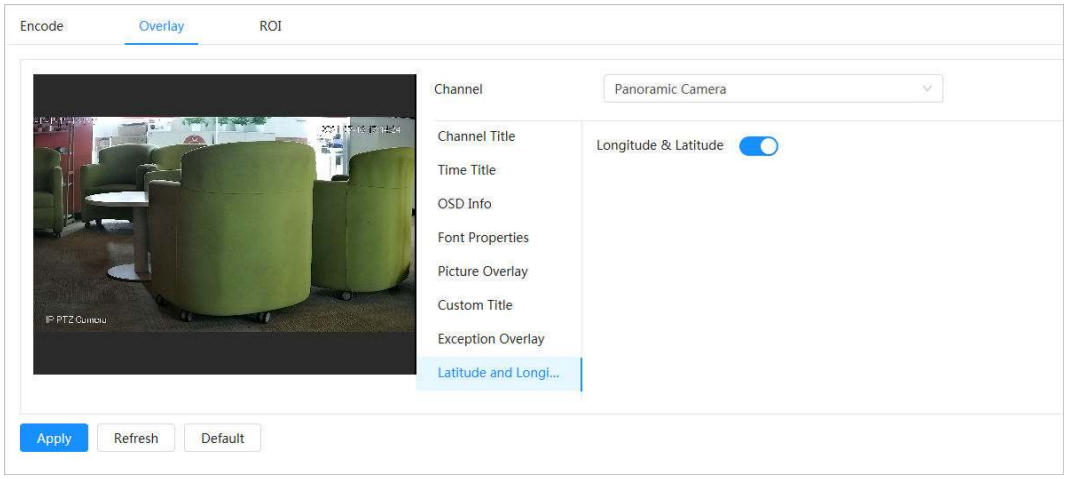
4.3.3.2.10 Longitude & Latitude

You can enable this function to display the latitude and longitude information of the cameras on the screen.

Procedure

Step 1 Select > **Camera** > **Encode** > **Longitude & Latitude**.

Figure 4-25 Longitude & latitude



Step 2 Enable **Longitude & Latitude** , and then click **Apply**.

4.3.3.2.11 Target Statistics

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

Procedure

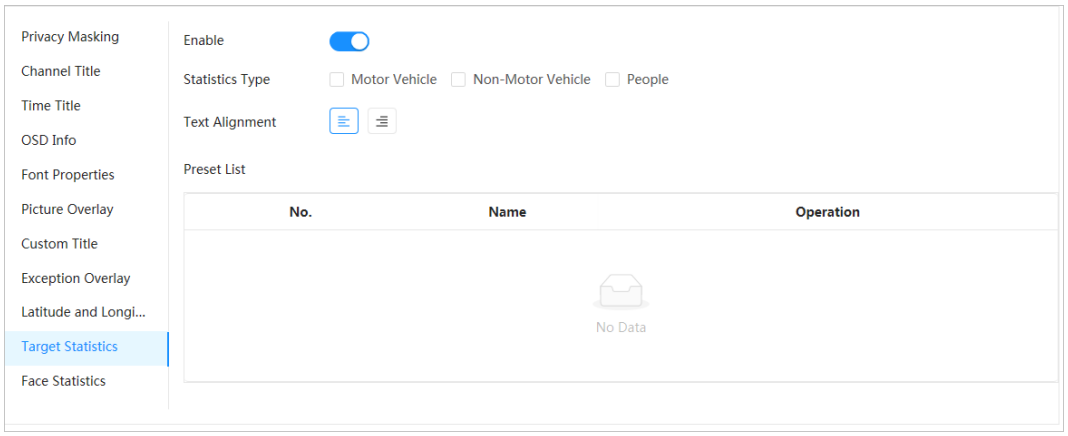
Step 1 Select > **Camera** > **Encode** > **Target Statistics**.

Step 2 Select **Enable**.

Step 3 Select the statistics type, and then select the text alignment.

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

Figure 4-26 Target statistics



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

Step 5 Click **Apply**.

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

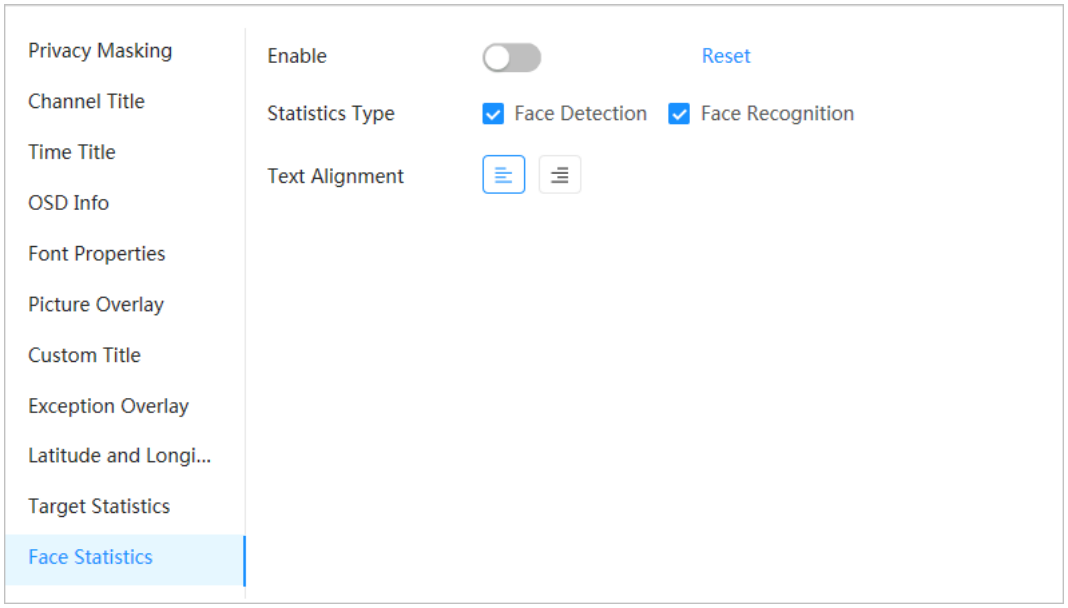
4.3.3.2.12 Face Statistics

After configuring the face statistics, the number of face statistics will be displayed in the image.

Procedure

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

Figure 4-27 Face statistics



Step 2 Select **Enable**, and then select Statistics Type.

- Face detection: The screen displays the quantity information of face detection.
- Face recognition: The screen displays the quantity information of face recognition.

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

Step 4 Click **Apply**.

Related Operations

Click **Reset** to clear the statistics data and start counting again.

4.3.3.3 ROI

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

Procedure

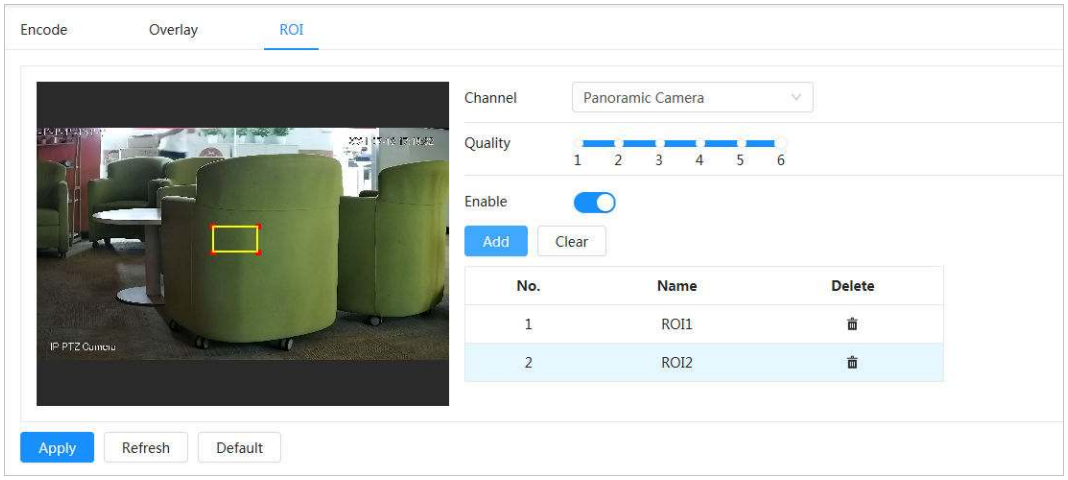
Step 1 Select > **Camera** > **Encode** > **ROI**.

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 4-28 ROI



Step 4 Click **Apply**.

4.3.4 Audio

You can configure audio parameters and alarm audio.

The function is available on select models.

4.3.4.1 Configuring Audio Parameters

Background Information

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.

Procedure

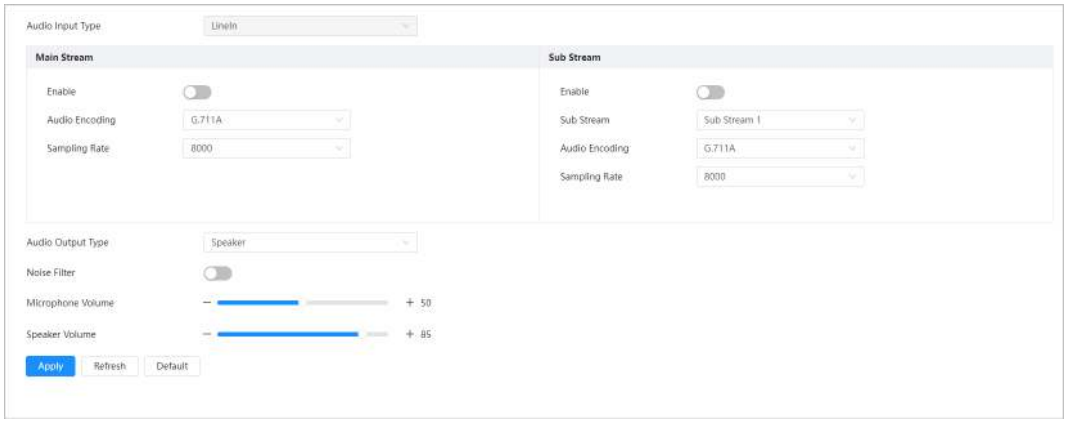
Step 1 Click on the upper-right corner of the webpage, and then select **Camera** > **Audio** > **Audio**.

Step 2 Select **Main Stream** 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 4-29 Audio



Step 3 Configure audio parameters.

Table 4-13 Description of audio parameters

Parameter	Description
Compression	Configure audio compression. The configured audio encode mode applies to both audio and intercom. The default value is recommended.
Sampling Frequency	Sampling number per second. The higher the sampling frequency is, the more the sample in a second will be, and the more accuracy the restored signal will be.
Audio Output Type	Select the audio output type of the Camera. ● LineOut: The Camera outputs audio signals through an external audio device. ● Speaker: The Camera outputs audio signals through its speaker.
Noise Filter	Enable this function, and the system auto filters ambient noise.
Microphone Volume	Adjusts microphone volume.
Speaker Volume	Adjusts speaker volume.

Step 4 Click **Apply**.

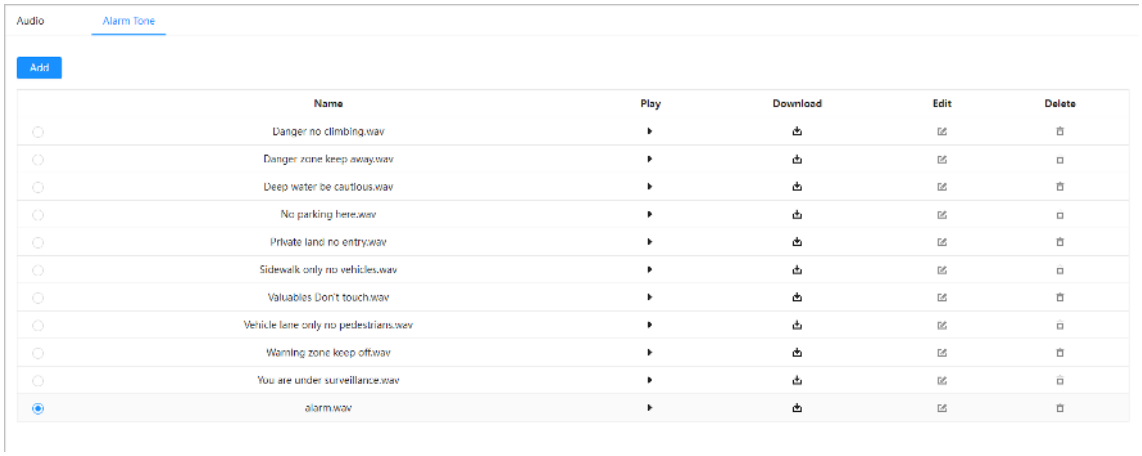
4.3.4.2 Configuring Alarm Tone

You can set the alarm audio to be played when an alarm is triggered. For some devices, you can record or upload alarm audios.

Procedure

Step 1 Click on the upper-right corner of the webpage, and then select **Camera** > **Audio** > **Alarm Tone**.

Figure 4-30 Alarm tone



Step 2 Click **Add**.

Figure 4-31 Add audio tone

Step 3 Configure the audio file.

- Select Record, enter the audio file name, and then click **Record**.

  Click **Stop** to complete recording.
- Select **Upload** , click **Browse**, select the audio file to be uploaded, and then click **Upload**.

- The format of recorded audio is .pcm. Audio recording is only supported by some devices.
- Audio file in the format of .wav can be uploaded.
- You can edit and delete recorded or uploaded audio.
  - Click to edit audio file.
  - Click to delete audio file.

Step 4 Select the audio file that you need.

Related Operations

- Play audio: Click to play the alarm audio.
- Download audio: Click to download the alarm audio to local storage. The audio is saved to the default download path of the browser.

4.4 Network

This section introduces network configuration.

4.4.1 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 the network.

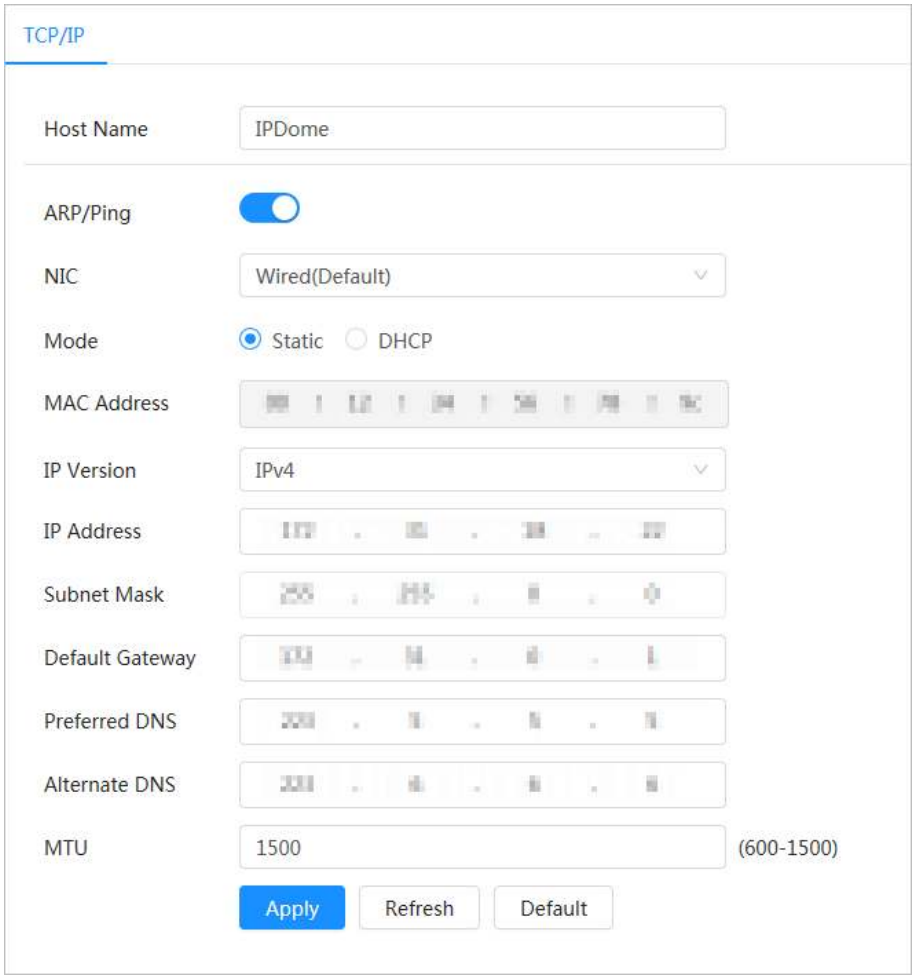
Prerequisites

The Camera has connected to the network.

Procedure

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

Figure 4-32 TCP/IP



Step 2 Configure TCP/IP parameters.

Table 4-14 Description of TCP/IP parameters

Parameter	Description
Host Name	Enter the host name. The maximum length is 15 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/ping command. This is enabled by default. During restart, you will have no more than 2 minutes to configure the device IP address by a ping packet with certain length, the server will be turned off in 2 minutes, or it will be turned off immediately after the IP address is successfully configured. If this is not enabled, the IP address cannot be configured with ping packet.
NIC	Select the Ethernet card that need to be configured, and the default one is **Wire**.
Mode	The mode that the Camera gets IP: ● **Static** Configure **IP Address** , **Subnet Mask**, and **Default Gateway** manually, and then click **Save**, the login page with the configured IP address is displayed. ● **DHCP** When there is DHCP server in the network, select **DHCP**, and the Camera acquires IP address automatically.
MAC Address	Displays host MAC address.
IP Version	Select **IPv4** or **IPv6**.
IP Address	When you select **Static** as **Mode**, enter the IP address and subnet mask that you need. ● IPv6 does not have 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

1. Keep the Camera that needs to be configured and the computer within the same local network, and then get a usable IP address.
2. Get the MAC address of the Camera from device label.
3. Open command editor on the computer and enter the following command.

Figure 4-33 Edit command

Windows syntax
arp –s <IP Address> <MAC> ping –l 480 –t <IP Address>
Windows example
arp -s 192.168.0.125 11-40-8c-18-10-11 ping -l 480 -t 192.168.0.125
UNIX/Linux/Mac syntax
arp –s <IP Address> <MAC> ping –s 480 <IP Address>
UNIX/Linux/Mac example
arp -s 192.168.0.125 11-40-8c-18-10-11 ping -s 480 192.168.0.125

4. Restart the Camera.
5. Check the computer command line, if information such as **Reply from 192.168.0.125…** is displayed, the configuration succeeds, and you can turn it off then.
6. Enter http://(IP address) in the browser address bar to log in.

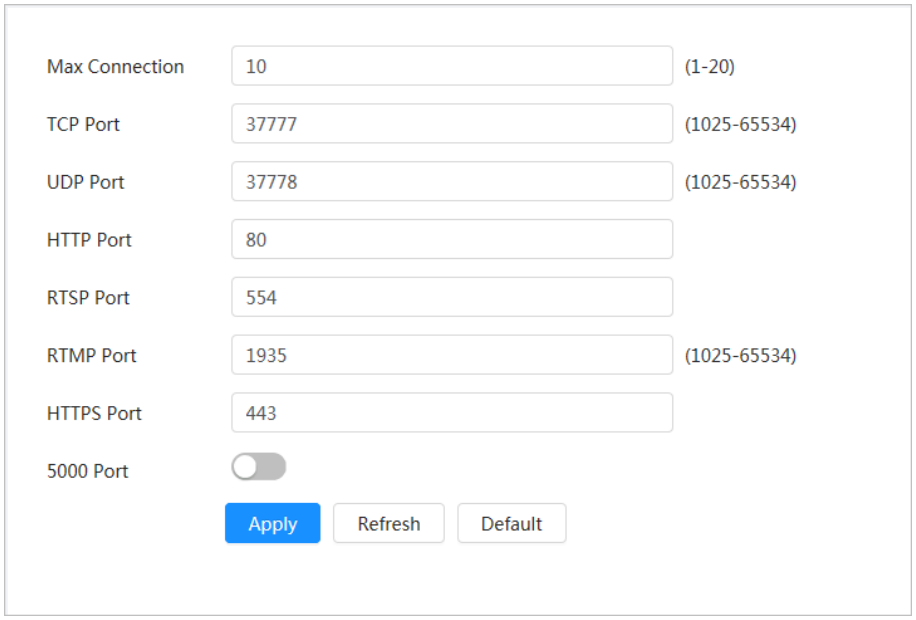
4.4.2 Port

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

Procedure

Step 1 Select > **Network** > **Port**.

Figure 4-34 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, 37776, 37780–37880, 39999, 42323 are occupied for specific uses, please do not use them.
- Do not use the same value of any other port during port configuration.

Table 4-15 Description of port parameters

Parameter	Description
Max Connection	The max number of users (web client, platform client or mobile phone client) that can connect to the Camera simultaneously. The value is 10 by default.
TCP Port	Transmission control protocol port. The value is 37777 by default.
UDP Port	User datagram protocol port. The value is 37778 by default.
HTTP Port	Hyper text transfer protocol port. The value is 80 by default.

Parameter	Description
RTSP Port	• Real time streaming protocol port, and the value is 554 by default. If you play live view with QuickTime, VLC or Blackberry smart phone, the following URL format is available. • When the URL format 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. 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 main stream (Subtype=0) and 1 means sub stream (Subtype=1). Example: If you require the sub stream of channel 2 from a certain device, then the URL should be: rtsp://admin:admin@192.168.1.112:554/cam/realmonitor?channel=2&=1 If username and password are not needed, then the URL can be: rtsp://ip:port/cam/realmonitor?channel=11&subtype=0
RTMP Port	Real Time Messaging Protocol Port. The port that RTMP provides service. It is 1935 by default.
HTTPS Port	HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer) communication 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.

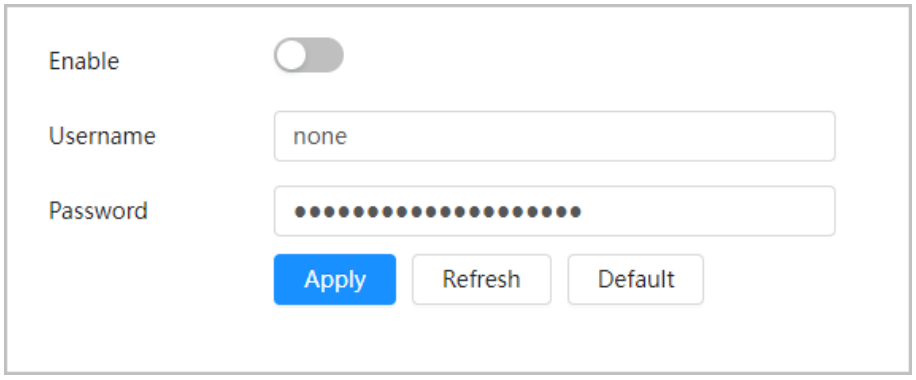
Prerequisites

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

Procedure

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

Figure 4-35 PPPoE



Step 2 Click , and then enter username and password.

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

Step 3 Click **Apply**.

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

4.4.4 DDNS

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

Prerequisites

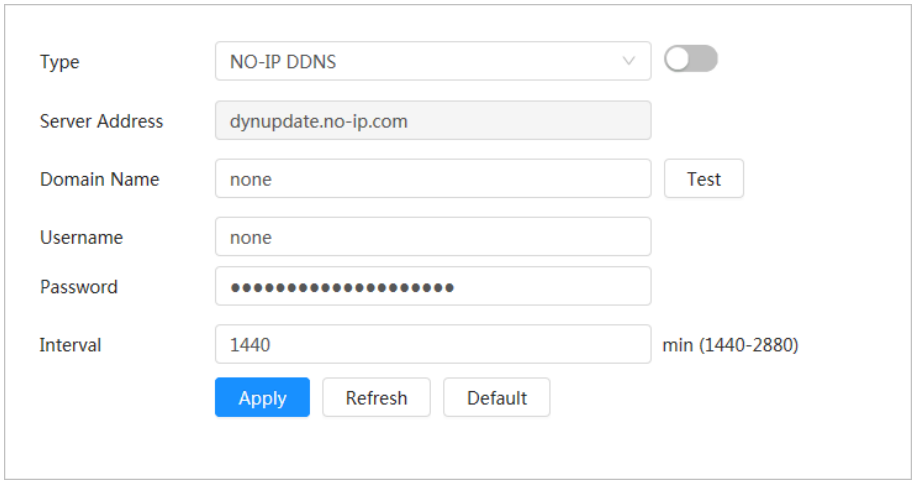
Check the type of DNS server supported by the Camera.

Procedure

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

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

Figure 4-36 DDNS



Step 2 Click to enable the function.

Step 3 Configure DDNS parameters.

Table 4-16 Description of DDNS parameters

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

Step 4 Click **Apply**.

Results

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

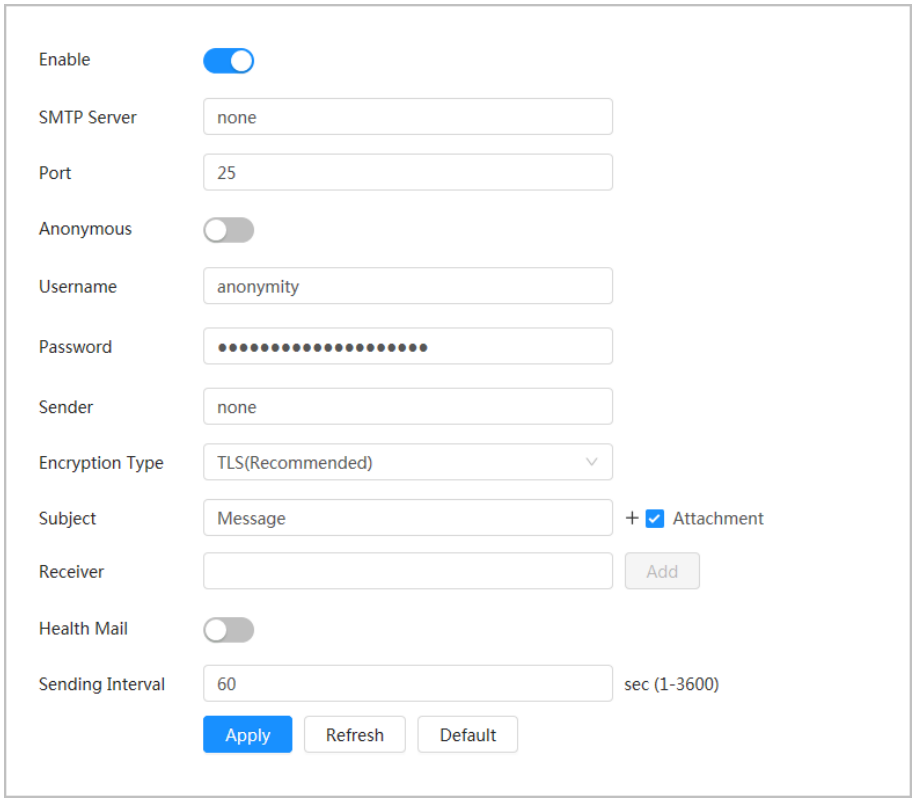
4.4.5 Email

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

Procedure

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

Figure 4-37 Email



Step 2 Click to enable the function.

Step 3 Configure email parameters.

Table 4-17 Description of email parameters

Parameter	Description	
SMTP Server	SMTP server address.	For details, see Table 4-18 .
Port	The port number of the SMTP server.	
Username	The account of SMTP server.	
Password	The password of SMTP server.	
Anonymous	Click , and the sender's information is not displayed in the email.	
Sender	Sender's email address.	
Encryption Type	Select from **None** , **SSL (Secure Sockets Layer)** and **TLS (Transport Layer Security)**. For details, see Table 4-18 .	
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.	

Parameter	Description
Receiver	• Receiver's email address. Supports 3 addresses at most. • After entering the receiver's email address, click **Test** to test whether the emails can be sent and received successfully.
Health Mail	The system sends test mail to check if the connection is successfully configured. Click 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	

Table 4-18 Description of major mailbox configuration

Mailbox	SMTP server	Authentication	Port	Description
gmail	smtp.gmail.com	SSL	465	You need to enable SMTP service in your mailbox.
		TLS	587	
Sina	smtp.sina.com	SSL	465	
		None	25	
126	smtp.126.com	None	25	
163	smtp.163.com	SSL	465/994	• You need to enable SMTP service in your mailbox. • The password should be "Authentication Password". Password for email login is invalid. Authentication Password: Authentication Password is obtained when the SMTP service is enabled.
		TLS	25	
		None	25	
QQ	smtp.qq.com	SSL	465	• "None" cannot be selected for authentication. • You need to enable SMTP service in your mailbox. • The password should be "Authentication Password". Password for email login is invalid. Authentication Password: Authentication Password is obtained when the SMTP service is enabled.
		TLS	587	

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.

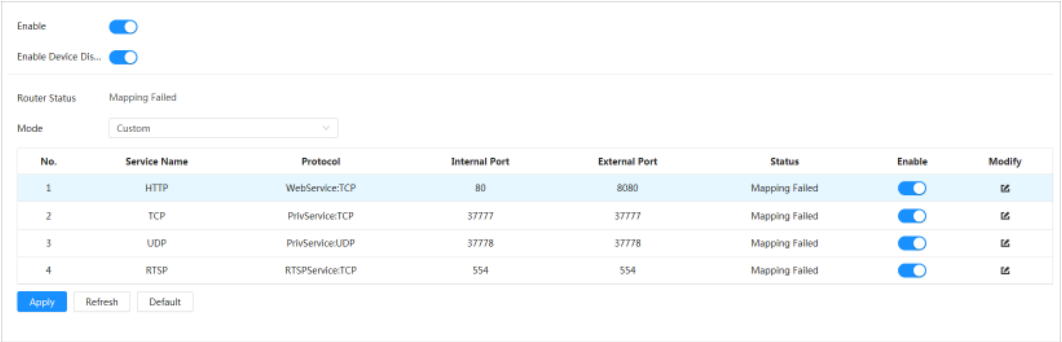
Prerequisites

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

Procedure

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

Figure 4-38 UPnP



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

- Select **Custom**, click and then you can change external port as needed.
- Select **Default**, and then the system finishes mapping with unoccupied port automatically, and you cannot edit mapping relation.
- Select **Enable Device Discovery** to search for the device through the PC's online neighbors. 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 then you 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 Builder and MG-SOFT MIB Browser to connect to the camera and manage and monitor the camera.

Prerequisites

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

Procedure

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

Figure 4-39 SNMP (1)

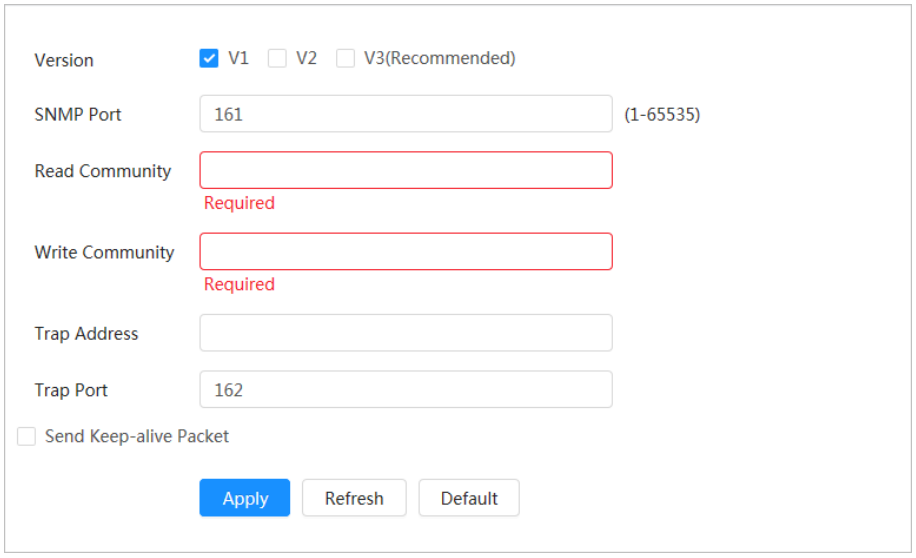
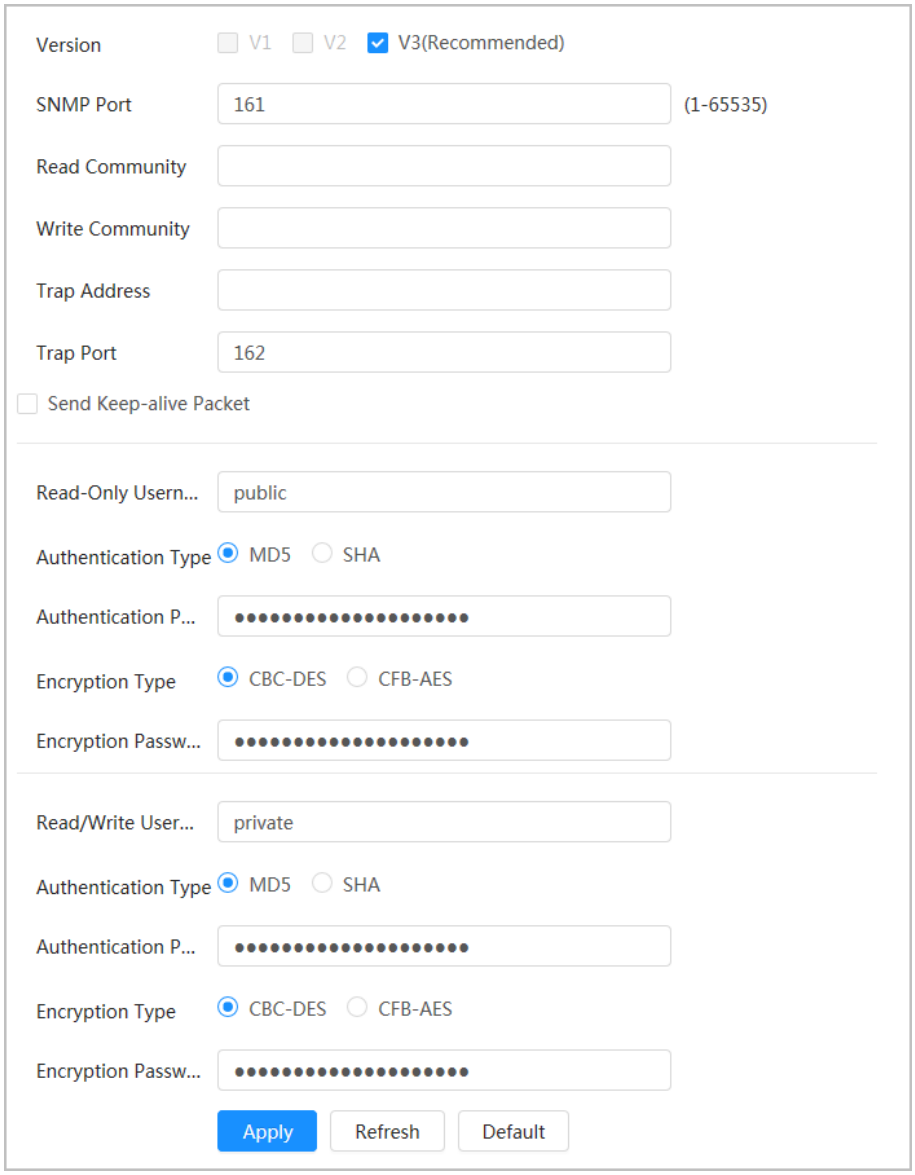


Figure 4-40 SNMP (2)



Step 2 Select SNMP version to enable SNMP.

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

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

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

Table 4-19 Description of SNMP parameters

Parameter	Description
SNMP Port	The listening port of the software agent in the device.

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

Step 4 Click **Apply**.

Results

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

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

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

4.4.8 Bonjour

Background Information

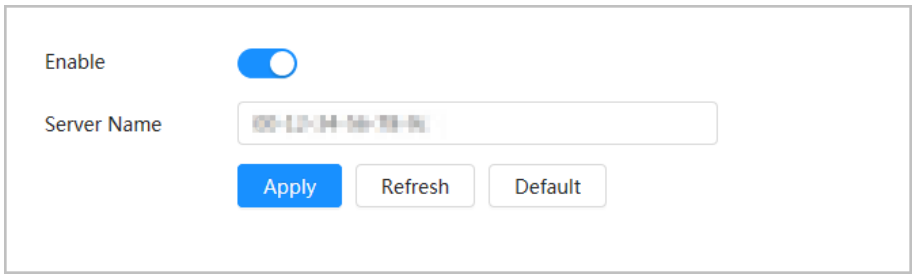
Enable this function, and the OS and clients that support Bonjour would find the camera automatically. You can have quick visit to the camera with Safari browser.

