IP Camera

User Manual

Version：26.2.43.4

Statement

Thank you for purchasing our product. If there are any questions or requests, please do not hesitate to contact the dealer.
This manual applies to IP camera and serves as a reference tool for your operating system. You can find information on how to implement the function in this manual, as well as a detailed menu. The photos, graphics, icons, etc. provided in the manual are for explanation and explanation purposes only, and may differ from the specific products. Please refer to the actual operation interface. Please fully understand the information in this manual before installing and using the system.
This manual may contain several technical incorrect places or printing errors, and the content is subject to change without notice. The updates will be added to the new version of this manual. We will readily improve or update the products or procedures described in the manual.

Before use

Visit our website (www.herospeed.net) for instructions, application tools and more.
Please check the equipment before use. For details of the school time configuration method, see “8.2.1 System Configuration ②Time Settings”.

Legal Disclaimer

- Should any reasons below cause the product destroyed or service stop, we will assume no responsibility for your or third party’s personal injury and property loss: ① No installation or use according to instruction strictly. ② For sake of state-building maintenance or public interest. ③ Cases of force majeure. ④ Your personal or third party reasons. (Include no limitation use of third party’s products, software or components)
- Our company has never guaranteed the products for improper or illegal purposes and uses. This product cannot be used as medical & safety devices or other applications that will cause danger or injury. And loss or responsibility caused by above uses, you must bear it by yourself.
- With correct installation and use, this product can detect the illegal intrusion, but it can not avoid accidents and personal injury or property damage due to these accidents. Please be on the alert in your daily life, reinforce your safety awareness.
- Our company assumes no responsibility for any indirect or occasional or special or punitive damages, request, property damage or any loss of data or file. Within the max scope of law allowed, our company’s compensation is no more than the products amount you paid.

Safety Instruction

This manual is intended to ensure that user can use the product properly without danger or any property loss. Please read it carefully and take care of it for further reference. Precaution measures are divided into “warnings” and “CAUTIONS” as below:
Warnings: Neglecting any of the warnings may cause death or serious injury.
CAUTIONS: Neglecting any of the CAUTIONS may cause injury or equipment damage.

 Warning Follow these safeguards to avoid death or serious injury	 Caution Follow these precautions to Prevent potential injury or Property loss



WARNING

- Electrical safety regulations of the nation and the region must be strictly followed during installation or use.
- Please use the matched power adapter from standard company.
- Do not connect multiple IPCs with one single power adapter (Overload for adapter may lead to over-heat or fire hazard.
- Shut down the power while connecting or dismounting the device. Do not operate with power on.
- The device should be firmly fixed when installed onto the wall or beneath the ceiling.
- Shut down the power and unplug the power cable immediately when there is smOKe, odor or noise rising from the IPC. Then contact the dealer or service center.
- Please contact the local dealer or latest service center when IPC works abnormally. Do not attempt to disassemble or modify the device yourself. (We shall shoulder no responsibility for problems caused by unauthorized repair or maintenance.



CAUTIONS

- Make sure the power supply voltage is correct before using the camera.
- Do not drop objects onto the device or vibrate the device vigorously, and keep the device away from locations where magnetic interference is present. Avoid installing the device where the surface is vibrating or subject to shock (ignoring this may damage the device).
- Do not aim the camera lens at the strong light such as sun or incandescent lamp. The strong light can cause fatal damage to the camera.
- Do not expose the IPC used indoors to places that may be exposed to rain or very humid.
- Store in a dry, non-corrosive atmosphere, away from direct sunlight, in poorly ventilated locations, or near heat sources such as heaters or heaters (ignoring this may result in a fire hazard).
- To avoid IPC damage, do not place the IPC in a location where there is soot or water vapor, too high temperatures, or lots of dust.
- Do not touch the heat sink of the product directly to avoid burns.
- When cleaning, wipe off the dirt on the casing with a soft cloth. When cleaning the dirt, it should be cleaned with a dry cloth. When the dirt is not easy to remove, it can be wiped clean with a neutral detergent. Do not use alkaline cleaner to wash. If there is dust on the lens, use a special lens paper to wipe it.
- Products connected to the Internet may face network security problems. Please strengthen the protection of personal information and data security. When you find that the product may have a network security risk, please contact us in time.
- Please understand that it is your responsibility to properly configure all passwords and other related product security settings, and keep your username and password in a safe place.
- Please keep all the original packaging materials of the product properly, so that when there is a problem, use the packaging materials to package the product and send it to the agent.

(**NOTE** Full-text IP camera is referred to as IPC for short)

Table of Contents

CHAPTER 1 PRODUCT INTRODUCTION 6

1.1 PRODUCT MANUAL 6
1.2 PRODUCT FEATURES 6

CHAPTER 2 OPERATING INSTRUCTIONS 8

2.1 NETWORK CONNECTION 8
2.1.1 Wired network connection 8
2.1.2 Wireless internet access 8
2.2 DETECTING,ACTIVATE AND CHANGING THE IP ADDRESS 9
2.3 SETTING THE IP CAMERA OVER THE WAN 10
2.3.1 Static IP Connection 10
2.3.2 Dynamic IP Connection 11

CHAPTER 3 ACCESS TO THE IPC BY CLIENT SOFTWARE 13

CHAPTER 4 ACCESS TO THE IPC BY WEB CLIENT 14

4.1 PREPARATION BEFORE INSTALL PLUGIN 14
4.2 ACTIVATE,LOGIN AND EXIT 14
4.2.1 Activate 14
4.2.2 Login 15
4.2.2 Change password 16
4.2.3 Forget password 17
4.2.4 Exit System 24
4.3 INSTALL THE LSIPCPLUGIN CONTROLS 24
4.4 MAIN INTERFACE DESCRIPTION 29

CHAPTER 5 PREVIEW 30

5.1 PREVIEW 30
5.2 IMAGE PARAMETERS 31
5.3 PTZ CONTROL 32
5.4 LICENSE PLATE RECOGNITION MODE 34
5.5 PREVIEW MODE 35

CHAPTER 6 PLAYBACK 37

CHAPTER 7 PICTURE 40

CHAPTER 8 CONFIGURATION 41

8.1 COMMON SETTINGS 41
8.2 LOCAL CONFIG 41
8.3 SYSTEM 42
8.3.1 System Config 42
8.3.2 Safety 47
8.4 NETWORK 51
8.4.1 Basic Setup 51
8.4.2 P2P 66
8.4.3 Email 68
8.5 VIDEO AND AUDIO 70
8.5.1 Video 70
8.5.2 Audio 71
8.5.3 ROI 72
8.6 IMAGE 73
8.6.1 Image 74
8.6.2 OSD 79
8.6.3 Privacy Mask 79

8.7 EVENT 80
8.7.1 Basic Event 80
8.6.2 Smart Event 97
8.7.3 One-Key Disarm 133
8.7.4 Statistical Analysis 135
8.7.5 Face Recognition 137
8.7.6 License Plate Recognition 140
8.7.7 Vehicle Record 145
8.8 STORAGE 146
8.8.1 Schedule Settings 146
8.8.2 Storage management 149
CHAPTER 9 MAINTAIN 152
9.1 DEVICE INFORMATION 152
9.2 UPGRADE 152
9.3 DEFAULT 153
9.4 AUTO MAINTAIN 154
9.5 IMPORT AND EXPORT 154
9.6 LOG 155
CHAPTER 10 FREQUENTLY ASKED QUESTIONS 156

Chapter 1 Product Introduction

1.1 Product Manual

IP camera is integrated video and audio acquisition, intelligent coding and network transmission and other functions of digital monitoring products. Using embedded operating system and high-performance hardware processing platform, with high stability and reliability to meet the diverse needs of the industry.
IP camera based on Ethernet control, image compression can be achieved through the network and transmitted to different users.
You can use the browser or client software to control the IP camera, and through the browser to set the IP camera parameters, such as system parameter settings, OSD display settings and other parameters; through the browser or client software configuration can also achieve motion detection, Abnormal alarm and other intelligent functions, the specific function parameters, please take the actual equipment.

1.2 Product Features

This section introduces the webcam from the product features, allowing you to become more familiar with and familiar with webcams.

- **System functions**
- **Video and capture functions**

The IP camera supports video recording and capture function. You can also install a memory card or configure a network storage disk to configure the recording and snapshot plan to achieve the planned recording and snapshot.

- **User management**

You can manage multiple different users through the system administrator "admin" user and configure different permissions for each user.

- **Video playback**

Support the TF card or SD card to support the IP camera to support video playback, query and playback card recording.

- **Event detection function**

The IP camera supports ordinary event and Smart event.

- **Ordinary event**

Ordinary event include Motion Detection, Video Tampering, Exception, Alarm Input/Output, Audible alarm output, etc.

- **Smart event**

Smart event include Intrusion Detection, Enter Area, Leave Area, Line Cross Detection, Loiter Detection, People Gather Detection,etc.

- **Internet function**

IP camera support TCP/IP, ICMP, HTTP, HTTPS, FTP, DHCP, RTP, RTSP, NTP, SMTP, UDP, TCP, DNS, DDNS and other network communication protocols; support ONVIF2.4, CGI, mainstream manufacturers agreement and other Internet protocols.

- **Other function**
- **Wi-Fi function**

With Wi-Fi function camera, support wireless connection router Wi-Fi hotspot or with a hot wireless NVR. With Wi-Fi hotspot camera, support mobile phone connected camera Wi-Fi hotspots, preview IPC real-time video.

- **PTZ function**

The IP camera supports PTZ functionality support features such as lens zoom, pan/tilt control,

and cruise settings.

- **Cloud storage function**

The IP camera supports the cloud storage function, which can store the device's all-day recording on the cloud server and the motion detection alarm information on the cloud server.



NOTE

- IP camera above product features depending on the specific model, please take the actual product technical parameters shall prevail.

Chapter 2 Operating instructions

2.1 Network Connection

CAUTIONS

If you have access to the Internet at your own risk, including but not limited to the product may be subject to network attacks, hacker attacks, virus infection, the company does not cause the product abnormalities, information disclosure and other issues, but the company will In time to provide you with product-related technical support.

After the IP camera is installed, you can preview and configure related function parameters through the browser.

2.1.1 Wired network connection

Before configuring the IP camera, make sure that the IP camera is connected to the computer and that you can access the IP camera you want to set up. There are two types of wired connections; you can directly connect the IP camera to the computer with a network cable as shown in Figure 2-1:



Figure 2-1

Set IP camera over the LAN via a switch or a router as shown in Figure 2-2:



Figure 2-2

2.1.2 Wireless internet access

Some IP cameras support wireless network transmission, in the wireless network environment, the IP camera and computer connection as shown in Figure 2-3.



Figure 2-3

2.2 Detecting,Activate and Changing the IP Address

To access the IP address of a IP camera, proceed as follows:

Step 1: Search IPC IP address.

- Using the Search tool, you can search all the online cameras in the LAN and display the IP, MAC address, version, port and other information of the cameras, as shown in Figure2-4:

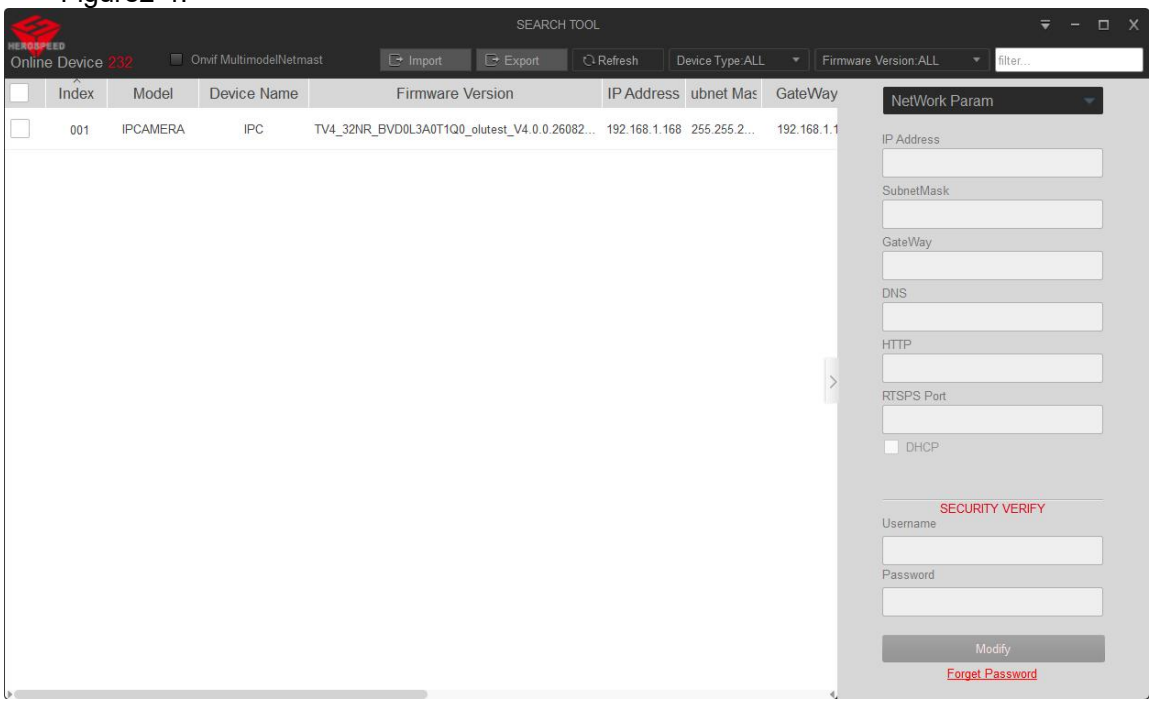


Figure 2-4

- Use the iVMS320/VMS247 client software to search for online devices. For details, refer to the iVMS320/VMS247 User Manual.

Step 2： Activate device.

- Select the device you wish to activate in the Search Tool, click "NetWork Param" on the right side of the interface, select "Activate" from the drop-down list, set a password, and click "Activate." When setting the network camera password, it must be 8 – 31 characters long and consist of a combination of at least two of the following types: numbers, lowercase letters, uppercase letters, and special characters. Security questions and a security email address are optional; if you wish to configure them later, you can do so via the web interface by navigating to Configuration > System > Safety >

User Management > Account Security Settings.

Step 3： Modify the IP address of the IP camera and connect the computer to the same network segment.

- In the Search Tool to select the device to modify the IP, right side of the interface directly modify the IP and gateway, enter the password, and click "Modify".

Step 4： Open the browser to enter the IP address of the camera, enter the web login screen.

NOTE

- When setting the IP address of the IP camera, please keep the device IP address and the computer IP address in the same LAN segment.
- The default IP address is 192.168.1.168 and the port number is 80.
- To access the IPC of different subnets, set the gateway of the IP camera after login. For details, see 8.3.1 Configuring TCP/IP.

2.3 Setting the IP camera over the WAN

This section explains how to connect the IP camera to the WAN with a static IP or a dynamic IP.

2.3.1 Static IP Connection

Before you start:

Please apply a static IP from an ISP (Internet Service Provider). With the static IP address, you can connect the IP camera via a router or connect it to the WAN directly.

- **The router is connected to the IP camera as shown in Figure 2-5:**

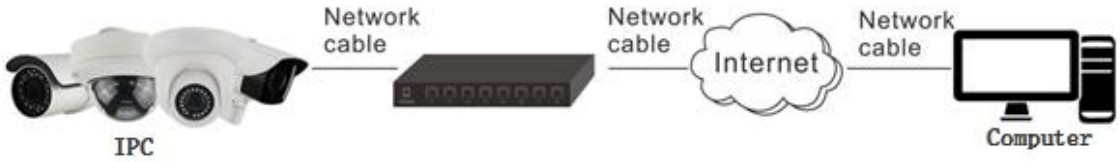


Figure 2-5

Specific steps are as follows:

Step 1： Connect the IP camera to the router.

Step 2： Assign a LAN IP address, the sub net mask and the gateway. For details, please refer to 8.3.1.

Step 3： Save the static IP in the router.

Step 4： Set port mapping, e.g., 80, 8000, and 554 ports. The steps for port mapping vary according to the different routers. Please call the router manufacturer for assistance with port mapping.

Step 5： Visit the IP camera through a web browser or the client software over the internet.

- **Directly through the static IP connection IPC, as shown in Figure 2-6:**

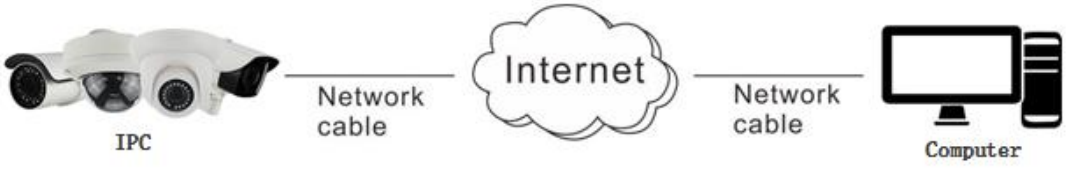


Figure 2-6

You can also save the static IP in the camera and directly connect it to the internet without using a router. For details, please refer to 8.3.1.

2.3.2 Dynamic IP Connection

Before you start:

Please apply a dynamic IP from an ISP. With the dynamic IP address, you can connect the IP camera to a modem or a router.