Bonjour is enabled by default.

Procedure

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

Figure 4-41 Bonjour



Step 2 Click , and then configure server name.

Step 3 Click **Apply**.

Results

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

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

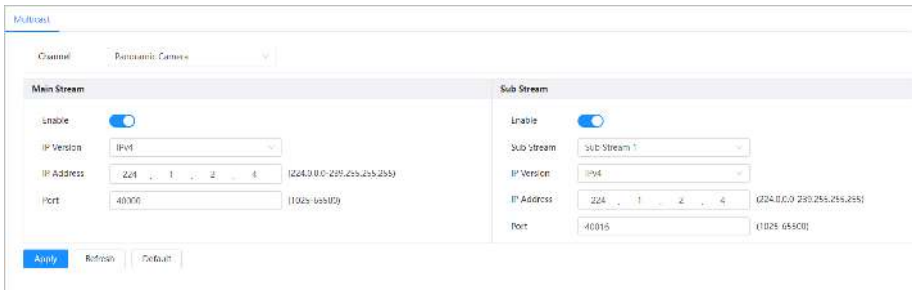
4.4.9 Multicast

When multiple users are viewing the device video image simultaneously through network, it might fail due to limited bandwidth. You can solve this problem by setting up a multicast IP (224.0.1.0–238.255.255.255) for the camera and adopt the multicast protocol.

Procedure

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

Figure 4-42 Multicast



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

Table 4-20 Description of multicast parameters

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

Step 3 Click **Apply**.

Results

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

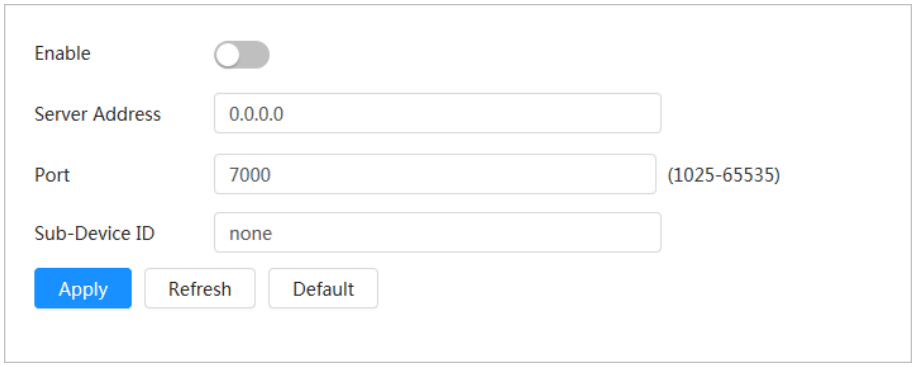
4.4.10 Register

After you enable this function, when the Camera is connected to the internet, it will report the current location to the specified server which acts as the transit to make it easier for the client software to access the Camera.

Procedure

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

Figure 4-43 Register



Step 2 Click , and then configure server name.

Table 4-21 Description of register parameters

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

Step 3 Click **Apply**.

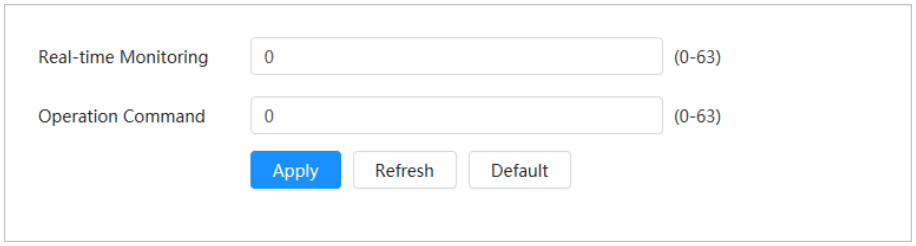
4.4.11 QoS

You can solve problems such as network delay and congestion with this function. It helps to assure bandwidth, reduce transmission delay, packet loss rate, and delay jitter to improve experience. 0–63 means 64 degrees of priority; 0 for the lowest and 63 the highest.

Procedure

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

Figure 4-44 QoS



Step 2 Configure QoS parameters.

Table 4-22 Description of QoS parameters

Parameter	Description
Real-time Monitor	Configure the priority of the data packets that used for network surveillance. 0 for the lowest and 63 the highest.
Command	Configure the priority of the data packets that are used for configure or checking.

Step 3 Click **Apply**.

4.4.12 Platform Access

4.4.12.1 P2P

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

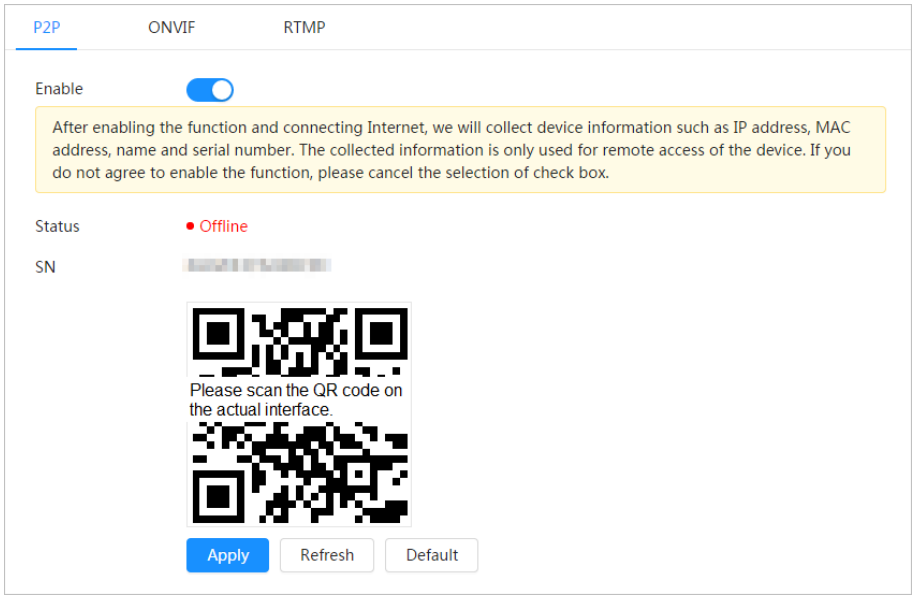
Background Information

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

Procedure

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

Figure 4-45 P2P



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

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

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

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

Step 5 Follow the instructions to finish the settings.

4.4.12.2 ONVIF

Background Information

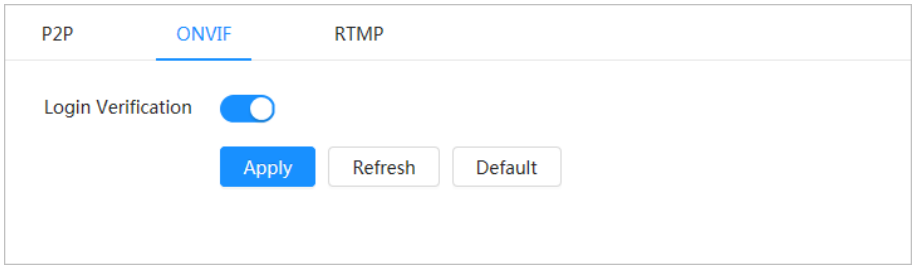
The ONVIF verification is enabled by default, which allows the network video products (including video recording device and other recording devices) from other manufacturers to connect to your device.

ONVIF is enabled by default.

Procedure

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

Figure 4-46 ONVIF



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

Step 3 Click **Apply**.

4.4.12.3 RTMP

Background Information

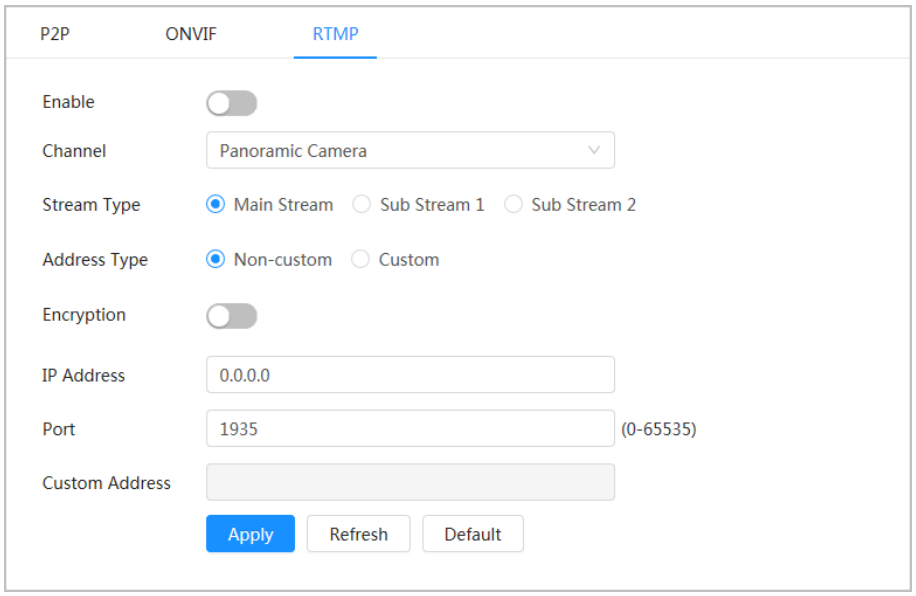
Through RTMP, you can access a third-party platform (such as Ali and YouTube) to realize video live view.

- 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.

Procedure

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

Figure 4-47 RTMP



Step 2 Click .

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

Step 3 Configure RTMP parameters.

Table 4-23 Description of RTMP parameters

Parameter	Description
Stream Type	The stream for live view. Make sure that the video format is H.264, H. 264 B 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.
IP Address	When selecting **Non-custom**, you need to enter server IP address and 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 by the server.

Step 4 Click **Apply**.

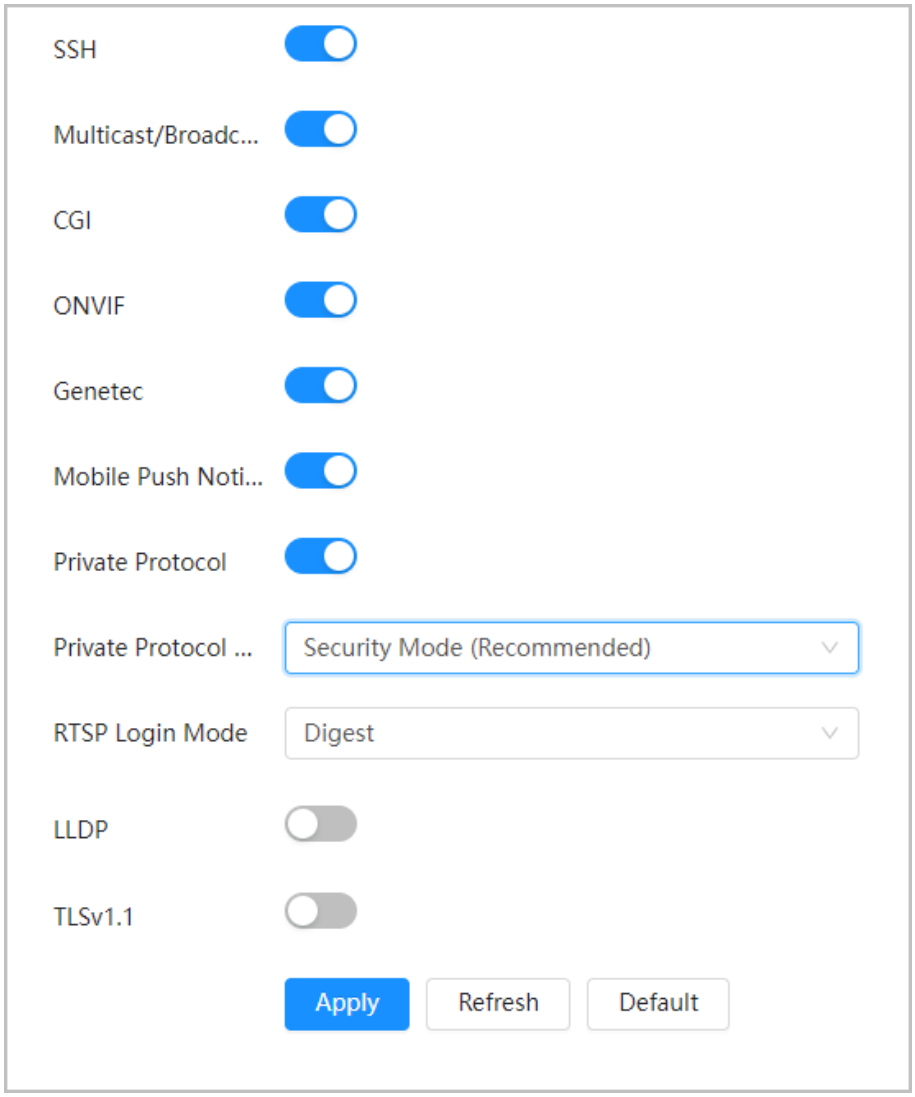
4.4.13 Basic Service

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

Procedure

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

Figure 4-48 Basic service



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

Table 4-24 Description of basic service parameters

Function	Description
SSH	You can enable SSH authentication to perform safety management. The function is closed by default. SSH: Secure Shell.
Multicast/Broadcast Search	Enable this function, and then when multiple users are viewing the device video image simultaneously through network, they can find your device with multicast/broadcast protocol.
CGI	Enable the function, and then other devices can access through this service. The function is enabled by default. CGI: Common Gateway Interface
ONVIF	
Genetec	
Mobile Push Notification	Enable this function, and then the system will send the snapshot that was taken when alarm is triggered to your phone. This is enabled by default.
Private Protocol	Select to whether to enable private protocol function.

Function	Description
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 is digest 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 adjustment functions, and might differ from the actual page.

It supports two ways to enter the page of **PTZ**. The following content of the chapter uses the button entry from the upper right corner of the page as an example.

- On the main webpage, click **PTZ**.
- Click on the upper right corner of the webpage, 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 that you can quickly call these parameters and adjust the PTZ to the correct position.

Procedure

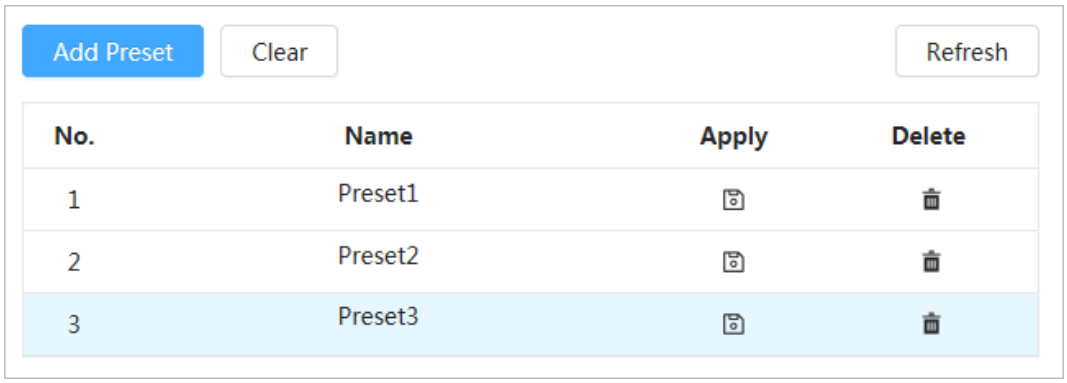
Step 1 Click , and then select **PTZ** > **Preset**.

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 4-49 Add preset



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

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 after configuration.

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.

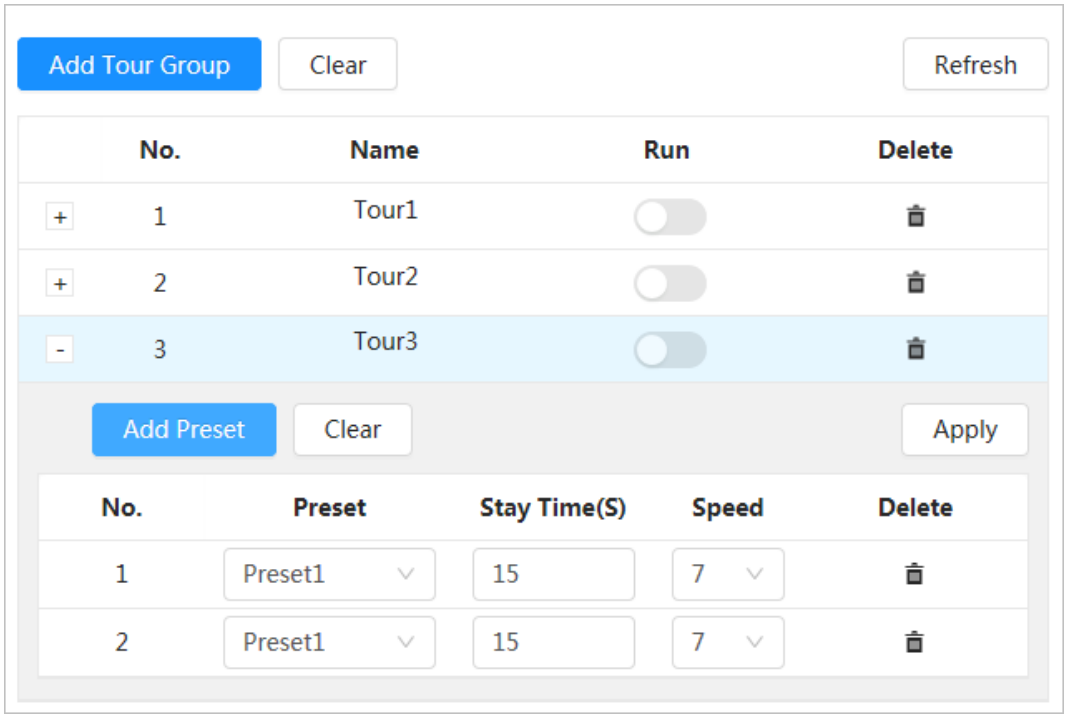
Step 3 Select tour group and then click **Add Tour Group** . Select the presets from the **Preset Point** drop-down list on the left.

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

Step 4 Configure **Stay Time(S)** and **Speed** to set the camera's stay time at the preset point and its rotating speed.

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

Figure 4-50 Tour group



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 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

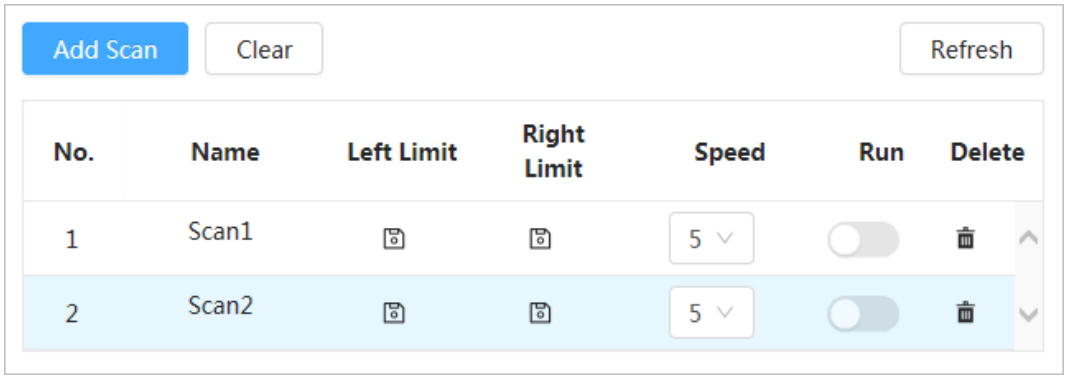
Step 1 Click , and then select **PTZ** > **Scan**.

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.

1. 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.
2. 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 4-51 Scan



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 means a record of a series of operations that makes to the Camera. The operations include horizontal and vertical movements, zoom and preset calling. Record and save the operations, and then you can call the pattern path directly.

Procedure

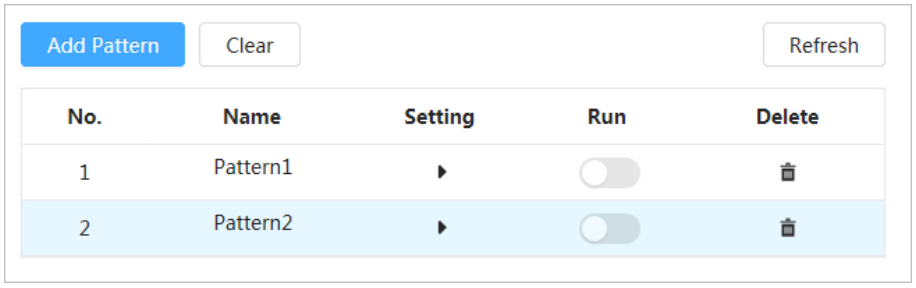
Step 1 Click , and then select **PTZ** > **Pattern**.

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 actual needs.

Step 4 Click to complete records.

Figure 4-52 Pattern



Step 5 Click to start the pattern.

Click to stop the pattern.

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.

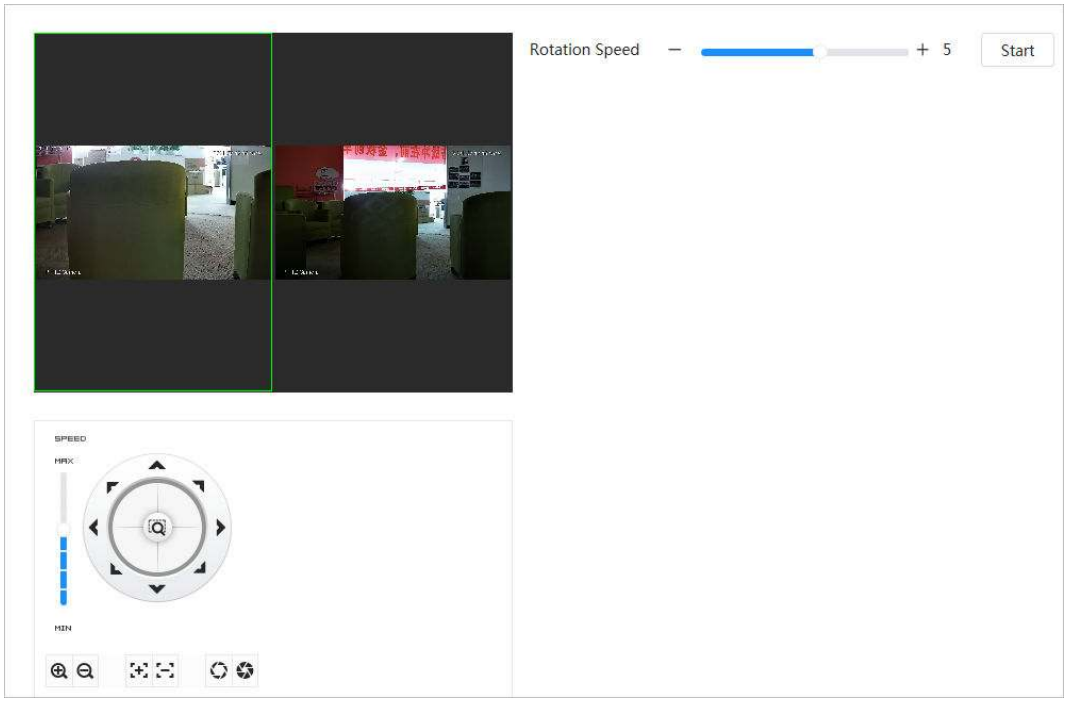
Procedure

Step 1 Click , and then select **PTZ** > **Pan**.

Step 2 Configure the rotation speed.

- Click **Start** and PTZ's horizontal rotation begins.
- Click **Stop** to stop the pan.

Figure 4-53 Pan



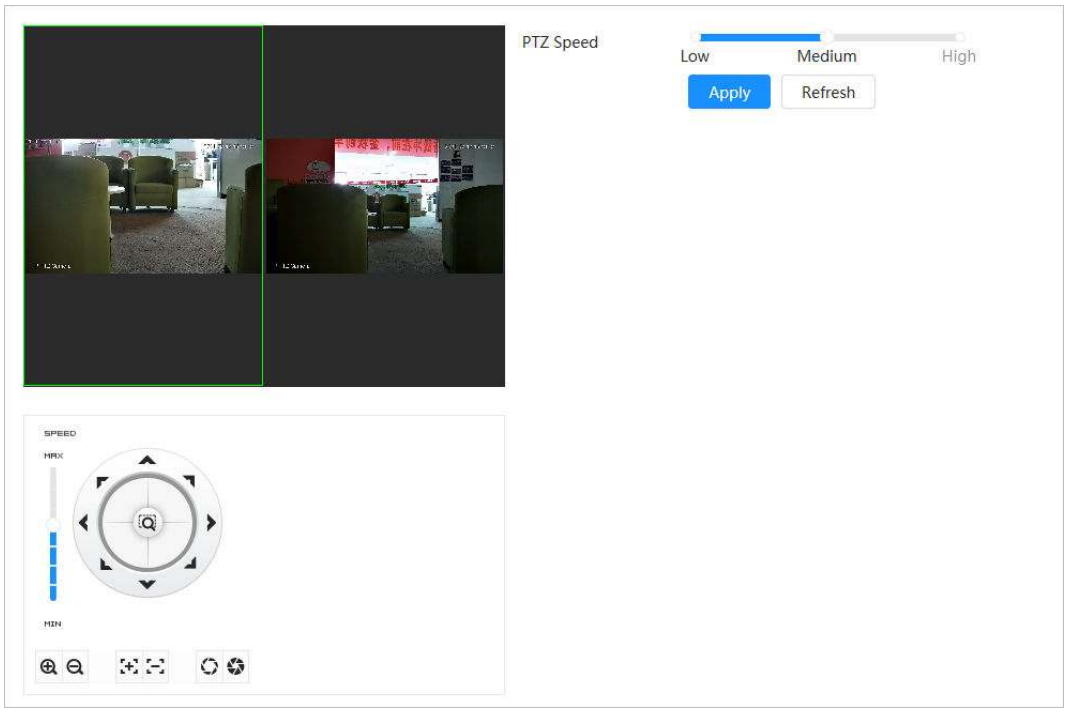
4.5.6 Configuring PTZ Speed

Configure the rotation speed when manually controlling the PTZ.

Procedure

Step 1 Click , and then select **PTZ** > **PTZ Speed**.

Figure 4-54 PTZ Speed



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 a certain period.

Prerequisites

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

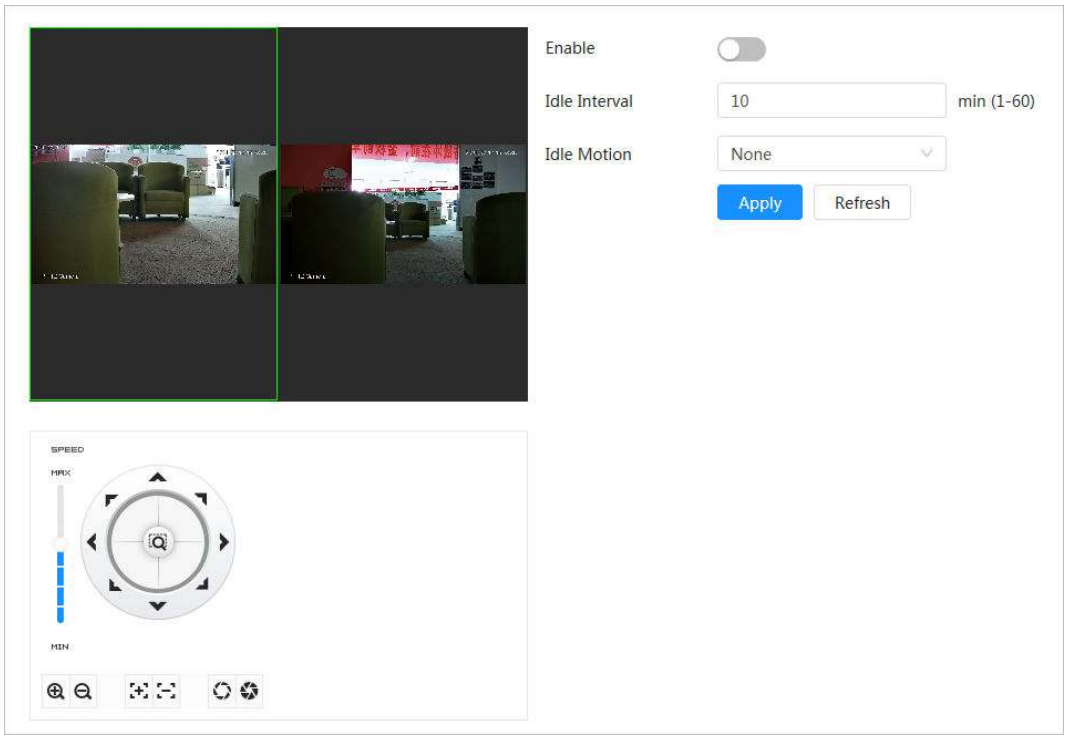
Procedure

Step 1 Click , and then select **PTZ** > **PTZ Speed**.

Step 2 Click to enable idle motion.

Step 3 Configure idle interval, and then select **Idle Motion**.

Figure 4-55 Idle motion



Step 4 Click **Apply**.

4.5.8 Configuring PowerUp

After configuring PowerUp, 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

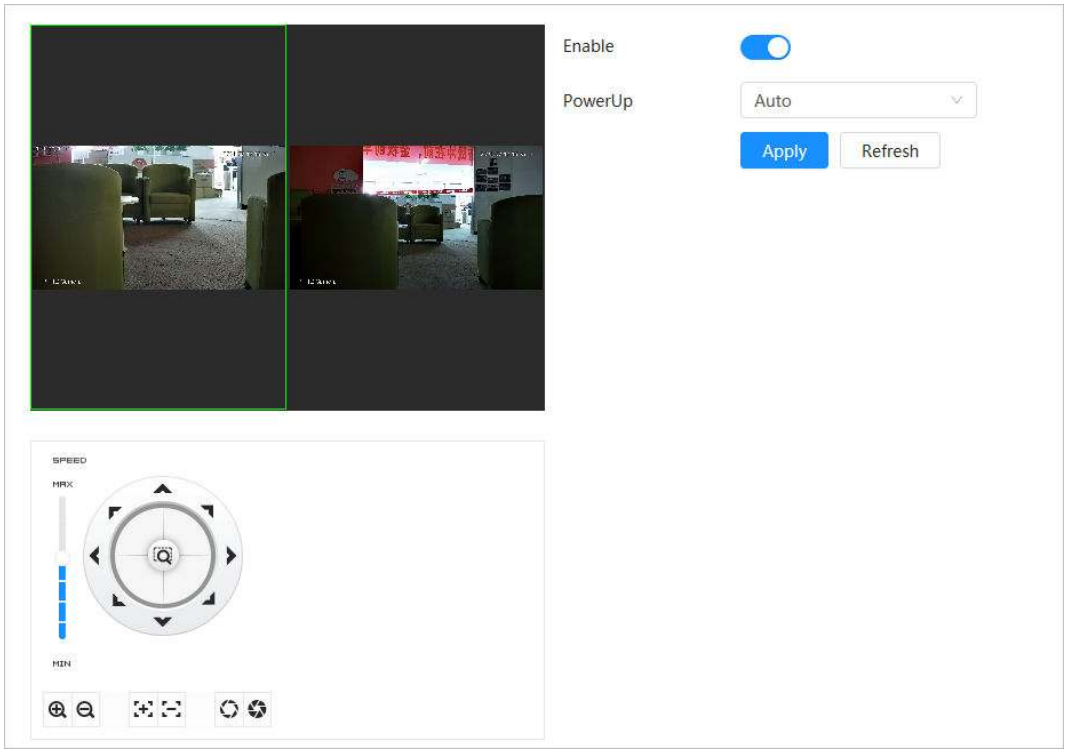
Step 1 Click , and then select **PTZ** > **PowerUp**.

Step 2 Click to enable PowerUp.

Step 3 Select PowerUp.

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

Figure 4-56 PowerUp



Step 4 Click **Apply**.

4.5.9 Configuring PTZ Rotation Limit

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

Procedure

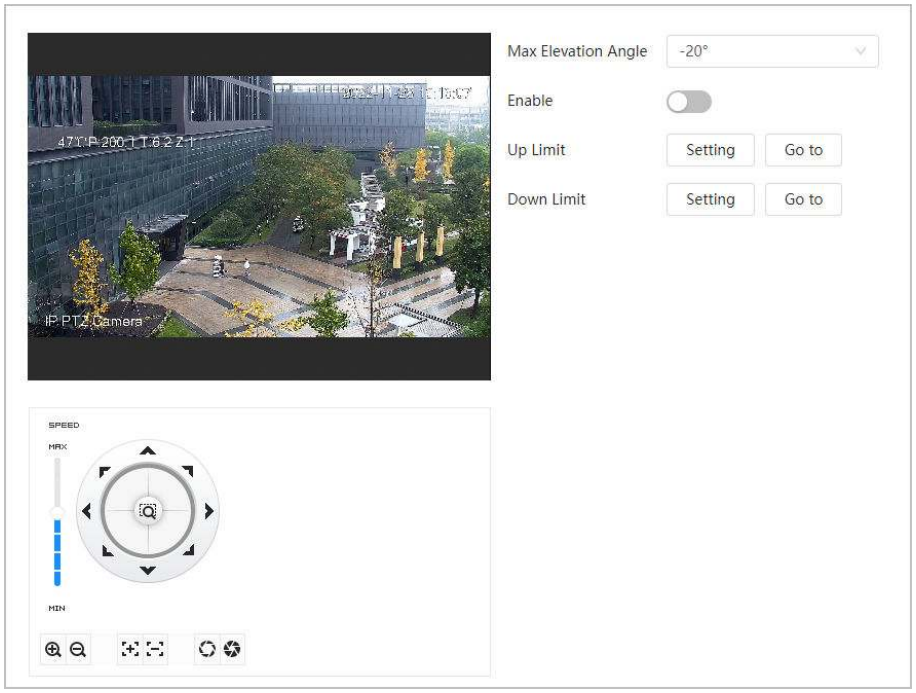
Step 1 Click, and then select **PTZ** > **PTZ Rotation Limit**.

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

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

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

Figure 4-57 PTZ rotation limit



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**.

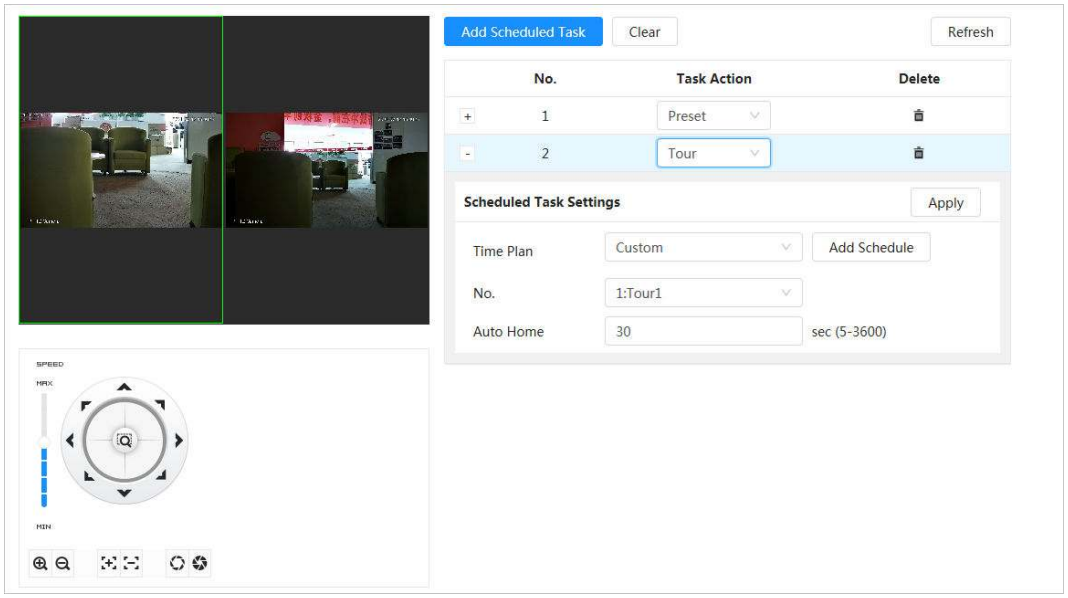
Step 3 Select **Task Action**.

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 scheduled task in the pop-up page and then click **Apply**.

To configure arming/disarming period, see "4.6.1.2.1 Adding Schedule".

Figure 4-58 Scheduled task



Step 5 Set the time for "Auto Home".

"Auto Home": When the scheduled task is interrupted by an artificial call to the PTZ, the device 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**.

Procedure

Step 1 Click and then select **PTZ** > **PTZ Maintenance**.

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

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

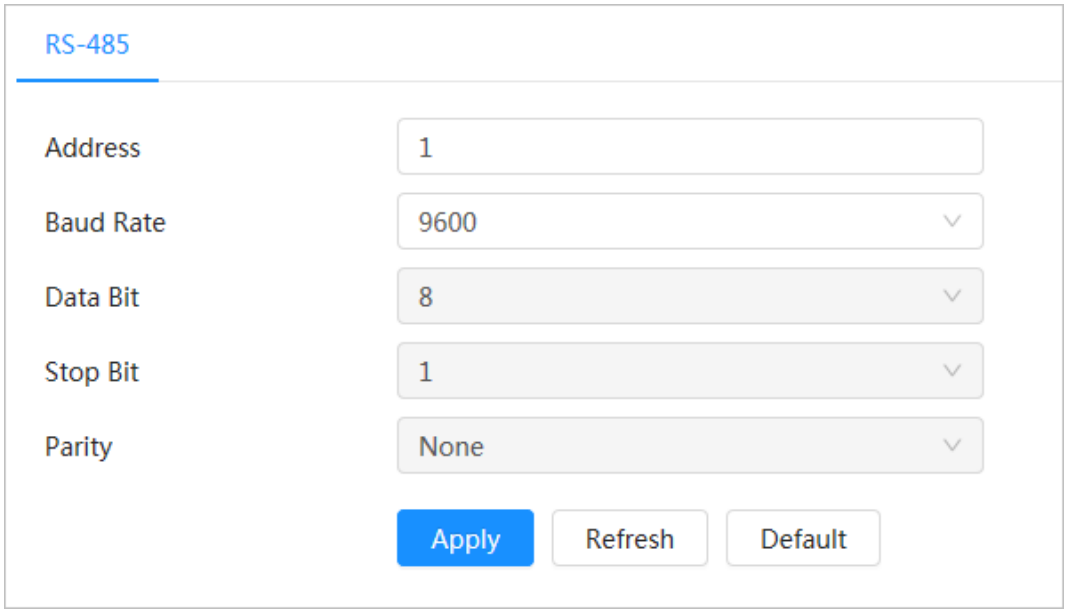
4.5.12 Configuring Protocol

Configure parameters for RS-485.

Procedure

Step 1 Click and then select **PTZ** > **Protocol**.

Figure 4-59 Configure protocol



Step 2 Click **Apply**.

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 an example.

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

4.6.1 Setting Alarm Linkage

4.6.1.1 Setting Alarm-in

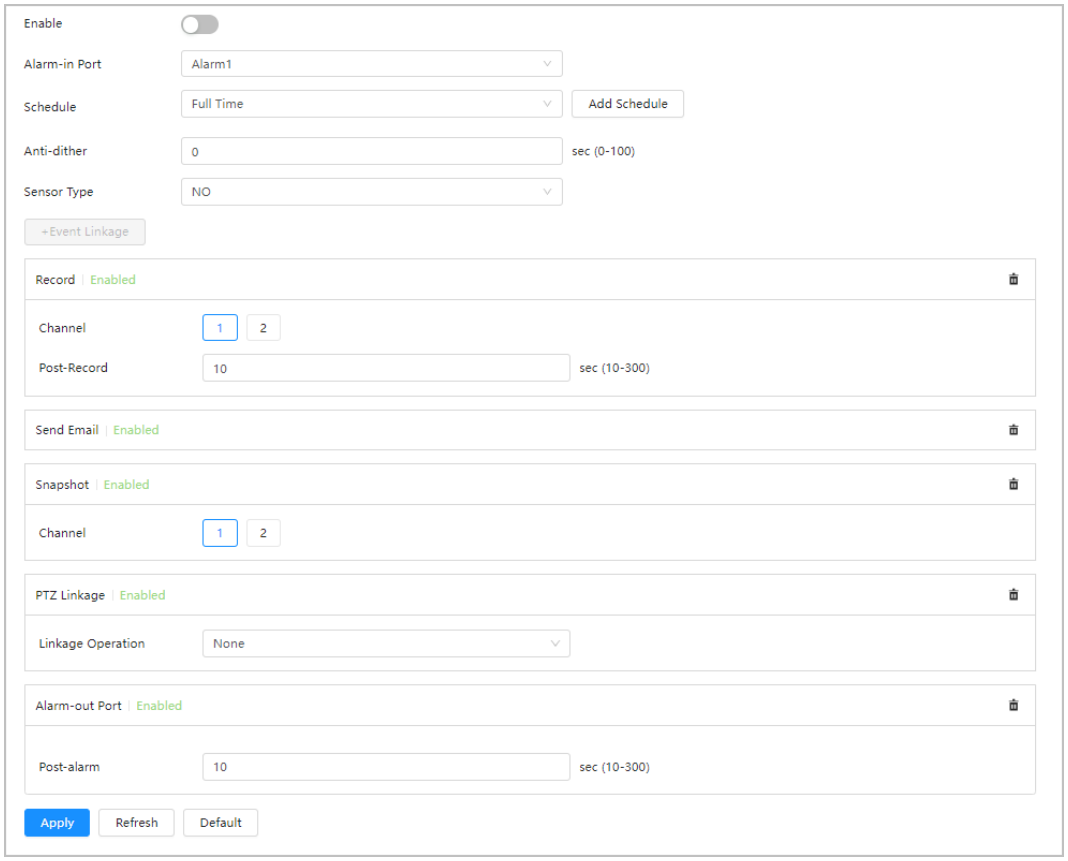
When an alarm is triggered by the device connected to the alarm-in port, the system performs the defined alarm linkage.

Procedure

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

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

Figure 4-60 Alarm linkage



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. For details, see "4.6.1.2 Alarm Linkage".

If the exiting schedules cannot meet the scene requirement, you can click **Add Schedule** to add new schedule. For details, see "4.6.1.2.1 Adding Schedule".

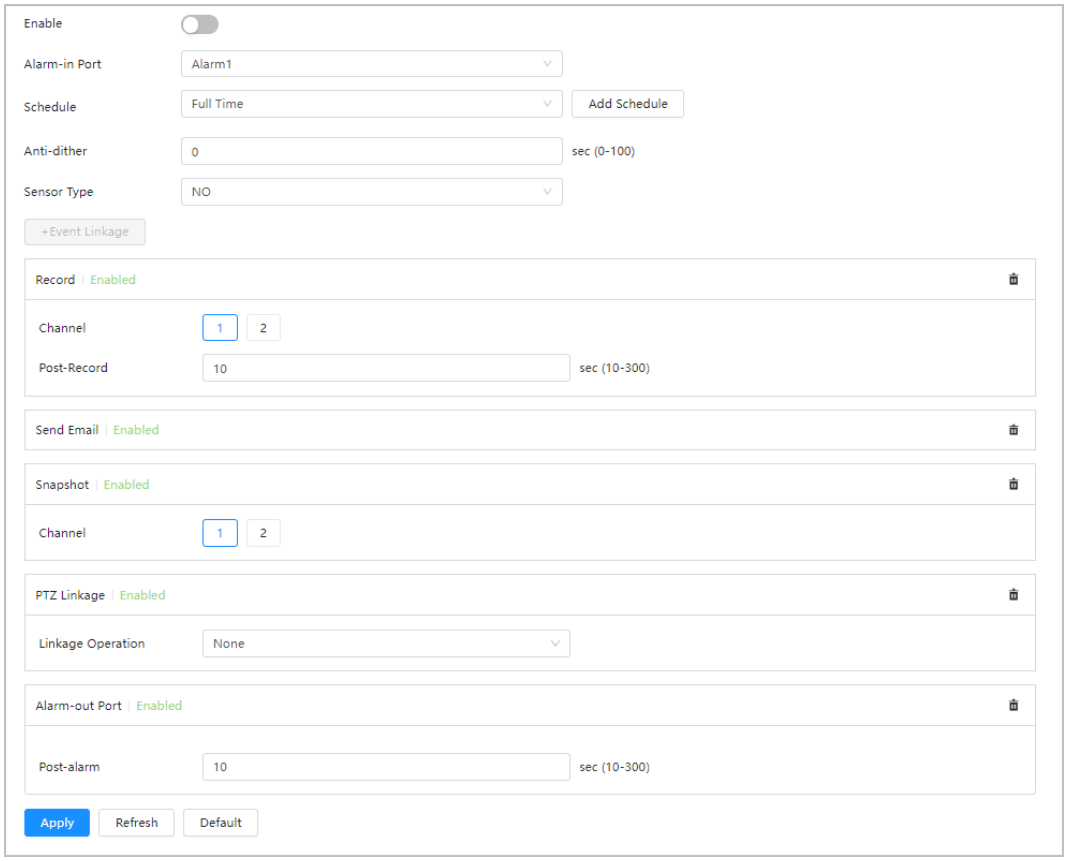
Step 5 Click **Apply**.

4.6.1.2 Alarm Linkage

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

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

Figure 4-61 Alarm linkage



4.6.1.2.1 Adding Schedule

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

Procedure

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

Step 2 Click **Time Plan Table**.

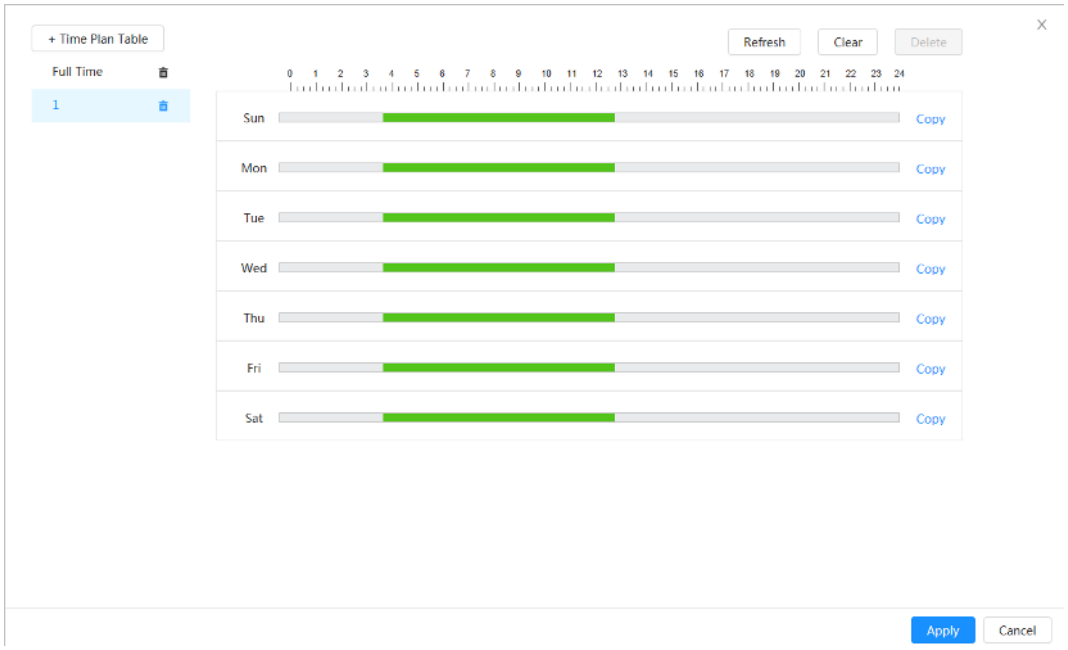
You can set up multiple time plan tables for selection.

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

Step 4 Configure arming periods.

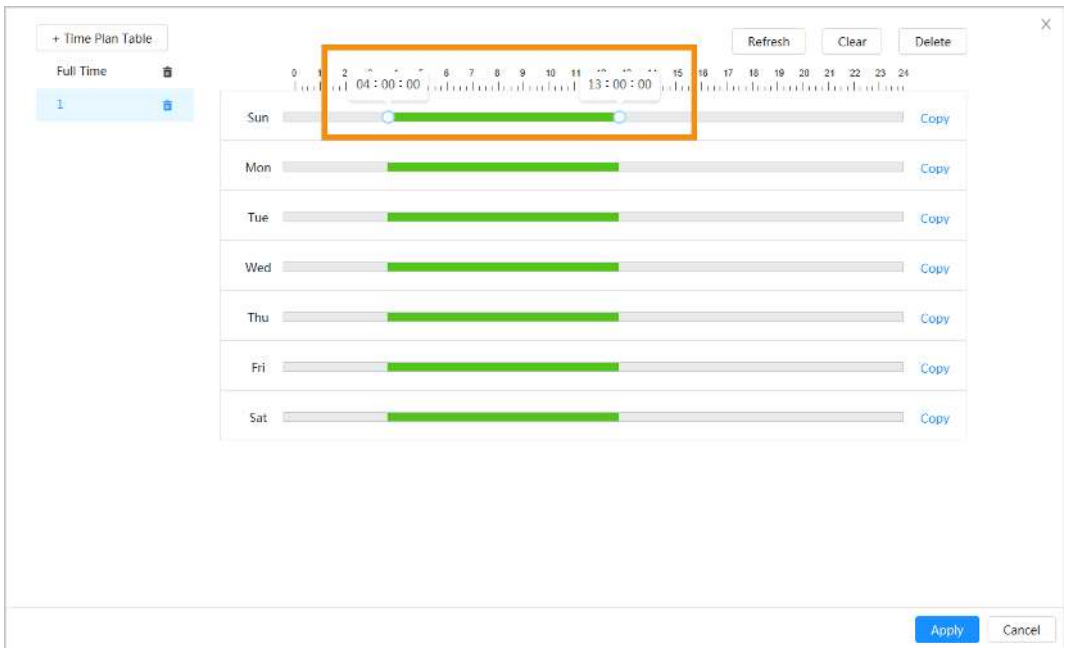
1. Press and drag the left mouse button on the timeline to set arming periods. Alarms will be triggered in the time period in green on the timeline.

Figure 4-62 Configuring arming period



2. Click the selected time period, and then enter the specific time in the text box to configure exact arming period.

Figure 4-63 Configuring exact arming period



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

Time plans for the current day can be quickly copied to other days.

Step 6 Click **Apply**.

4.6.1.2.2 Record Linkage

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

Prerequisites

- After the corresponding alarm type (**Normal** , **Motion**, or **Alarm**) is enabled, the record channel links recording. For details, see "6.3 Setting Record Plan".
- Enable auto record mode, the record linkage will take effect. For details, see "6.2 Setting Record Control".

Setting Record Linkage

On the **Alarm** page, click to enable record linkage, select the channel as needed, 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.

Click to delete record function.

Figure 4-64 Record linkage

4.6.1.2.3 Snapshot Linkage

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

Prerequisites

After the corresponding alarm type (**Normal** , **Motion**, or **Alarm**) is enabled, the snapshot channel links capturing picture. For details, see "6.3 Setting Record Plan".

Setting record linkage

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

Click to delete snapshot function.

Figure 4-65 Snapshot linkage

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 to enable alarm-out linkage, select the channel as needed, and then configure **Post alarm**.

When alarm delay is configured, alarm continues for an extended period after the alarm ends. Click to delete alarm-out linkage function.

Figure 4-66 Alarm-out linkage

4.6.1.2.5 Email Linkage

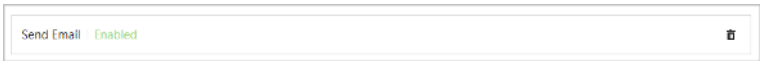
When an alarm is triggered, the system will automatically send an email to users.

Email linkage takes effect only when SMTP is configured. For details, see "4.4.5 Email".

On the **Alarm** page, click **Event Linkage**, and then select **Send Email**.

Click to delete email linkage function.

Figure 4-67 Email linkage



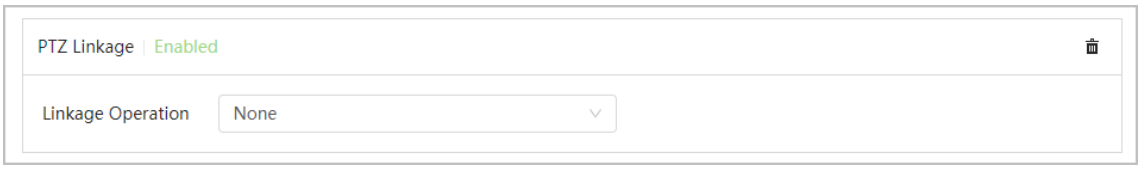
4.6.1.2.6 PTZ Linkage

When an alarm is triggered, the system will automatically link PTZ devices.

On the **Alarm** page, click **Event Linkage**, select **PTZ Linkage**, and then select the **Linkage Operation**.

Click to delete PTZ linkage function.

Figure 4-68 PTZ linkage



4.6.1.3 Subscribing Alarm

4.6.1.3.1 Alarm Types

Following are the alarm types and preparations of alarm events.

Table 4-25 Description of alarm types

Alarm Type	Description	Preparation
Motion Detection	The alarm is triggered when a moving object is detected.	Motion detection is enabled. For details, see "4.6.3.1 Setting Motion Detection".
Disk Full	The alarm is triggered when the free space of SD card is less than the configured value.	The SD card no space function is enabled. For details, see "4.6.2.1 Setting SD Card Exception".
Disk Error	The alarm is triggered when there is a failure or malfunction in the SD card.	SD card failure detection is enabled. For details, see "4.6.2.1 Setting SD Card Exception".
Video Tampering	The alarm is triggered when the camera lens is covered or there is a defocus in video images.	Video tampering is enabled. For details, see "4.6.3.2 Setting Video Tampering".
External Alarm	The alarm is triggered when there is an external alarm input.	The device has alarm input port and external alarm function is enabled. For details, see "4.6.1.1 Setting Alarm-in".
Security Warning	The alarm is triggered when there is a security warning.	Security warning is enabled. For details, see "9.6 Security Warning"
Audio Detection	The alarm is triggered when there is an audio connection problem.	Abnormal audio detection is enabled. For details, see "4.6.4 Setting Audio Detection".
AI Event	The alarm is triggered when an AI event is triggered.	Enable IVS, crowd map, face detection or people counting, and other intelligent functions.
Scene Changing	The alarm is triggered when the device monitoring scene changes.	Scene changing detection is enabled. For details, see "4.6.3.3 Setting Scene Changing".
Voltage Detection	The alarm is triggered when the device detects abnormal voltage input.	Voltage detection is enabled. For details, see "4.6.2.3 Setting Tampering Detection".
Security Exception	The alarm is triggered when the device detects malicious attack.	Voltage detection is enabled. For details, see "9.1 Security Status".

4.6.1.3.2 Subscribing Alarm Information

Background Information

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

Functions of different devices might vary.

Procedure

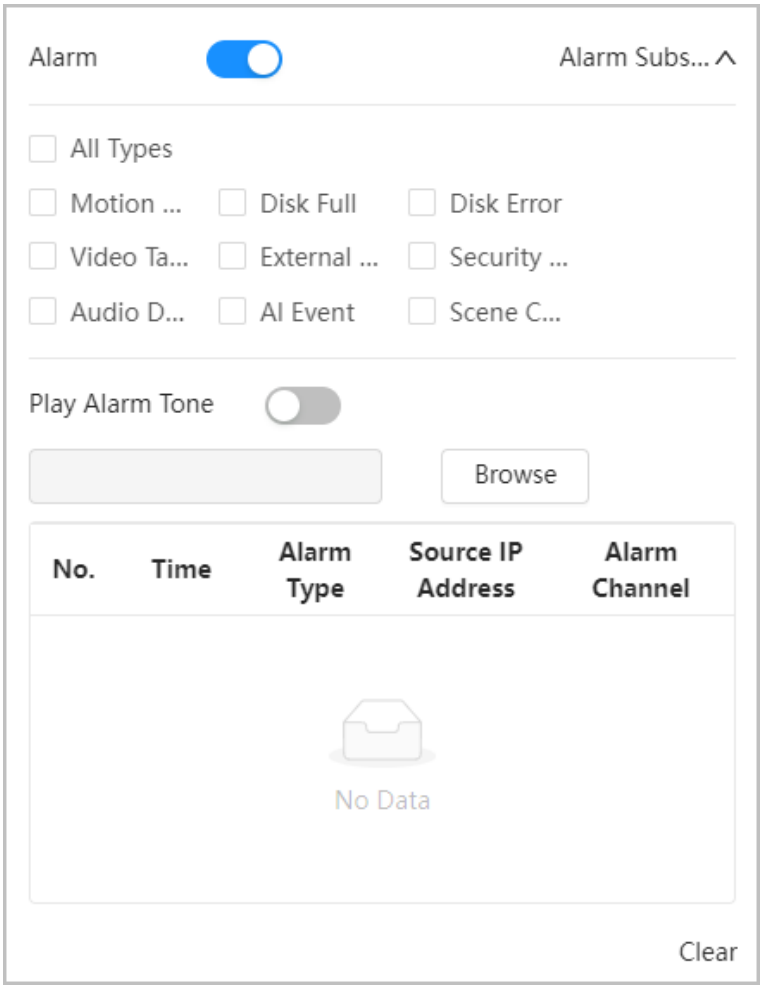
Step 1 Click on the right-upper corner of the webpage.

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

When the subscribed alarm event is triggered and the alarm subscription page is not displayed, a number is displayed on, and the alarm information is recorded automatically.

Click to view the details in the alarm list. You can click **Clear** to clear the record.

Figure 4-69 Alarm (subscription)



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

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

4.6.2 Setting Exception

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

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

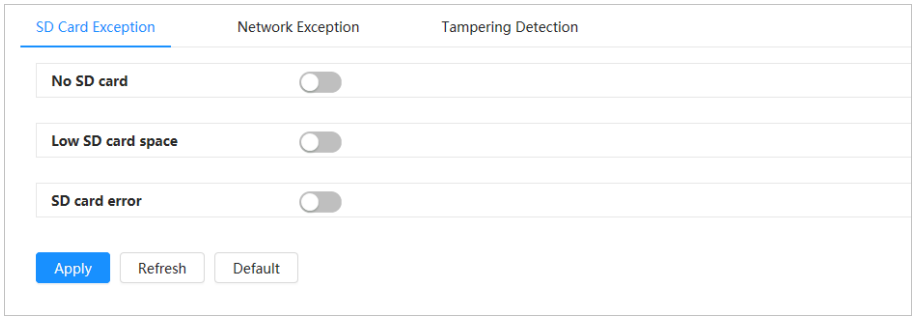
4.6.2.1 Setting SD Card Exception

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

Procedure

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

Figure 4-70 SD card exception



Step 2 Click to enable the SD card detection functions.

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

Step 3 Set alarm linkage actions. For details, see "4.6.1.2 Alarm Linkage".

Step 4 Click **Apply**.

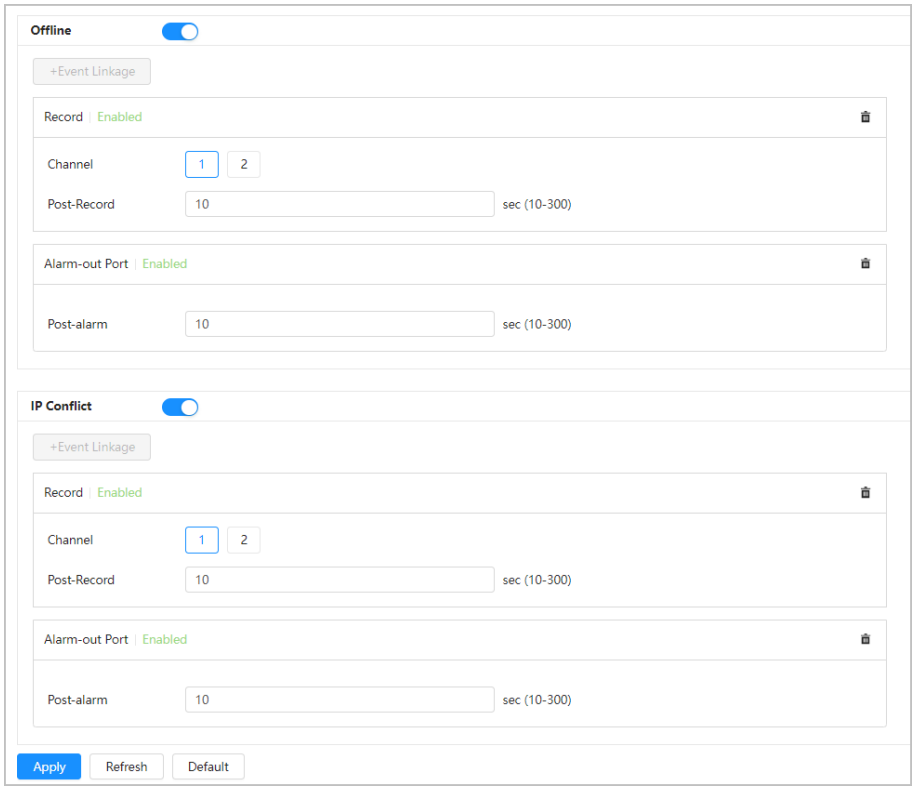
4.6.2.2 Setting Network Exception

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

Procedure

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

Figure 4-71 Network exception



Step 2 Click to enable the network detection function.

Step 3 Set alarm linkage actions. For details, see "4.6.1.2 Alarm Linkage".

Step 4 Click **Apply**.

4.6.2.3 Setting Tampering Detection

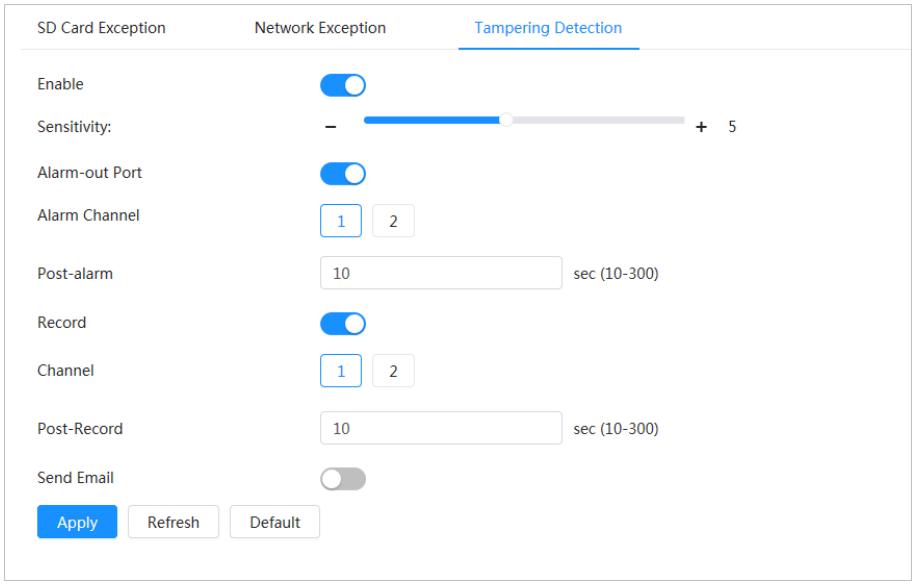
Procedure

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

Step 2 Click to enable the tampering detection function.

Step 3 Configure alarm parameters.

Figure 4-72 Setting tampering detection



Step 4 Click **Apply**.

4.6.3 Setting Video Detection

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

4.6.3.1 Setting Motion Detection

Background Information

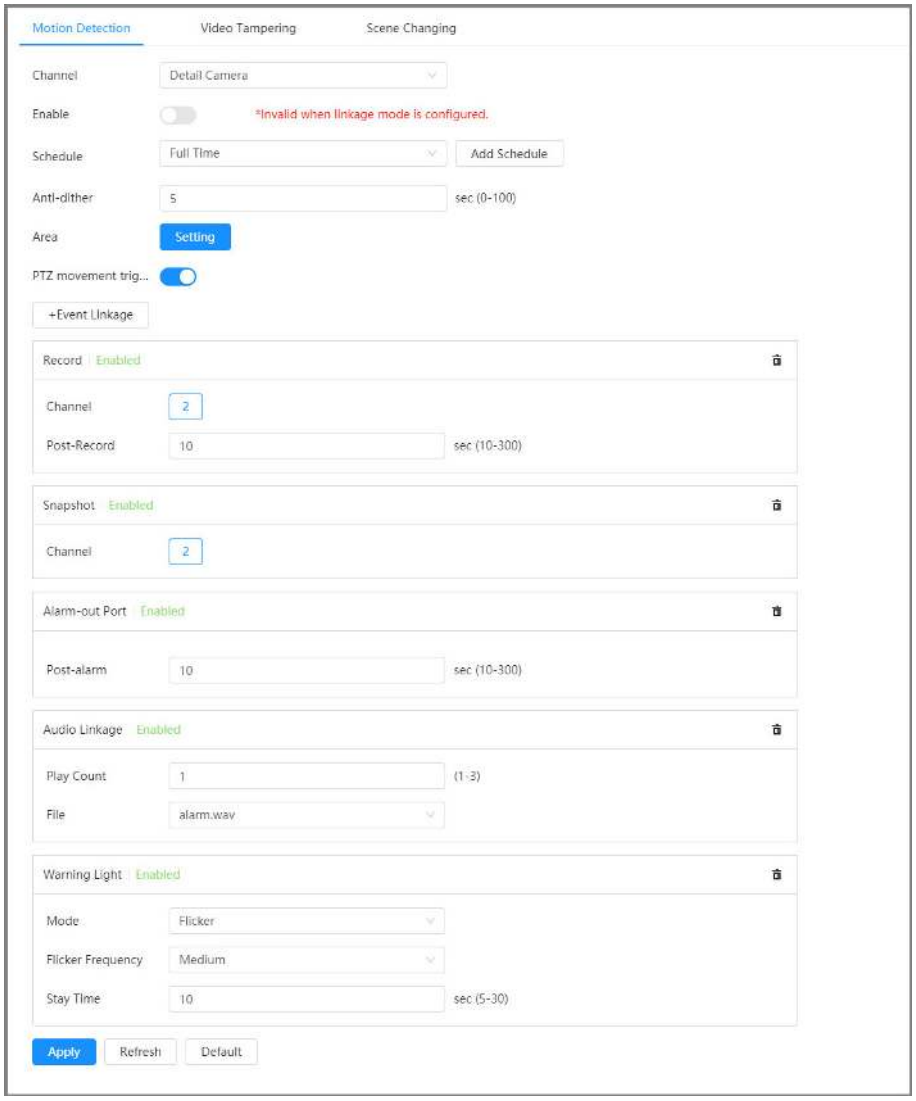
The system performs an alarm linkage when a moving object appears in the image and its moving speed reaches the configured sensitivity.

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

Procedure

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

Figure 4-73 Motion detection



Step 2 Select the Camera from **Channel**.

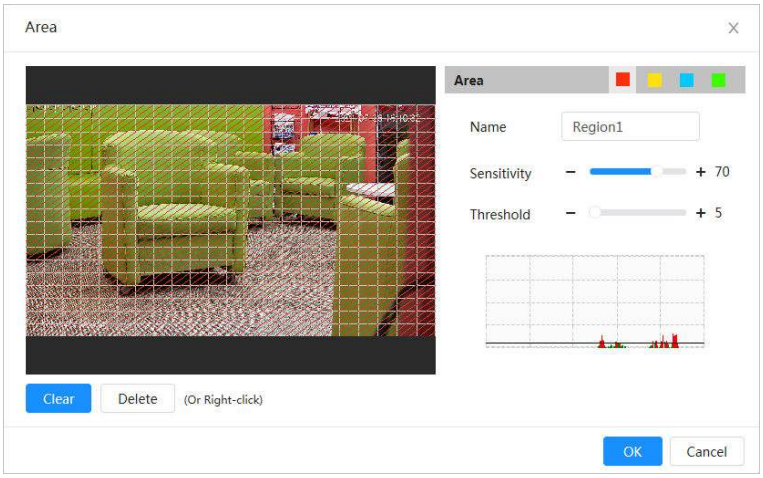
Step 3 Click to enable the motion detection function.

You cannot enable the motion detection function when linkage mode is configured.

Step 4 Set the area for motion detection.

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

Figure 4-74 Area



2. Select a color and set the region name.
   - Select a color on to set different detection parameters for each region.
3. Select an effective area for motion detection in the image and set **Sensitivity** and **Threshold**.
   - Sensitivity: Sensitive degree of outside changes. The higher sensitivity is, the easier to trigger the alarm.
   - Threshold: Effective area threshold for the motion detection. The smaller the threshold is, the easier the alarm is triggered.
   - The whole video image is the effective area for the motion detection by default.
   - The red line in the waveform indicates that the motion detection is triggered, and the green one indicates that there is no motion detection. Adjust sensitivity and threshold according to the waveform.
4. Click **OK**.

Step 5 Set arming periods and alarm linkage action.

For some devices, you can set warning light linkage and audio linkage for the motion detection. For details of other linkages, see "4.6.1.2 Alarm Linkage".

- **Warning Light Linkage** : When an alarm is triggered, the warning light will automatically flicker.

  The default mode is **Flicker** , you can configure **Flicker Frequency** and **Stay time** to set the frequency and duration of the warning light.
- **Audio Linkage** : When an alarm is triggered, the system will automatically activate an audio alarm.

  You can configure **Play Count** to the set the number of playbacks for audio, and select an audio file from **File** as needed.

If the exiting schedules cannot meet the scene requirement, you can click **Add Schedule** to add a new schedule. For details, see "4.6.1.2.1 Adding Schedule".

Anti-dither: After the anti-dither time is set, the system only records one motion detection event in the period.

Step 6 Click **Apply**.

4.6.3.2 Setting Video Tampering

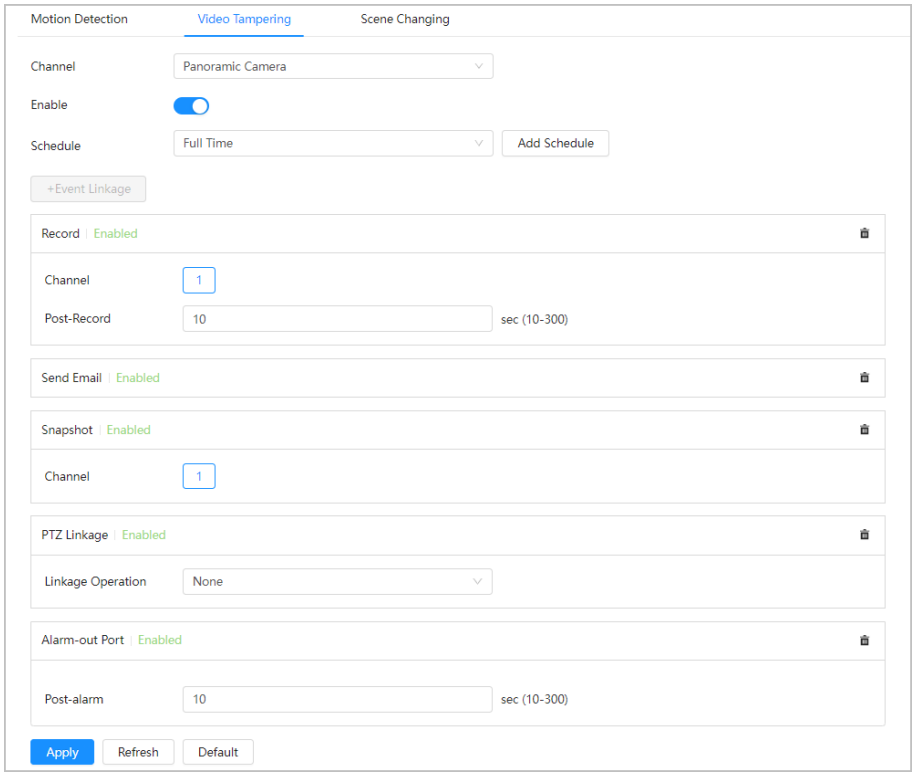
The system performs alarm linkage when the lens is covered or video output is mono-color caused by light and other reasons.