- **The router is connected to the IP camera**

Specific steps are as follows:

Step 1： Connect the IP camera to the router.

Step 2： Assign a LAN IP address, the sub net mask and the gateway. For details, please refer to 8.3.1.

Step 3： In the router, set the PPPoE user name, password and confirm the password.

Step 4： Set port mapping, e.g., 80, 8000, and 554 ports. The steps for port mapping vary according to the different routers. Please call the router manufacturer for assistance with port mapping.

Step 5： Apply a domain name from a domain name provider.

Step 6： Configure the DDNS settings in the setting interface of the router.

Step 7： Visit the camera via the applied domain name.

NOTE

- The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after rebooting the camera. To solve the inconvenience of the dynamic IP, you need to get a domain name from the DDNS provider (E.g. DynDns.com). Please follow the steps below for normal domain name resolution and private domain name resolution to solve the problem.

- **Normal Domain Name Resolution as shown in Figure 2-7:**

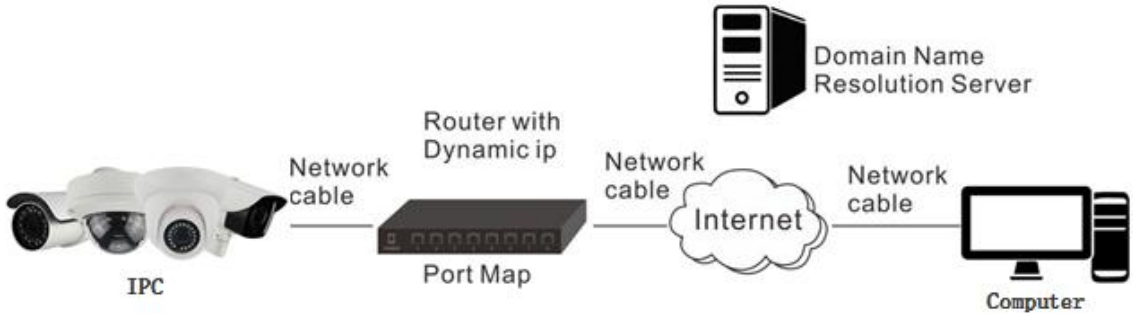


Figure 2-7

Specific steps are as follows:

Step 1: Apply a domain name from a domain name provider.

Step 2: Configure the DDNS settings in the DDNS Settings interface of the IP camera. For details, please refer to 8.3.1.

Step 3: Visit the camera via the applied domain name.

- **Private Domain Name Resolution, as shown in Figure 2-8:**

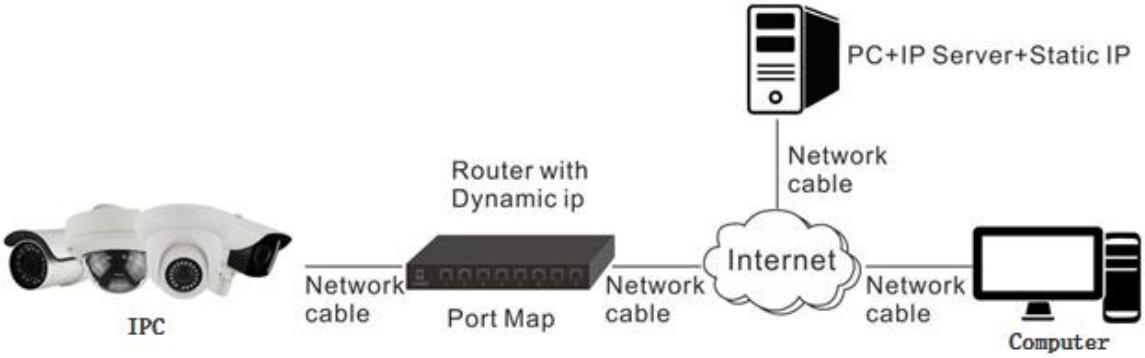


Figure 2-8

Specific steps are as follows:

Step 1: Install and run the IP Server software in a computer with a static IP.
Step 2: Access the IP camera through the LAN with a web browser or the client software.
Step 3: Enable DDNS and select IP Server as the protocol type. For details, please refer to 8.3.1.

Chapter 3 Access to the IPC by Client Software

The iVMS320/VMS247 client software is available on the company website (www.herospeed.net). You can use this software to view live video and manage IPC. Follow the installation prompts to install the software. The control panel and real-time view interface of the iVMS320/VMS247 client software are shown in Figure 3-1.

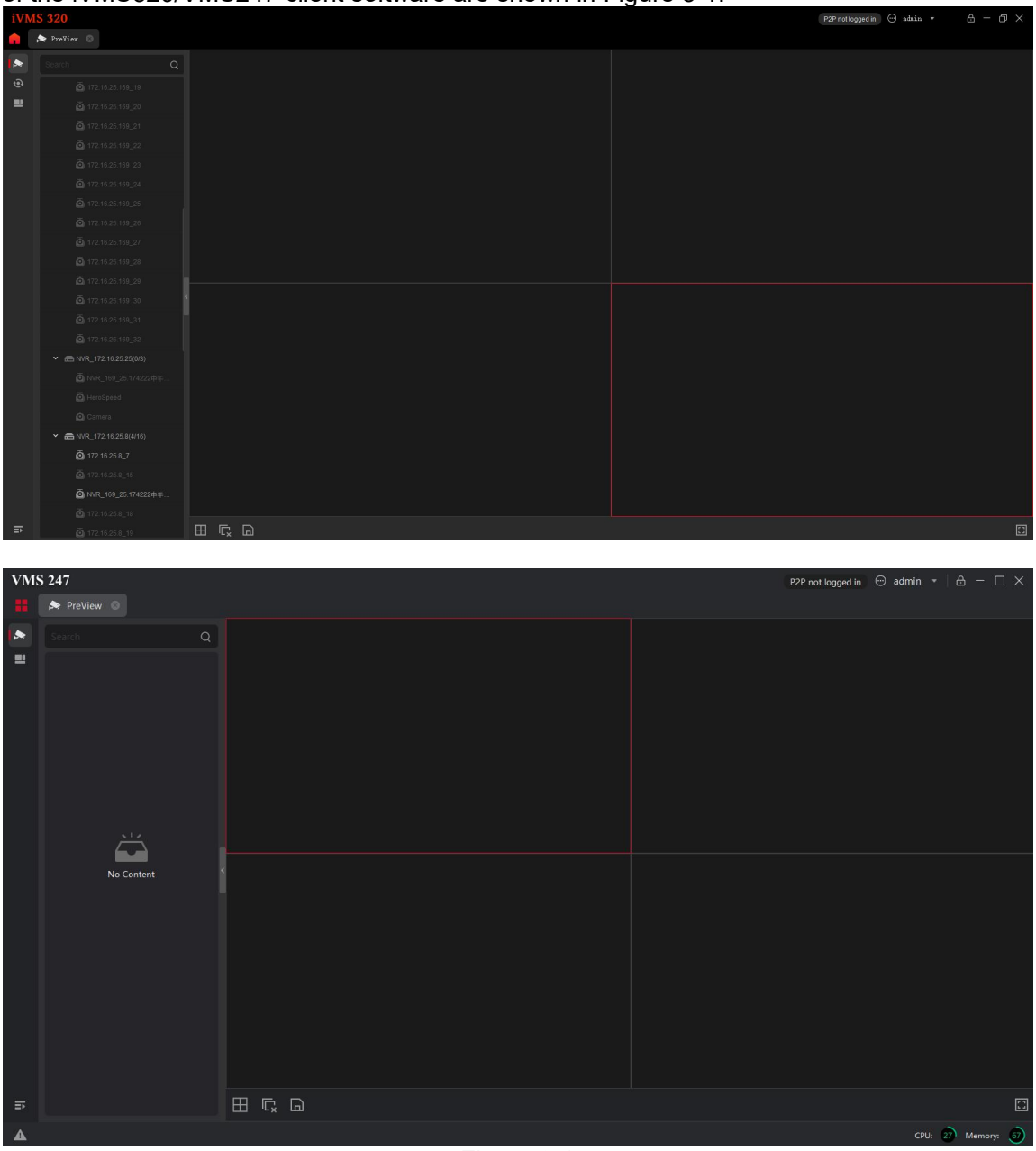


Figure 3-1

NOTE

- For detailed information about the software, please refer to the user manual of the iVMS 320/VMS247 Client Software.
- Please activate IPC before connecting to the client.

Chapter 4 Access to the IPC by Web Client

4.1 Preparation before install plugin

In ensuring the IPC and the current user's computer after completion of all the hardware connection and power equipment normal, open the computer, run ping the IP address of the IPC (NOTE the IP address of the IPC in LAN must be unique). Such as IPC IP for 192.168.1.168, run ping 192.168.1.168. If the network IPC responds as shown in Figure 4-1, it indicates that the network connection is normal, you can open a browser to log in to the webcam web page.

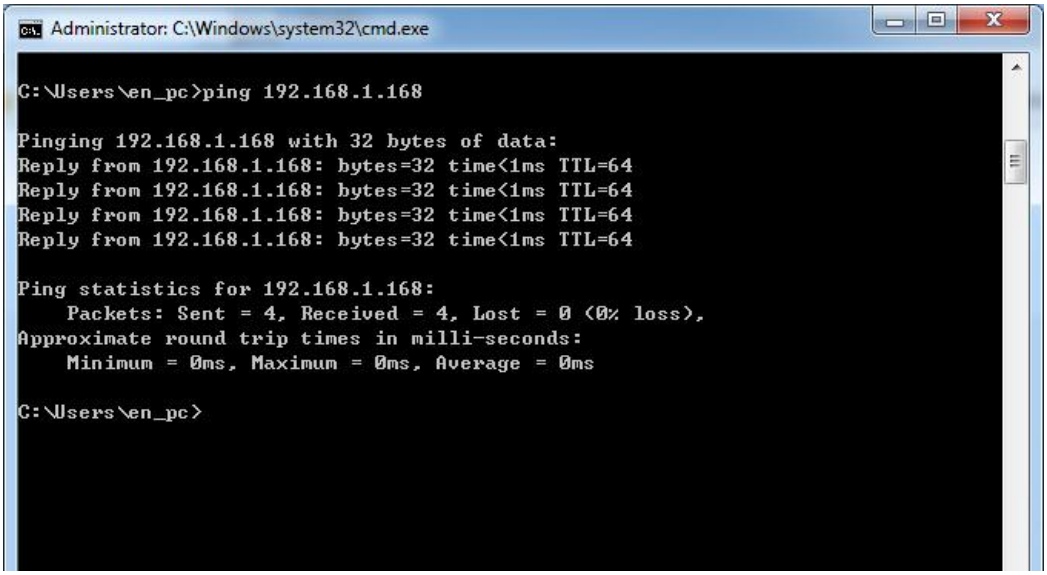


Figure 4-1

4.2 Activate,Login and Exit

4.2.1 Activate

Open a browser on your computer and enter the IPC address in the web address bar (the default address used for the first time is: http://192.168.1.168) to enter the device activation interface, as shown in Figure 4-2.

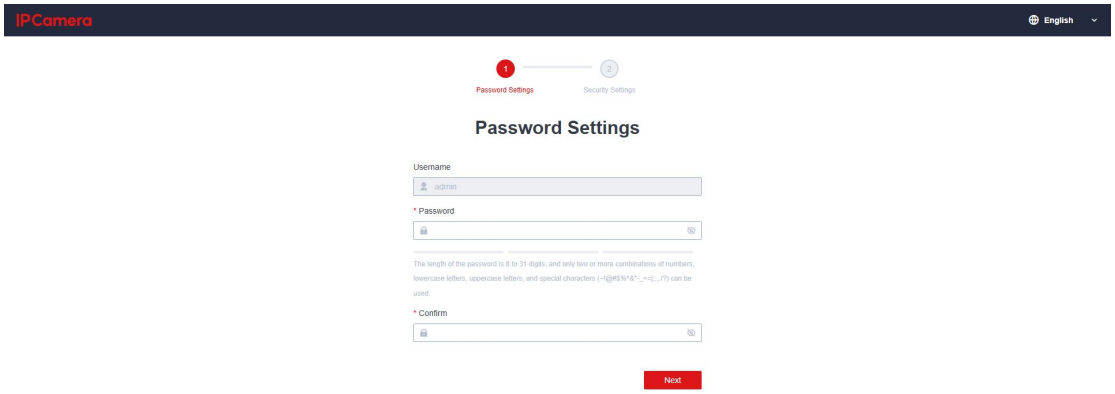


Figure 4-2

After setting the password, click "Next" to enter the security settings interface, as shown in Figure 4-3 below. You can select the desired options or click "Skip", if you wish to configure or modify security settings later, you can do so by navigating to "Configuration > System > Safety > Account Security Settings".

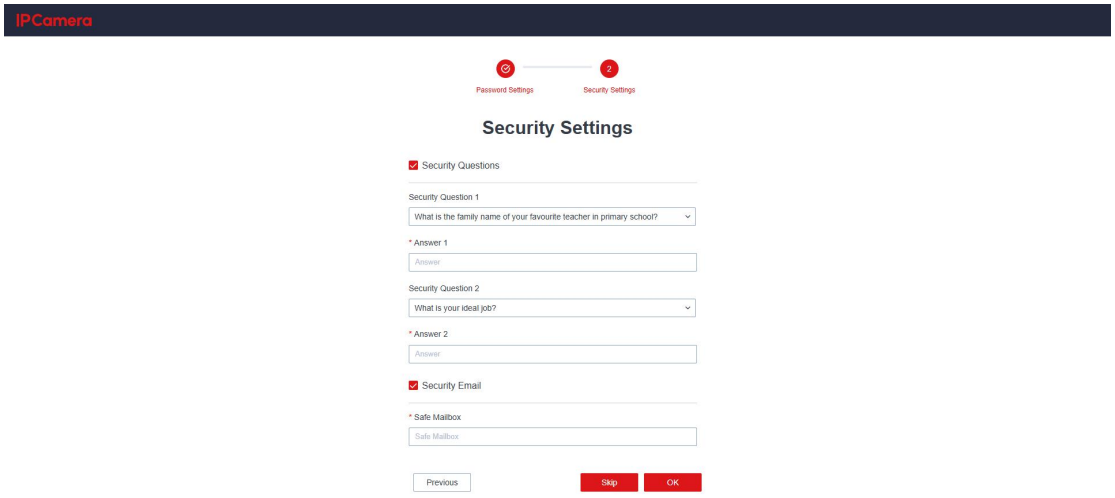


Figure 4-3

4.2.2 Login

After activating the device, enter the login interface, as shown in Figure 4-4.

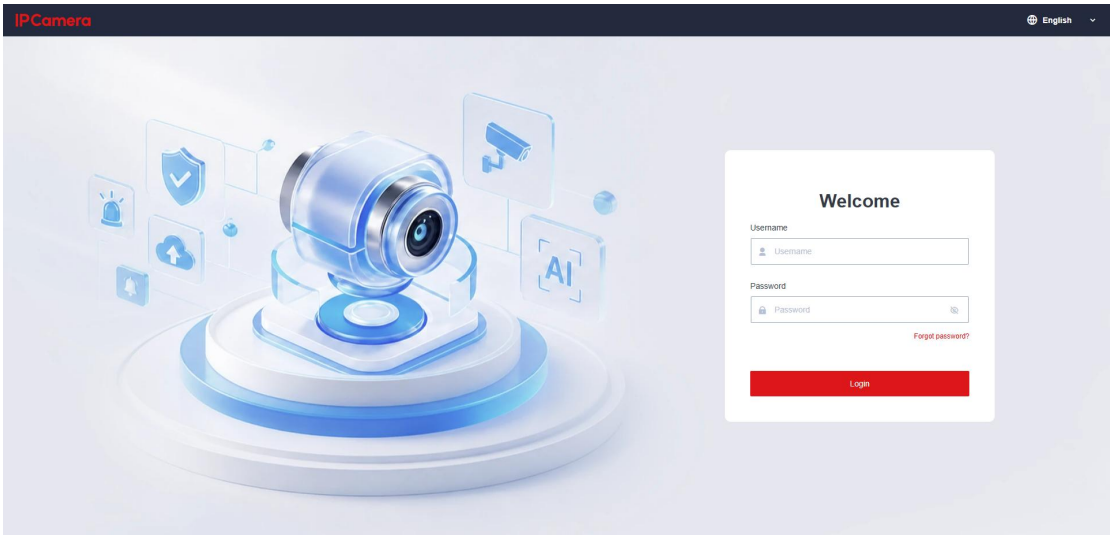


Figure 4-4

Select system language (Simplified Chinese, Traditional Chinese, English, Ukrainian, Korean, Polish, French, Japanese, Spanish, Portuguese, Italian, Hebrew, Arabic, Thai, Vietnamese, Hungarian,Czech are supported), enter the username and password: click "login".

NOTE

- If you have modified the IP address of the IP camera, please log in with the newly set IP address.