Procedure

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

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

Figure 4-75 Video Tampering



Step 3 Set arming periods and alarm linkage action. For details, see "4.6.1.2 Alarm Linkage".

If the exiting schedules cannot meet the scene requirement, you can click **Add Schedule** to add a new schedule. For details, see "4.6.1.2.1 Adding Schedule".

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

Step 4 Click **Apply**.

4.6.3.3 Setting Scene Changing

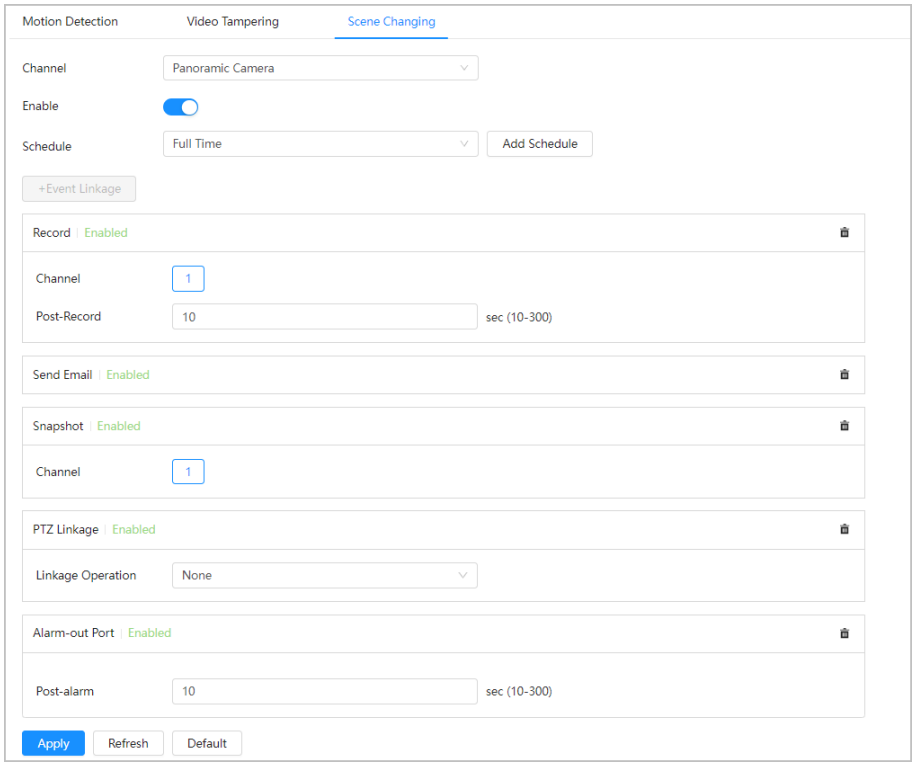
The system performs alarm linkage when the image switches from the current scene to another one.

Procedure

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

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

Figure 4-76 Scene changing



Step 3 Set arming periods and alarm linkage action. For details, see "4.6.1.2 Alarm Linkage".

If the exiting schedules cannot meet the scene requirement, you can click **Add Schedule** to add a new schedule. For details, see "4.6.1.2.1 Adding Schedule".

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

Step 4 Click **Apply**.

4.6.4 Setting Audio Detection

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

Procedure

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

Step 2 (Optional) Select audio channels.

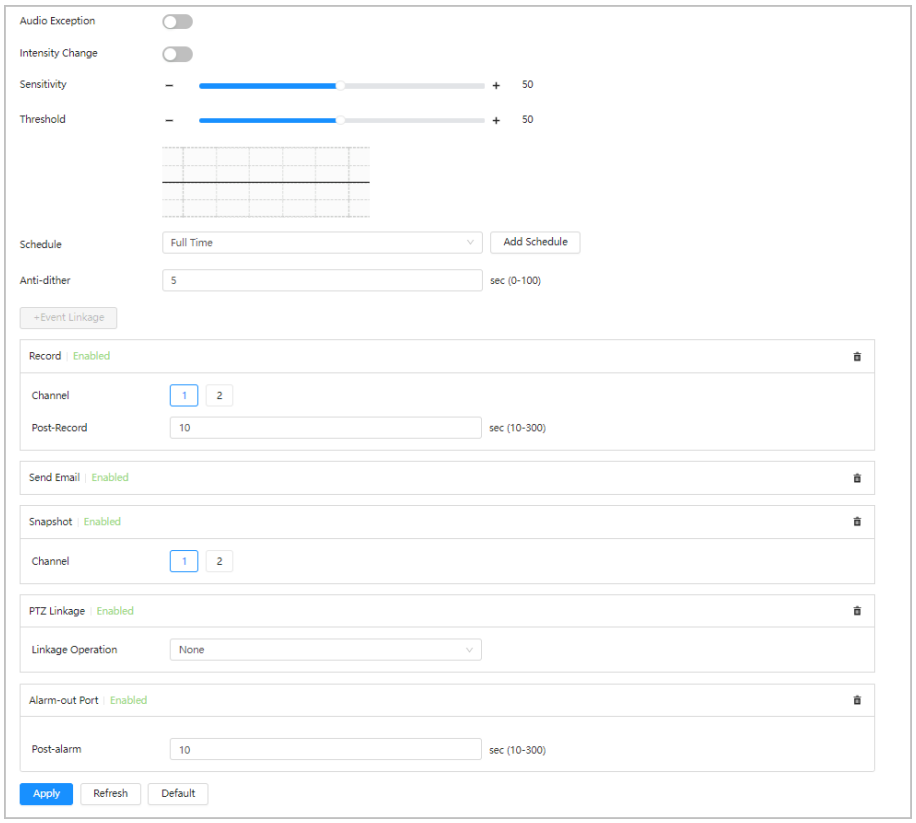
When the Camera supports multiple audio channels, it supports the selection of different audio channels.

Step 3 Configure parameters of audio detection.

- Input abnormal: Click next to **Audio Exception**, and the alarm is triggered when the system detects abnormal sound input.
- Intensity change: Click next to **Intensity Change** and then set **Sensitivity** and **Threshold**. The alarm is triggered when the system detects that the sound intensity exceeds the configured threshold.
  - ◇ The alarm is easier to be triggered with higher sensitivity or smaller threshold. Set a high threshold for noisy environment.

◇ The red line in the waveform indicates audio detection is triggered, and the green one indicates no audio detection. Adjust sensitivity and threshold according to the waveform.

Figure 4-77 Audio detection



Step 4 Set arming periods and alarm linkage action. For details, see "4.6.1.2 Alarm Linkage".

If the exiting schedules cannot meet the scene requirement, you can click **Add Schedule** to add a new schedule. For details, see "4.6.1.2.1 Adding Schedule".

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

Step 5 Click **Apply**.

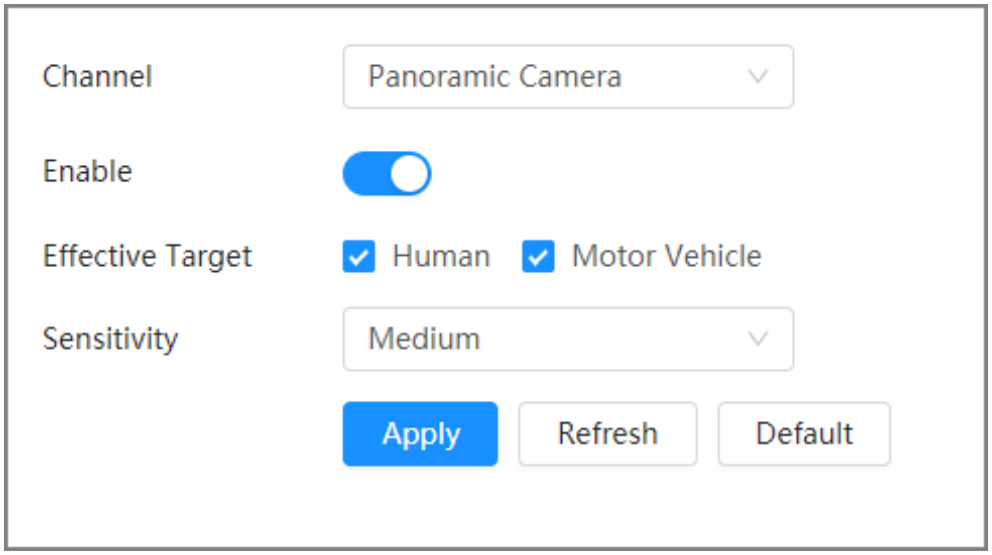
4.6.5 Setting Smart Motion

After configuring smart motion, an alarm is triggered when an effect target appears in the image.

Procedure

Step 1 Select > **Event** > **Smart Motion**.

Figure 4-78 Smart motion detection



Step 2 Select the Camera from **Channel**.

When you select **Detail Camera**, smart motion detection is invalid when linkage mode is configured.

Step 3 Click to enable the motion detection function.

Step 4 Select an effective target.

You can select human, motor vehicle, or both.

Step 5 Select the sensitivity.

The higher sensitivity is, the easier to trigger the alarm.

Step 6 Click **Apply**.

4.6.6 Setting Upload

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

Procedure

Step 1 Select **Event** > **Auto Upload**.

Step 2 Click to enable the function.

Step 3 Click **Add**, and then configure parameters of HTTP upload method.

You can add 2 piece of server information at most.

Figure 4-79 Image upload

Table 4-26 Description of HTTP mode parameters

Parameter	Description
IP/Domain name	The IP address and port number of the server which the report will be uploaded to.
Port	
Path	The storage path of the server for the report.
Event type	Select the event type form the drop-down list. You can select more than one types at the same time.
Test	Test the network connection between the camera and the server.

Step 4 Click **Apply**.

4.7 Storage

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

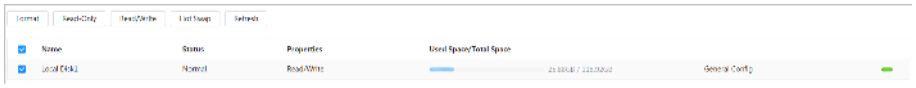
Functions might vary with different models.

Select > **Storage**.

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

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

Figure 4-80 Local



4.8 System

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

4.8.1 General

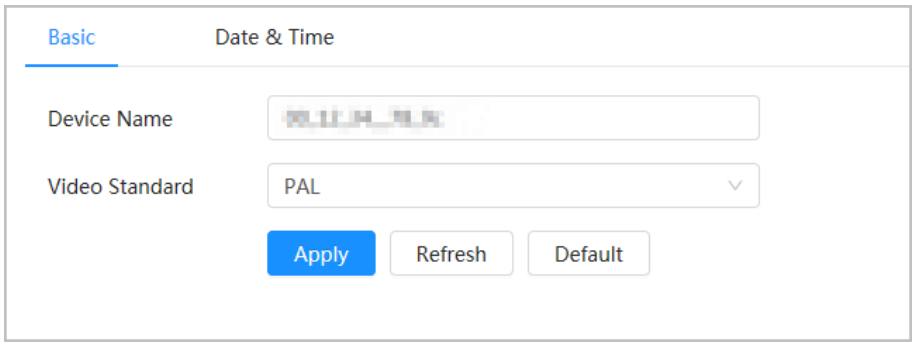
4.8.1.1 Basic

You can configure device name, language and video standard.

Procedure

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

Figure 4-81 Basic



Step 2 Configure general parameters.

Table 4-27 Description of general parameters

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

Step 3 Click **Apply**.

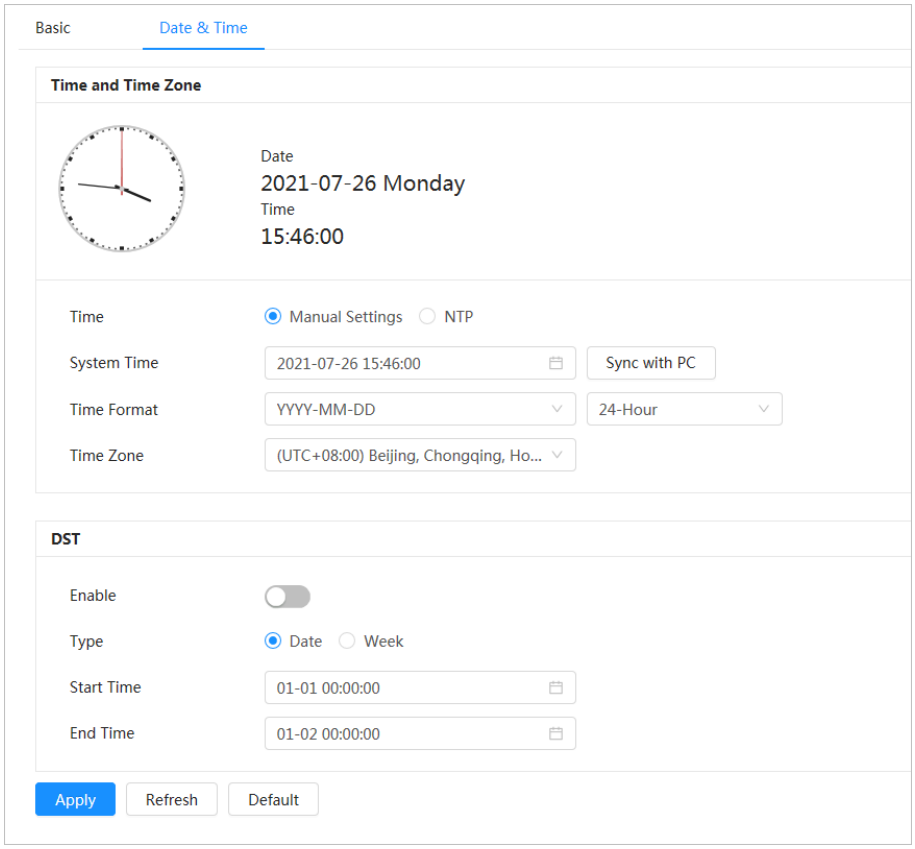
4.8.1.2 Date & Time

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

Procedure

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

Figure 4-82 Date and time



Step 2 Configure date and time parameters.

Table 4-28 Description of date and time parameters

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

Managing users and groups are only available for administrator users.

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

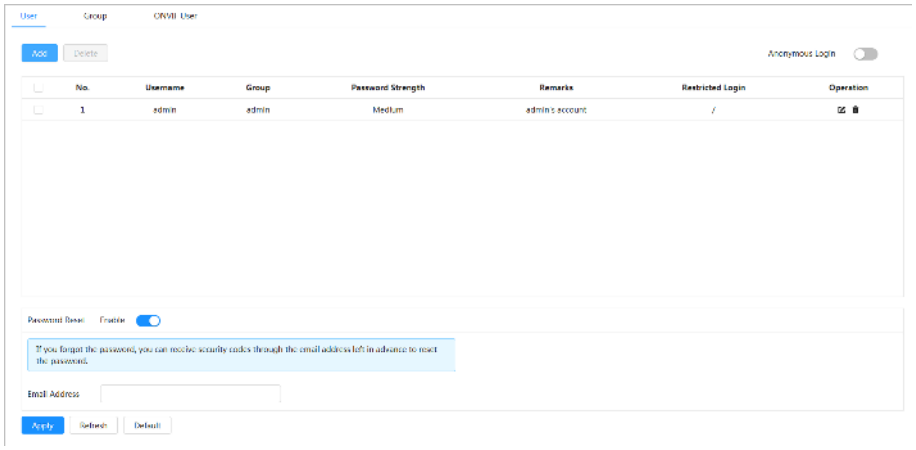
4.8.2.1 Adding User

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

Procedure

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

Figure 4-83 User



Step 2 Click **Add**.

Figure 4-84 Add user (system)

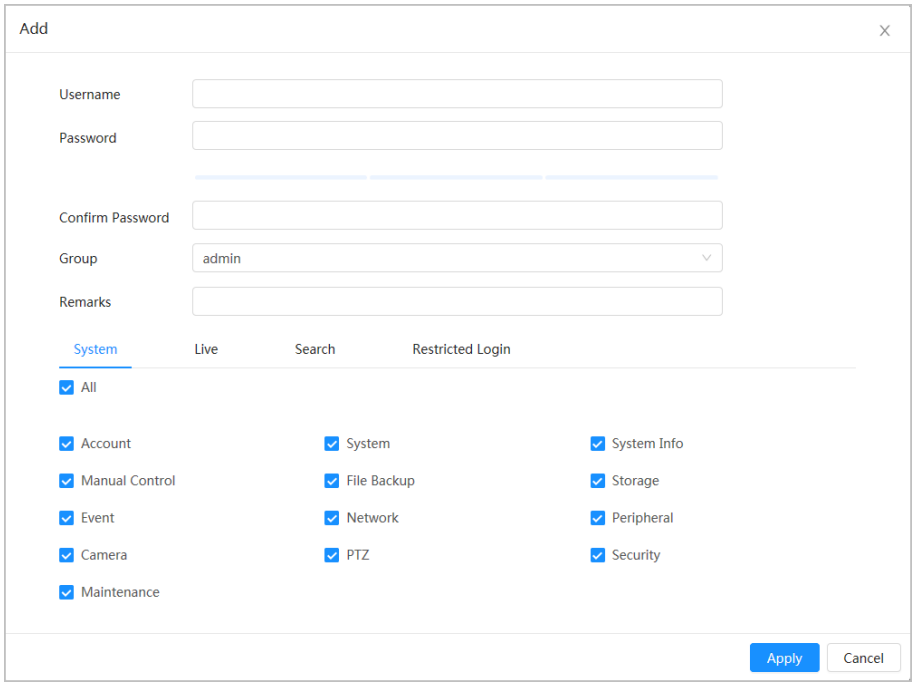


Figure 4-85 Add user (live)

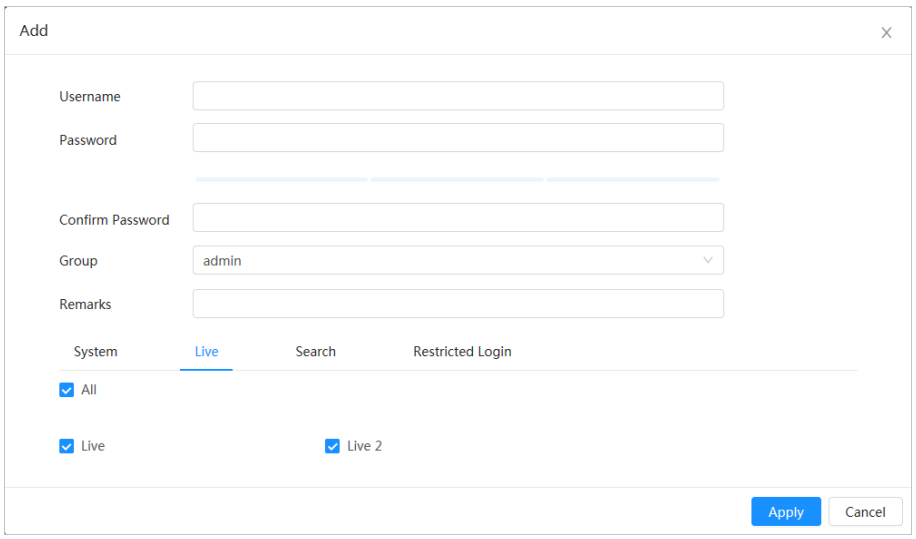


Figure 4-86 Add user (search)

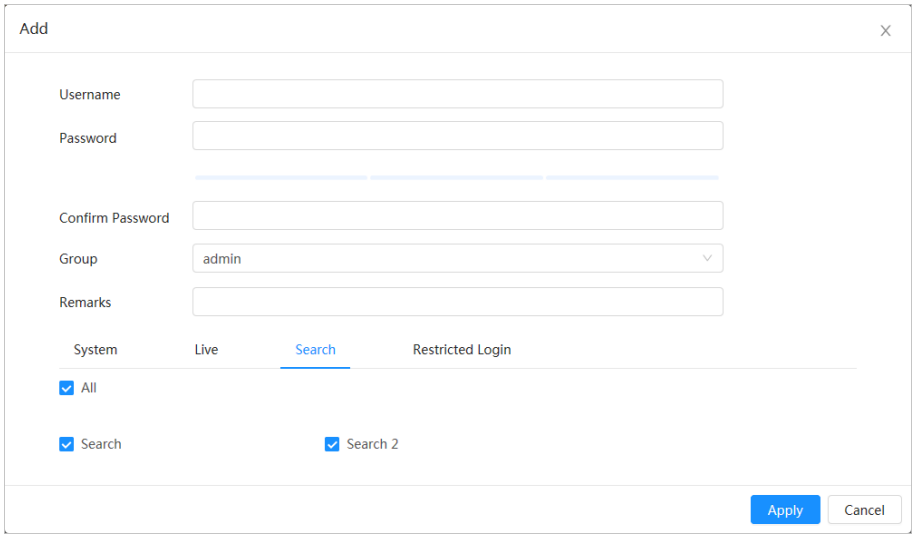
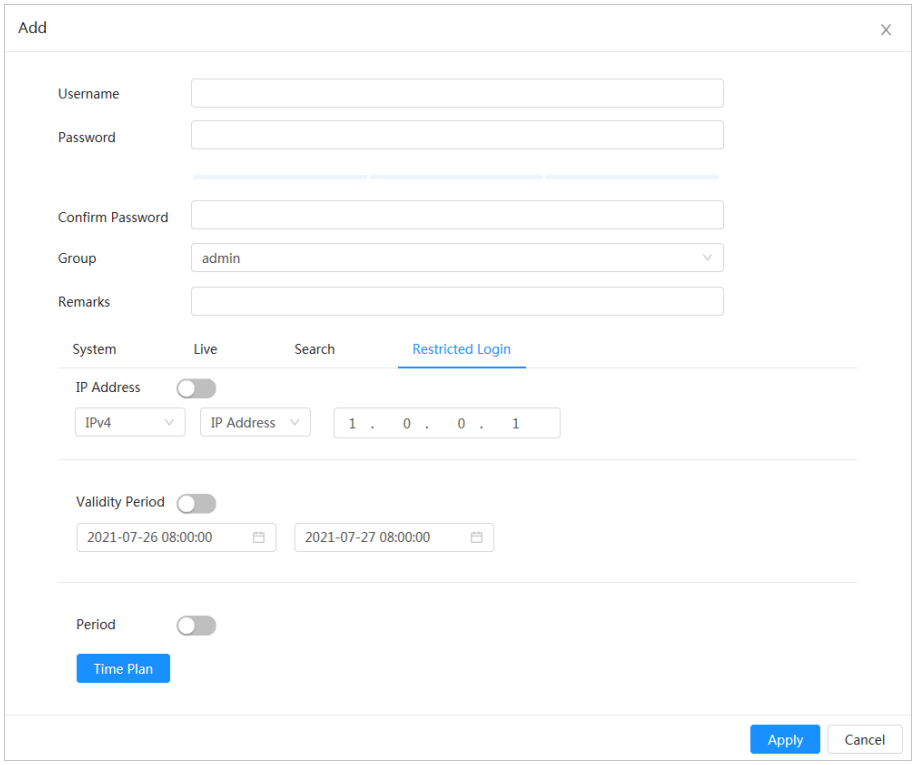


Figure 4-87 Add user (restricted log)



Step 3 Configure user parameters.

Table 4-29 Description of user parameters

Parameter	Description
Username	User's unique identification. You cannot use existed user name.
Password	Enter password and confirm it again. The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).
Confirm Password	

Parameter	Description
Group Name	The group that users belong to. Each group has different authorities.
Remarks	Describe the user.
System	Select authorities as needed. It is recommended to give fewer authorities to normal users than premium users.
Live	Select the live view authority for the user to be added.
Search	Select the search authority for the user to be added.
Restricted Login	Set the computer address that allows the defined user to log in to the Camera and the validity period and time range. You can log in to the webpage with the defined IP in the defined time range of validity period. • IP address: You can log in to web through the computer with the set IP. • Validity period: You can log in to web in the set validity period. • Time range: You can log in to web in the set time range. Set as follows: 1. IP address: Enter the IP address of the host to be added. 2. IP segment: Enter the start address and end address of the host to be added.

Step 4 Click **Apply**.

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

Related Operations

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

  For admin account, you can only edit the password.
- Click to delete the added users.

  The admin account cannot be deleted.

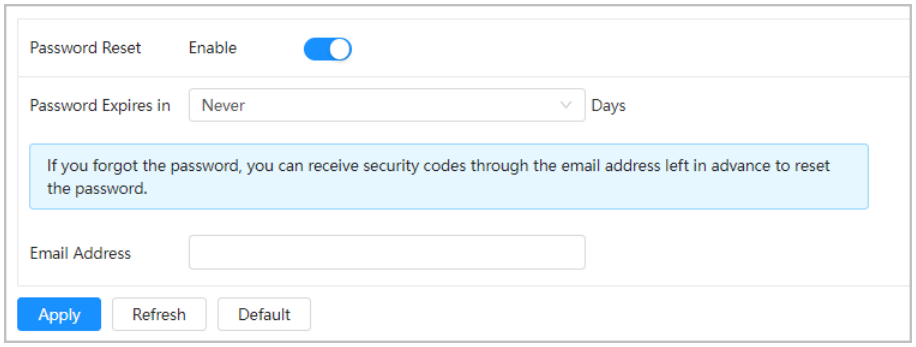
4.8.2.2 Resetting Password

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

Procedure

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

Figure 4-88 Resetting password



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

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

Step 3 Set the password expiration days, and then enter the reserved email address.

Step 4 Click **Apply**.

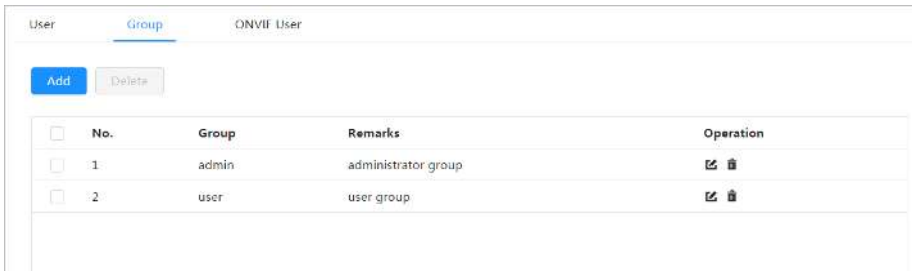
4.8.2.3 Adding User Group

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

Procedure

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

Figure 4-89 Group name



Step 2 Click **Add**.

Figure 4-90 Add group

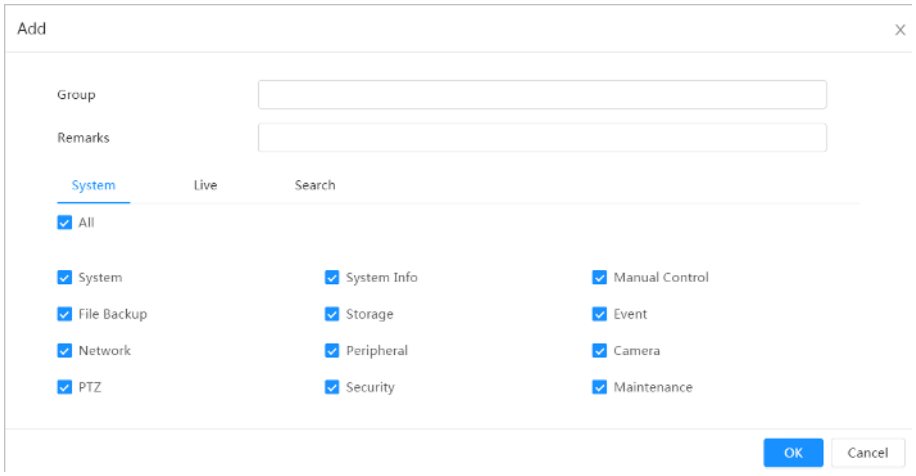


Table 4-30 Description of user group parameters

Group Authority	Admin	User	Functions
System	YES	NA	System time setting and 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 configuration and more.
Event	YES	NA	Video detection settings, audio detection settings, alarm settings and more.
Network	YES	NA	IP settings, SMTP settings, SNMP settings, AP Hotspot settings and more.
Peripheral	YES	NA	External light, wiper and serial port settings.
Camera	YES	NA	Camera property settings, audio and video settings and more.
PTZ	YES	NA	Preset settings, tour settings and more.
Security	YES	NA	HTTPS settings, RTSP over TLS settings and more.
Maintenance	YES	NA	Automatic maintenance settings and 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 Camera correspond to the authority control respectively. Only user with specified authority can use corresponding function; the admin group has all the authorities.

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

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

The newly added group displays in the group name list.

Related Operations

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

  For admin account, you can only edit the password.
- Click to delete the added users.

  The admin account cannot be deleted.

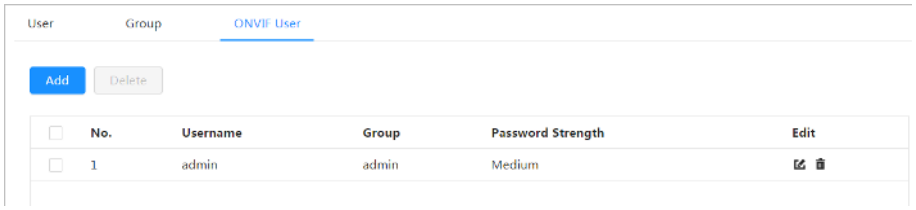
4.8.2.4 ONVIF User

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

Procedure

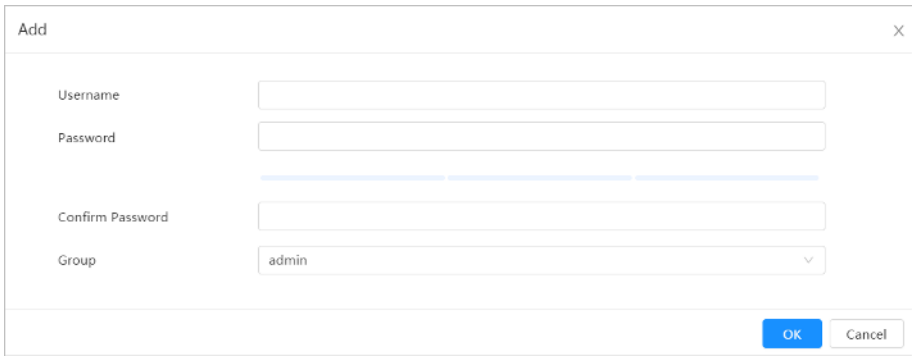
Step 1 Select > **System** > **Account** > **ONVIF User**.

Figure 4-91 ONVIF user



Step 2 Click **Add**.

Figure 4-92 Add ONVIF user



Step 3 Configure user parameters.

Table 4-31 Description of ONVIF user parameters

Parameter	Description
Username	User's unique identification. You cannot use existed username.
Password	Enter password and confirm it again. The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).
Confirm Password	
Group Name	The group that users belong to. Each group has different authorities.

Step 4 Click **OK**.

The newly added user displays in the username list.

Related Operations

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

  For admin account, you can only edit the password.

- Click to delete the added users.

  The admin account cannot be deleted.

4.8.3 Peripheral Management

4.8.3.1 Configuring Wiper

Procedure

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

Step 2 Configure working mode of wipers.

Figure 4-93 Wiper

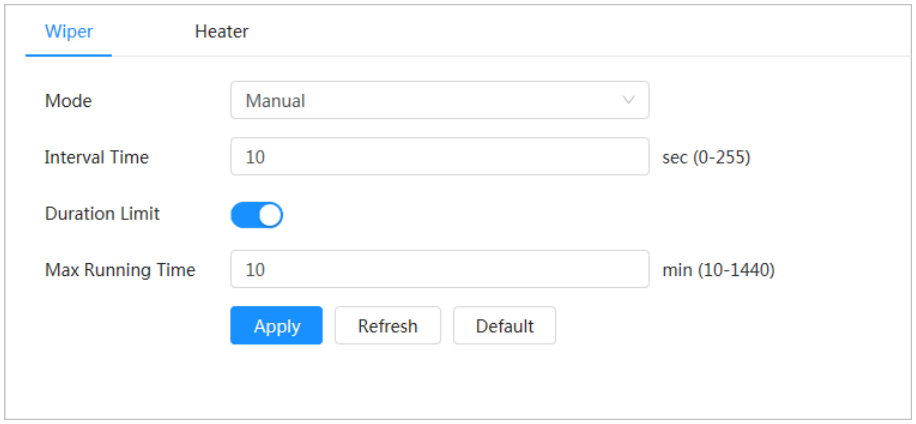


Table 4-32 Configure parameters of wiper

Parameter	Description
Mode	Select the start mode of wiper. Only manual mode is supported at present.
Interval Time	The interval time between stop mode and start mode. For example, set the time to10 seconds, and the wiper will work every 10 seconds.
Duration Limit	Enable **Duration Limit** and configure **Max Running Time**, the wiper will automatically turn off when it runs up to this time.
Max Running Time	

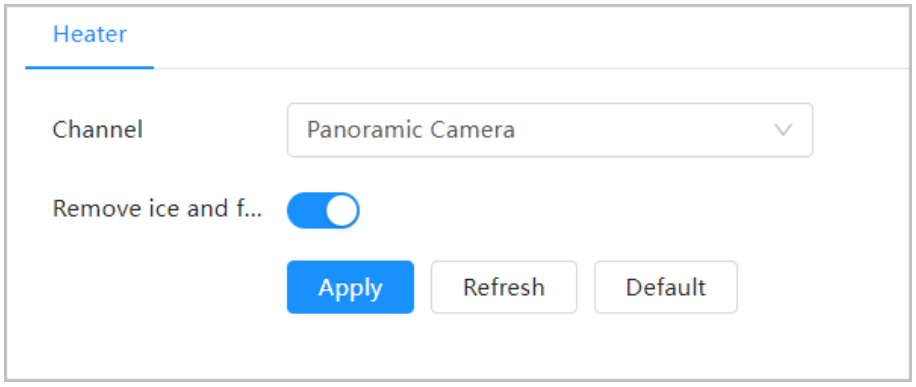
Step 3 Click **Apply**.

4.8.3.2 Configuring Heater

Procedure

Step 1 Select > **System** > **Peripheral** > **Heater**.

Figure 4-94 Heater



Step 2 Select the channel, click to enable **Remove ice and fog** , and then click **Apply**.

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 double-channel devices.

Click **Live** on the main webpage to enter **Live** page.

Pages might vary with different models.

Figure 5-1 Live page

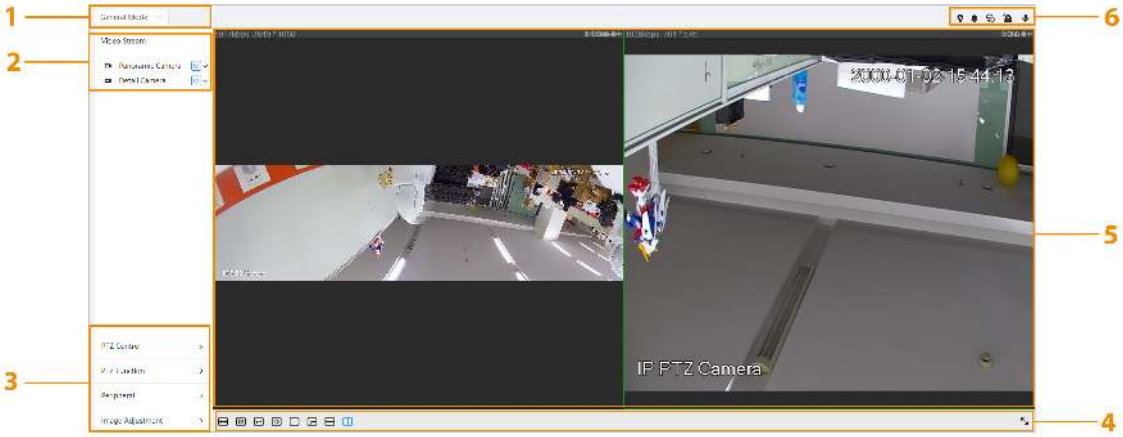


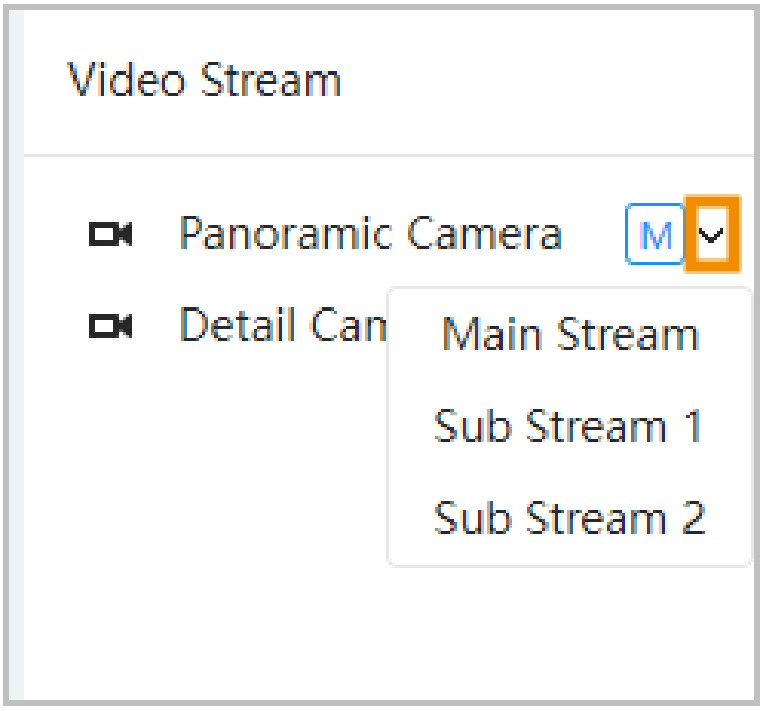
Table 5-1 The description of live page

Number	Function	Description
1	Display mode	Switch the video display mode. It includes general mode, face mode and metadata mode. For details, see "5.5 Display Mode".
2	Channel list	Displays all channels. You can select the channel as needed and set the stream type.
3	Image adjustment	Adjusts the images in the live viewing. For details, see "5.4 Window Adjustment Bar".
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. For details, see "5.3 Live View Function Bar".

5.2 Configuring Encoding

On the left side of the live page, click ⌄ on the right side of the video channel to select the video stream.

Figure 5-2 Configure video stream



- **Main Stream**: It has large bit stream value and image with high resolution, but also requires large bandwidth. This option can be used for storage and monitoring. For details, see "4.3.3.1 Encode".
- **Sub Stream**: It has small bit stream value and smooth image, and requires less bandwidth. This option is normally used to replace main stream when bandwidth is not enough. For details, see "4.3.3.1 Encode".
- M means the current stream is main stream; S1 means the current stream is sub stream 1; S2 means the current stream is sub stream 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 the live video.

The live view function bar might vary depending on the different models.

Table 5-2 Description of live view function bar

Icon	Function	Description
	Warning Light	Display the status of alarm sound. Click this icon to forcibly turn on or off the alarm sound.

Icon	Function	Description
	Alarm	Display the status of warning light. Click this icon to forcibly turn on or off the warning light.
	Force Alarm	Displays alarm output state of the corresponding channel. When the 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-in status to view other areas. You can zoom video image through two operations. ● Click the icon, and then select an area in the video image to zoom in; right-click on the image to resume the original size. ● Click the icon, and then scroll the mouse wheel in the video image to zoom in or out.
,	Snapshot	Capture one picture of the current image, and it will be saved to the configured storage path. About viewing or configuring storage path, see"4.2 Local".
,	Triple Snapshot	Capture three pictures of the current image, and they will be saved to the configured storage path. About viewing or configuring storage path, see"4.2 Local".
,	Record	Record video, and it will be saved to the configured storage path. About viewing or configuring storage path, see"4.2 Local".
	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 5-3 Description of adjustment bar

Icon	Function	Description
	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. It supports **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 image and real-time image. ● General: It is between **Realtime** and **Fluent**.
	AI Rule	Click the icon, and then select **Enable** to display AI rules and detection box; select Disable to stop the display. It is enabled by default.
	Anti-aliasing	Click this icon to enable or disable anti-aliasing function.
	Multi-channel screen display	This icon is displayed only on multi-channel devices. Click the icon to select the channel screen display mode.

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 of the page to adjust the current video screen.

Figure 5-3 PTZ Control

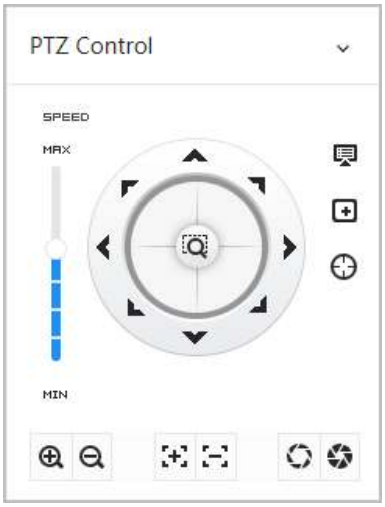


Table 5-4 Description of PTZ control functions

Function	Description
	This function supports control device toward eight directions, including up, down, left, right, left up, right up, left down and right down. Click , in the selected area of 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 the rotation with a speed of 1.
	Zoom : Adjust the zooming of images.
	Focus : Adjust the degree of camera focus.
	Iris : Adjust the iris of images.
	PTZ Menu : Click to enter PTZ menu, and then configure the camera setting, PTZ setting, system management and other functions according to the actual page.
	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.
	Manual Track : Click the icon, select the tracking target in the **Live** page, and then the Camera tracks the selected target.

5.4.3 PTZ Function

On the **Live** page, click the **PTZ Function** on the lower left corner of the page. Before calling PTZ function, please see "4.5 PTZ" to configure PTZ function.

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

Figure 5-4 PTZ function

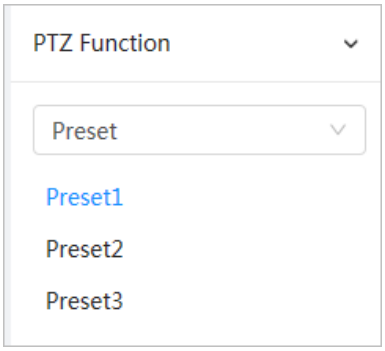


Table 5-5 Description of PTZ function

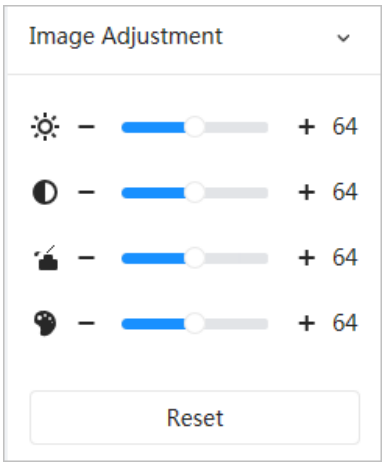
Parameter	Description
Scan	Configure the scan number. Click **Start** , and the Camera will scan back and forth at a certain speed according to the set boundary. Click **Stop** to finish scan.
Preset	Configure preset number, and then click **View** to position the Camera to the corresponding point. The preset contains PTZ's horizontal angle, tilt angle, lens focal length and other parameters.
Tour	Configure tour number. Click **Start** and the Camera 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 Camera 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** to pinpoint to a point.

5.4.4 Image Adjustment

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

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

Figure 5-5 Image adjustment



- (Brightness adjustment): Adjusts the overall image brightness, and changes the value when the image is too bright or too dark. The bright and dark areas will have equal changes.
- (Contrast adjustment): Changes the value when the image brightness is proper but contrast is not enough.

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

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

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

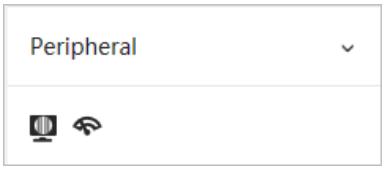
5.4.5 Peripheral Management

Configure the peripheral devices of PTZ Camera.

Background Information

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

Figure 5-6 Peripheral management



- : Water removal. Click the icon, enter the max running time, and then click **Apply**.
- : Click the icon to enable or disable wiper function.

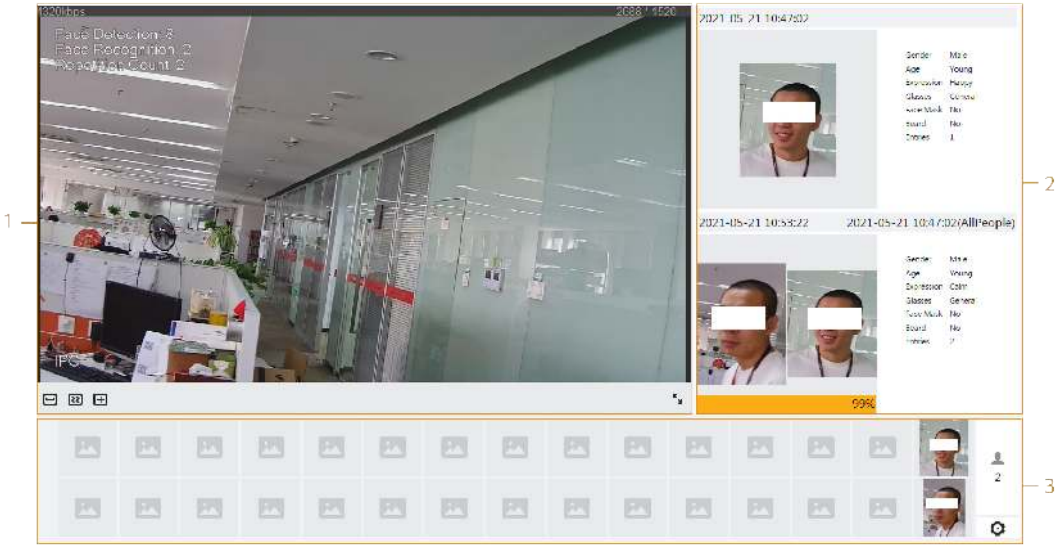
5.5 Display Mode

It includes general mode, face mode and metadata mode. For general mode, see "5.1 Live Page". Before previewing with face mode and metadata mode, configure corresponding AI function in advance.

Preview Mode

- Select **Face Mode** on the upper left corner of the **Live** page, and then the **Live** page turns into **Face Mode**.

Figure 5-7 Face mode page



- Select **Metadata Mode** on the upper left corner of the **Live** page, and then the **Live** page turns into **Metadata Mode**.

Figure 5-8 Metadata mode page

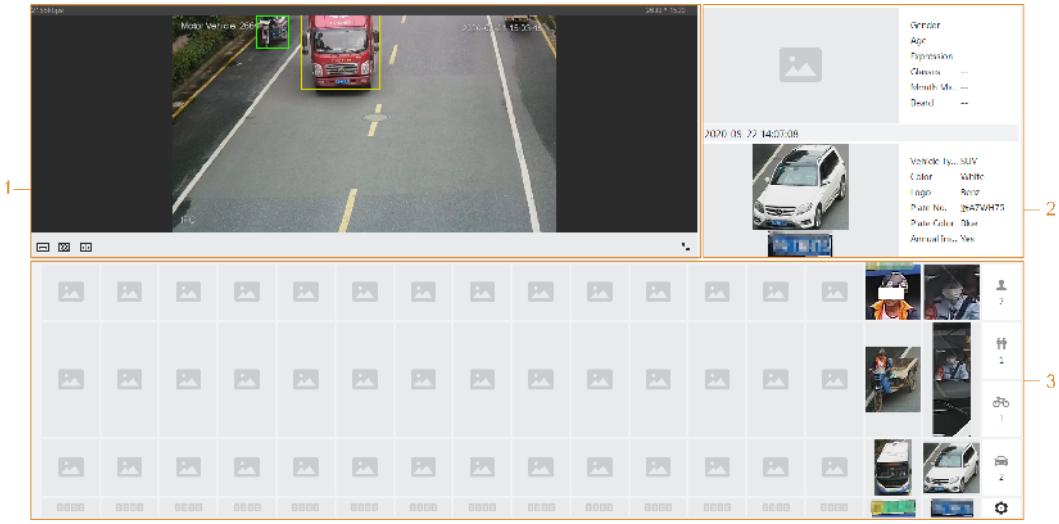


Table 5-6 Description of display mode

Number	Function	Description
1	Live view	Displays the real-time monitoring image. For details, see "5.4.1 Adjustment".
2	Details	Displays the captured image and details.
3	Captured image	Enable statistics of people faces, human bodies, motor vehicles and non-motor vehicles. ● Click the image to view its detailed information in the "Captured image". ● Click ⚙ to change the properties shown in the "Captured image". For details, see "Configuring Display Properties".

Configuring Display Properties

Under face mode or metadata mode, click ⚙ on the right lower corner of the page. Select the properties to be displayed on the **Live** page, and then click **Apply**. Properties shown in blue boxes indicate that they are selected, and properties shown in gray boxes indicate that they are not selected. Properties might vary depending on different modes.

Figure 5-9 Configuring detection properties (face mode)

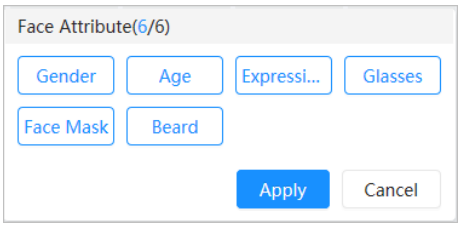
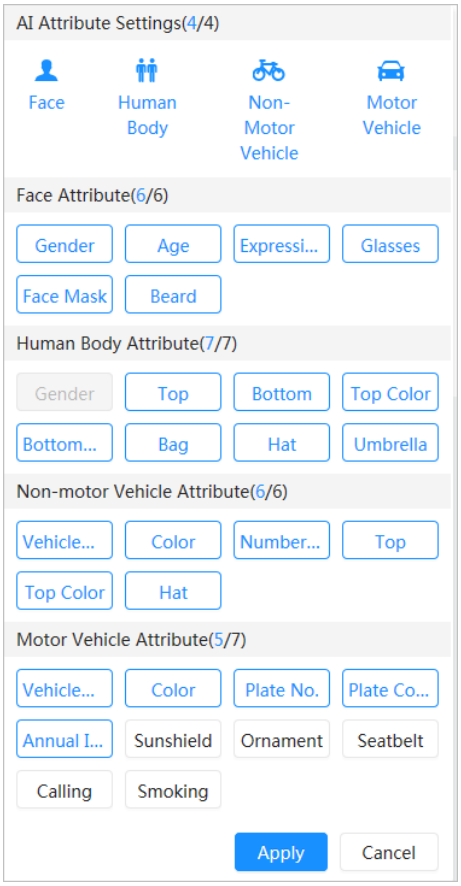


Figure 5-10 Configuring detection properties (metadata mode)



6 Record

This chapter introduces the functions and operations of video playback.

6.1 Playback

6.1.1 Playing Back Video

This section introduces the operation of video playback.

Prerequisites

- This function is available on the Camera with SD card.
- Before playing back video, configure record time range, record storage method, record schedule and record control. For details, see "6.2 Setting Record Control", "6.3 Setting Record Plan", and "6.4 Storage".

Procedure

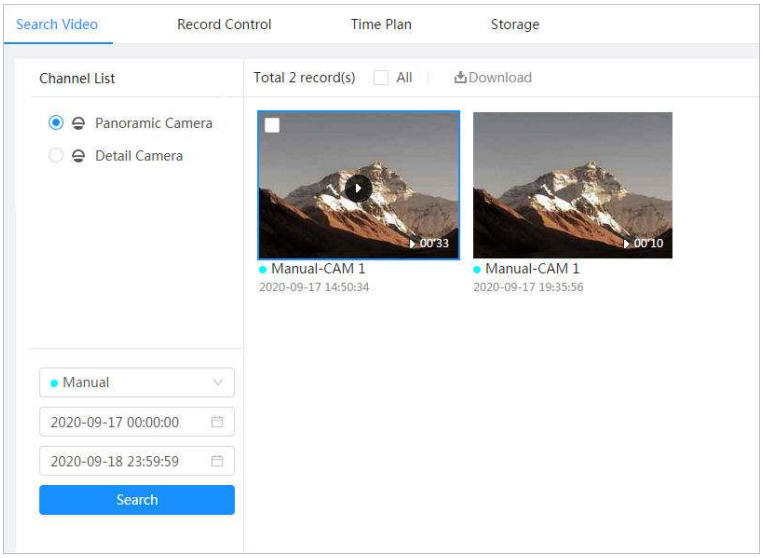
Step 1 Select **Record** > **Search Video**.

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

- Click **All** , and 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, such as **Motion Detection**, **Video Tamper** and **Scene Changing**.
- The dates with blue dots indicate there are videos recorded on those days.

Figure 6-1 Search video



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

Figure 6-2 Video playback

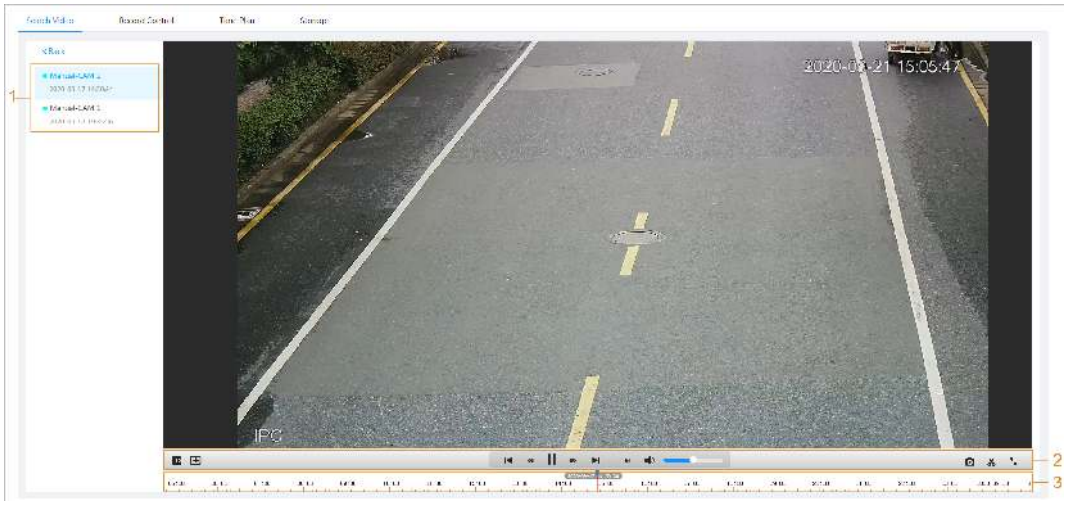


Table 6-1 Description of video playback page

No	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 to the **Search Video** page.
2	Digital Zoom	You can zoom in or out video image of the selected area through two operations. ● Click the icon, and then select an area in the video image to zoom in; right-click on the image to resume the original size. In zoom in state, drag the image to check other area. ● Click the icon, and then scroll the mouse wheel in the video image to zoom in or out.
	AI Rule	Click, and then select **Enable** to display AI rules and detection box; select **Disable** to stop displaying AI rules. It is disabled by default. AI rules are valid only when you enabled the rule during recording.

No	Function	Description
	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 the playback. ● : Click the icon to stop playing recorded videos. The icon changes to , click the icon to play recorded videos. ● : Click the icon to speed up the playback. ● : 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 picture of the current image, and it will be saved to the configured storage path. About viewing or configuring storage path, see "6.4.1 Local Storage".
	Video clip	Click , and clip a certain recorded video and save it. For details, see "6.1.2 Clipping Video".
	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.

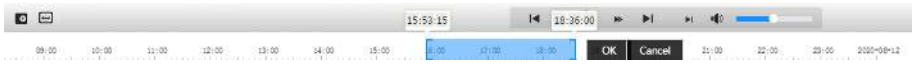
6.1.2 Clipping Video

Procedure

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 the target video.

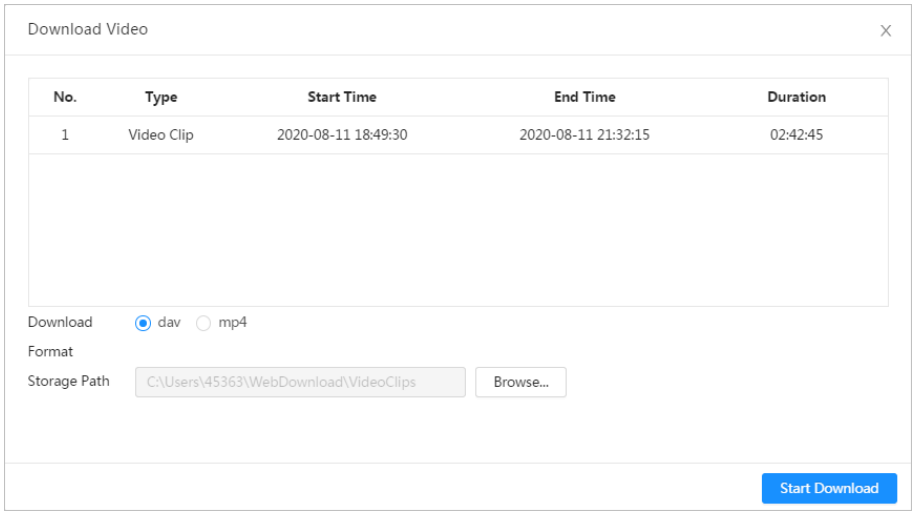
Figure 6-3 Clipping video



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

Step 4 Select the download format and storage path.

Figure 6-4 Clipping video



Step 5 Click **Start Download**.

The playback stops and the clipped file is saved in the configured storage path. For details of storage path, see "4.2 Local".

6.1.3 Downloading Video

Background Information

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

- Playback and downloading at the same time is not supported.
- Operations might vary with different browsers.
- For details of viewing or setting storage path, see "4.2 Local".

Procedure

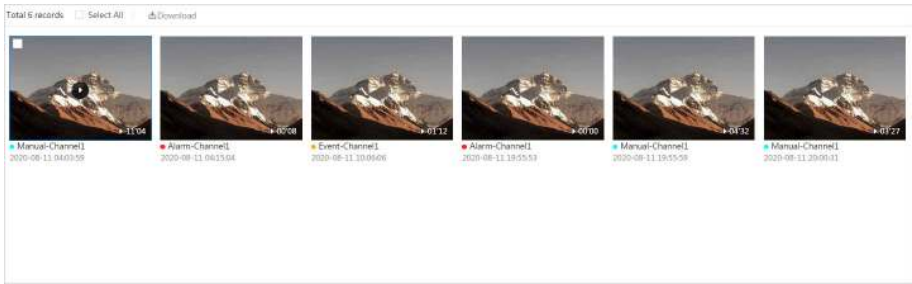
Step 1 Select **Record** > **Search Video**.

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. The icon at the upper left corner of the selected file changes to ☑.
- Select ☐ next to **Select All** to select all searched videos.

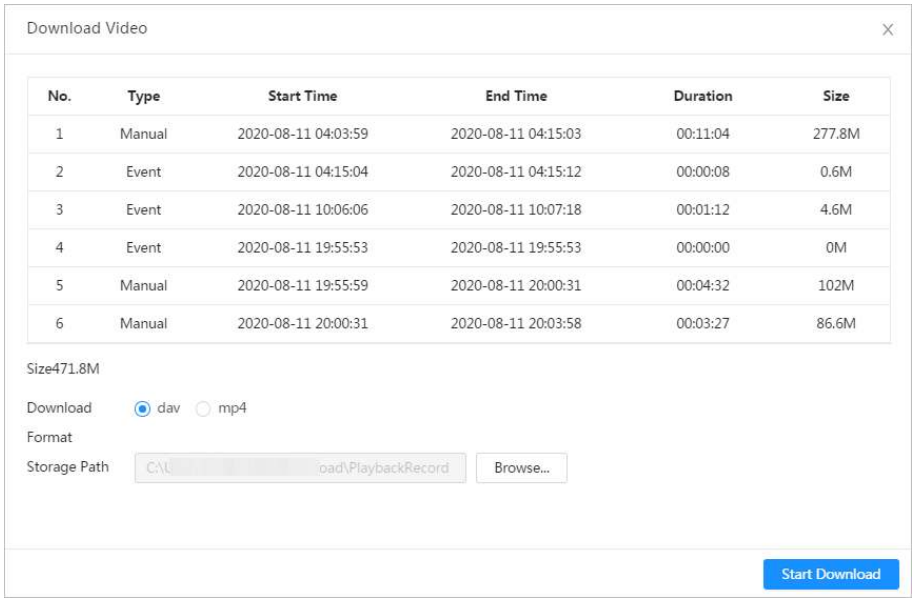
Figure 6-5 Select video file



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	Manual	2020-08-11 04:03:59	2020-08-11 04:15:03	00:11:04	277.8M
2	Event	2020-08-11 04:15:04	2020-08-11 04:15:12	00:00:08	0.6M
3	Event	2020-08-11 10:06:06	2020-08-11 10:07:18	00:01:12	4.6M
4	Event	2020-08-11 19:55:53	2020-08-11 19:55:53	00:00:00	0M
5	Manual	2020-08-11 19:55:59	2020-08-11 20:00:31	00:04:32	102M
6	Manual	2020-08-11 20:00:31	2020-08-11 20:03:58	00:03:27	86.6M

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 Setting Record Control

Background Information

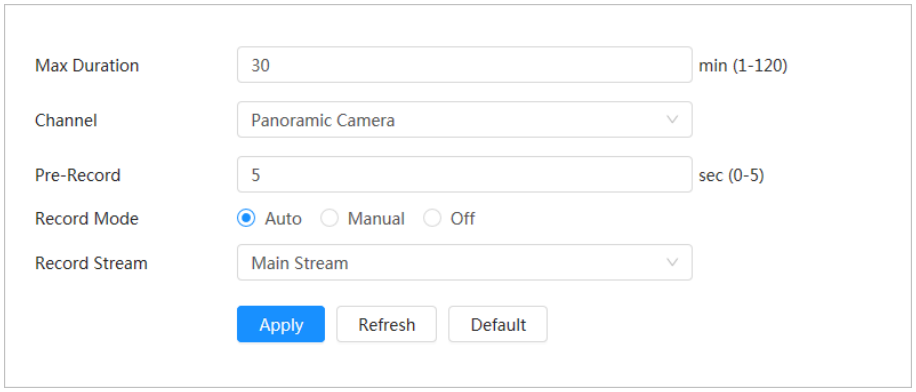
Set parameters such as pack duration, pre-event record, disk full, record mode, and record stream.

When a smart SD card is inserted into a device that supports smart SD card, make sure that the SD card has been authenticated before using the video recording function. For details, see "4.2 Local".

Procedure

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

Figure 6-7 Record control



Step 2 Set parameters.

Table 6-2 Description of record control parameters

Parameter	Description
Max Duration	The time for packing each video file.
Channel	Select the camera that needs to configure record control parameters.
Pre-Record	The time to record the video in advance of a triggered alarm. For example, if the pre-event record is set to be 5 seconds, the system saves the recorded video 5 seconds before the alarm. When an alarm or motion detection links recording, and the recording is not enabled, the system saves the recording within the pre-event record time to the video file.
Record Mode	• **Manual** : the system starts recording. • **Auto** : the system starts recording in the configured time period of record plan. • **Off** : the system does not record.
Record Stream	Select record stream, including **Main Stream** and **Sub Stream**.

Step 3 Click **Apply**.

6.3 Setting Record Plan

Background Information

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

Set certain days as holiday, and when the **Record** is selected in the holiday schedule, the system records video as 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 intelligent events)
- Red represents alarm record plan (such as recording triggered by alarm-in).

1. Select a record type, and left-click and drag on the timeline to set the recording period of each event.

Figure 6-8 Configure through timeline

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

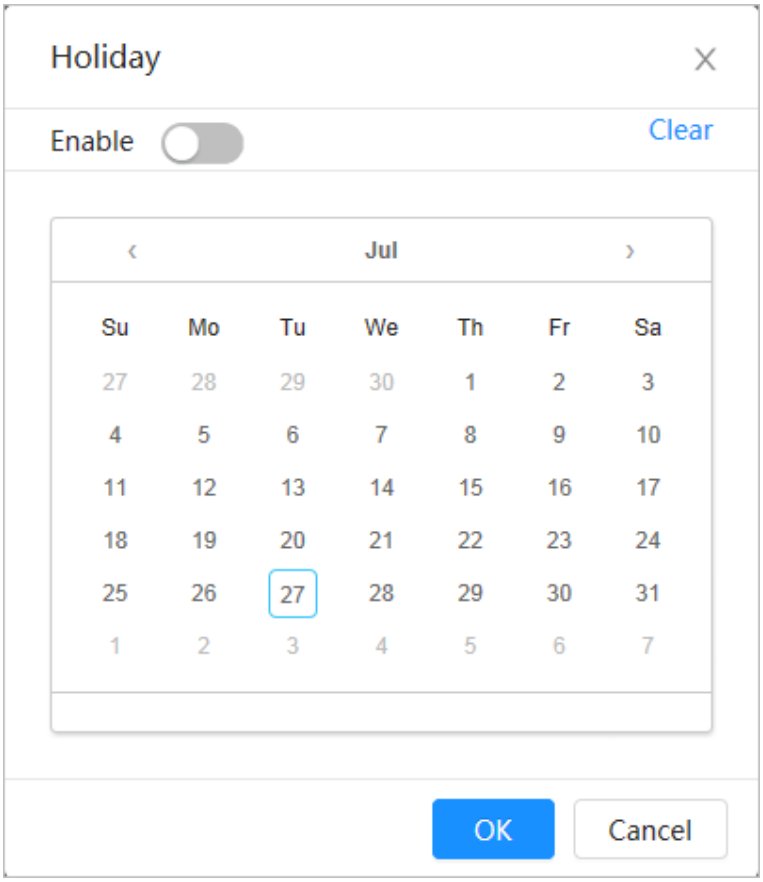
Figure 6-9 Configure accurate time period

- Click **Copy**, and select the days that you want to copy to in the prompt page.
- Select the **Select All** check box 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 plan



1. Click to enable the holiday plan, and select the days that you need to set as holiday.
2. 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**.

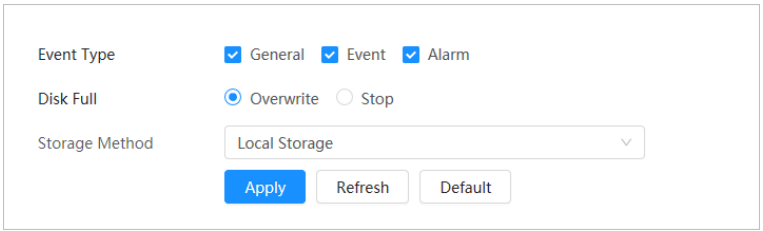
6.4 Storage

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

Procedure

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

Figure 6-11 Live



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

Table 6-3 Description of storage parameters

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 server or NAS.

Step 3 Click **Apply**.

6.4.1 Local Storage

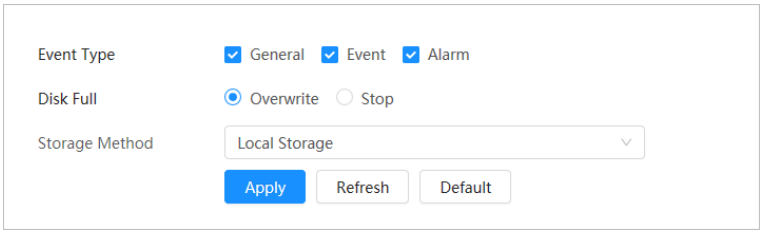
Procedure

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 SD card.

Figure 6-12 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.

Procedure

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

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

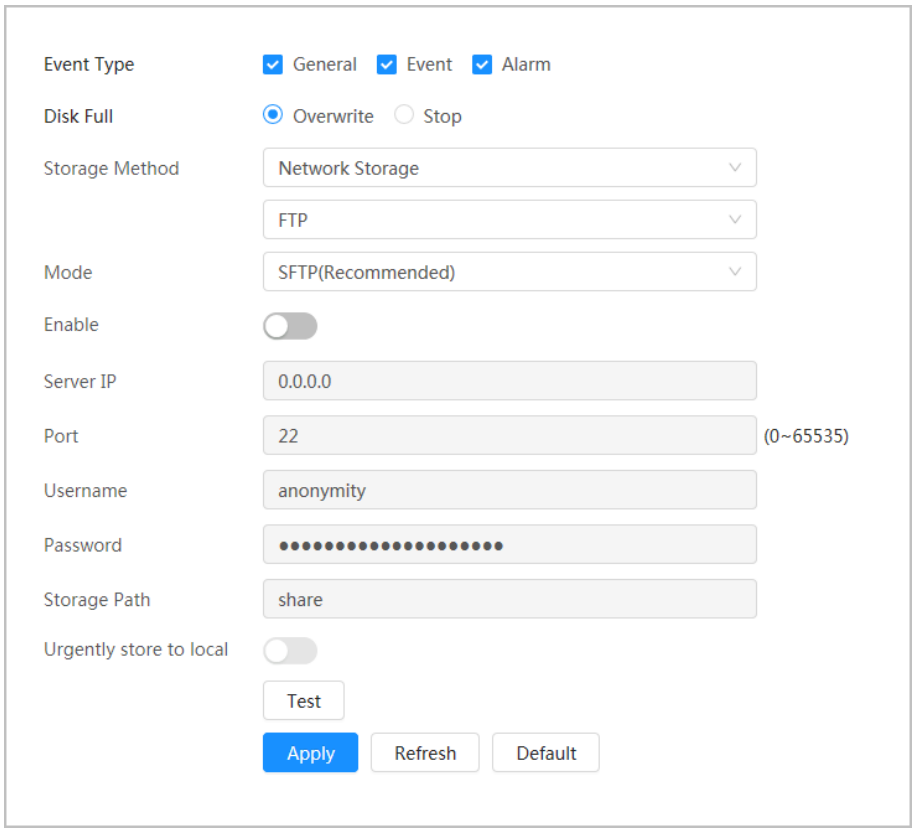
- **Overwrite** : Cyclically overwrite the earliest video when the disk is full.
- **Stop** : Stop recording when the disk is full.

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

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

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

Figure 6-13 FTP



Step 5 Configure FTP parameters.

Table 6-4 Description of FTP parameters

Parameter	Description
Server IP	The IP address of the FTP server.
Port	The port number of the FTP server.
Username	The username to log in to the FTP server.
Password	The password to log in to the FTP server.
Storage Path	The destination path in the FTP server.
Urgently store to local	Click , and when the FTP server does not work, all the files are saved to the internal SD card.

Step 6 Click **Save**.

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

6.4.2.2 NAS

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

Procedure

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

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

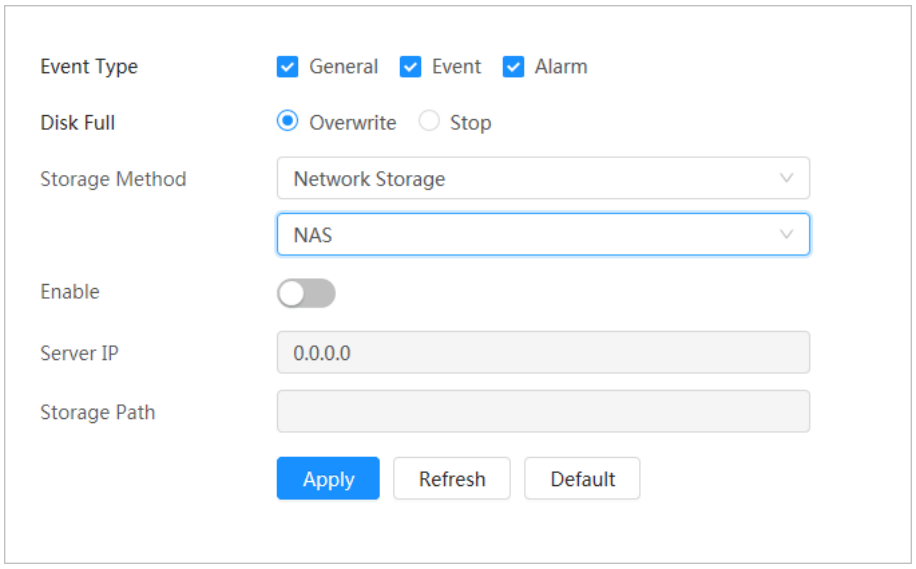
- **Overwrite** : Cyclically overwrite the earliest video when the disk is full.
- **Stop** : Stop recording when the disk is full.

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

Step 4 Select NAS protocol type.