4.2.2 Change password

After successful login, if your password is too simple,the interface prompts to change the password, as shown in Figure 4-5:

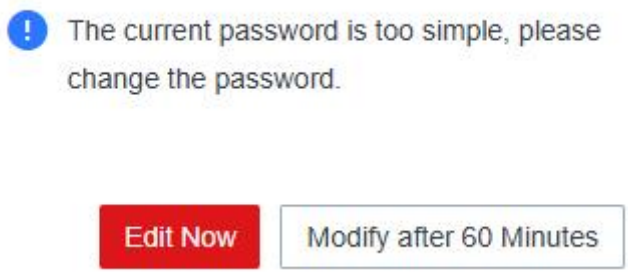


Figure 4-5

For the account security recommendations click "Edit Now", enter the user interface to modify the password, as shown in Figure 4-6:

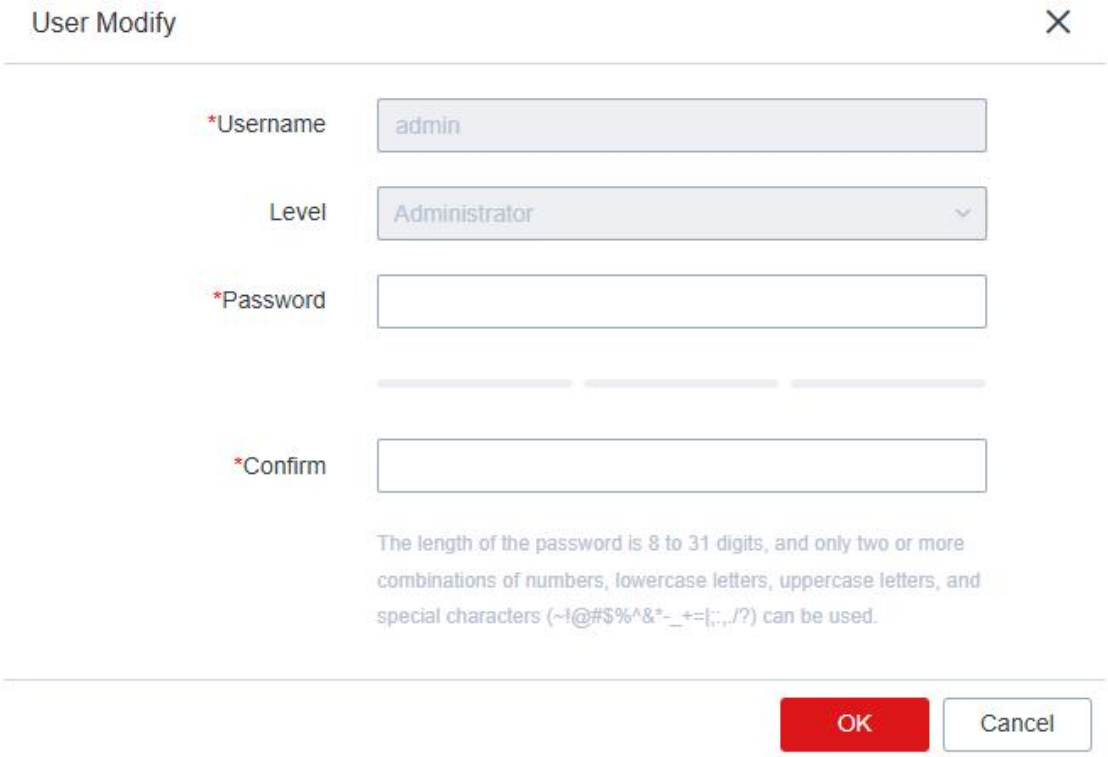


Figure 4-6

To change your password, follow these steps:

Step 1: Enter the new password in the Password and Confirm Password fields;

Step 2: Click "OK" to complete the password modification.

NOTE

- When setting a new password, you must set at least 8 digits and contain both letters and numbers to set it successfully.
- When the IPC password is "123456", each time you log in, you will be prompted to change the password. You can select "Modify after 60 Minutes". After 60 minutes, the interface will automatically pop up the password modification interface.

4.2.3 Forget password

When you forget your password, you can reset the password in three ways: Security Question Verification and E-mail Verification.

Security question verification

Step 1: On the login interface, click "Forgot password?", you can choose between two methods on the identity verification screen. (as shown in Figure 4-7 ①)

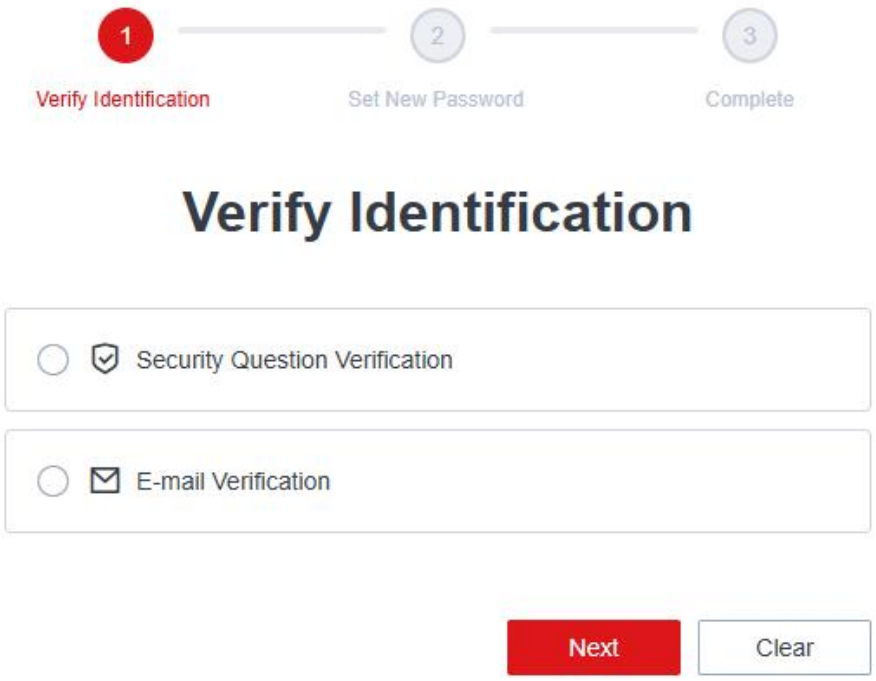


Figure 4-7 ①

Step 2: Select the verification method as "Security Question Verification" (as shown in Figure 4-7 ②), enter the answers to security questions 1 and 2, and click "Next".

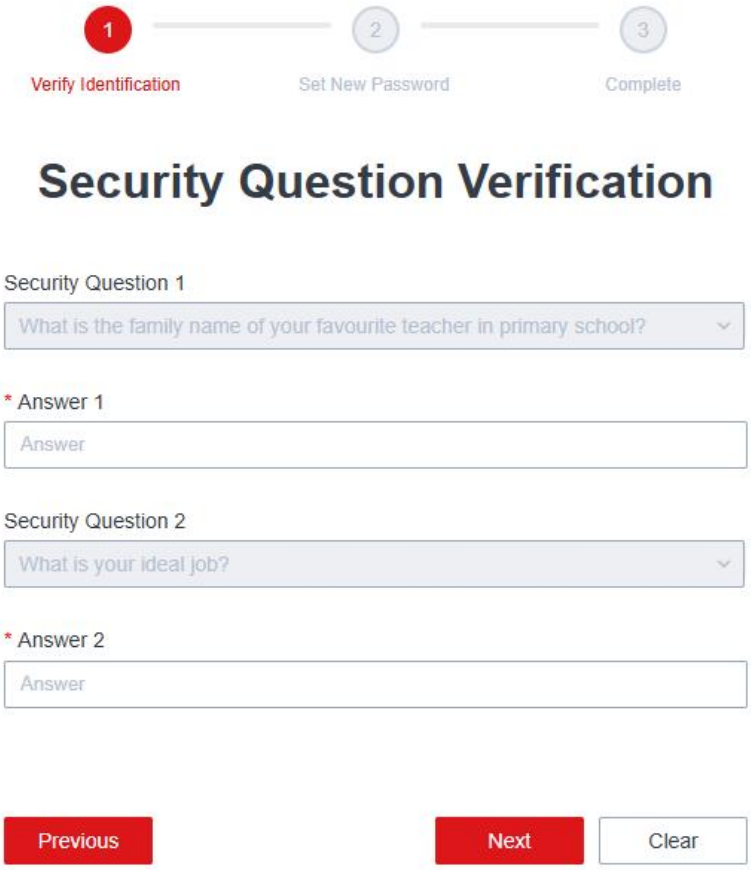


Figure 4-7 ②

Step 3: Enter the new password and confirm the password (as shown in Figure 4-7 ③), and click "Next".

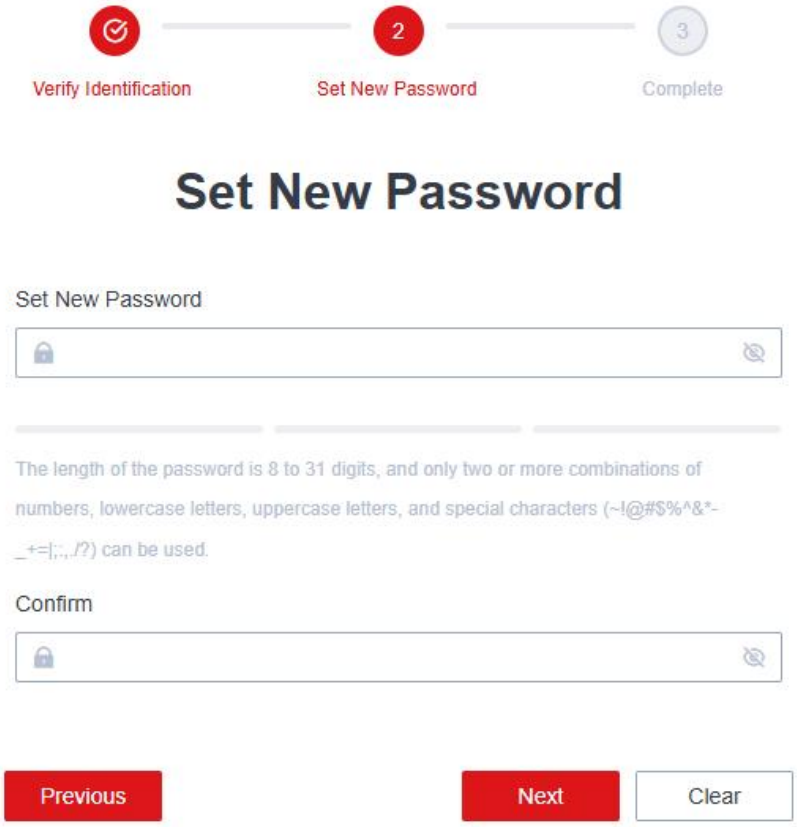


Figure 4-7 ③

Step 4: Click "Re-register" to return to the login interface (as shown in Figure 4-7 ④).

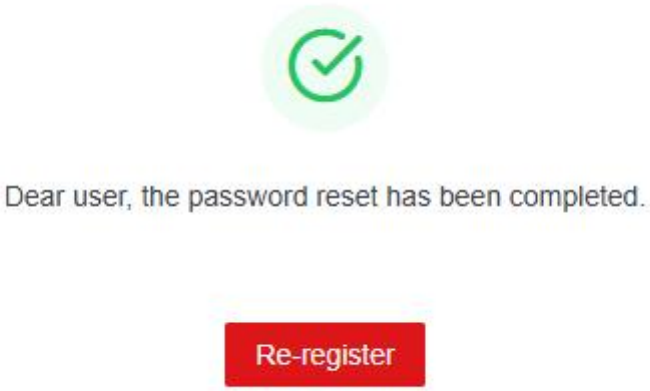


Figure 4-7 ④

Secure Email Verification

Step 1: On the login interface, click "Forgot password?", you can choose between two methods on the identity verification screen. (as shown in Figure 4-8 ①)

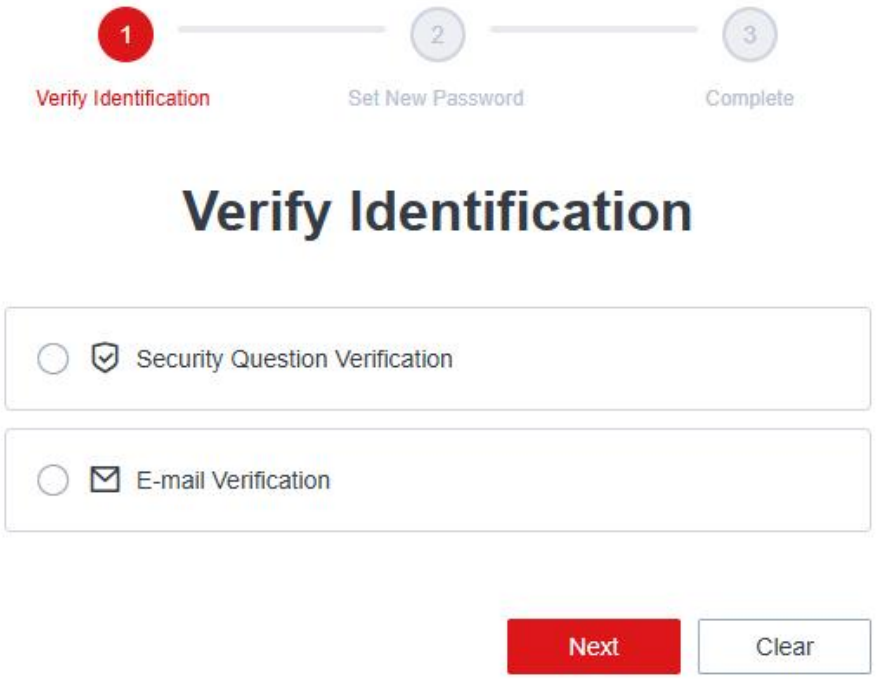


Figure 4-8 ①

Step 2: Select the verification method as "E-mail Verification" (as shown in Figure 4-8 ②).

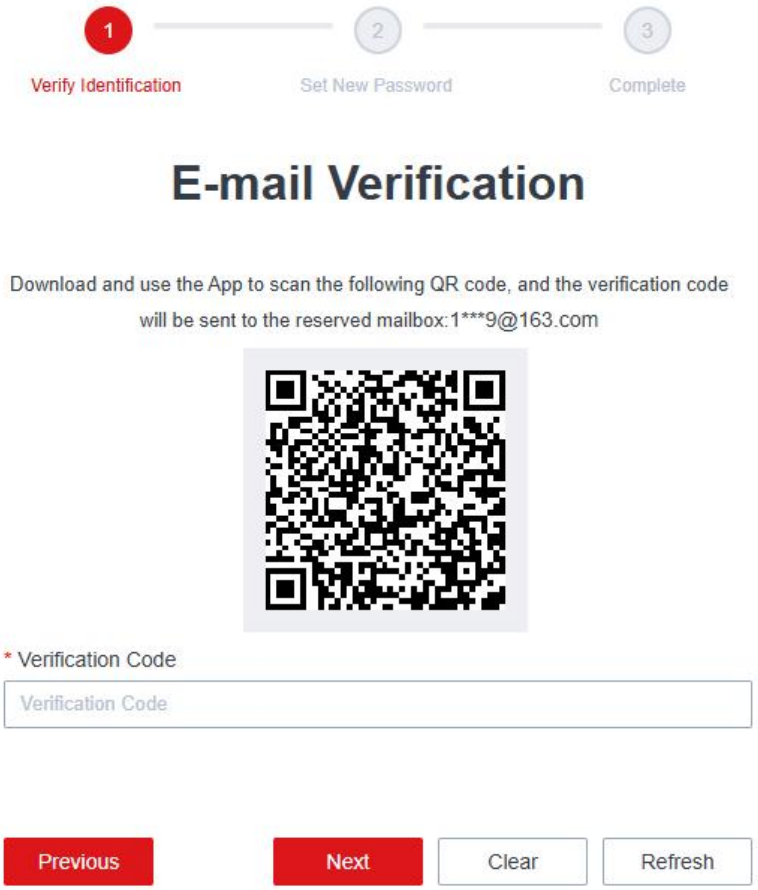


Figure 4-8 ②

Step 3: Use the APP to scan the QR code, get the verification code from the security mailbox and enter it, then click "Next".

Step 4: Enter the new password and confirm the password (as shown in Figure 4-8 ③), and click "Next".

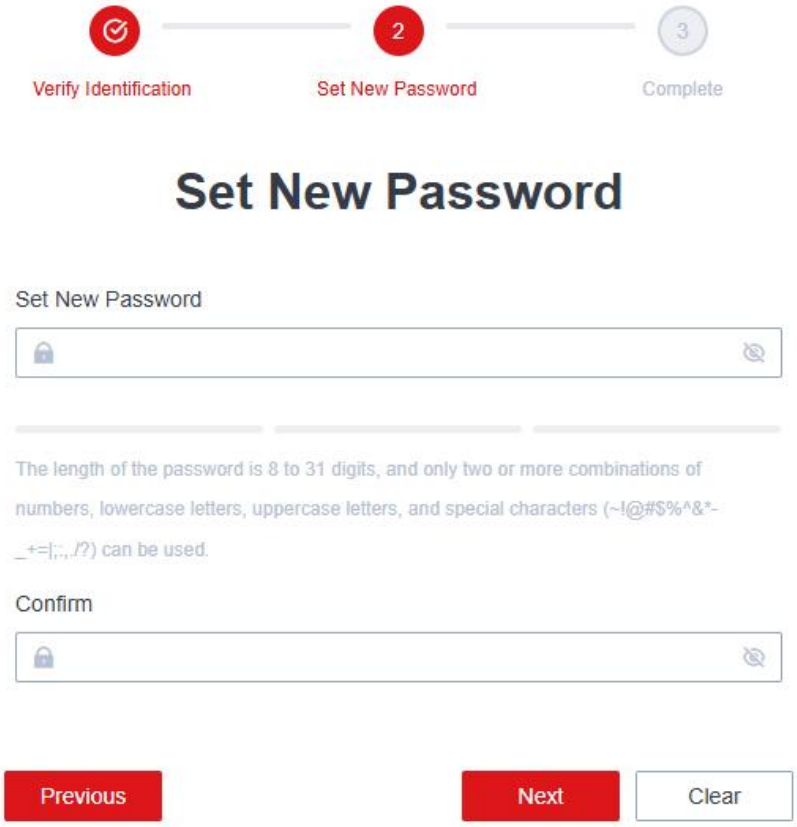


Figure 4-8 ③

Step 5: Click "Re-register" to return to the login interface (as shown in Figure 4-8 ④).

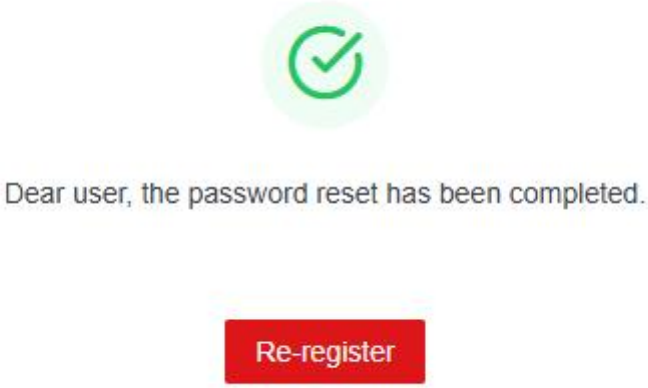


Figure 4-8 ④

NOTE

- When setting a new password, you must set at least 8 digits and contain both letters and numbers to set it successfully.
- You can only retrieve your password through the security question after setting it.
- You can only retrieve your password through the security mailbox after setting it.

4.2.4 Exit System

When you enter the IP camera main interface, you can click the upper right corner of the "" safe exit system.

4.3 Install the LsIPCPlugin Controls

NOTE

- When you use Chrome browser or 360 browser, you need to download and install the controls after login.
- The plugin of smart IP camera is "LsIPCPlugin".

Open Google-Chrome and log in to IPC to enter the preview interface, as shown in Figure 4-9.

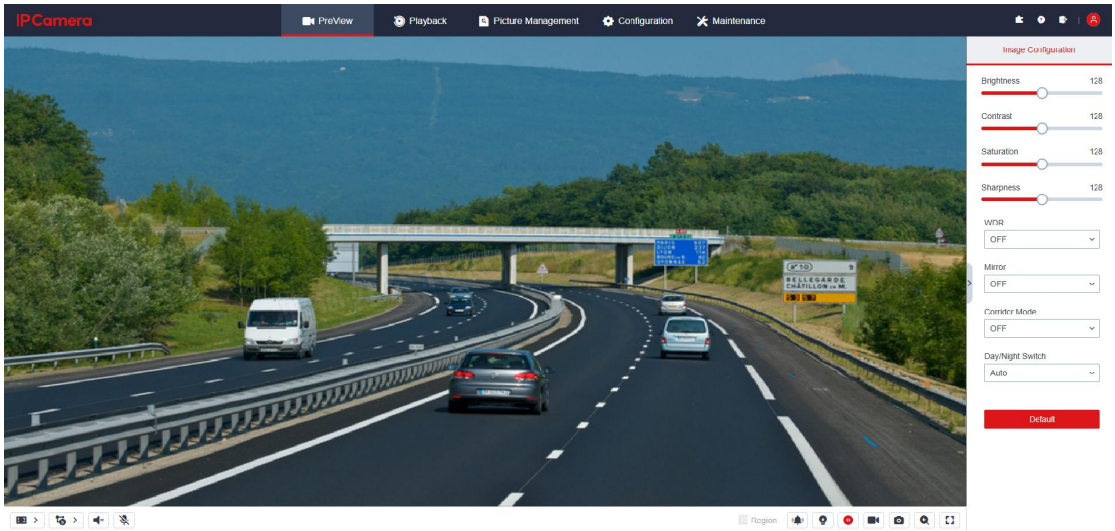


Figure 4-9

Click "Download Plug-in" in the upper right corner, select the control storage path, click "Download", click "Open", select "English" → "OK" → "Next" → "Next" → "Next" → "Install" → "Finish" in Figure 4-10 (①、②、③、④、⑤、⑥) to complete the installation:

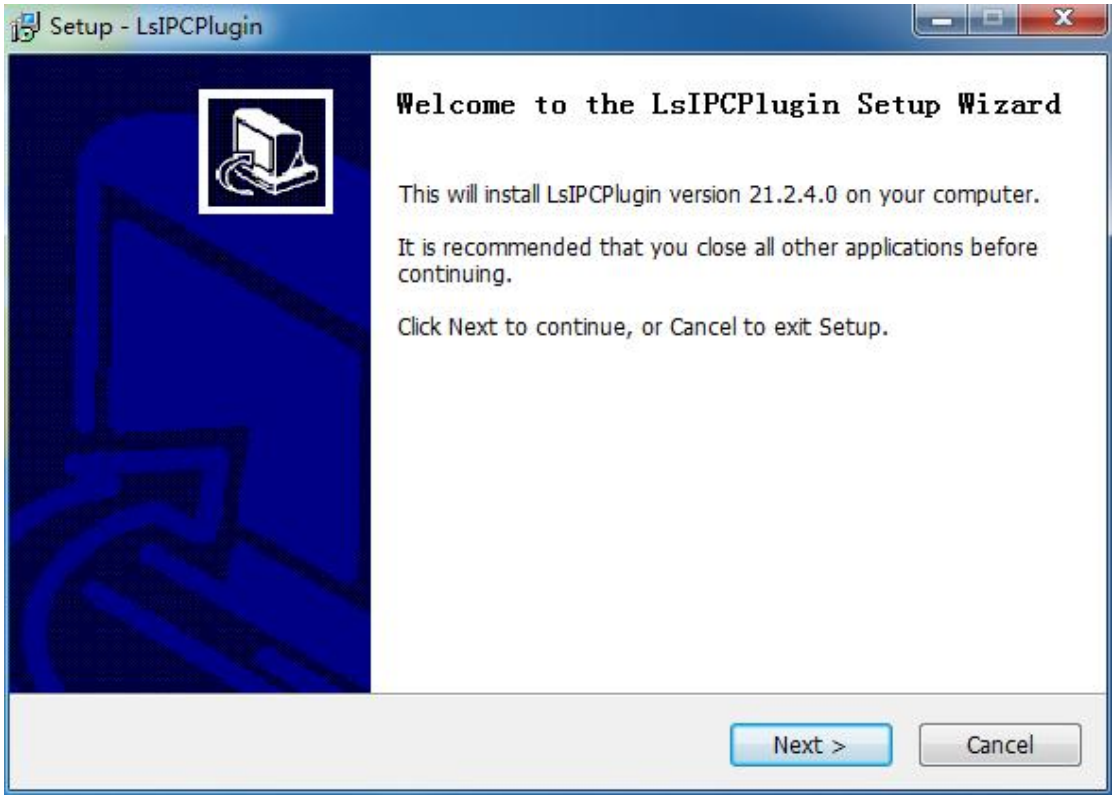


Figure 4-10 ①

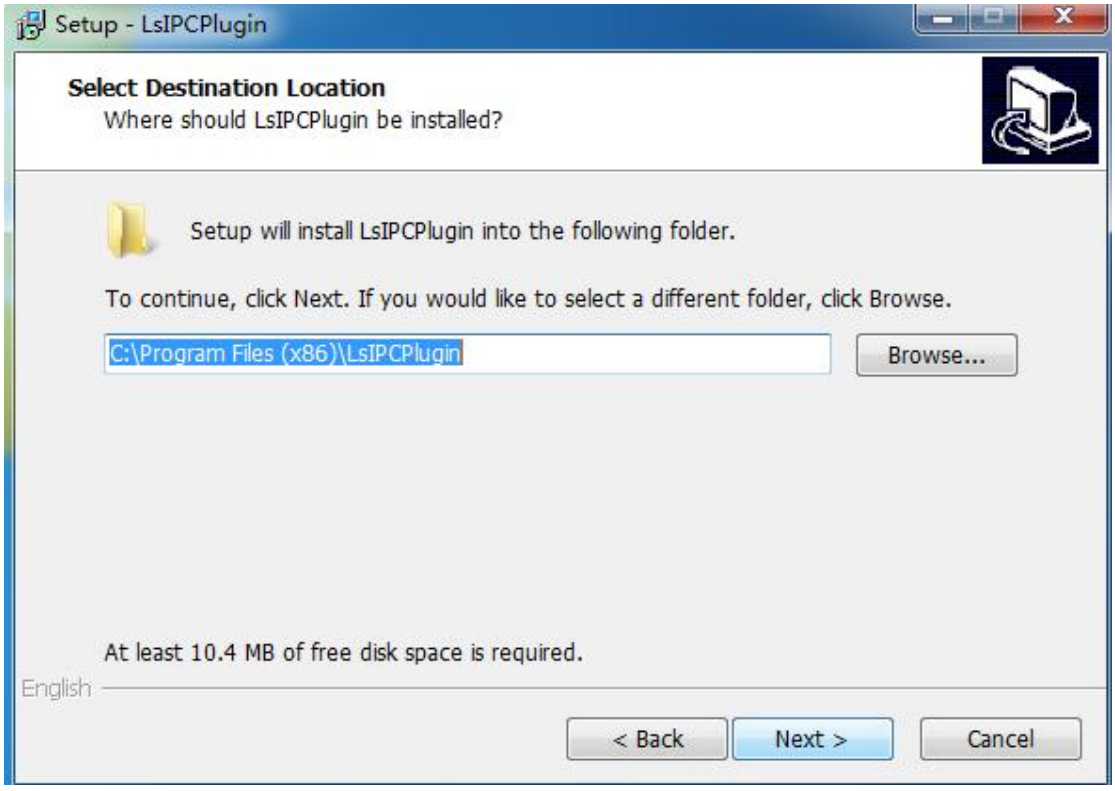


Figure 4-10 ②

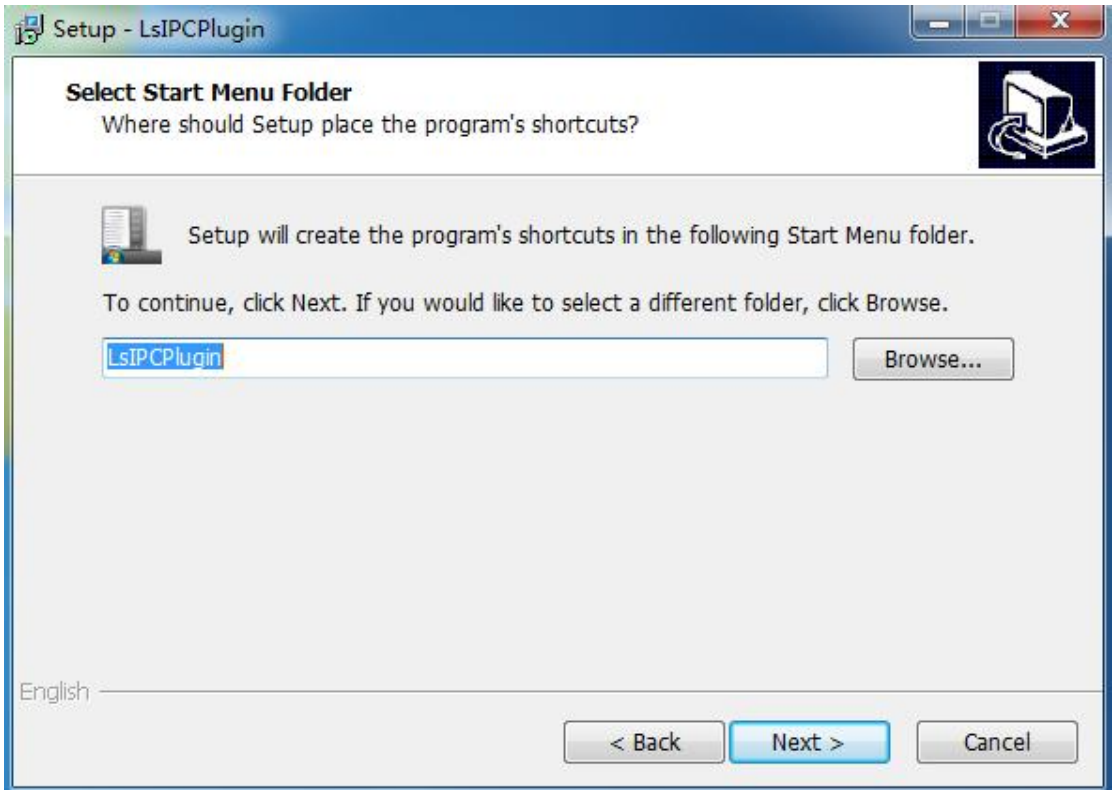


Figure 4-10 ③

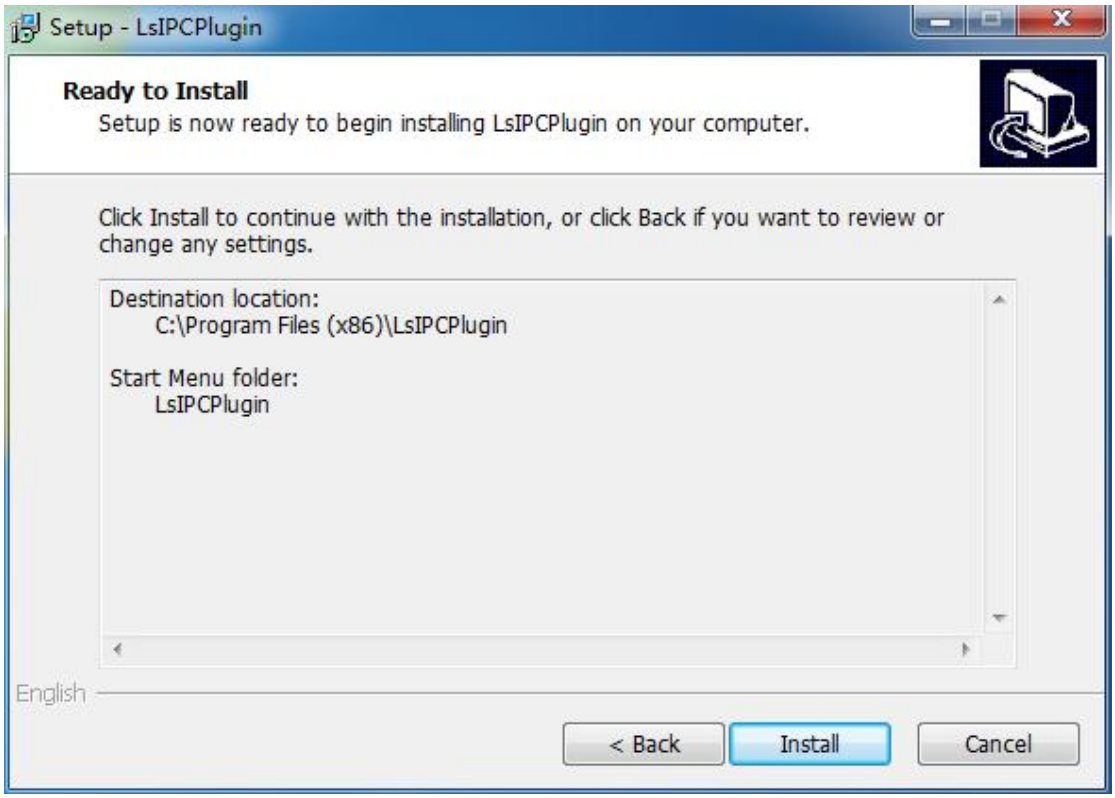


Figure 4-10 ④

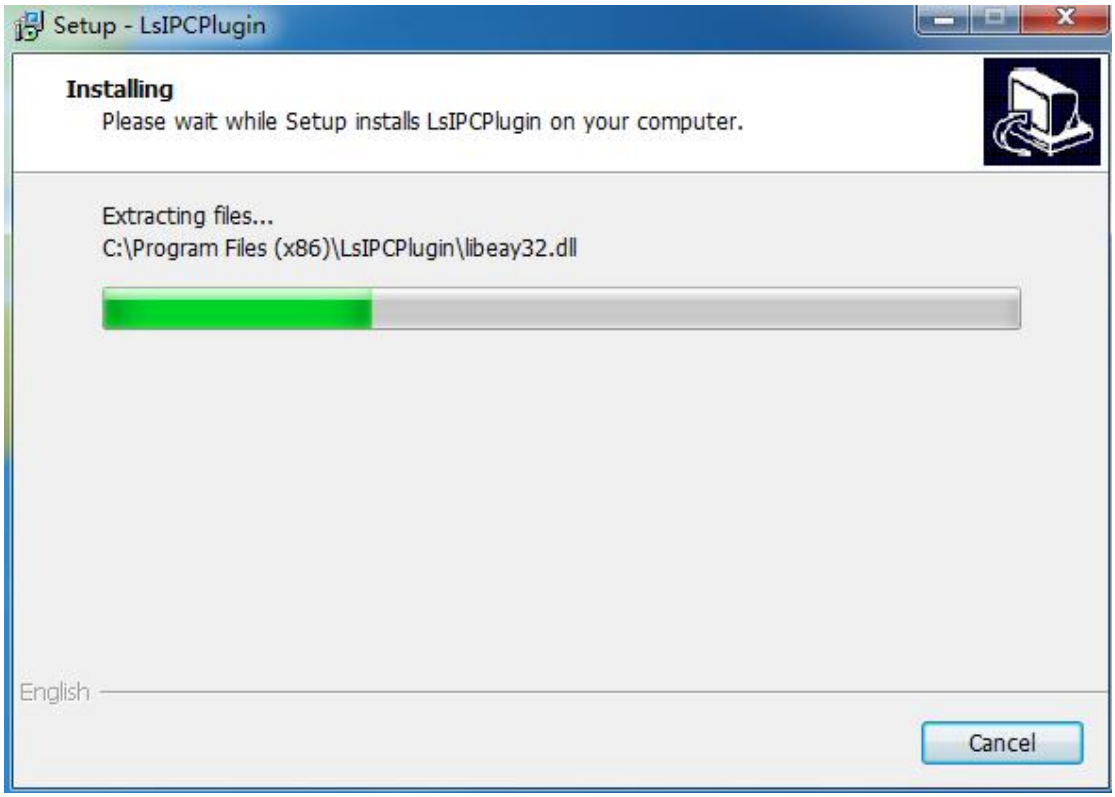


Figure 4-10 ⑤

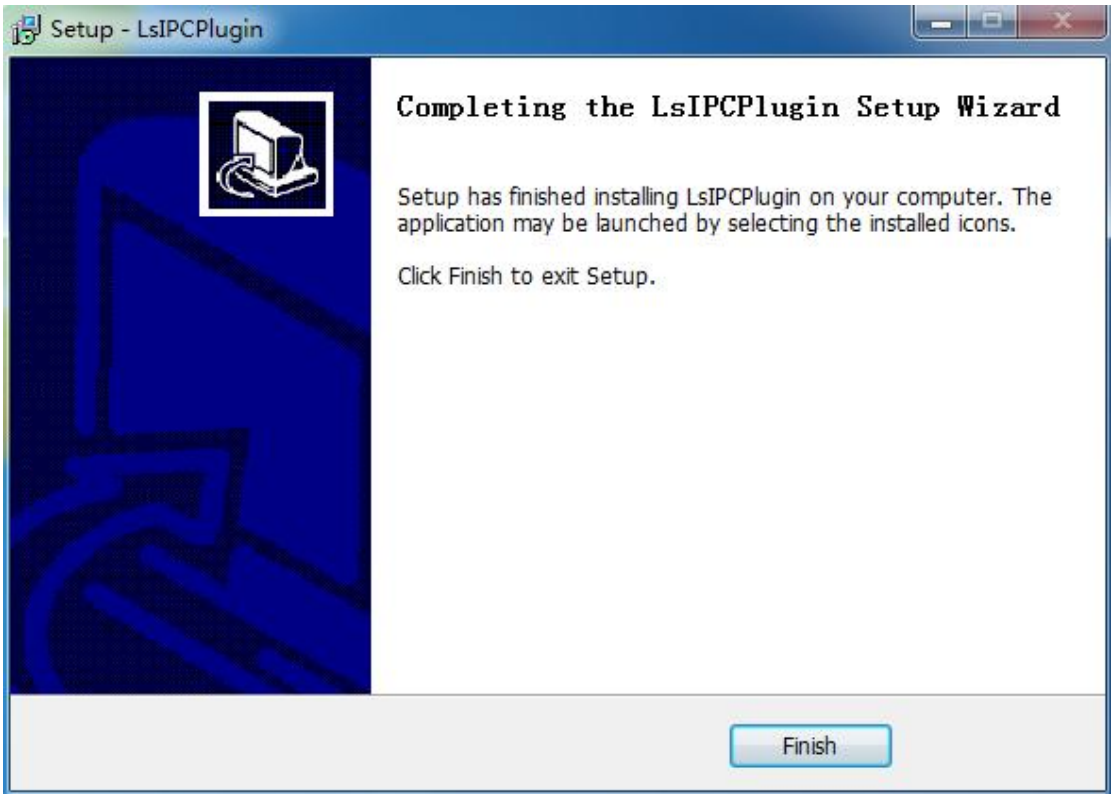


Figure 4-10 ⑥

Notice

If the system prompt "installation failure", please uncheck the "cancel protection mode" in the setting safety of "Internet options" and enter the "custom level" ActiveX control Settings as show in Figure 4-10, and reinstall LsIPCPlugin after save settings.

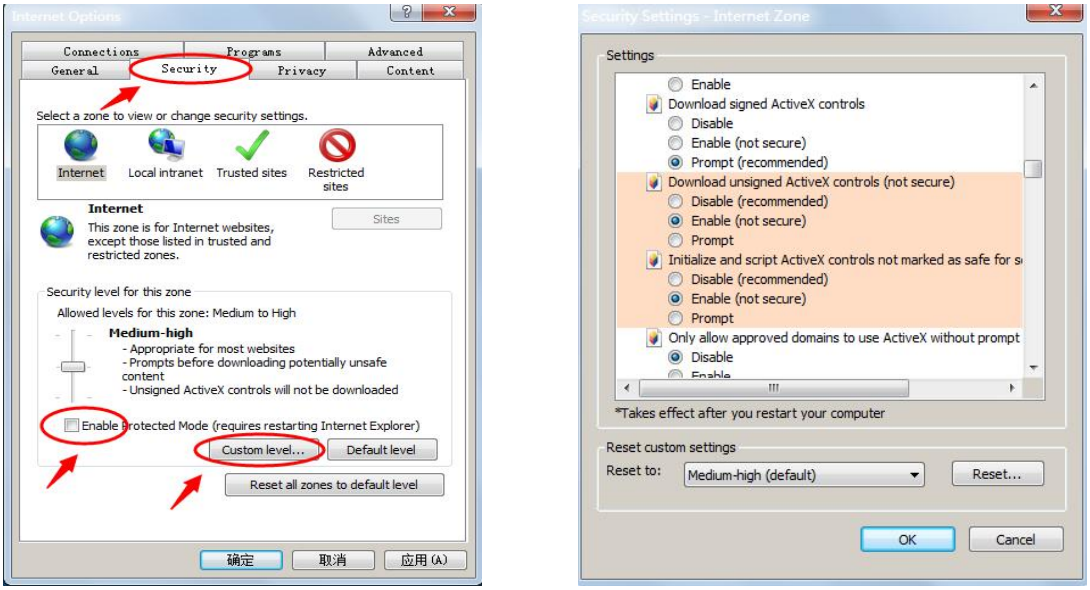


Figure 4-11

4.4 Main interface description

In the IPC main interface, you can preview real-time video, playback, configuration and Maintain and other functions, the interface shown in Figure 4-12:

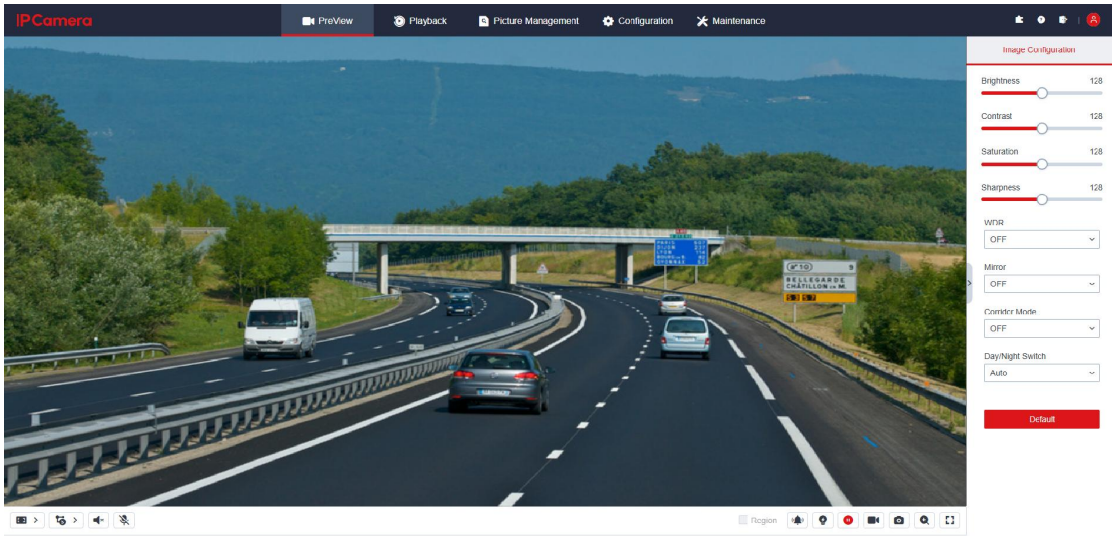


Figure 4-12

【PreView】 For IPC monitoring screen preview, you can switch the code stream preview, preview can also be achieved video, capture, electronic zoom and other functions.

【Playback】 Select the time or video type to find the device TF card in the video and playback.

【Picture Management】 Used to query, view and download image files stored in the IP camera EMMC/TF card.

【Configuration】 Click into the IPC configuration interface for system configuration and function configuration.

【Maintenance】 Used to view device information, upgrade, restore default, maintain, import and export parameters, log query.

【Image Config】 Used to set image parameters, WDR, mirroring, corridor mode, day and night conversion，etc.

NOTE

- IP camera main interface layout function and other information, please take the actual equipment function prevail.

Chapter 5 PreView

5.1 PreView

Click "

" to enter the IPC preview interface, as shown in Figure 5-1:

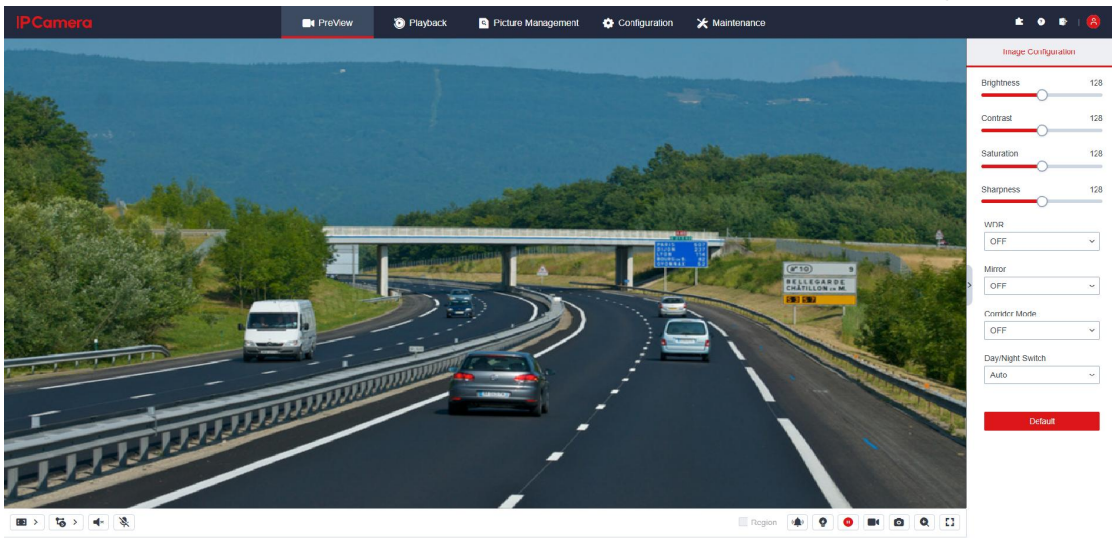


Figure 5-1

【switching window size】In the real-time preview interface on the bottom left of the preview ratio option, click "4: 3", "16: 9", "1:1", "full screen" to switch the video preview scale.

【switching option】Select live preview stream on the bottom left of the real-time preview interface.

The preview interface operation buttons are shown in Table 5-1.

Icon	Description
	The window size is 32:9.
	The window size is 4:3.
	The window size is 16:9.
	The preview screen is displayed in its original size.
	Self-adaptive window size.
	To switch the real-time preview stream.
	Start/Stop live view.
	Manually start/stop recording.

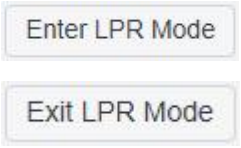
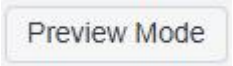
	Manually capture the picture.
	Turn on / off the electronic zoom function, turn on the electronic zoom function, in the preview image, hold down the left mouse button to select the electronic zoom area, the interface shows the region to enlarge the image.
	Turn on/off Sound.
	Open / Close talk back.
	Turn on/off EPTZ.
	Used to adjust parameters supporting PTZ IPC and switch between license plate recognition and non-license plate recognition modes.
	Enter/exit LPR preview mode.
	You can select to display the alert zones for currently configured and enabled events.
	The video stream will be displayed in different preview modes depending on the set bitrate mode. The playback window can be used to view the video stream preview in different preview modes.
	Clicking will activate a light alarm, which will last for 10 seconds.
	Clicking will activate a sound alarm, which will last for 10 seconds.
	Clicking will play the video in full screen.

Table 5-1

5.2 Image Parameters

In the real-time preview interface, you can quickly set the commonly used image parameters. Click "Image Configuration" on the right to enter the commonly used image parameter configuration page, as shown in Figure 5-2:

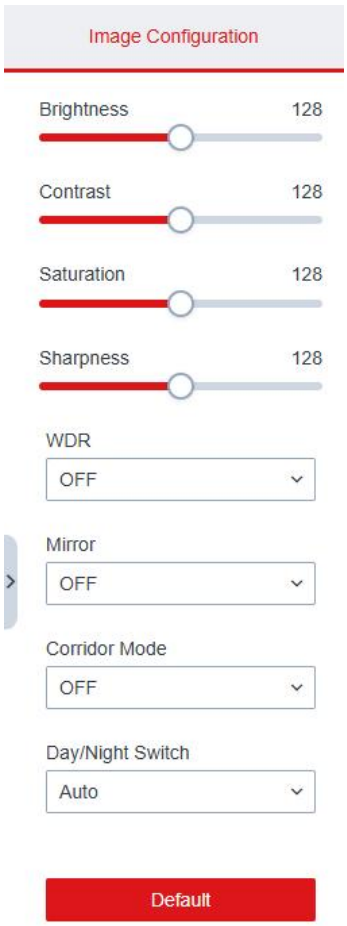


Figure 5-2

Supports quick configuration of brightness, contrast, saturation, sharpness, wide dynamic range, mirror, corridor mode, day and night mode, and can restore the default values of the configuration items on this page.

NOTE

For specific setting options and instructions, please refer to the corresponding chapter 8.5.

5.3 PTZ Control

In the preview interface of AF camera and PTZ camera, click "PTZ" to enter the PTZ control page, where you can set the pan/tilt rotation direction of the camera, zoom in/out, focus -/focus +, one-key focus, lens initialization, and cruise, as shown in Figure 5-3:

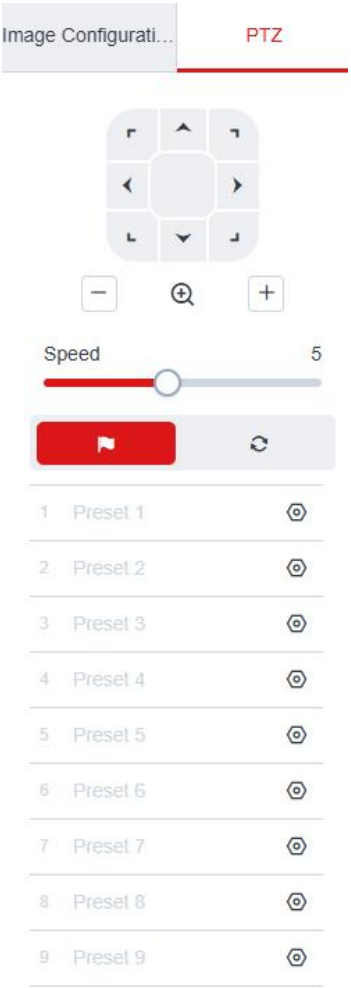


Figure 5-3

The description of the PTZ control interface operation buttons is as follows: Table 5-2:

图标	说 明
	PTZ steering, control the direction of the PTZ rotation, support up, down, left, right, upper left, lower left, upper right, lower right direction control.
	Zoom +/Zoom -, when you press and hold the "Zoom -" key, the lens zooms out and the scene becomes smaller; when you press and hold the "Zoom+" key, the lens zooms in and the scene is enlarged.
	Focus +/Focus -, in manual focus mode, click "Focus -" to make nearby objects clear, and click "Focus +" to make distant objects clear.
	Aperture +/Aperture -: When the monitoring screen is relatively dark, in the exposure mode of Aperture Priority or Manual mode, click "Aperture +" to increase the aperture, and click "Aperture -" to reduce the aperture.