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

Figure 6-14 NAS



Step 5 Select **Enable**, and then configure NAS parameters.

Table 6-5 Description of NAS parameters

Parameter	Description
Server IP	The IP address of the NAS server.
Storage Path	The destination path in the NAS server.
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 picture playback, including setting snapshot parameters, setting snapshot plan and snapshot storage.

7.1 Playback

This section describes playing back pictures and downloading pictures.

7.1.1 Playing Back Picture

This section introduces the operation of picture playback.

Prerequisites

- This function is available on the camera with SD card.
- Before playing back picture, configure snapshot time range, snapshot storage method, snapshot plan. For details, see"7.2 Setting Snapshot Parameters", "7.3 Setting Snapshot Plan" and "7.5 Storage".

Procedure

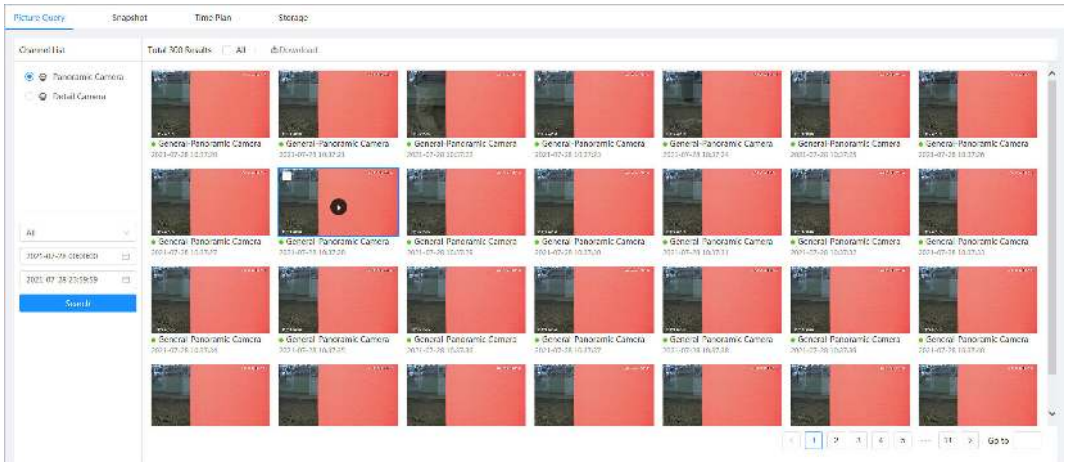
Step 1 Select **Record** > **Picture Query**.

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

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

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

Figure 7-1 Picture query



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

Figure 7-2 Picture playback

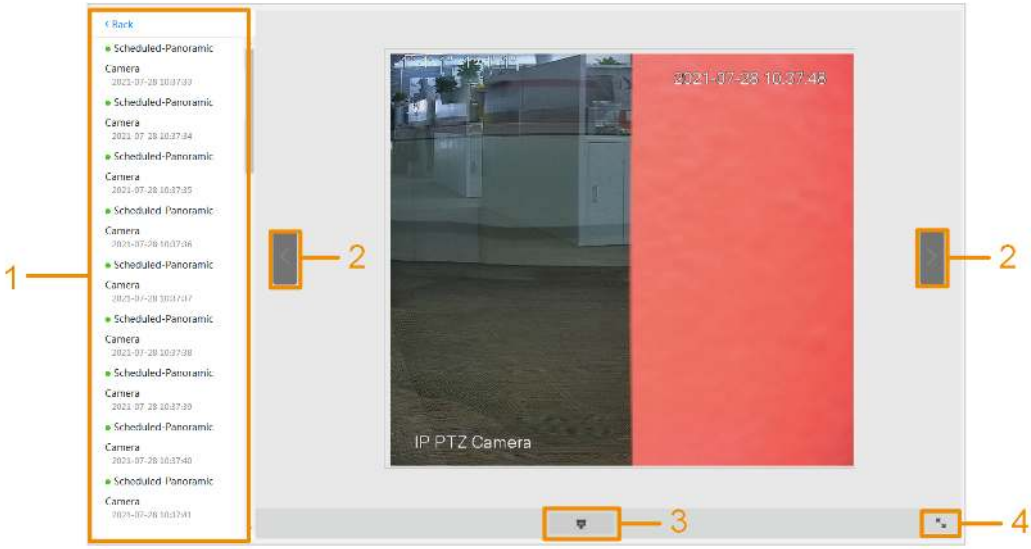


Table 7-1 Description of playback page

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

7.1.2 Downloading Picture

Background Information

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

- Operations might vary with different browsers.
- For details of viewing or setting storage path, see "4.2 Local".

Procedure

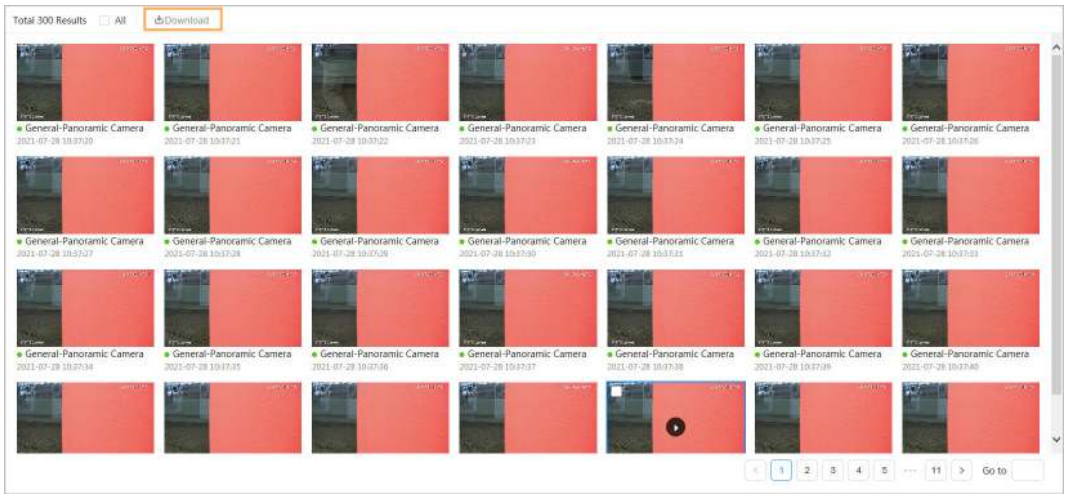
Step 1 Select **Picture** > **Picture Query**.

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

Step 3 Select the pictures to be downloaded.

- Select ☐ at the upper-right corner of each picture file to select one or multiple pictures. The icon in the upper left corner of the selected file changes to ☑.
- Select ☐ next to **Select All** to select all searched pictures.

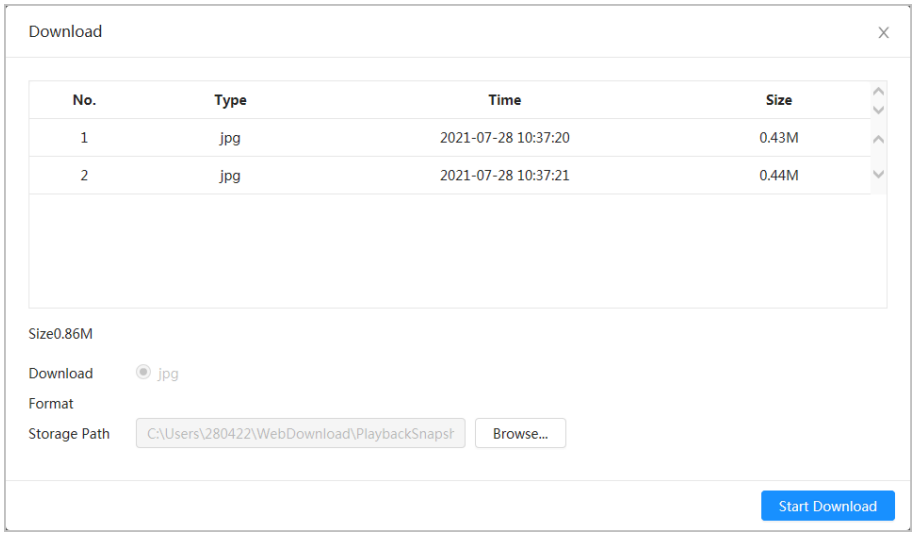
Figure 7-3 Select picture file



Step 4 Click **Download**.

Step 5 Select the download format and storage path.

Figure 7-4 Download picture



Step 6 Click **Start Download**.

The downloaded pictures are saved in the configured storage path. For details of storage path, see "4.2 Local".

7.2 Setting Snapshot Parameters

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

Procedure

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

Step 2 Select the channel and set the parameters.

Figure 7-5 Snapshot

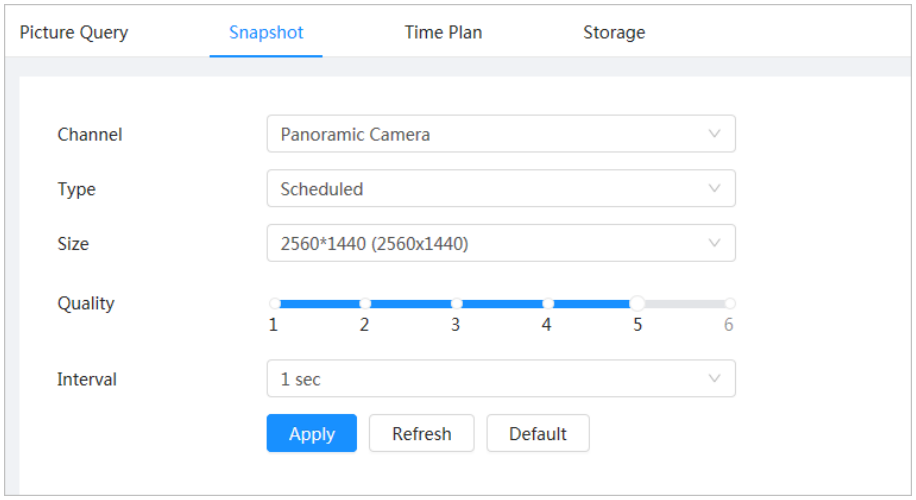


Table 7-2 Description of snapshot parameters

Parameter	Description
Type	You can select from **General** and **Event**. ● **General** : Capture images in the defined period. For details, see "7.3 Setting Snapshot Plan". ● **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	It is the same with the resolution of the main stream.
Quality	Set the quality of the snapshot. The higher the value, the better the quality.
Interval	Set the frequency of snapshot. You can select **Custom** to set the frequency as needed.

Step 3 Click **Apply**.

7.3 Setting Snapshot Plan

According to the configured snapshot plan, the system enables or disables snapshot at corresponding time.

Background Information

After the corresponding alarm type (**General** , **Event**, and **Alarm**) is enabled, the camera channel links snapshot.

Procedure

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

Step 2 Select camera 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 intelligent events); red represents alarm snapshot plan (such as snapshot triggered by alarm-in).

1. Select a snapshot type, and directly press and drag the left mouse button to set the time period for normal snapshot on the timeline.

Figure 7-6 Configure through timeline

2. Click the selected time range and then enter a specific time in the time text box to configure an accurate start and end time.

Figure 7-7 Configure accurate time period

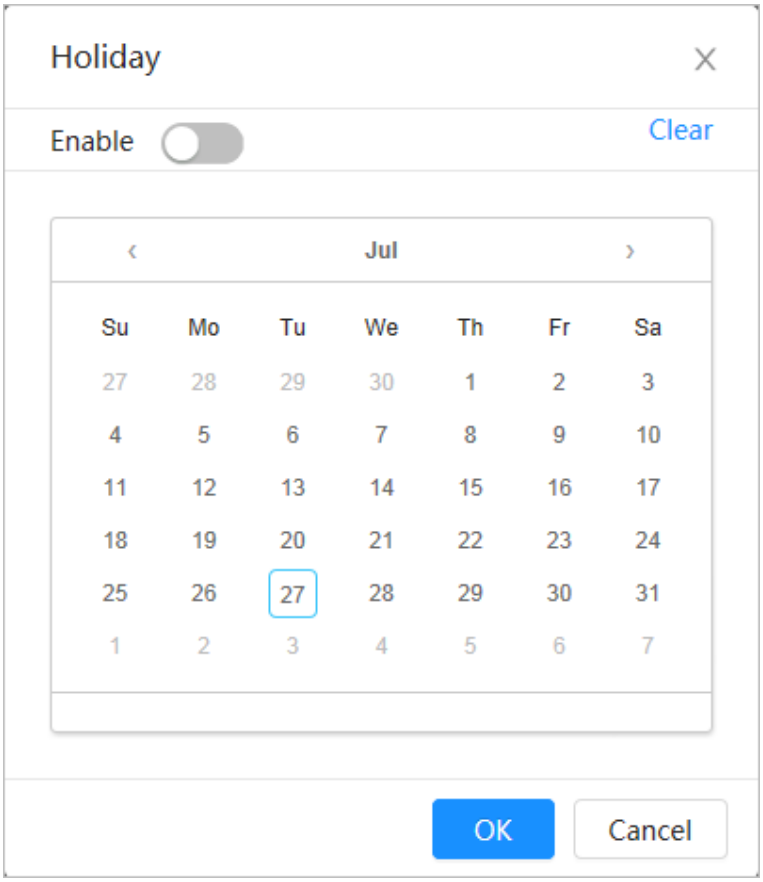
- Click **Copy** next to a day, and select the days that you want to copy to on the prompt page, you can copy the configuration to the selected days. Select the **Select All** check box to select all day to copy the configuration.

- You can set 6 time periods per day.

Step 3 Click **Apply**.

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

Figure 7-8 Holiday plan



1. Click to enable the holiday configuration, and select the days that you need to set as holiday.
2. Click **Clear** to cancel the selection.

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

Step 5 Click **OK**.

7.4 Snapshot by Location

When the Camera goes to a certain preset point, the current screen image is captured.

Prerequisites

Add the presets in advance. For details of adding presets, see "4.5.1 Configuring Presets".

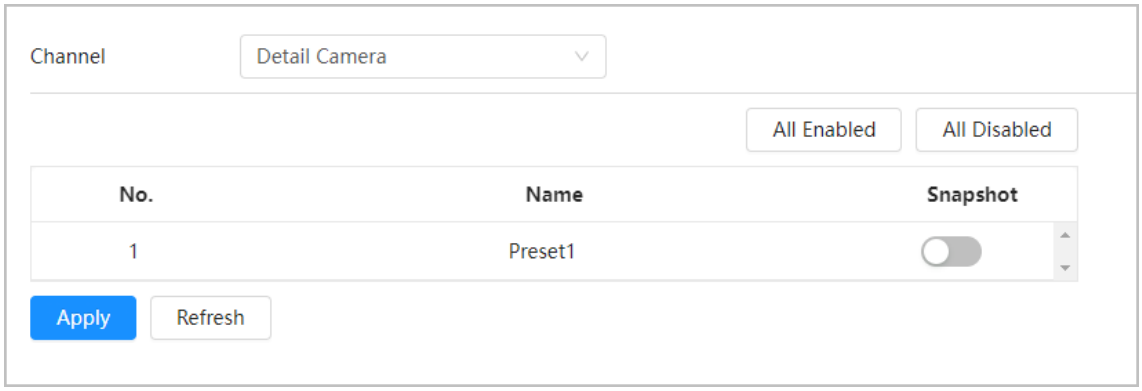
Procedure

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

Step 2 Click corresponding to the preset point to enable its capture function, or click **All Enabled** to enable the capture function of all preset points.

Click **All Disabled** to disable the capture function of all preset points.

Figure 7-9 Snapshot by location



Step 3 Click **Apply**.

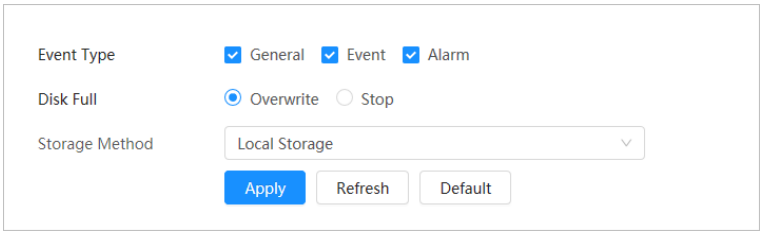
7.5 Storage

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

Procedure

Step 1 Select **Picture** > **Storage**.

Figure 7-10 Live



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

Table 7-3 Description of storage parameters

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 is full. ● **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**.

7.5.1 Local Storage

Procedure

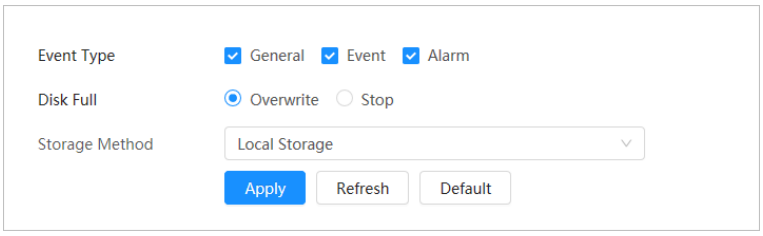
Step 1 Select **Picture** > **Storage**.

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 7-11 Local storage



Step 4 Click **Apply**.

7.5.2 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.

7.5.2.1 FTP

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

Procedure

Step 1 Select **Picture** > **Storage**.

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

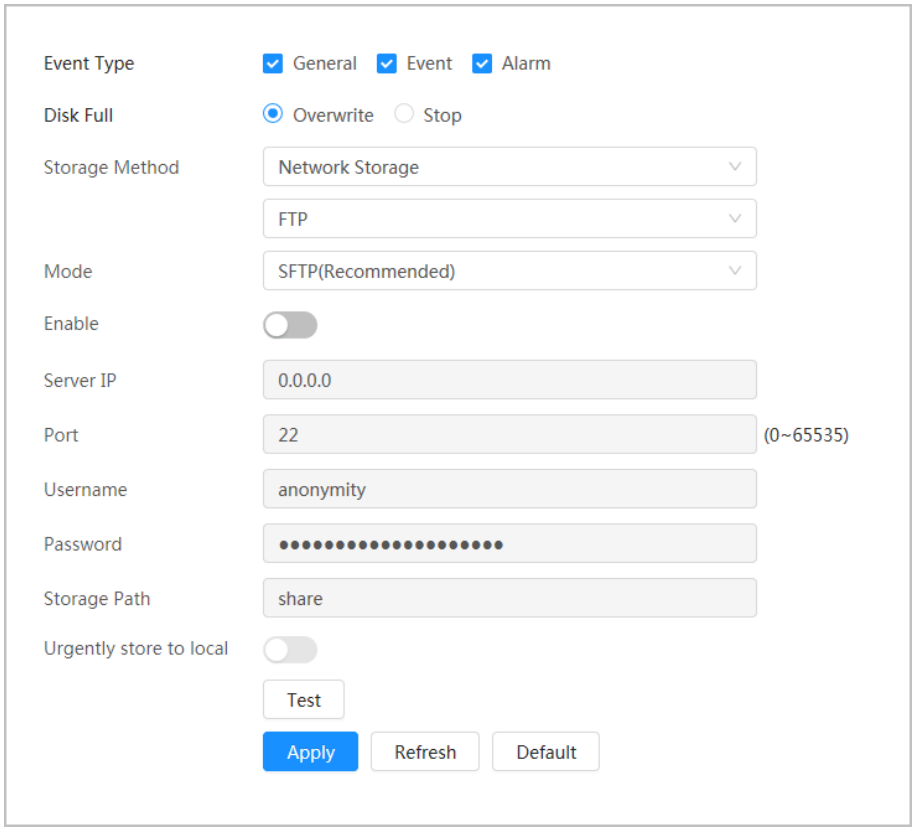
- **Overwrite** : Cyclically overwrite the earliest snapshot when the disk is full.
- **Stop** : Stop snapshot when the disk is full.

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

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 7-12 FTP



Step 5 Configure FTP parameters.

Table 7-4 Description of FTP parameters

Parameter	Description
Server IP	The IP address of the FTP server.
Port	The port number of the FTP server.
Username	The username to log in to the FTP server.
Password	The password to log in to the FTP server.
Storage Path	The destination path in the FTP server.
Urgently store to local	Click , and when the FTP server does not work, all the files are saved to the internal SD card.

Step 6 Click **Save**.

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

7.5.2.2 NAS

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

Procedure

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.

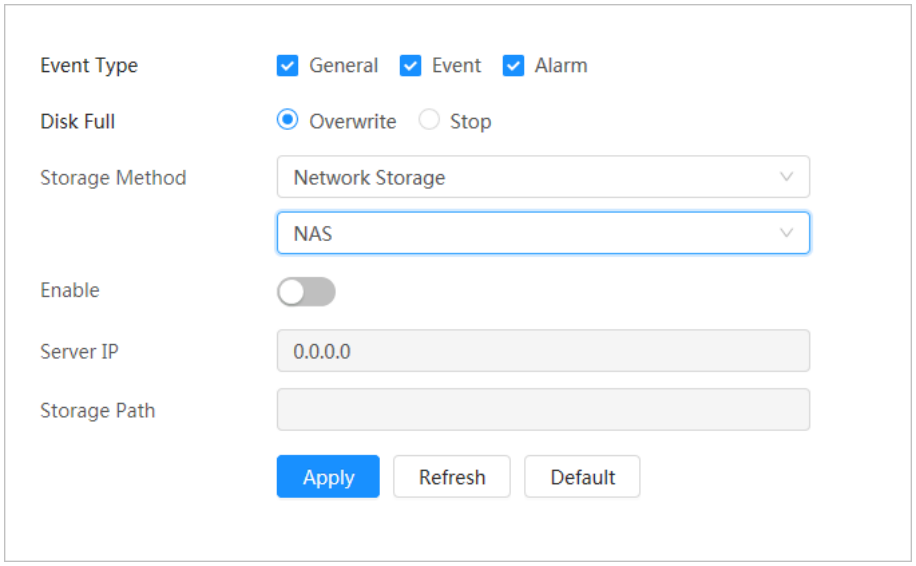
- **Stop** : Stop snapshot when the disk is full.

Step 3 Select **Network storage** in **Storage Method**, and select **NAS** to save the snapshots in 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 7-13 NAS



Step 5 Select **Enable**, 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 smart plan, panoramic linkage and tour plan.

The device supports panoramic camera channel and detail camera channel. Snapshots and functions in this section are for reference only, and might differ from the actual models.

8.1 Configuring Smart Plan

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

Background Information

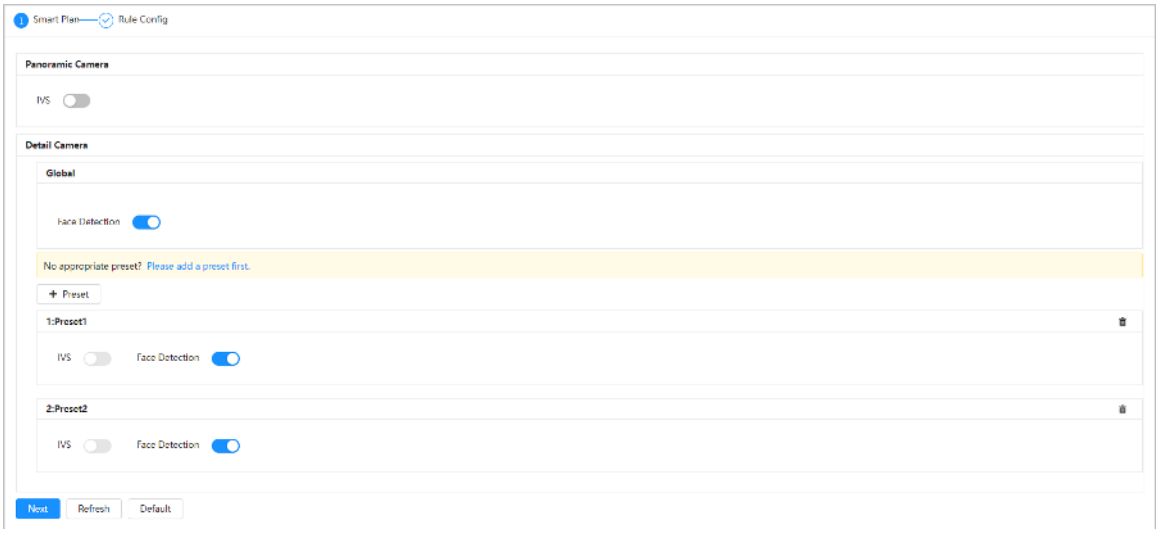
- Smart plans of different devices might vary in actual page.
- Calibrate the Camera before configuring the smart plans. For details, see "8.4 Panoramic Linkage".

Procedure

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

Step 2 Enable the intelligent functions of the **Global** and **Preset** as required, and then click **Next**.

Figure 8-1 Enable AI function

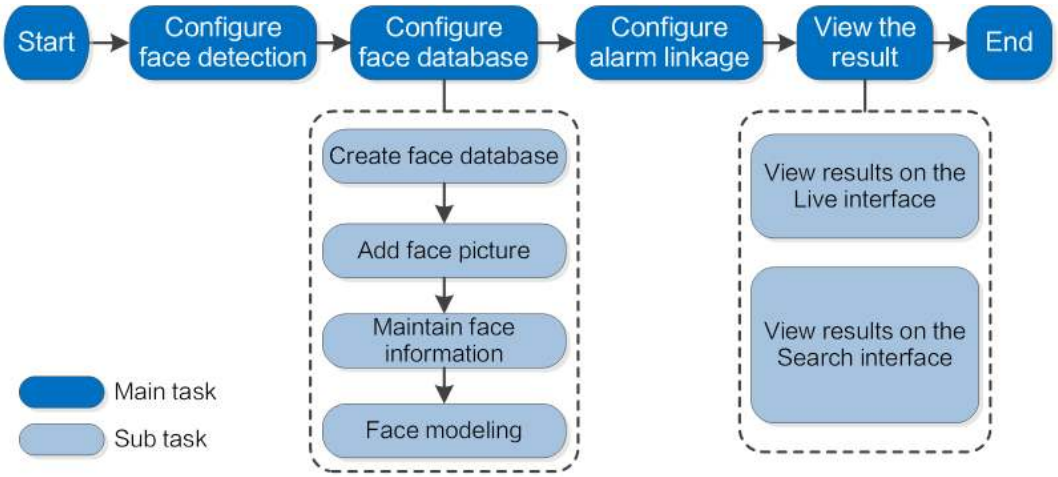


Step 3 Configure smart function rule as required.

8.2 Configuring Face Detection

When a face is detected in the detection area, the system performs alarm linkage, such as recording and sending emails.

Figure 8-2 Face detection flowchart



8.2.1 Configuring Face Detection Rules

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

Procedure

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

Step 2 Select **Face Detection** for the detail camera and click **Next**.

Step 3 Click **Face Detection** to enter the configuration page.

Step 4 (Optional) Click the icon on the right of the screen to draw detection area, exclusion area and filtering target model on the monitoring screen.

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

Step 5 Configure relevant parameter of face detection.

Figure 8-3 Configure face detection rules

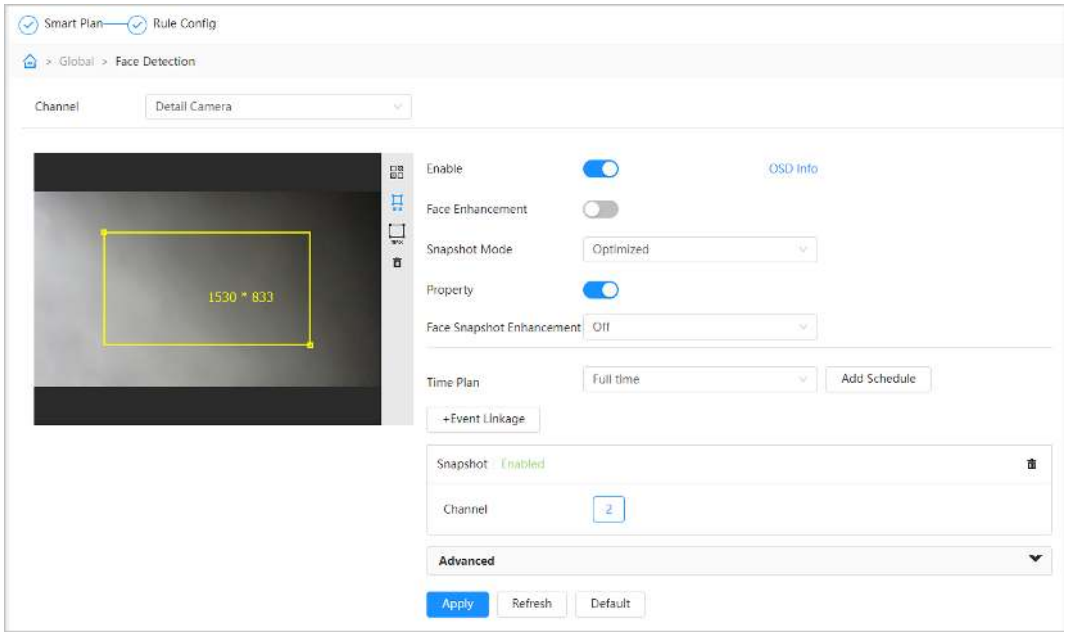


Table 8-1 Description of face detection parameters

Parameter	Description
OSD Info	Click it to configure the on-screen display on the **Overlay** page.
Face Enhancement	Select **Face Enhancement** to preferably guarantee clear faces with low stream.
Snapshot Mode	• Real-time: The device takes snapshot immediately when it detects faces. • Optimized: The device captures the clearest images within the optimized duration after it detects faces. You can configure the **Optimized Duration** in the **Advanced** area. • Quality Priority: Only when the quality of the captured face image is higher than the set quality threshold will the device capture the image. You can configure the **Quality Threshold** in the **Advanced** area.
Property	Click **Property** to enable the properties display during face detection.

Parameter	Description
Face Snapshot Enhancement	• Off: Faces in the snapshots are not enhanced. • Manual: You can configure the degree of face snapshot enhancement by yourself. ◇ **NR Level** : Noise reduction level. The value ranges from 0 to 100. The larger the value is, the less the noise will be. ◇ **Sharpening Level** : Changes the sharpness of picture edges. The higher the value is, the clearer the picture edges will be. If the value is too big, image noise is more likely to appear. ◇ **Edge Brightening Level** : The higher the value is, the edges of the face appear clearer and more outstanding. ◇ **Edge Darkening Level** : The higher the value is, the more pronounced and emphasized the edges in the snapshots. • Auto: Face snapshot enhancement is automatically adjusted.
Advanced	• **Quality Threshold** : Set the quality threshold of the captured image. • **Optimized Duration** : Set a time period to capture the clearest picture after the camera detects face.

Step 6 Set arming periods and alarm linkage action.

- Click **Add Schedule** to add time plan. For details, see "4.6.1.2.1 Adding Schedule".
- Click **Event Linkage** to set the linkage action and configure linkage parameters. For details, see "4.6.1.2 Alarm Linkage".

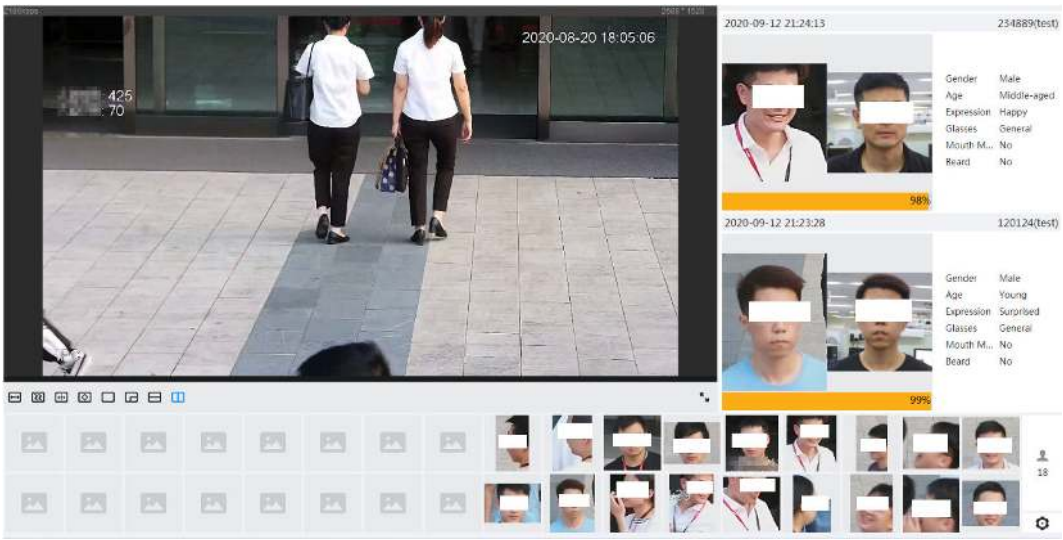
Step 7 Click **Apply**.

8.2.2 Viewing Face Detection Results

In the main page, click **Live** and then select **Face Mode** from the display mode drop-down list on the upper-left corner to view the live page of face detection.

- The live image is displayed at the left side, and the captured face pictures and attribute information are displayed at the right side. When the recognition is successful, the captured face pictures, pictures in the database and the similarity of the face pictures and pictures in the database are displayed at the right side; the snapshot counting result and thumbnails are displayed at the bottom of the live image.
- Click ⚙ to set the attributes. For details, see "Configuring Display Properties".

Figure 8-4 Face detection result



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

8.3.1 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 actual object according to one horizontal ruler and three vertical rulers calibrated by the user and the corresponding actual distance.

Applicable Scene

- Medium or distant view with installation height of more than three meters. Scenes with parallel view or ceiling-mounted are not supported.
- Calibrate horizontal plane, not vertical walls or sloping surfaces.

- This function is not applicable to scenes with distorted view, such as the distorted views captured by super wide-angle or fisheye camera.

Notes

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

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

Procedure

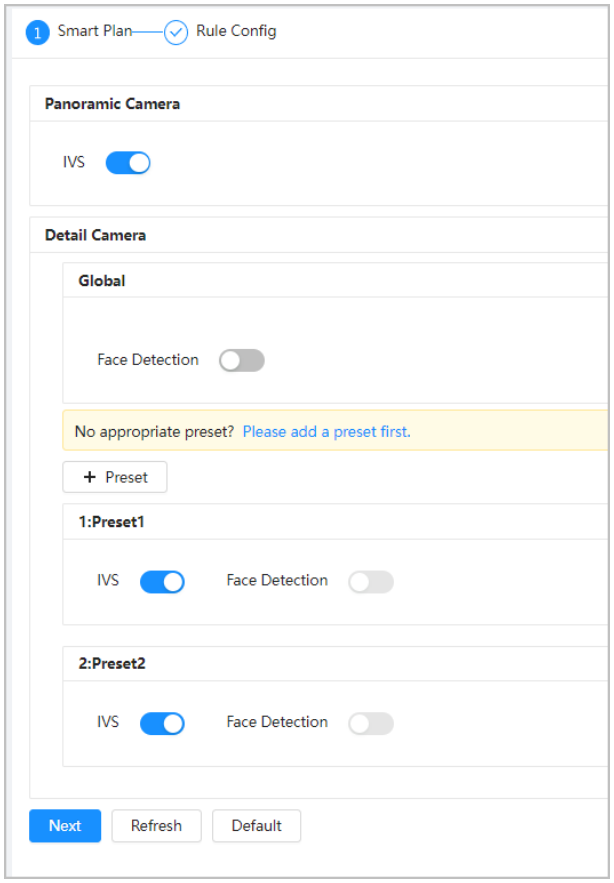
Step 1 Select **AI** > **AI Config** > **Smart Plan**.

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

For some models, select **IVS** in the **Panoramic Camera** tab and **Detail Camera** tab as needed in **AI** > **AI Config** > **Smart Plan** to enable the IVS function, and then click **Next**.