Speed 5	PTZ speed adjustment: On models equipped with motorized lenses, the gimbal speed can be adjusted to change the rotation speed of the gimbal.
	One-touch focus to manually focus the lens.
	Human tracking: after detecting a human figure, it can automatically track.
	Initialize the lens, initialize the lens parameters.
	Preset point button to switch to the preset point management page.
	Cruise route button to switch to the cruise route management page.

Table 5-2

5.4 License Plate Recognition Mode

For network cameras that support license plate recognition, click "PTZ & License Plate Recognition" in the preview interface to enter the corresponding operation window. Click the "Enter License Plate Recognition Mode" button to enter the license plate recognition preview mode (mainly applicable to access control scenarios). In this mode, the preview window will be divided into a playback area, a capture area, and a list area. In addition to normal preview operations such as playback/stop, image capture, and local recording, you can also perform operations such as warning area display, manual recognition, and standard license plate recognition configuration, as shown in Figure 5-4 below.

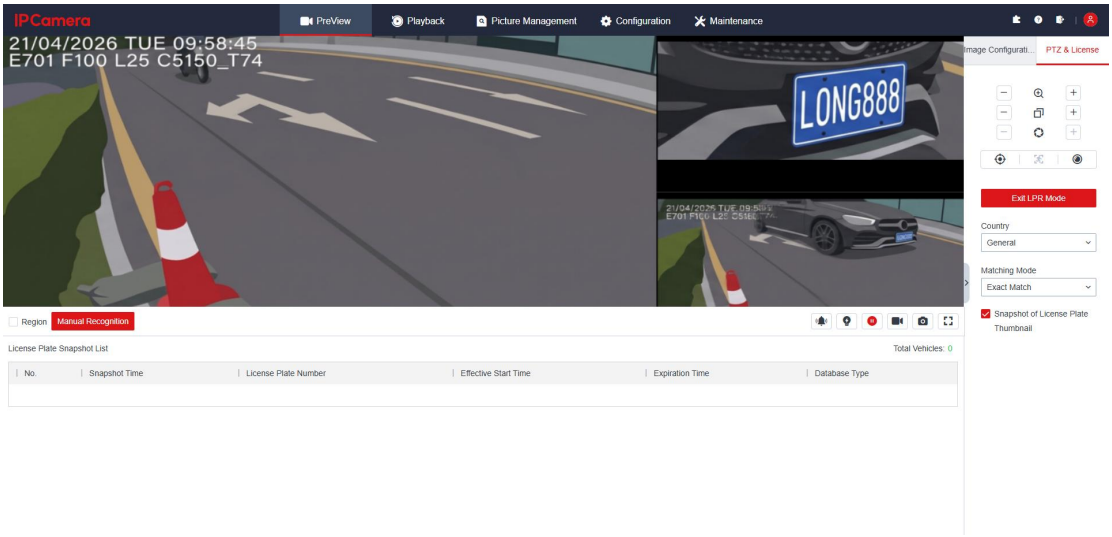


Figure 5-4

【Region】Checking the "Region" box will display alert zones for enabled and configured events; unchecking the box will disable their display.

【Manual Recognition】If the device fails to recognize the license plate automatically or if the recognition result differs from the manual judgment, clicking the "Manual Recognition" button will allow for a single manual license plate recognition attempt.

【Country】This setting allows you to filter license plates based on their country of origin, improving recognition accuracy.

【Matching Mode】Used to set the matching mode. The default is exact matching, and fuzzy matching is optional. You can set the number of characters allowed to be mismatched, with a default of 1, 2, or 3. Fuzzy matching is performed based on the set number of characters allowed to be mismatched. Characters within the set number of mismatched characters can be identified and compared.

【Snapshot of License Plate Thumbnail】This setting determines whether to capture license plate images. Checking this box will capture an image of the license plate during license plate recognition and display it in the corresponding window. Unchecking this box will neither capture nor display an image.

5.5 Preview Mode

The fisheye camera allows switching between preview modes in the preview interface. Different preview modes are supported for different stream mode. The preview mode operation bar on the left side of the preview interface (expanded by default, can be hidden) displays different preview modes according to the set stream mode. The playback window shows the video stream previews for different preview modes, as shown in Figure 5-5 below.

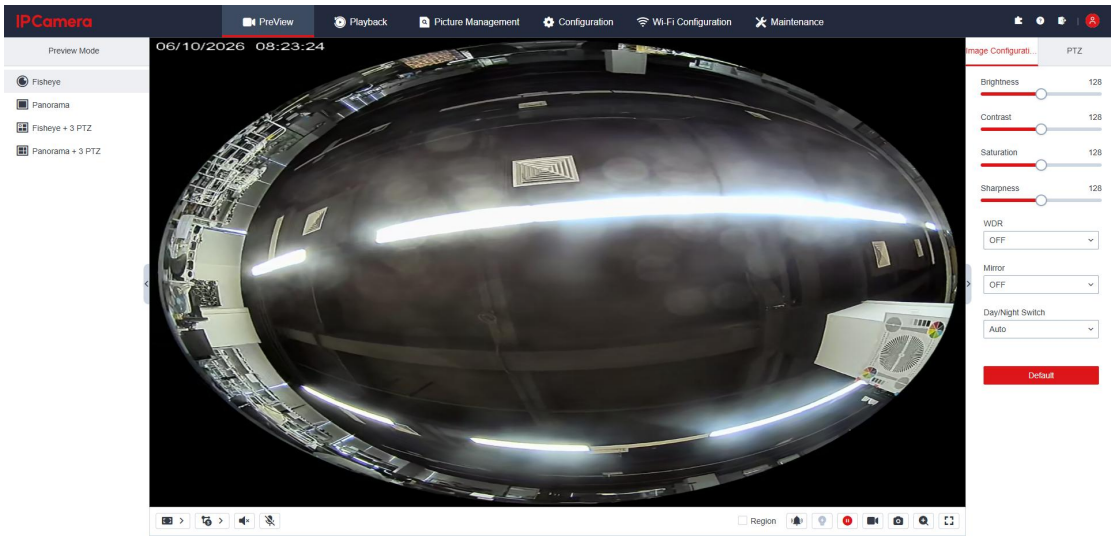


Figure 5-5

【Fisheye】Outputs a circular video stream, playing in full-size mode by default.

【Panorama】Outputs a 360-degree panoramic stitched image, using 2*180=360-degree stitched images, divided into two parts (top and bottom), playing in full-size mode by default.

【Fisheye + 3PTZ】Outputs one circular video stream and three PTZ views, playing in full-size mode by default. The playback window order, from top to bottom and left to right, is: Fisheye, PTZ Video 1, PTZ Video 2, PTZ Video 3.

By default, the screen is divided into three equal parts, and the corresponding video is played in the three PTZ video playback windows. with the PTZ video playback windows supporting PTZ-related operations such as direction control, zoom +, zoom -, preset points, and cruise settings.

【Panorama + 3PTZ】Outputs one panoramic video stream and three PTZ streams, playing in full-screen mode by default. The playback window order, from top to bottom and left to right, is: Panorama, PTZ Video 1, PTZ Video 2, PTZ Video 3.

By default, the screen is divided into three equal parts, and the corresponding video is played in the three PTZ video playback windows. with the PTZ video playback windows supporting PTZ-related operations such as direction control, zoom +, zoom -, preset points, and cruise settings.

【4PTZ】In 4PTZ preview mode, four PTZ video streams are played. The playback window order, from top to bottom and left to right, is: PTZ Video 1, PTZ Video 2, PTZ Video 3, PTZ Video 4.

By default, the screen is divided into four equal parts, and the corresponding video is played in the four PTZ video playback windows. with the PTZ video playback windows supporting PTZ-related operations such as direction control, zoom +, zoom -, preset points, and cruise settings.

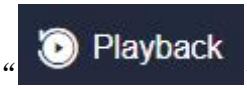
【4PTZS】Divides the fisheye circular video into four equal parts and merges them into a single 4-in-1 video stream for playback. The 4PTZS video playback window does not support PTZ-related operations.



NOTE

For detailed settings and explanations of the fisheye parameters, please refer to the corresponding chapter 8.2.

Chapter 6 Playback

In the main interface, click “ 

” into the video playback interface.

Playback interface can be stored in the camera EMMC / TF card within the video file for query, playback and download operations. as show in Figure 6-1:

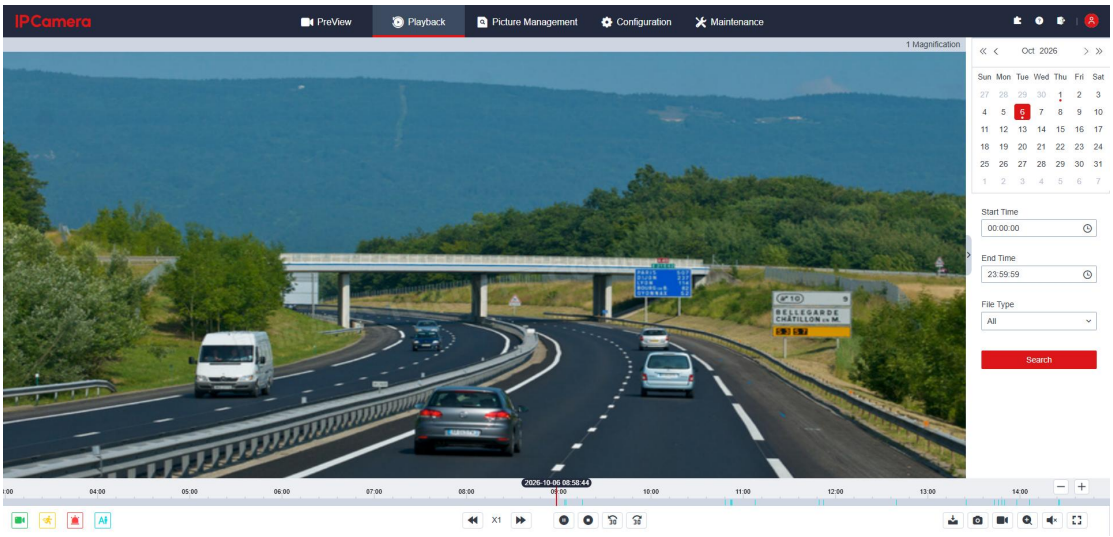


Figure 6-1

Here you can according to the video type (ordinary video, alarm video) and video time to query EMMC / TF card in the video file, the query to the video file playback, screenshots, clips and download.

【Video search】Select the start time, end time, file type (All video,Normal Record, Motion Detection, Area Intrusion,Line Cross Detection,Loiter Detection,Personnel Gathering, Enter Area, Leave Area, Face Detection, Illegal Parking, Line Crossing Counting, Sound Detection), click " 

" to find, meet the conditions of the video file will be on the right side of the calendar interface to select the red date (red date on behalf of the day of video), select the start time, Displayed on the timeline.At the same time, the date of the video recording will be marked with a dot.

【Play/Stop】After searching for the video, click "  " to start playing the video. At this time, the button becomes "  " and click to pause the video,and click ”  ” to stop playing the video.

【Slow Play/Fast Forward】 When playing a video, click "  " to slow down the video

playback speed, click " " to speed up the video playback speed, see the upper right corner of the interface for the specific playback speed.

【Skip Back/Forward 30 Seconds】While playing a video, click " " to jump back 30 seconds forward to play the video, or click " " to jump back 30 seconds.

【Drag and drop】Video playback, the left mouse button click on the time axis to play the position, drag left and right, drag it to the middle of the yellow time point position, playback channel to play the point in time recording.

【Electronic zoom】During video playback, click " ", press and hold the mouse to select the area to be enlarged in the playback interface, release the mouse, the area is enlarged, click the right mouse button to restore the zoom, then the button becomes " ", click to close the electronic zoom.

【Capture】Video playback, click " " to capture the current playback screen image, the interface pops up the capture picture folder, which shows just captured the picture.

【Audio】If the video file has audio, click the " " audio button during playback to turn on and off the playback of the recorded file.

【Timeline magnification】Click the right side of the window on the right side of the " " button, the interface below the time axis is enlarged, the maximum can be amplified to 5min a grid.

【The timeline is reduced】When the timeline is zoomed in, click the " " button to return to the recording timeline before zooming in.

【Video File Query and Download】 Select the date, time period and video type in the calendar. Click " " on the right side of the window to pop up the video download interface. The interface will automatically search all the video files of the corresponding time range and video type, As shown in Figure 6-2:

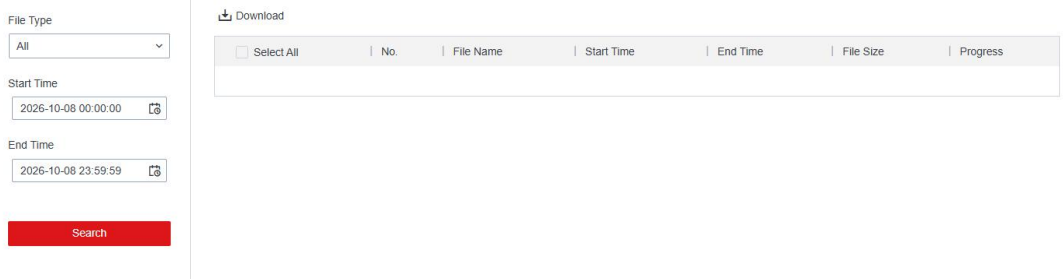


Figure 6-2

【Prev Page】Flip function, click "<" to switch to the previous page.

【Next Page】Flip function, click ">" to switch the next page.

【Download】Select "☐" in front of the serial number of the file to be downloaded, click "Download" , the file starts to download, and wait for the download progress to complete, Downloaded files will be saved under "Configuration > Local Config > Record Files Settings >Save downloaded files to.".

NOTE

- No EMMC/TF card storage video camera and no video playback settings interface, please take the camera physical specific functions shall prevail.
- EMMC storage requires the camera to support EMMC hardware,please refer to the actual product.
- Before querying the video, please make sure that the EMMC/TF card status in the device is "in use" and the 8.7.1 Rec Setup have been configured.
- Please refer to 8.1 Local Configuration for the settings of the video and picture saved in the playback interface.
- During playback, click "Download" to pause playback.

Chapter 7 Picture

Click “ Picture Management ” in the main interface to enter the Picture Management.Can query and download the picture files stored in the camera EMMC/TF card, as shown in Figure 7-1.

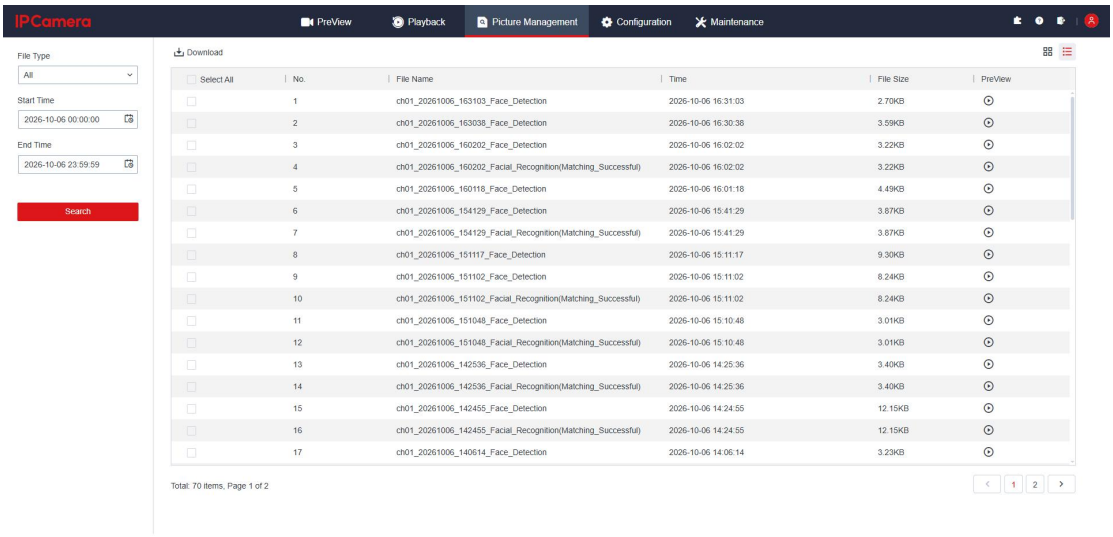


Figure 7-1

【Search】 Select the file type on the left side of the interface, set the image query time, and click ” Search ” to list the eligible image information in the list on the right.

【Preview】 On the right side of the file list, double-click " " to preview the picture.

【Download】 Check the image you want to view and click “ Download ” to save the image information to your local computer. Support multiple images at the same time to download at the same time.

【View】 Click " " at the top right of the interface to display the file in view mode.

NOTE

- The picture is stored in the EMMC/TF card of the device.
- EMMC storage requires the camera to support EMMC hardware,please refer to the actual product.

Chapter 8 Configuration

Click “ Configuration ” in the main interface to enter the local configuration interface. Here you can set the device system, network, video, images, events and other parameters.

8.1 Common Settings

In the main interface, click "Configuration → Common Settings" to enter the Common Settings interface, where you can quickly configure the network camera’s video parameters, image settings, OSD, and time settings, as shown in Figure 8-1.