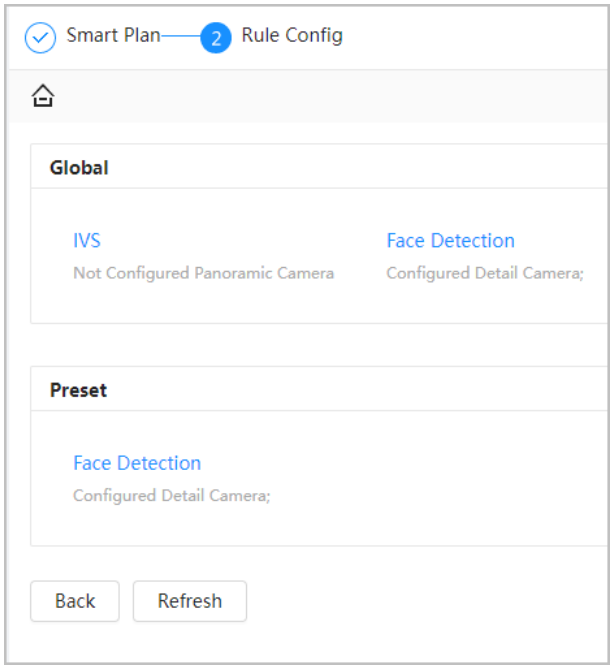
In the **Detail Camera** tab, add a preset first if there is no appropriate preset.

Figure 8-5 Configure smart plan (IVS)



Step 3 Click **IVS** in the **Global** tab or **IVS** in the **Preset** tab.

Figure 8-6 Rule configuration



The former is for the panoramic camera and the latter for the detail camera.

Figure 8-7 Global configuration for IVS (1)

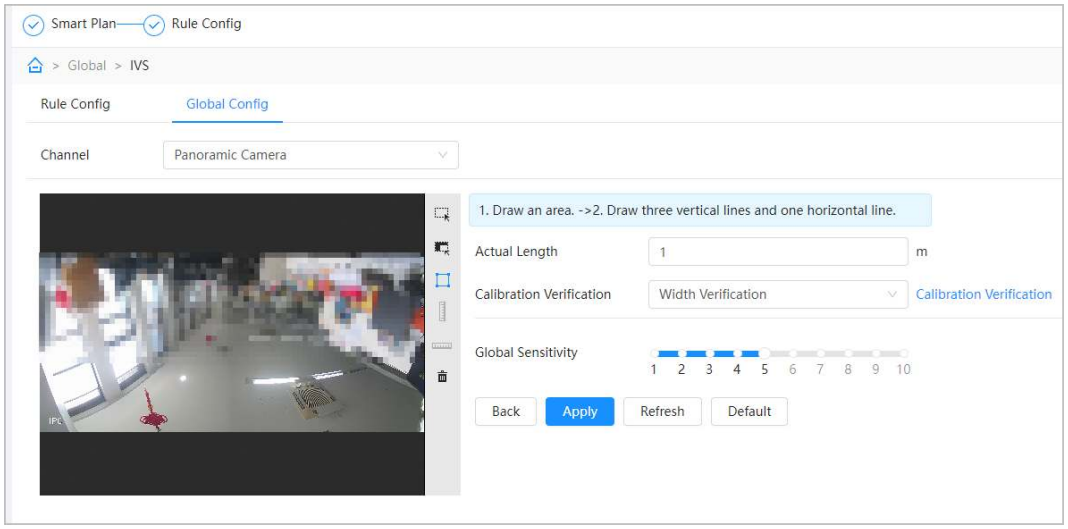
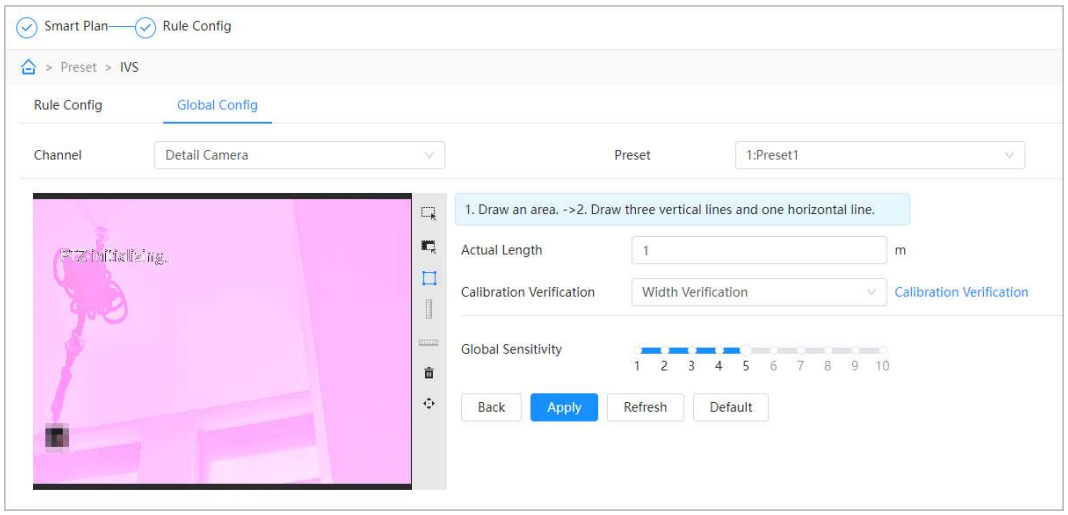


Figure 8-8 Global configuration for IVS (2)



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

1. Click and draw a calibration area in the image, and right-click to finish the drawing.
2. Click the ruler icon to draw one horizontal ruler and three vertical rulers in the calibration area.
   - indicates vertical ruler, and indicates horizontal ruler.
   - Select an added ruler, and click to delete the ruler.
3. 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 is higher.

Step 6 Click **Apply**.

Related Operations

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

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

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

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

8.3.2 Rule Configuration

This section introduces the rules used on IVS, including crossing virtual fence, tripwire, intrusion, abandoned object, fast moving, parking detection, crowd gathering, missing object, 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 8-2 Description of IVS functions

Rule	Functions	Applicable Scene
Crossing virtual fence	When the target crosses the warning line toward the defined direction, an alarm is triggered and then the system performs configured alarm linkages.	Scenes with median strips such as roads, and airports.
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 alarm is triggered, and the system performs defined alarm linkages.	
Abandoned object	When an object is abandoned in the detection area over the configured time, an alarm is triggered, and then the system performs 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 in the scenes with dense targets, frequent occlusion, and people staying. ● In scenes with complex foreground and background, false alarm might be triggered for abandoned or missing object.
Missing object	When an object is taken out of the detection area over the defined time, an alarm is triggered, and then the system performs defined alarm linkages.	
Parking detection	When the target stays over the defined time, an alarm is triggered, and then the system performs defined alarm linkages.	Road monitoring and traffic management.

Rule	Functions	Applicable Scene
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 monitoring area. The light direction should be vertical to the motion direction.
Crowd gathering	When the crowd gathers or the crowd density is large, an alarm is triggered, and then the system performs defined alarm linkages.	Scenes with medium or long distance, such as outdoor plaza, government entrance, station entrance and exit. It is not suitable for short-distance view analysis.
Loitering detection	When the target loiters over the shortest alarm time, an alarm is triggered, and then the system performs defined alarm linkages. After alarm is triggered, if the target stays in the area within the time interval of alarm, then alarm will be triggered again.	Scenes such as park and hall.

Procedure

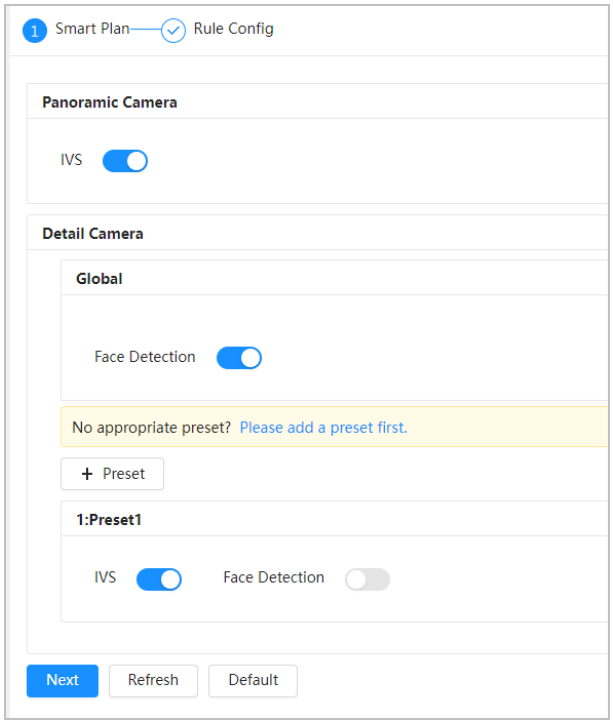
Step 1 Select **AI** > **AI Config** > **Smart Plan**.

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

For some models, select **IVS** in the **Panoramic Camera** tab and **Detail Camera** tab as needed in **AI** > **AI Config** > **Smart Plan** to enable the IVS function, and then click **Next**.

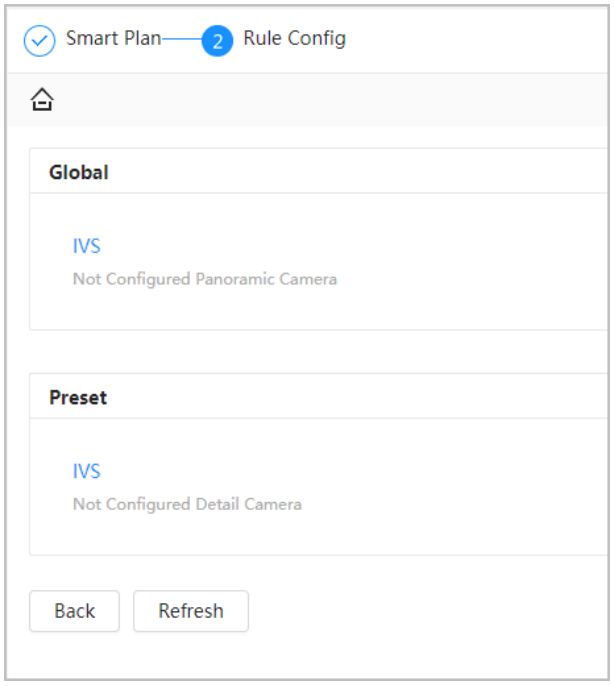
In the **Detail Camera** tab, add a preset first if there is no appropriate preset.

Figure 8-9 Configure smart plan (IVS)



Step 3 Click **IVS** in the **Global** and **Preset** tab, and then click **Next**.

Figure 8-10 Rule configuration



Only the detail camera supports selecting the preset.

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

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 8-11 Tripwire (1)

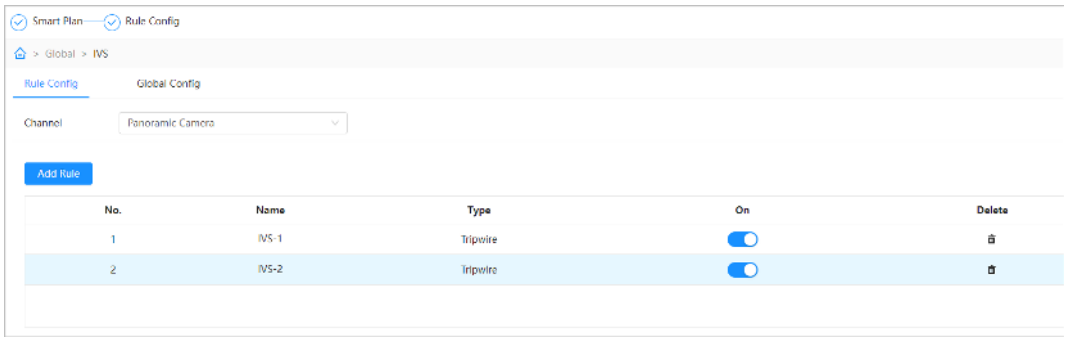
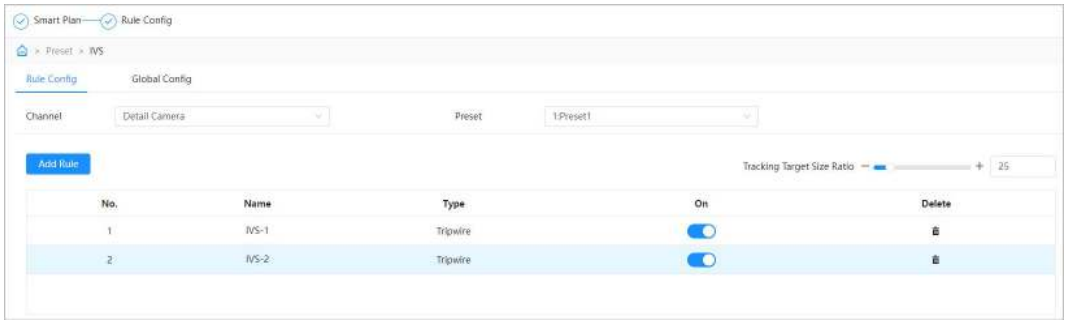


Figure 8-12 Tripwire (2)



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.

Figure 8-13 Draw the rule

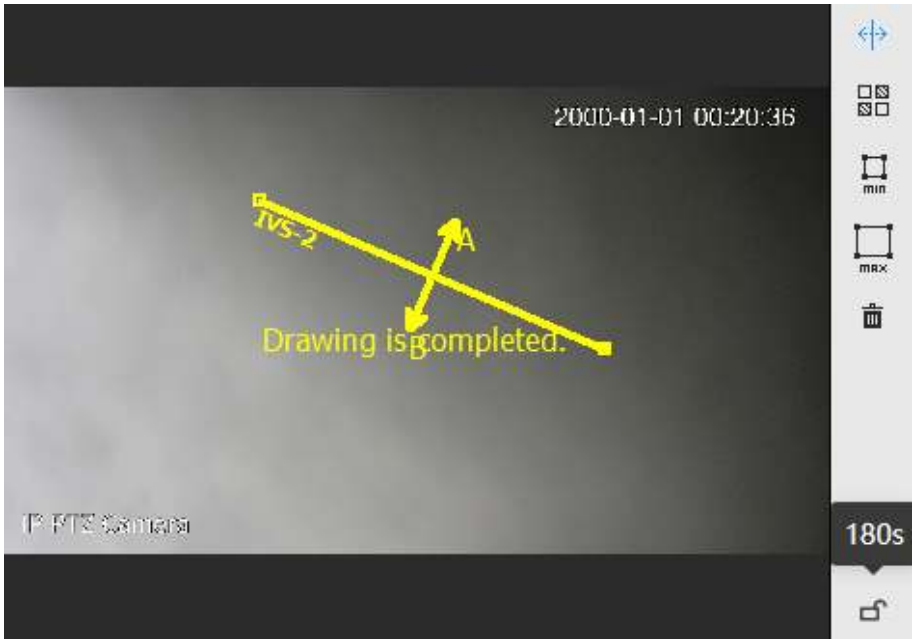


Table 8-3 Description of IVS analysis drawing rules

Rule	Description
Tripwire	Draw a detection line.
Crossing Virtual Fence	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 alarm triggered 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.
Intrusion	
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 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.
- 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 alarm is 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 pixel size is displayed.

- Click to delete the detection line.
- Click to lock the PTZ for 180 seconds, during which it cannot track so that you can set up intelligent rules. Click again to manually unlock it. This function is only supported by some devices.

Step 7 Set rule parameters for IVS.

Figure 8-14 IVS parameters

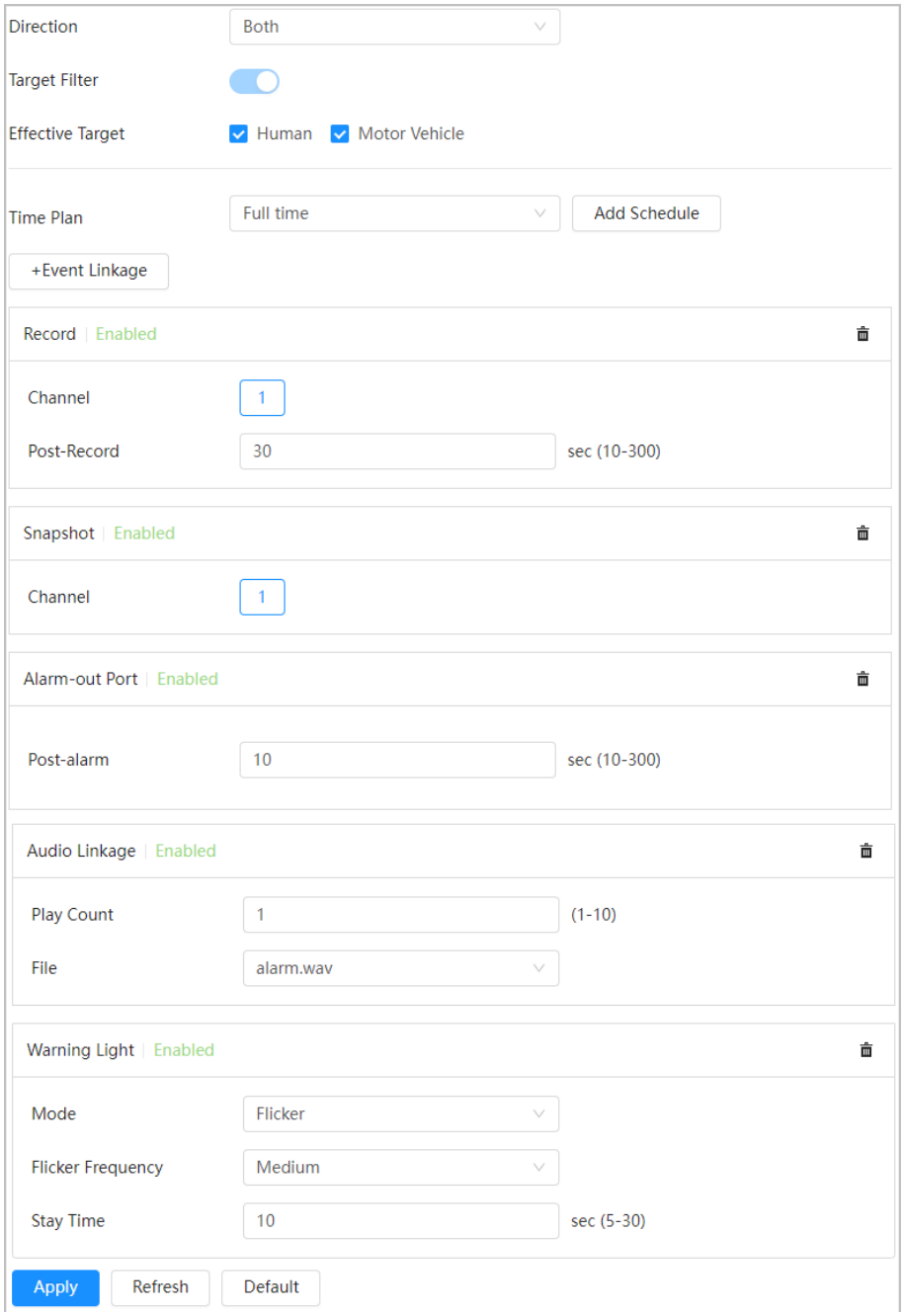


Table 8-4 Description of IVS parameters

Parameter	Description
Tracking Target Size Ratio	Set the tracking target size ratio. The default is 25.

Parameter	Description
Direction	Set the direction of rule detection. ● When setting tripwire and crossing fence, select A->B, B->A, or A<->B. ● When setting intrusion, select Enter, Exit, or Both.
Target Filter	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**.
Effective Target	
Action	When setting intrusion action, select **Appears** 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. For details, see "4.6.1.2.1 Adding Schedule".
- Click **Event Linkage** to set the linkage action and configure linkage parameters. For details, see "4.6.1.2 Alarm Linkage".

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. For details, see "4.6.1.3.2 Subscribing Alarm Information".

8.4 Panoramic Linkage

After the calibration of the panoramic camera and the detail camera, the panoramic camera can be used as the main camera to view panoramic images. and the detail camera can be used as a subordinate camera to view detailed images.

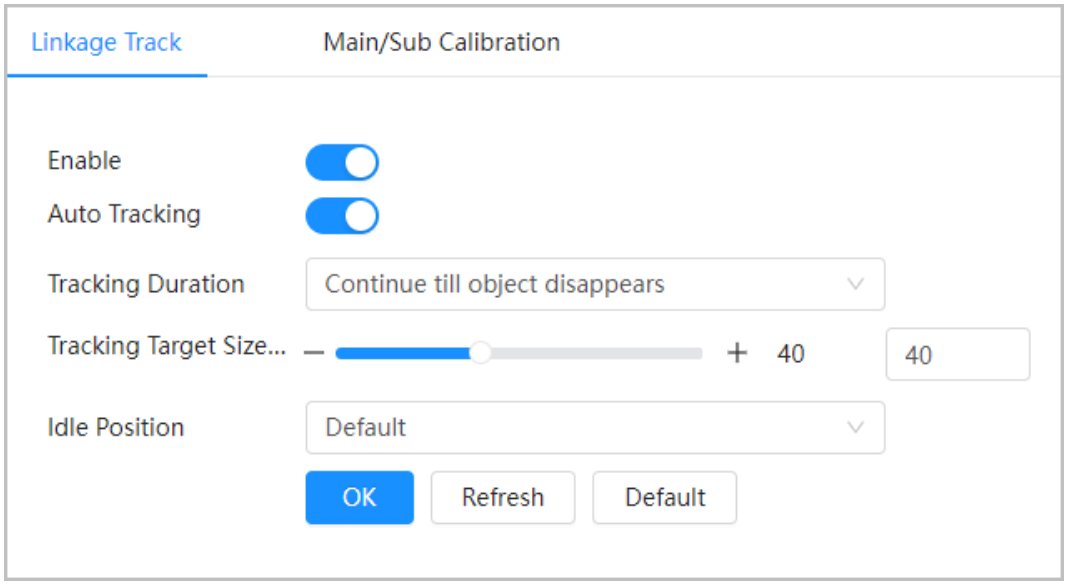
8.4.1 Linkage Track

After you set the main and sub calibration, when the panoramic camera's smart rules trigger an alarm, the detail camera will automatically link to the corresponding position and track the object until it goes out of the detection range or reaches the set tracking time.

Procedure

Step 1 In the main page, select **AI** > **AI Config** > **Panoramic Linkage** > **Linkage Track**.

Figure 8-15 Linkage track



Step 2 Click beside **Enable** to enable linkage track.

Only linkage track is enabled can manual position and manual linkage take effect.

Step 3 Click beside **Auto Tracking** to enable the auto tracking.

Step 4 Configure the parameters of linkage track.

Table 8-5 Parameter Description

Parameter	Description
Tracking Duration	You can configure the duration of linkage track. ● **Continue till object disappears** : When the panoramic camera's smart rules trigger an alarm, the detail camera will automatically track the object until it goes out of the detection range in panoramic image. ● **Custom** : You can manually set the tracking period. ● **Track until objects captured by detail camera disappear** : When the panoramic camera's smart rules trigger an alarm, the detail camera will automatically track the object until it goes out of the detection range by the detail camera.
Tracking Target Size Ratio	Set the ratio of the tracked object's size in the detail camera's image. The ratio refers to the proportion of the tracked object to the camera image.

Parameter	Description
Idle Position	In the idle position, the detail camera remains stationary. ● **None** : After the linkage track ends, the detail camera stops moving and remain fixed at the last tracked location. ● **Default** : After the linkage track ends, the detail camera returns to the forward position. ● **Preset** : After setting up the presets, the idle position will include the option of the corresponding presets. After the linkage track ends, the detail camera returns to the corresponding presets.

Step 5 Click **OK**.

8.4.2 Main/sub Calibration

Main and sub calibration types include manual calibration and automatic calibration.

- Manual calibration: Select the same point for calibration in the panoramic camera channel and the detail camera channel. When there are multiple obvious static marks in the monitoring environment, the calibration can be completed accurately with the help of the marks. If the user has special requirements for the calibration results, manual calibration can be applied.
- Auto calibration: The camera selects the calibration point in the monitoring picture through the algorithm, which has high calibration speed and accuracy. Auto calibration can be applied when the user has no special requirements for calibration results.

8.4.2.1 Manual Calibration

Procedure

Step 1 Select **AI** > **Panoramic Linkage**.

Step 2 Select **Manual** from the type drop-down list.

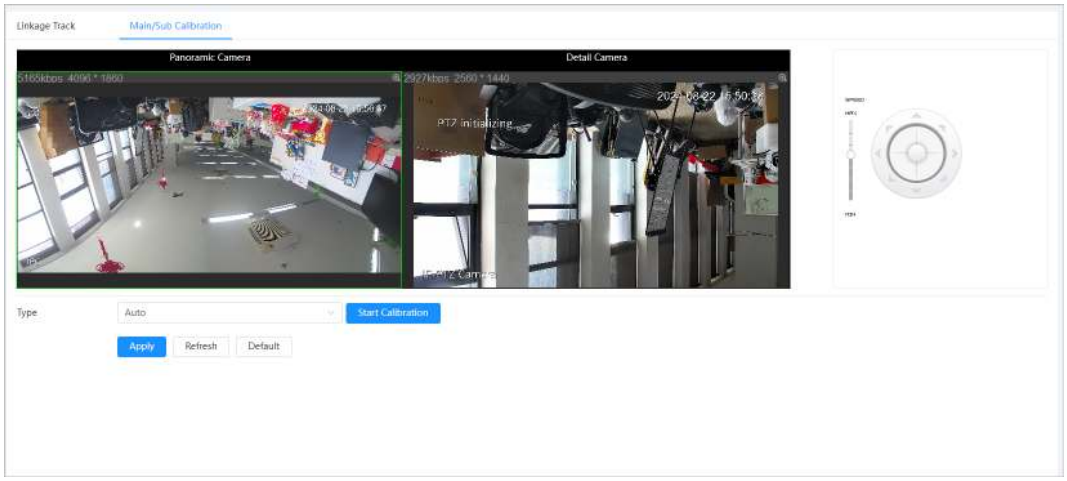
Step 3 Select the calibration scene in turn, and then adjust the detail camera PTZ to the appropriate calibration position to calibrate the panoramic camera and the detail camera.

At least 4 pairs of calibration dots are needed to ensure the views of the detail camera and the panoramic camera as similar as possible, up to 10 groups.

1. Click **Add**.
2. Move the point in the panoramic camera channel on the left and the detail camera channel on the right of the monitoring picture respectively, and the two points in the two channels serve as a group of calibration.
3. Click .

- We recommend you to calibrate from far to near, clockwise or counterclockwise, and the calibration points are evenly distributed.
- The calibration point is a corner point with obvious position characteristics, such as a clear point on an object or a boundary crossing point.

Figure 8-16 Main/sub calibration



Step 4 Click **Apply**.

8.4.2.2 Auto Calibration

Procedure

Step 1 Select **AI** > **Panoramic Linkage**.

Step 2 Select **Auto** from the type drop-down list.

Step 3 Click **Start Calibration**.

Wait for the calibration progress to complete.

If you are not satisfied with the calibration results, you can carry out auto calibration again.

Step 4 Click **Apply**.

9 Security

9.1 Security Status

Background Information

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

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

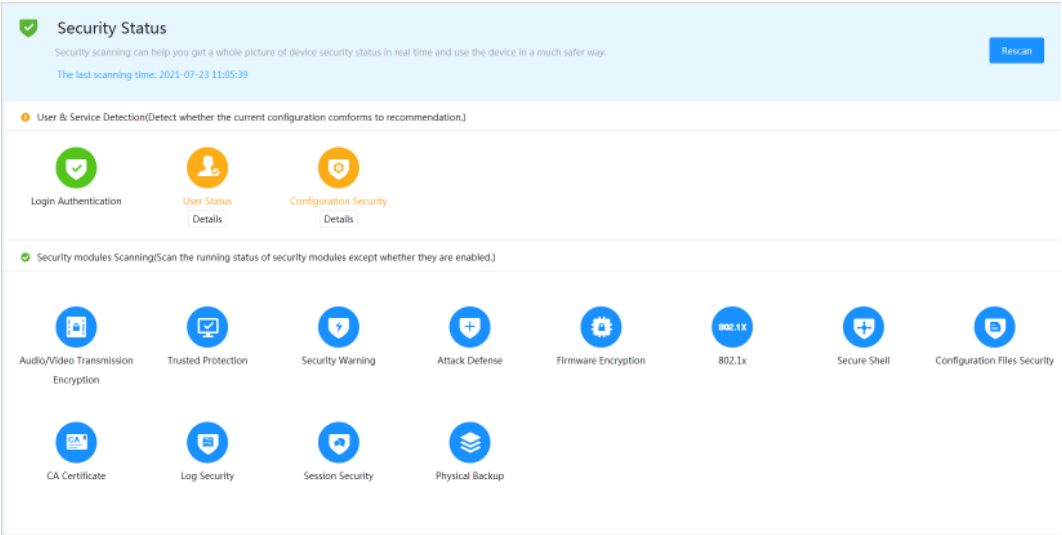
Procedure

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

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

During the scanning, the icon is grey. When the icon turns blue, the scanning is complete.

Figure 9-1 Security status



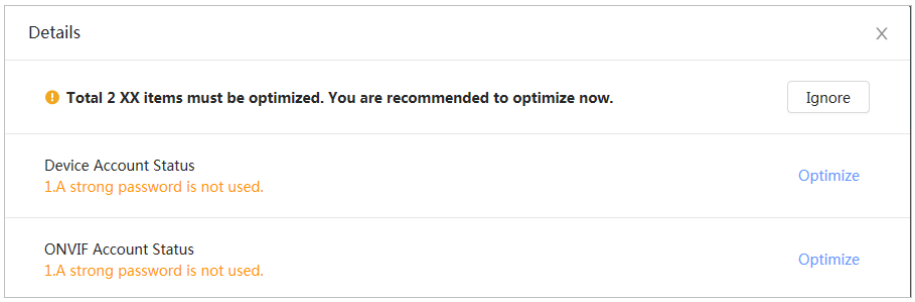
Related Operations

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

1. Click **Details** to view the details of the scanning result.
2. Click **Ignore** to ignore the exception, and it will not be scanned in next scanning.

   Click **Joint Detection**, and the exception will be scanned in next scanning.
3. Click **Optimize**, and the corresponding page is displayed, and you can edit the configuration to clear the exception.

Figure 9-2 Security status



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.

Procedure

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

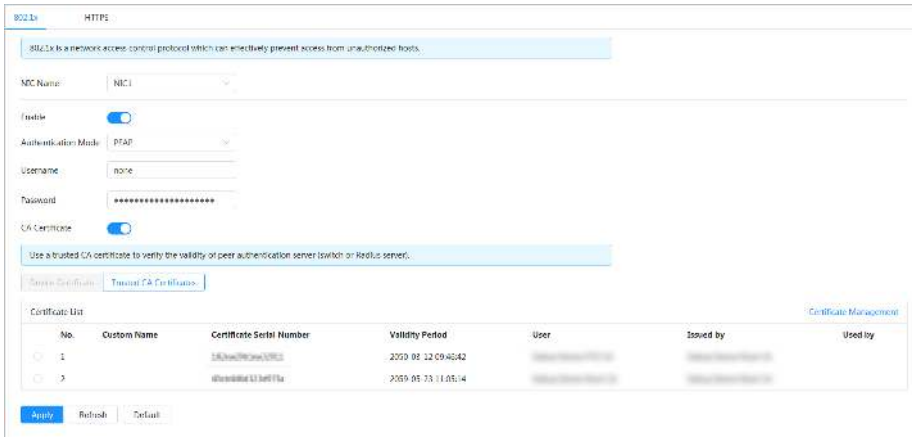
Step 2 Select the NIC name as needed, and click to enable it.

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

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

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

Figure 9-3 802.1x (PEAP)



- TLS: Transport Layer Security. It is applied in two communication application programs to guarantee the security and integrity of the data.
  1. Select TLS as the authentication mode.

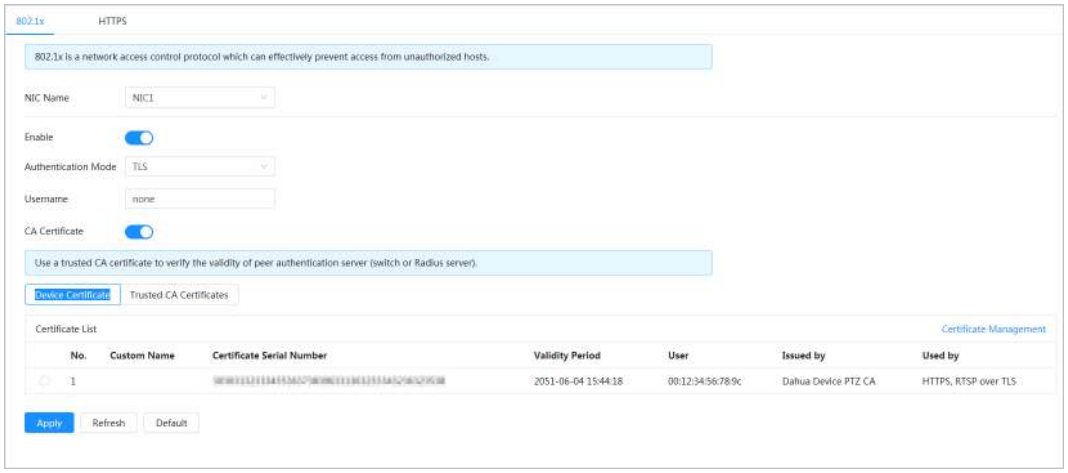
2. Enter the username.
3. Select the certificate from the certificate list in the **Device Certificate** page.

   If there is no certificate in the list, click **Certificate Management** at the left navigation bar. For details, see "9.4.1 Installing Device Certificate".

4. (Optional) Click next to CA certificate, and select the trusted CA certificate in list.

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

Figure 9-4 802.1x (TLS)



Step 4 Click **Apply**.

9.2.2 HTTPS

Background Information

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.

After HTTPS is enabled, TLSv1.1 and earlier versions are supported by default. However, earlier version of TLS may have security risks. Please select carefully.

Procedure

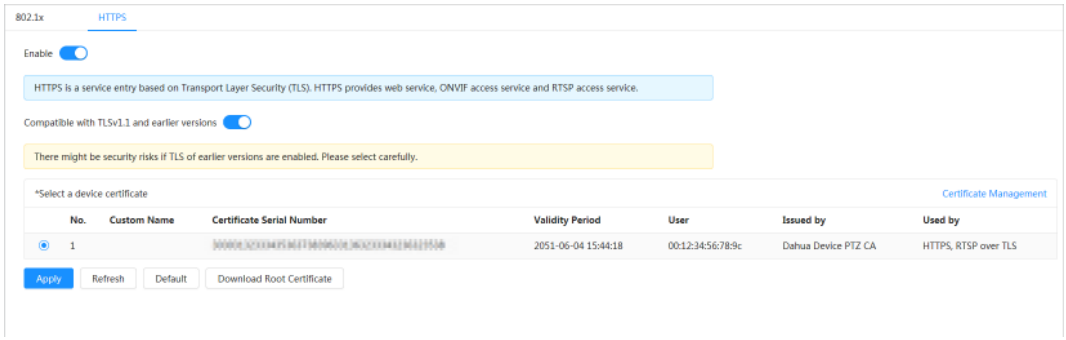
Step 1 Select **Security** > **System Service** > **HTTPS**.

Step 2 Click to enable it.

Step 3 Select the certificate.

If there is no certificate in the list, click **Certificate Management** at the left navigation bar.

Figure 9-5 HTTPS



Step 4 Click **Apply**.

9.3 Attack Defense

9.3.1 Firewall

Configure firewall to limit access to the Camera.

Procedure

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

Step 2 Click to enable the firewall function.