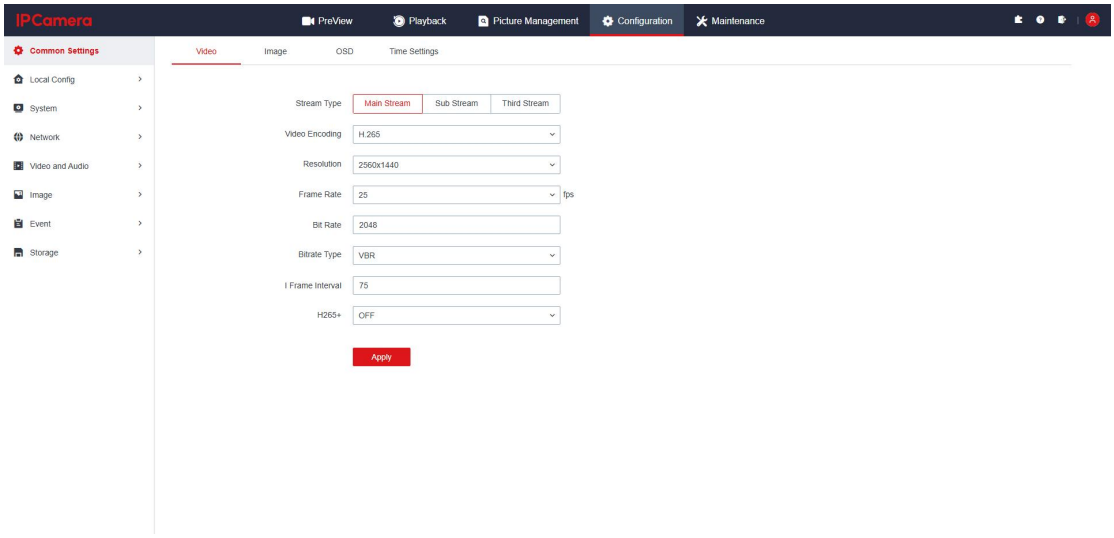


Figure 8-1

NOTE

- For detailed parameter configurations, refer to the help text of the corresponding module.

8.2 Local Config

In the main interface, click "Configuration → Local Config" to enter the local configuration interface, where you can set the "Record File Settings", "Picture and Clip Settings"storage path. Change the path by selecting Browse, as shown in Figure 8-2.

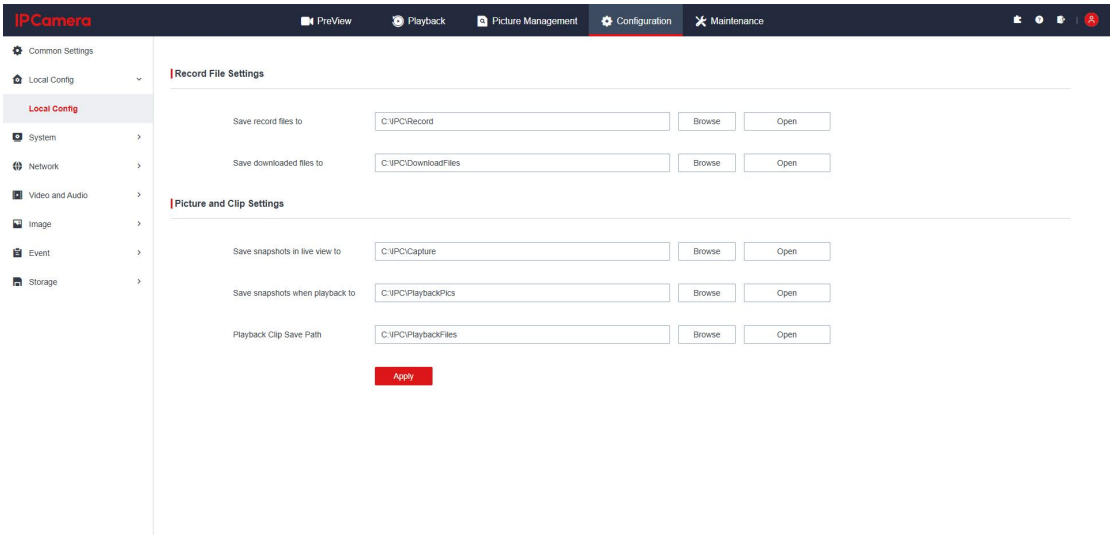


Figure 8-2

【Record File Settings】Set the saving path of the recorded video files. Valid for the record files you recorded with the web browser.

【Save record files to】Set the saving path for the manually recorded video files.

【Save downloaded files to】Set the saving path for the download files.

【Picture and Clip Settings】Set the saving paths of the captured pictures and clipped video files. Valid for the pictures you captured with the web browser.

【Save snapshots in live view to】Set the saving path of the manually captured pictures in live view mode.

【Save snapshots when playback to】Set the saving path of the captured pictures in playback mode.

【Playback clip Save Path】Set the saving path of the clipped video files in playback mode.

NOTE

- The local configuration needs to install middleware,otherwise the configuration cannot be performed .
- Safari browser does not support middleware, so it cannot support local configuration..

8.3 System

In the main interface, click "Configuration → System" to enter the system configuration interface. The system consists of system configuration and security.

8.3.1 System Config

In the main interface, click "Configuration → System → System Config" to enter the system configuration interface.

① Time Settings

In the System Configuration interface, click "Time Settings" to enter the time setting interface, where you can set the device time, as shown in Figure 8-3-1.

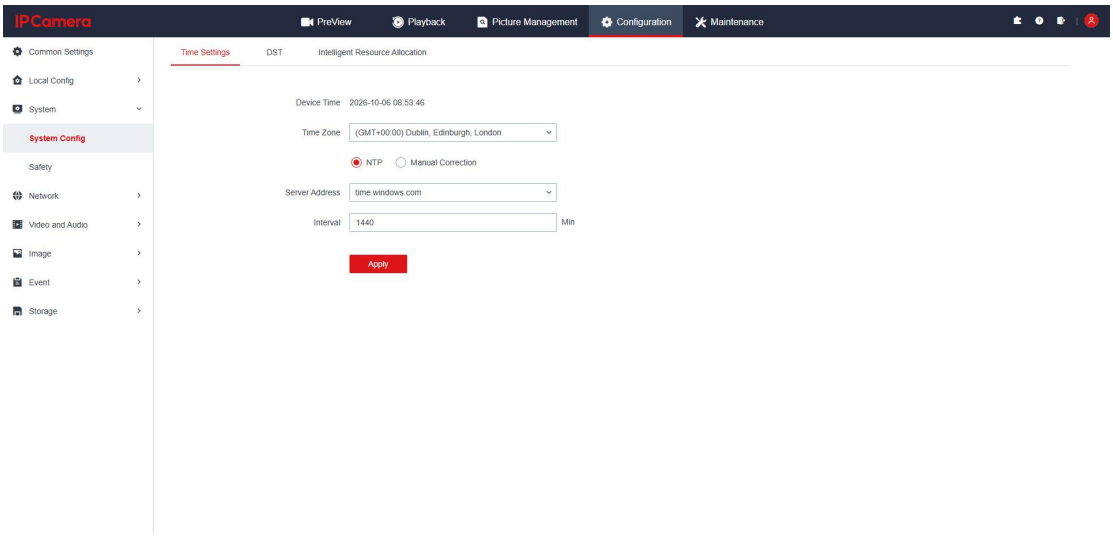


Figure 8-3-1

【Time Zone】Displays the current device selection time zone.

【Device Time】Displays the current time of the device.

【NTP】The IPC time will synchronization with network, and you can change the different time zones. (This feature requires that IPC network environment can connect to the Internet.) Click on the "Apply" after completing the settings.

【Sever Address】SNTP server address, including "time.windows.com", "time.nist, gov", "time-nw.nist.gov", "time-a.nist.gov", "time-b.nist.gov" Optionally, you can also enter the SNTP server address through "Custom".

【Interval】The time interval between the IPC and the SNTP server is 1440 minute by default. You can set "1 ~ 10080".

【Manual Correction】Setting the IPC 's date and time manually. Click on the "Apply" after completing the settings.

【Sync. with computer time】The IPC will synchronize with the computer time and date that your connect currently. Click on the "Application" after completing the settings.

② DST

Daylight saving time(DST) refers to the system of artificially stipulating local time for energy conservation. The unified time used during the implementation of this system is called “DST”. In the System Configuration interface, click "DST" to enter the daylight saving time setting interface, where you can enable daylight saving time, set daylight saving time, end time and end time, as shown in Figure 8-3-2.

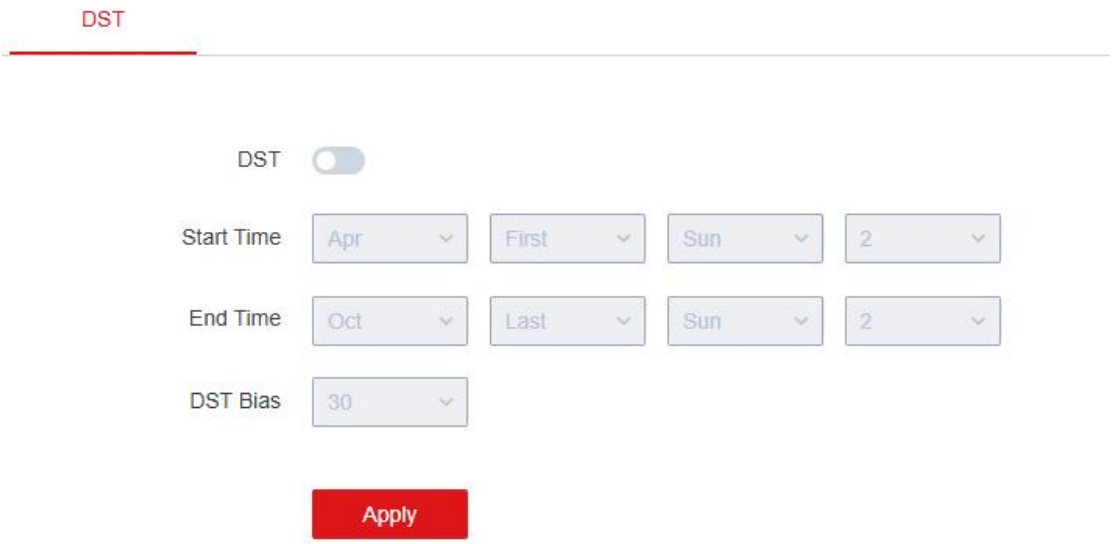


Figure 8-3-2

③Intelligent Resource Allocation

In the system configuration interface, click "Intelligent Resource Allocation" to enter the intelligent resource allocation interface, where you can set the device intelligent related resource allocation, as shown in Figure 8-3-3 below:

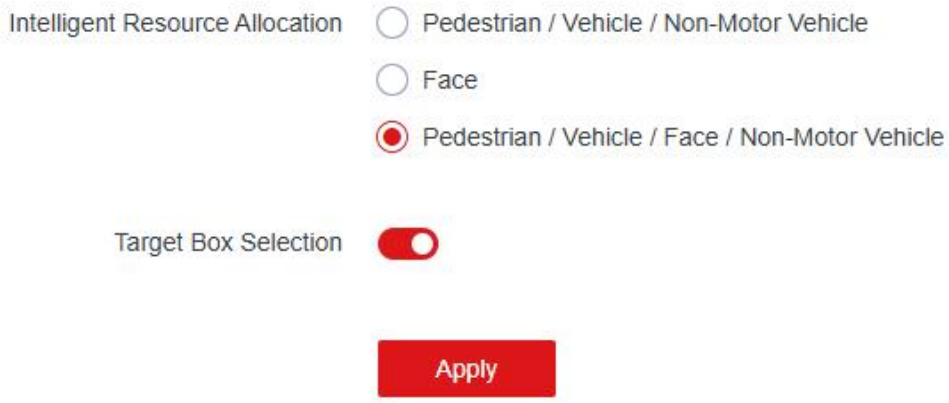


Figure 8-3-3

【Intelligent Resource Allocation】 It supports dynamic allocation of intelligent resources. Depending on the algorithm model supported by the device, there will be different configuration options. Please refer to the interface of the specific device for details.
【Target Selection】 supports target selection. When enabled, a rectangular frame will appear around the detected target.

NOTE

- Some cameras do not support intelligent resource allocation. Please refer to the actual camera for details.
- Supported intelligent resource configuration items vary depending on the device's capabilities. Please refer to the actual camera for details.
- Changes to intelligent resource allocation configuration require a device restart for them to take effect.

④Electronic Pan-tilt Unit

In the system configuration interface, click "Electronic Pan-tilt Unit" to enter the electronic pan-tilt unit interface, where you can set the device EPTZ, as shown in Figure 8-3-4 below:

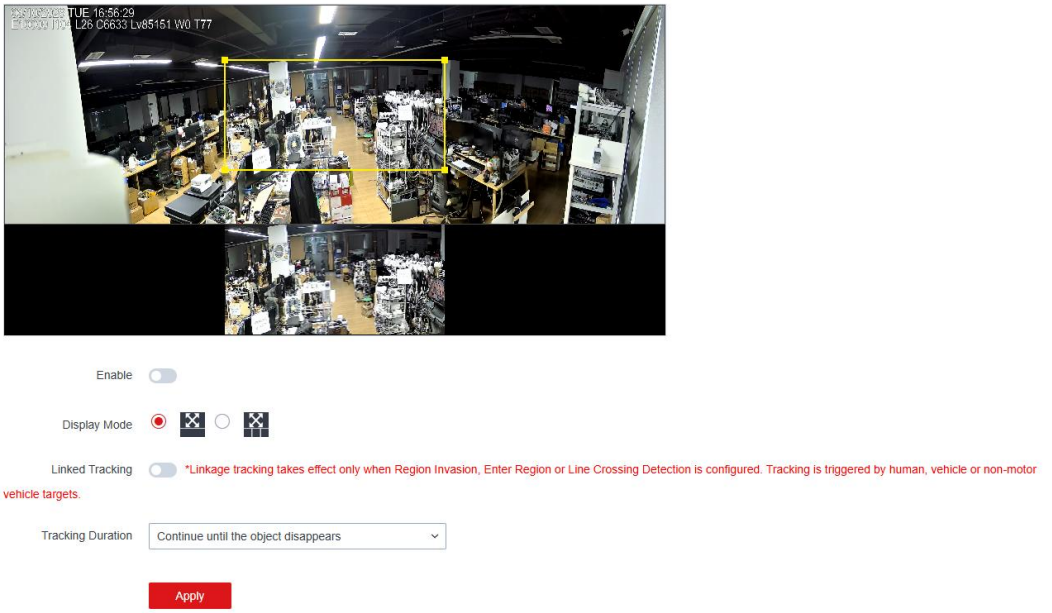


Figure 8-3-4

【Enable】 The electronic gimbal can be turned on and off. When it is off, there will be no electronic gimbal effect even if EPTZ is enabled in the preview interface..
【Display Mode】 It supports two display modes, with the default being a two-window mode. Users can choose the mode according to their actual application scenario.
【Linked Tracking】 Linked tracking can be enabled or disabled. When enabled, linked tracking can be performed when the intelligent function for detecting intrusion into a region, entering a region, or crossing boundaries is configured and activated.
【Tracking Duration】The default duration is until the object disappears, but users can customize the duration from 5 to 300 seconds according to their actual application needs.

NOTE

- Some cameras do not support electronic pan-tilt unit. Please refer to the actual camera for details.

⑤ Fisheye Parameters

In the system configuration interface, click "Fisheye Parameters" to enter the fisheye parameter configuration interface, where you can set the fisheye-related parameters, as shown in Figure 8-3-5 below:

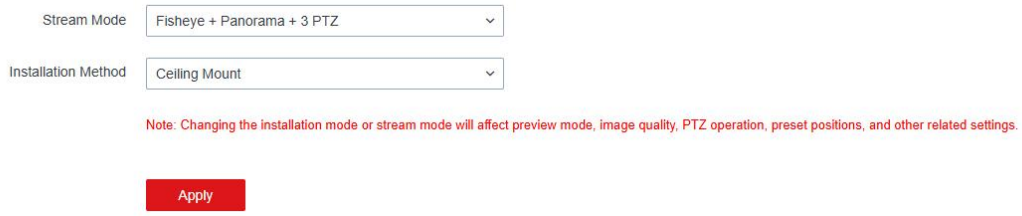


Figure 8-3-5

The available options for Stream Mode and Installation Method are shown in Figure 8-3-6.