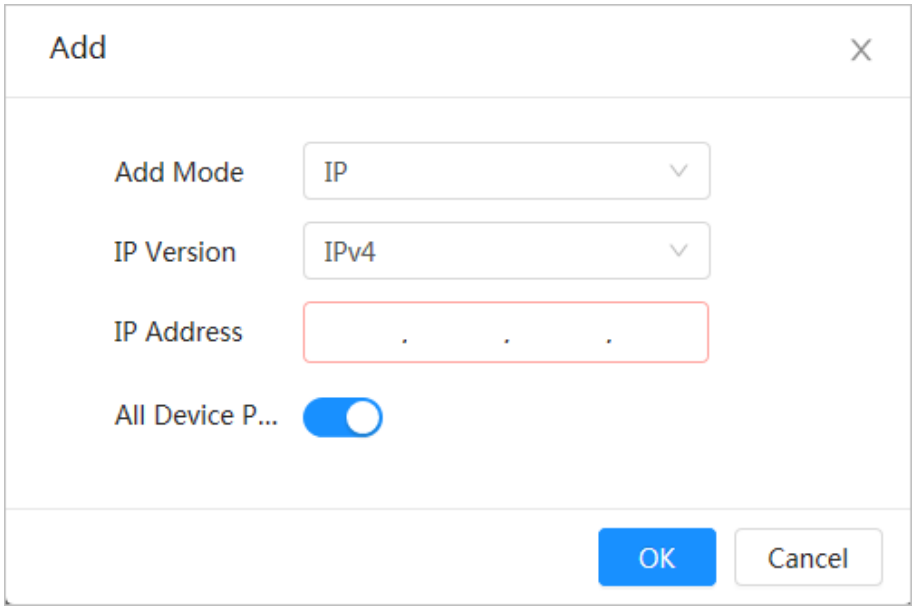
Figure 9-6 Firewall

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

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

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

Figure 9-7 Firewall



Step 5 Click **Apply**.

Related Operations

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

9.3.2 Account Lockout

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

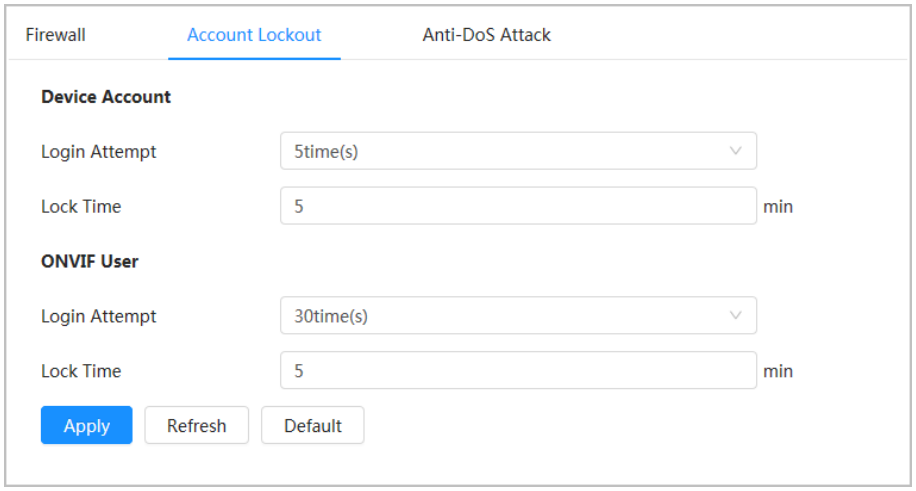
Procedure

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

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

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

Figure 9-8 Account lockout



Step 3 Click **Apply**.

9.3.3 Anti-DoS Attack

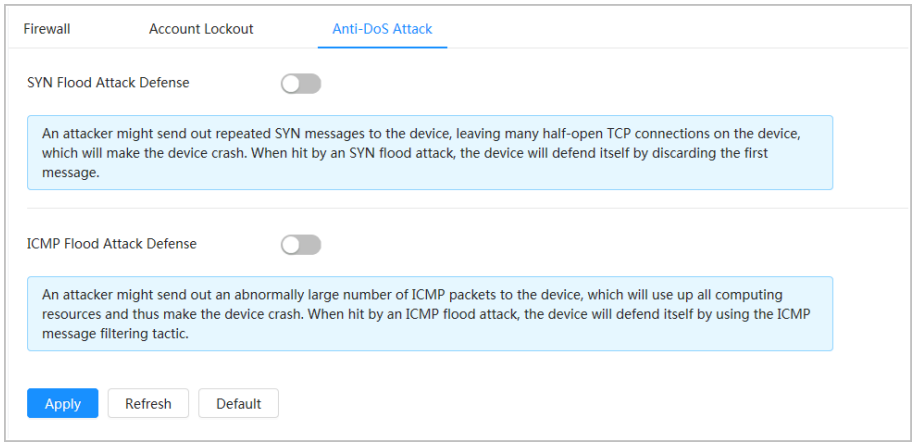
You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the Camera against DoS attack.

Procedure

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

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

Figure 9-9 Anti-DoS attack



9.4 CA Certificate

9.4.1 Installing Device Certificate

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

9.4.1.1 Creating Certificate

Creating certificate in the Camera.

Procedure

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

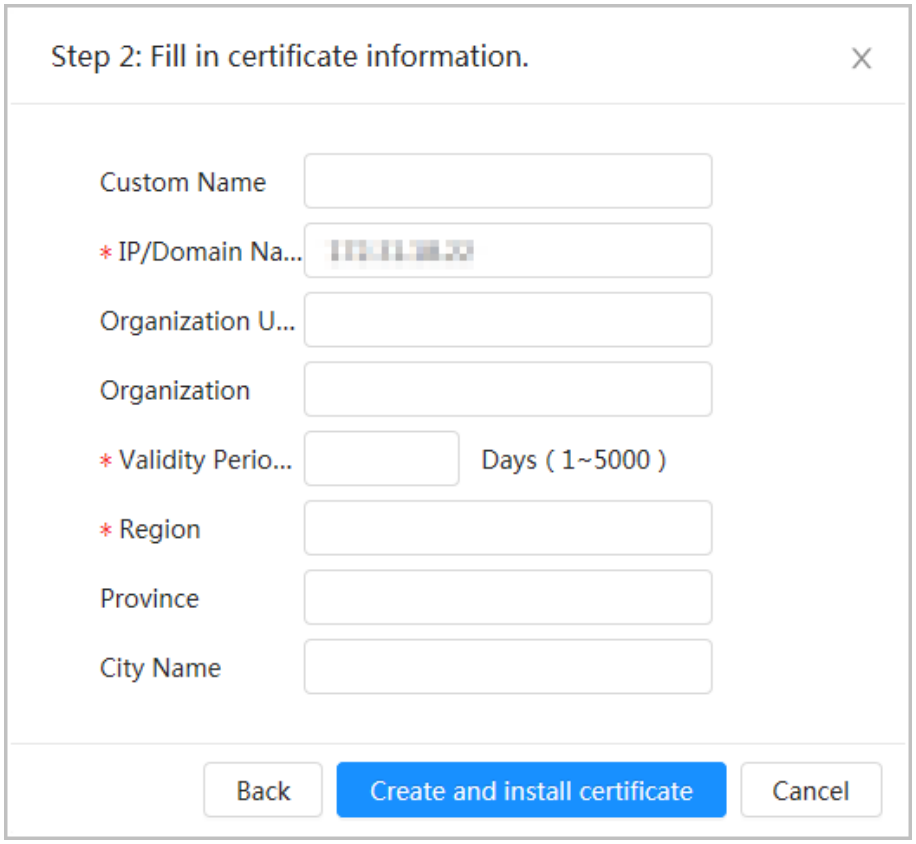
Step 2 Select **Installing Device Certificate**.

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

Step 4 Enter the certificate information.

"IP/Domain Name": Enter the IP or domain name of the Camera.

Figure 9-10 Certificate information (1)



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

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

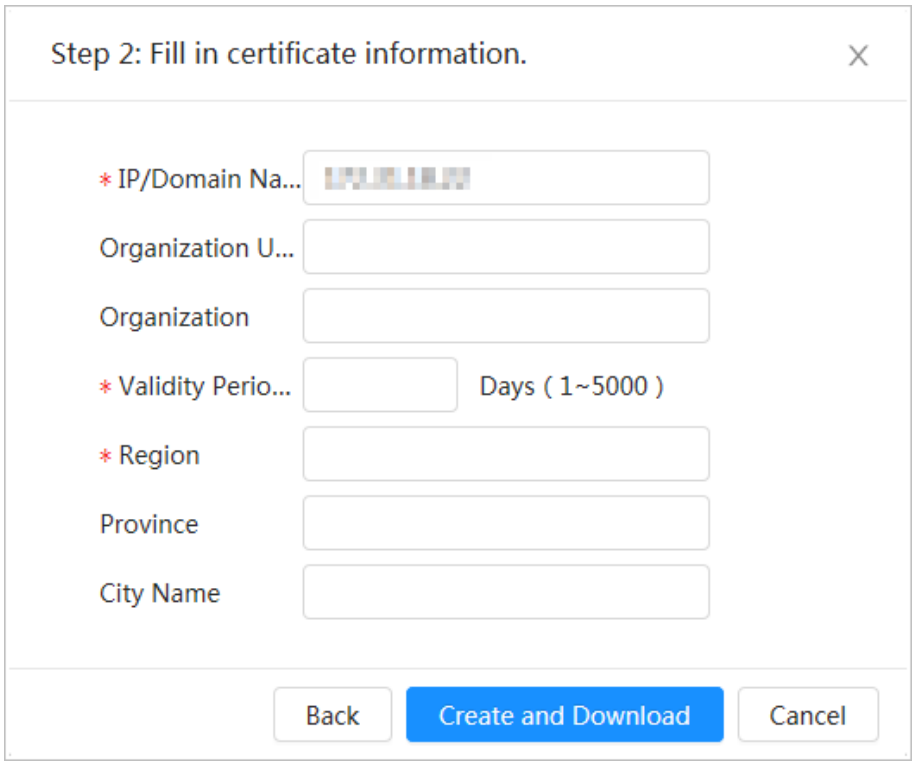
Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

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.

Figure 9-11 Certificate information (2)



Step 5 Click **Create and Download**.

Save the request file to your computer.

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

Step 7 Import the signed CA certificate.

1. Save the CA certificate to the computer.
2. Select **Installing Device Certificate** , click **Apply for CA Certificate and Import (Recommended)**, and then click **Next**.
3. Click **Browse** to select the signed CA certificate.
4. Click **Install and Import**.

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

   - Click **Recreate** to create the request file again.

- Click **Import Later** to import the certificate next time.

Related Operations

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

Procedure

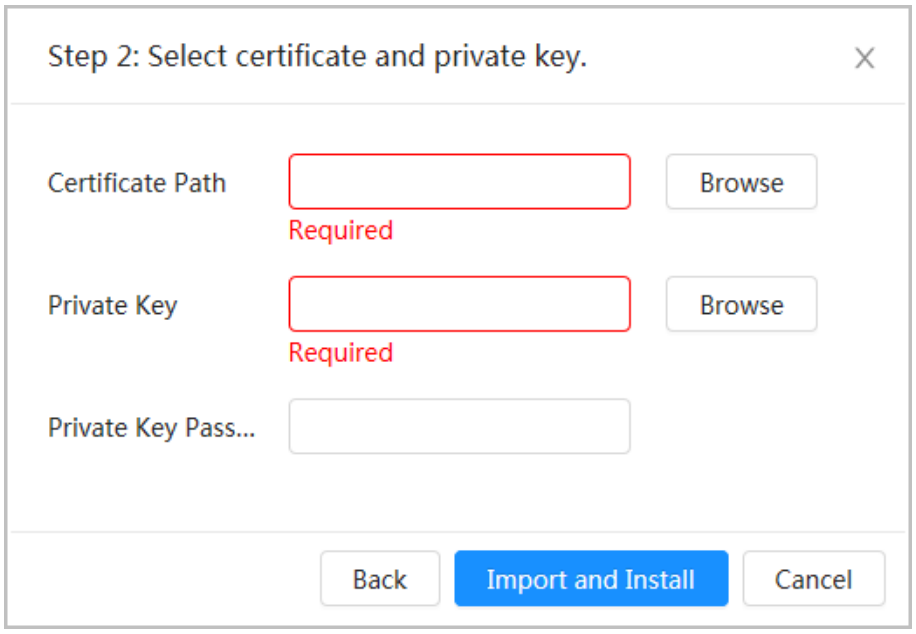
Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

Step 2 Select **Installing Device Certificate**.

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

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

Figure 9-12 Certificate and private key



Step 5 Click **Import and Install**.

After the certificate is created successfully, you can view the created certificate on the **Device Certificate** 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 the camera accesses the LAN through 802.1x, the CA certificate is required.

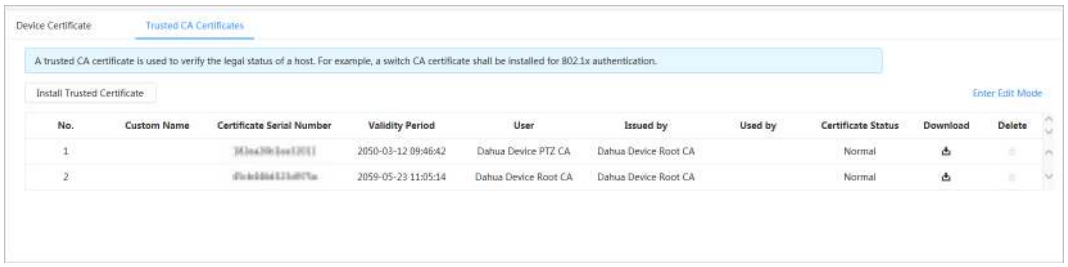
Procedure

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

Step 2 Select **Installing Trusted Certificate**.

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

Figure 9-13 Installing trusted certificate



Step 4 Click **OK**.

After the certificate is created successfully, you can view the created certificate on the **Trusted CA Certificate** 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 A/V Encryption

The device supports audio and video encryption during data transmission.

Background Information

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

Procedure

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

Step 2 Configure the parameters.

Figure 9-14 A/V encryption

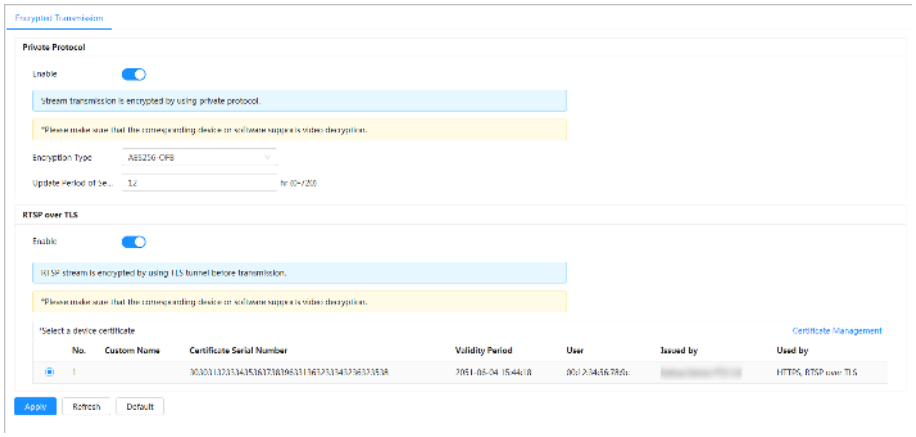


Table 9-1 A/V encryption parameter

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

Step 3 Click **Apply**.

9.6 Security Warning

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

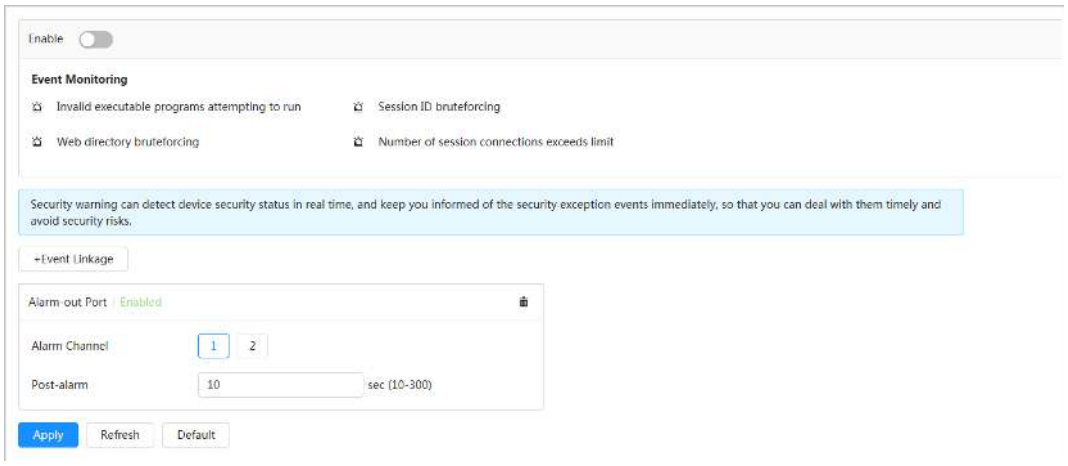
Procedure

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

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

Step 3 Configure the parameters.

Figure 9-15 Security warning



Step 4 Set arming periods and alarm linkage action. For details, see "4.6.1.2 Alarm Linkage".

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

Step 5 Click **Apply**.

10 Maintenance Center

10.1 One-click Diagnosis

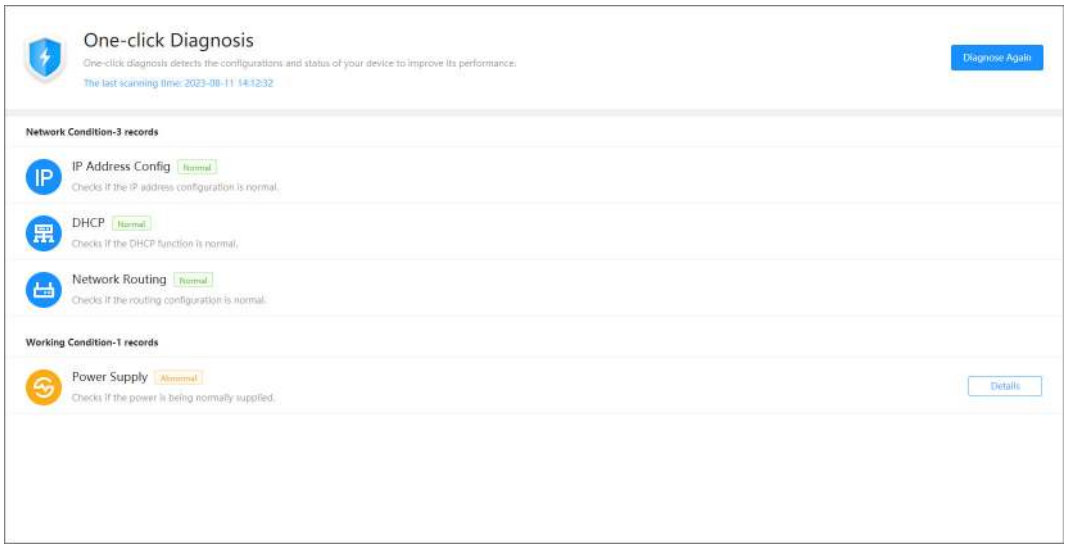
Procedure

Step 1 Select **Maintenance Center** > **One-click Diagnosis**.

Step 2 Click **Diagnose**.

Diagnosis information are generated and displayed on the page.

Figure 10-1 One-click diagnosis



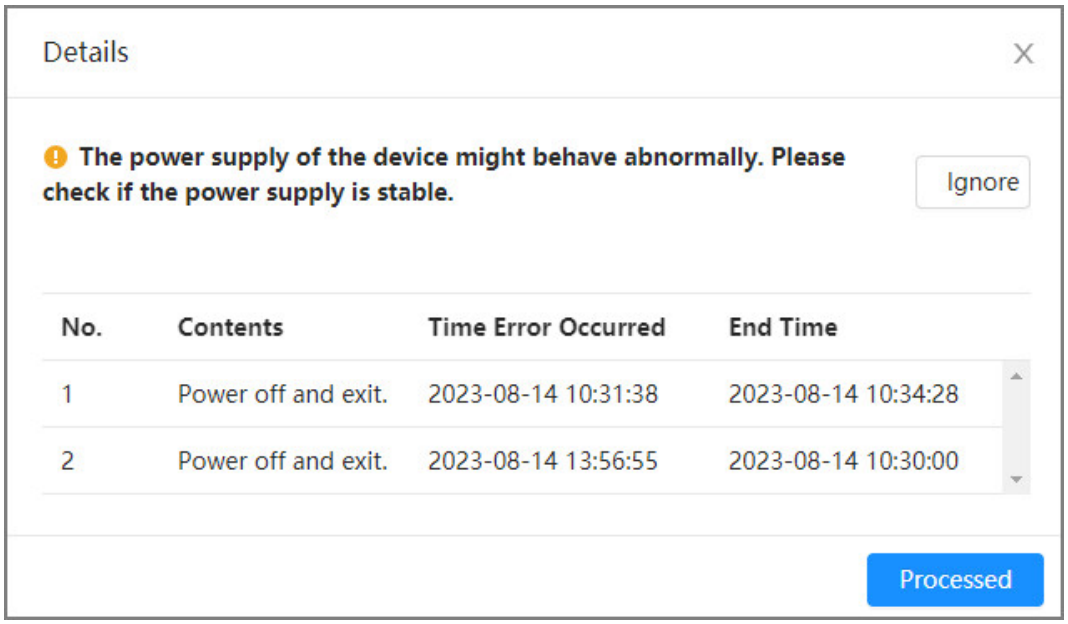
Related Operations

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

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

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

Figure 10-2 Details



10.2 System Information

10.2.1 Viewing Version Information

Select **Maintenance Center** > **System Info** > **Version**. You can view the device model, system version, web version and other version information.

10.2.2 Viewing Online User

Select **Maintenance Center** > **System Info** > **Online User**. You can view the information of the user who logged in the Camera.

10.2.3 Viewing Legal Information

Select **Maintenance Center** > **System Info** > **Legal Info**. You can view the corresponding information under different tabs, including software license agreement, privacy policy, and open source software notice.

10.3 Log Information

10.3.1 Viewing Local Log

View and back up the log information of the system.

Background Information

The log type includes **All** , **System**, **Config**, **Storage**, **Alarm Event**, **Record**, **Account**, **Security**, **PTZ Operation**, and **Clear Log**.

- **System** : Includes program start, abnormal close, close, program reboot, device closedown, device reboot, system reboot, and system upgrade.
- **Config** : Includes saving configuration and deleting configuration file
- **Storage** : Includes configuring disk type, clearing data, hot swap, FTP state, and record mode.
- **Alarm Event (recording events such as video detection, AI, alarms, and anomalies)** : 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.
- **PTZ Operation** : Includes preset, tour group, scan, pattern and other PTZ basic operations.
- **Clear Log** : Clears the log.

Procedure

Step 1 Select **Maintenance** > **Log Info** > **Local Logs**.

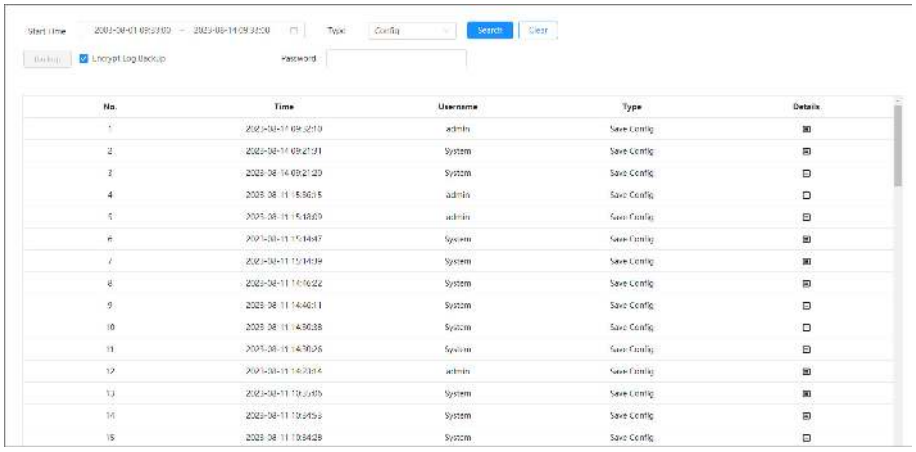
Step 2 Configure the start time and end time, and then select the log type.

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

Step 3 Click **Search**.

- Click or click a certain log to view the detailed information in **Details** area.
- Click **Backup** to back up all found logs to local PC. If you select **Encrypt Log Backup** and set **Password**, you need to enter a password when opening a local log file.
- Click **Clear** to clear logs.

Figure 10-3 Search local logs



10.3.2 Setting Remote Log

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

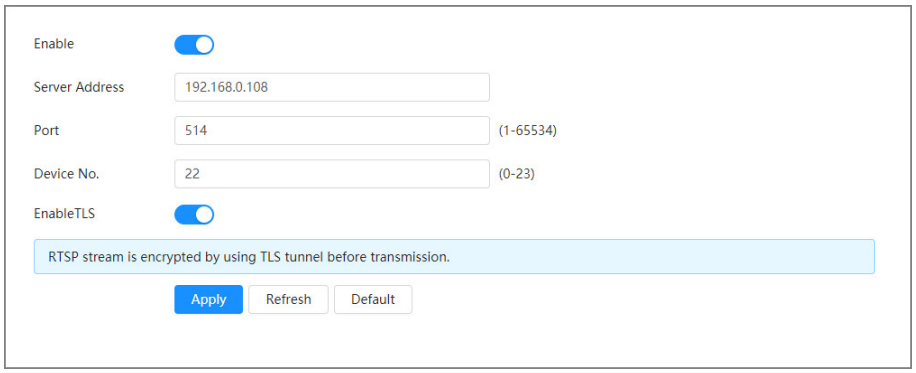
Procedure

Step 1 Select **Maintenance Center** > **Log Info** > **Remote Log**.

Step 2 Click to enable remote log function.

Step 3 Configure address, port and device number.

Figure 10-4 Remote log



Step 4 Click corresponding to **EnableTLS** to encrypt RTSP stream by using TLS tunnel before transmission to prevent data leakage.

Step 5 Click **Apply**.

10.4 Manager

10.4.1 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. For details, see "4.8.2 Account".
- View system logs and analyze them, and process the abnormity in time.
- Back up the system configuration regularly.
- Restart the device and delete the old files regularly.
- Update firmware in time.

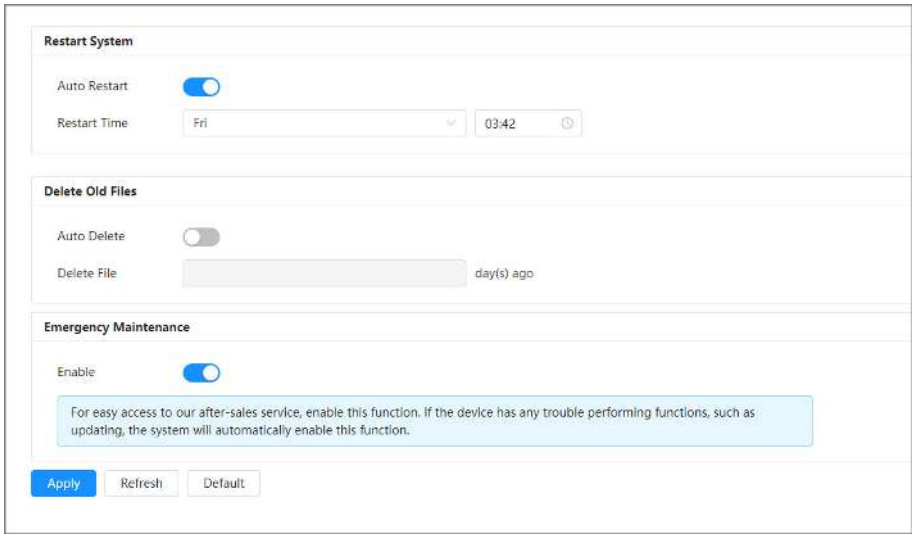
10.4.2 Maintenance

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

Procedure

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

Figure 10-5 Maintenance



Step 2 Configure auto maintain parameters.

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

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

Step 3 Click **Apply**.

10.4.3 Import/Export

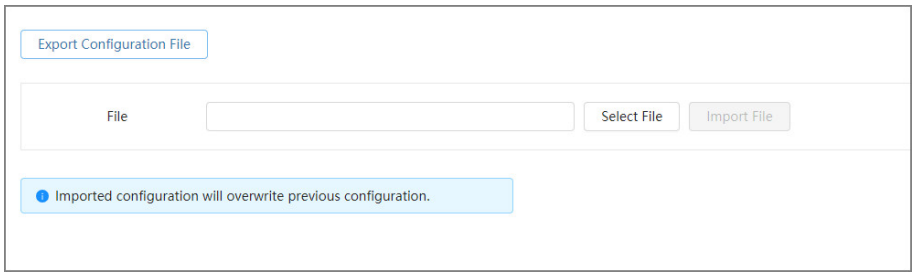
Background Information

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

Procedure

Step 1 Select **Maintenance Center** > **Manager** > **Import/Export**.

Figure 10-6 Import/export



Step 2 Import and export.

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

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

10.4.4 Default

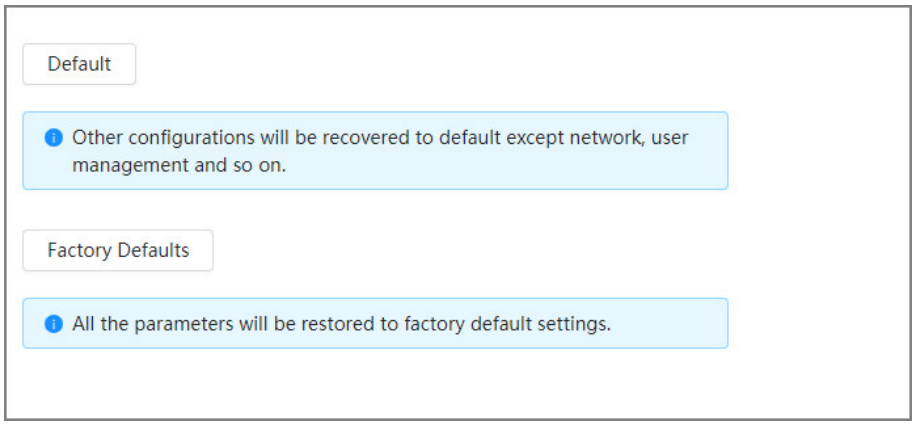
Restore the device to default configuration or factory settings.

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

Select **Maintenance Center** > **Manager** > **Default**.

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

Figure 10-7 Default



10.5 Update

Background Information

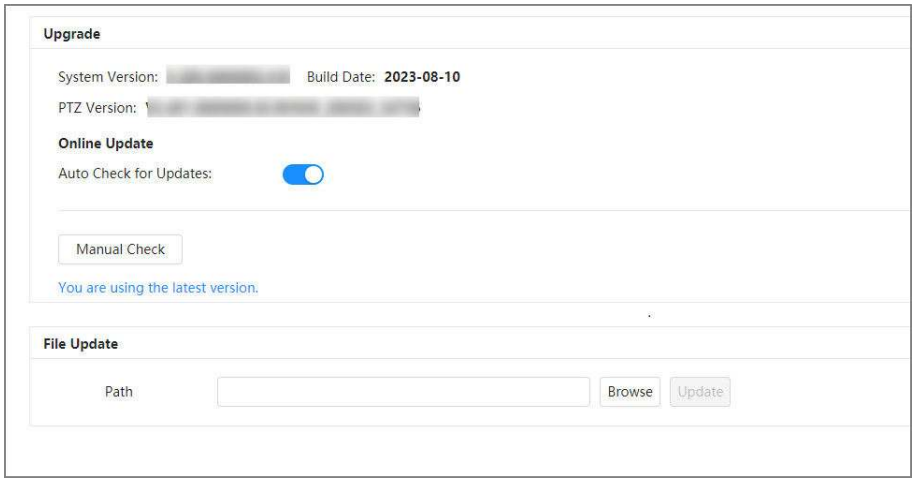
Upgrading to the latest system can refine camera functions and improve stability.

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

Procedure

Step 1 Select **Maintenance Center** > **Upgrade**.

Figure 10-8 Upgrade



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

The upgrade file should be a .bin file.

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

Step 3 Click **Upgrade**.

The upgrade starts.

10.6 Advanced Maintenance

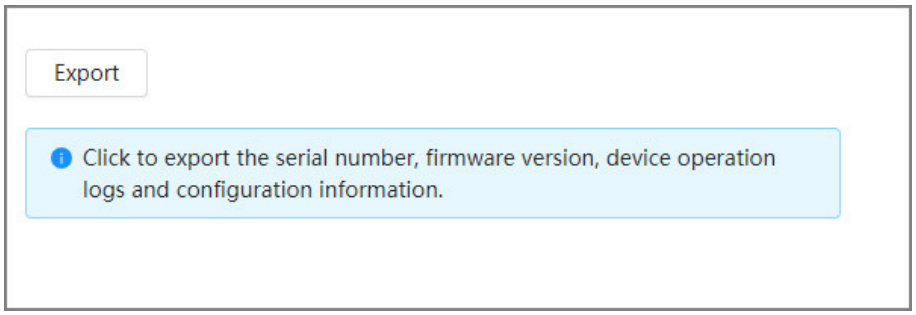
10.6.1 Export

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

Procedure

Step 1 Select **Maintenance Center** > **Advanced Maintenance** > **Export**.

Figure 10-9 Export



Step 2 Click **Export** , the page displays an export progress. Click **End Export** to cancel the current export.

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

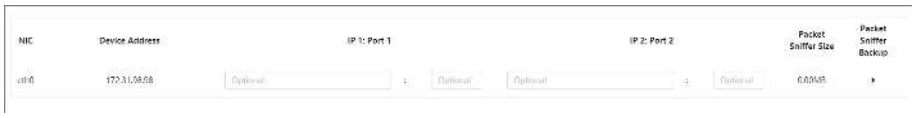
10.6.2 Packet Capture

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

Procedure

Step 1 Select **Maintenance Center** > **Advanced Maintenance** > **Packet Capture**.

Figure 10-10 Packet Capture



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

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

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

Step 3 Capture.

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

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

10.6.3 Run Log

Run log refers to the serial port information automatically recorded by the Camera during operation. Viewing the run log helps to locate problems and improve work efficiency.

Procedure

Step 1 Select **Maintenance Center** > **Advanced Maintenance** > **Run Log**.

Figure 10-11 Run log

Step 2 Export the log.

- Select one log, and then click . You can export the log one by one.
- Select more than one log, and then click **Export**. You can export the logs in batch.

If a SD card is installed, click next to **Store Running Logs Locally**. The logs will be stored in real-time on the SD card.

Related Operations

- Click **Refresh** to refresh information displayed on the page.
- Select one or more logs, and then click **Delete** to delete the log.

After deleting the log, it cannot be recovered.

11 App Center

This chapter introduces the basic information of the app center.

11.1 Application Overview

Select **App Center** > **Application Overview**. You can view the device basic information, application resource overview, application running overview, and application information.

In the **Application Info** , click **Go to**, and then you can enter the **Application** page.

Figure 11-1 Application overview

11.2 Application

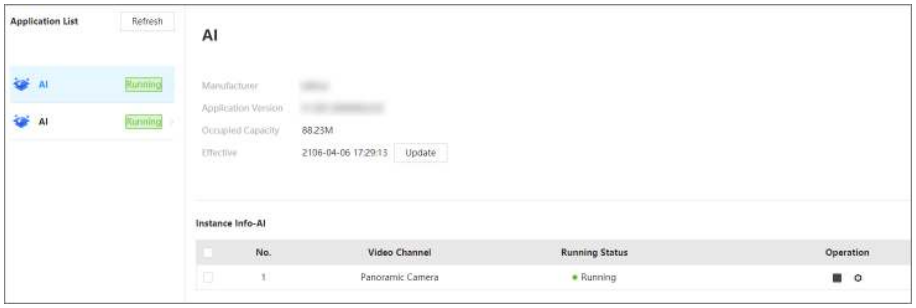
Click **App Center** > **Application**. You can view the basic information of the application, stop and start the application.

- Click **Refresh** to refresh the page information.
- Click **Update** to import the license and avoid license expiration.
- Click to stop the application and click to start the application.

  When you stop the application:

  - Target statistics and face statistics are not available in **Camera** > **Encode** > **Overlay**.
  - **Intelligent** is not available on the main page.
- Click to enter the **Smart Plan** page, and then you can configure the smart plan.

Figure 11-2 Application



Appendix 1 Security Commitment and Recommendation

Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters: upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use repeating characters, such as 111, aaa, etc.
2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.
3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.
4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.
5. **Set and update password reset information in a timely manner**

   Dahua device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access Web services through secure channels.
2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, we recommend you to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.
3. **Turn off non-essential services and use safe mode**

   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

   If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up complex passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.
4. **Change HTTP and other default service ports**

   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allow list**

   It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.
2. **MAC address binding**

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

   Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**

   According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

   We recommend you to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188