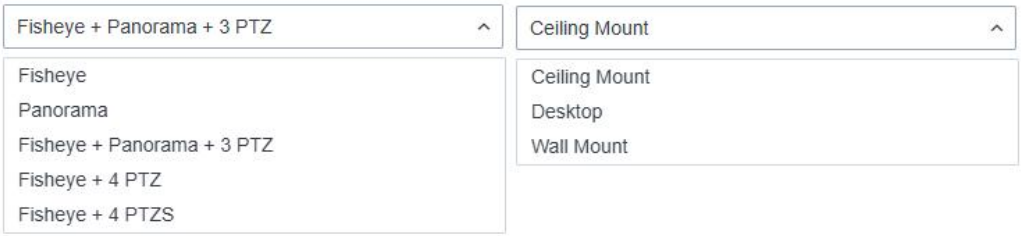


Figure 8-3-6

【Stream Mode】Supports 5 stream modes, with fisheye as the default. Users can adjust the stream settings according to their application scenarios. The preview modes for different stream modes are as follows:

- Fisheye stream mode: Preview mode only shows fisheye.
- Panorama stream mode: Preview mode only shows panorama.
- Fisheye + Panorama + 3PTZ stream mode: Preview mode includes fisheye, panorama, fisheye + 3PTZ, and panorama + 3PTZ.
- Fisheye + 4PTZ stream mode: Preview mode includes fisheye and 4PTZ.
- Fisheye + 4PTZS stream mode: Preview mode includes fisheye and 4PTZS.

【Installation Method】Supports 3 installation methods, with ceiling mount as the default. Users can select the appropriate installation method based on the actual installation location to ensure that the image is always upright.

NOTE

- Some network cameras support the "Fisheye Parameters" configuration function; please refer to the actual interface for details.
- Modifying the stream mode and installation method requires restarting the device and will affect the preview mode, image effects, PTZ, etc., and some settings will be reset.

8.3.2 Safety

In the main interface, click "Configuration → System → Safety" to enter the user management settings interface, where you can add, edit, delete the user, you can also query the current online user information,and you can also set up security services for login.
When the current user is in the administrator role, the user can create other users as needed; you can create up to 10 users, as shown in Figure 8-3-7.

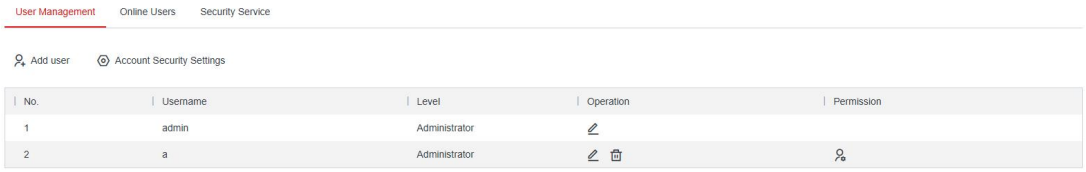


Figure 8-3-7

① Add a User

Step 1: Click “Add User” to add a user.
Step 2: Input the User Name, select User Type and input Password.
Step 3: Click “OK” to complete the user to add.

Add User as shown in Figure 8-3-8.

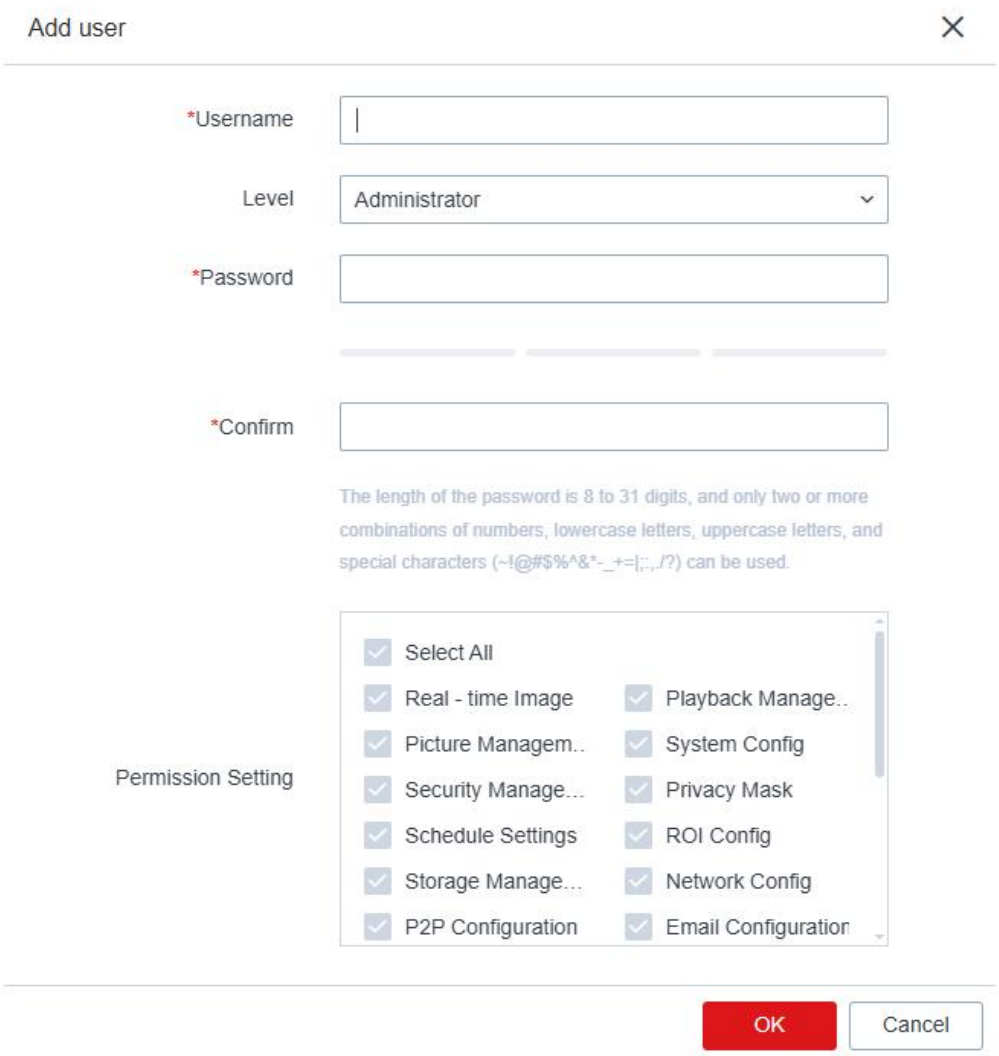


Figure 8-3-8

CAUTIONS

- In order to improve the security of the product network, please change the password of the user name regularly. It is recommended to update the maintenance every 3 months. If the IP camera is used in a high security risk environment, it is recommended to update once a month or every week.
- It is recommended that the system administrator manage the user effectively, remove the unrelated user and shut down the unnecessary network port.

NOTE

- The admin user cannot be deleted and you can only change the *admin* password.
- User permission description:

Administrator -- all permissions.
Operator -- All permissions (cannot make system security parameter settings).
User -- only preview permission.

- When setting a password for your network camera, the password must be 8-31 characters long and can only contain two or more combinations of numbers, lowercase letters, uppercase letters, and special characters (currently supported are ~!@#$%^&*-_+=|；：，./？)..

Password strength rules are as follows:
- If the set password contains three or more types (numbers, lowercase letters, uppercase letters, special characters), it is a strong password.
- If the password is set to a combination of numbers and special characters, lowercase letters and special combinations of characters, capital letters and special characters, lowercase letters and uppercase letters, are in the password.
- If the password is set to a combination of numbers and lowercase letters, numbers and uppercase letters, ,lowercase letters and uppercase letters are weak passwords.
- Password length is equal to 8, the password contains only one type of character, password and user name or password is the user name of the write, the above types of passwords are risk password, do not recommend this set.

To better protect your privacy and improve product safety, we recommend that you change your risk password to a high-strength password.

②Modify the (admin user) password

Step 1: In the user list, click the “Edit” button after the admin user to enter the user interface.
Step 2: Enter a new password in the Password and Confirm Password fields;
Step 3: Click "OK" to complete the password modification.

NOTE

- When the IPC password is “123456”, each time you log in, you will be prompted to change the password. You can select “Modify after 60 Minutes”. After 60 minutes, the interface will automatically pop up the password modification interface.
- After changing the admin password, it is recommended to configure security questions or a security email address in the "Account Security Settings" interface so that the password can be reset if forgotten.
- After modifying the administrator password, when the PC and the device are on the same LAN segment, click "Forget" to reset the password by answering the security question or security mailbox.
- When you change your password again, you don't have to set a new security question. When you forget your password, you can reset it with the last security question you set.

③ Edit the User

Step 1: In the user list, select the user to be modified, and click " " to enter the user editing interface.
Step 2: Edit the user type or password, enter the confirm password;
Step 3: Click "OK" to finish editing the user.

NOTE

- The password setting rule is the same as the password rule when adding a user.

④ Delete Users

Step 1: Click to select the user you want to delete and click " ".

Step 2: Click "OK" on the pop-up dialogue box to delete the user.

⑤ Permission Setting

Step 1: Select the user for whom you want to configure permissions from the user list, and click the " " button;

Step 2: After modifying the relevant permissions, click "OK" to save the settings.

NOTE

- Administrator: Possesses full permission, permission cannot be modified..
- Operator: Cannot configure security management permission or modify real-time image permission, other permission can be freely modified.
- User: Has access to real-time images only, permission cannot be modified.

⑥ Security Service

Through the security service settings, illegal logins can be locked according to the settings. The number of incorrect passwords, incorrect security questions, and incorrect verification codes entered will be verified. If the number exceeds the test, the device will be locked to avoid some illegal operations, as shown in Figure 8-3-9:

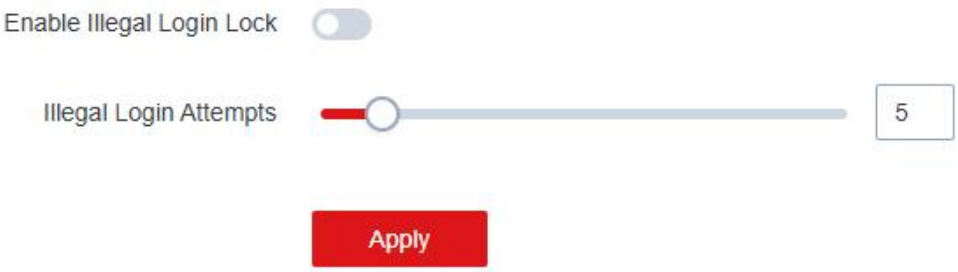


Figure 8-3-9

Step 1: Click "Security Service" to enter the security service page.
Step 2: Check "Enable Illegal Login Lock".
Step 3: Drag the slider or enter a value to set the number of error attempts.
Step 4: Click “Apply”.

NOTE

- Illegal login lock is not enabled by default.
- The default number of error attempts is 5, which can be configured from 3 to 20. The lock time is 30 minutes each time.
- The lock is only for the current operating terminal. Restarting the device during the lock period can remove the restriction.

8.4 Network

8.4.1 Basic Setup

① TCP/IP

The TCP/IP interface is used to view and configure network parameters such as the camera's IP address. You can enable DHCP or manually modify to configure the IPC network parameters.

Enable DHCP:

Connect IPC to the router with DHCP enabled, enable DHCP, then IPC will obtain the corresponding IP address, subnet mask, default gateway, and preferred DNS server information.

The specific steps for manually modifying network parameters are as follows:

Step 1: In the main interface, click "Configuration → Network → Basic Settings → TCP / IP" to enter the TCP / IP interface, as shown in Figure 8-4-1.

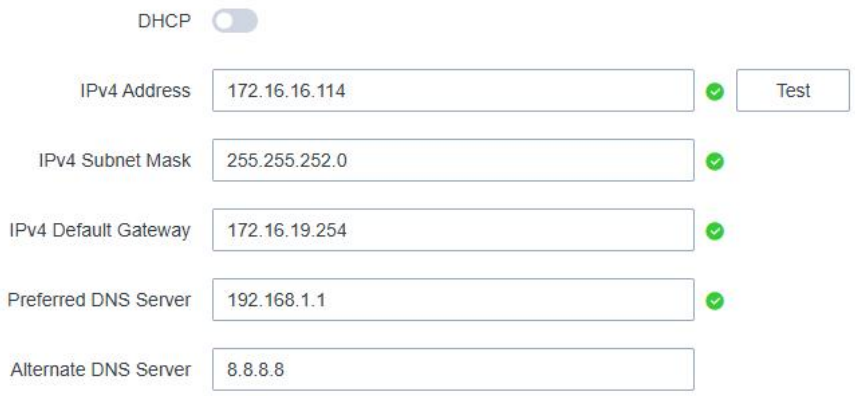


Figure 8-4-1

Step 2: Set the IP address, subnet mask, gateway, and DNS.

Step 3: Click "Test" to make sure the modified IP address is available in the LAN.

Step 4: Click "Apply" to save the configuration.

Port

In the main interface, click "Configuration → Network → Basic Settings → TCP / IP" to enter the TCP / IP interface, where you can set the IPC network port and protocol port, the network port has HTTP port (default is 80), RTSP port (default is 554) , HTTPS port (default is 443), P2P port(default is 6000). As shown in Figure 8-4-2.



Figure 8-4-2

【P2P Port】When the App is directly connected to the device, the "Private port" is entered into the P2P port.

NOTE

Please do not arbitrarily modify the port parameters; when there is a port conflict need to modify the port number, please modify the following information:

- HTTP and HTTPS port: use the browser login need to add the address after the port number. If you repair HTTP port number 8555, when you use the browser login, you need to enter .
- RTSP port: real-time transmission protocol port, to ensure that the modified port is

available.

- AL platform devices do not support the P2P port.

② HTTPS

HTTPS protocol is a network protocol built by SSL+HTTP protocol that can perform encrypted transmission and identity authentication, which can improve the security of WEB access.

The specific steps to install and enable HTTP are as follows:

Step 1: In the main interface, click "Configuration → Network → Basic Settings → HTTPS " to enter the HTTPS interface,as shown in Figure 8-4-3:

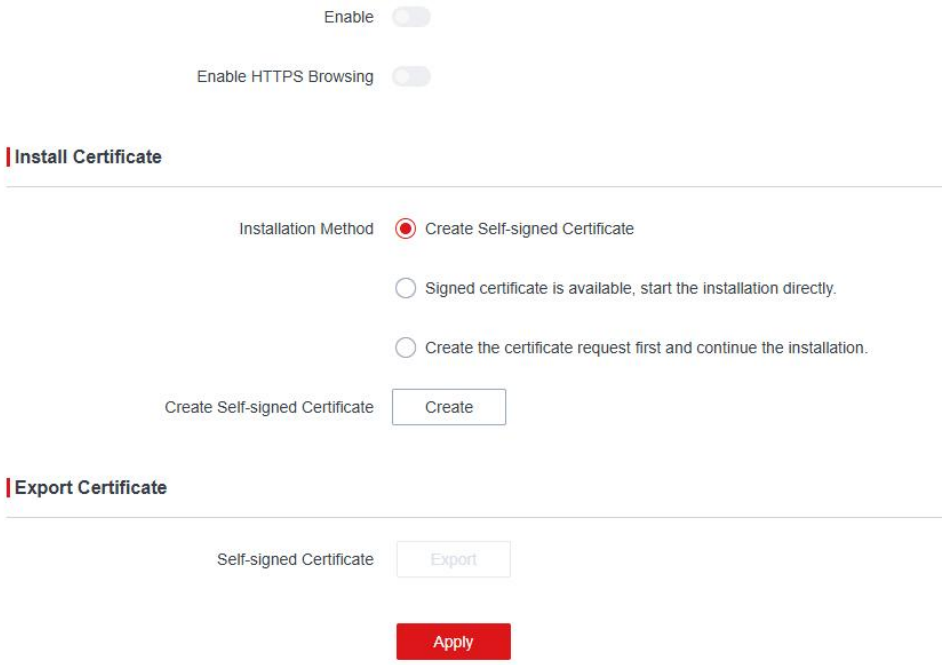


Figure 8-4-3

Step 2: Install the certificate according to the actual situation. You can choose to "Create Self-signed Certificate", "Signed certificate is available, start the installation directly" or "Create the certificate request first and continue the installation".

Step 3: If you have installed a certificate, the certificate details will be displayed. Check "Enable" and click "Apply" to enable the HTTPS function. Check "Enable HTTPS Browsing" to automatically convert the input IP address into an HTTPS address to improve network security.

Step 4: Click "Apply" to save the configuration.

【Create Self-signed Certificate】Select "Create Self-signed Certificate" in the installation method, click "Create", open the private certificate creation window, fill in parameters such as country, domain name/IP, validity period, etc.; click "OK".

【Signed certificate is available, start the installation directly】Check "Signed certificate is available, start the installation directly", click "Create" to open the authorization certificate

creation window, fill in parameters such as country, domain name/IP, and click "OK" to complete the request. When you receive the signed valid certificate, you can download or delete the certificate request, or install the downloaded security certificate.

【Create the certificate request first and continue the installation】In the installation method, select "Create the certificate request first and continue the installation", click "Browse" to select the existing signed certificate, then click "Install", and click "Apply" after completion.

【Export Certificate】Exporting a self-signed certificate.

NOTE

- Users install certificates based on actual conditions.
- It is recommended to create a certificate request and upload a certificate issued by an authoritative certificate authority (CA) for authentication, providing a range of security levels.

③ DDNS

After the DDNS (Dynamic Domain Name Server) parameter is set, when the IP address of the IPC changes frequently, the system can dynamically update the relationship between the domain name and the IP address on the DNS server. You can use the domain name to access the IPC directly without recording the constantly changing IP address.

Prerequisites

Before configuring DDNS, make sure that the device supports the type of domain name resolution server, and log in to the DDNS service provider's website to register user name, password, domain name, and other information on the WAN PC.

The specific operation steps are as follows:

Step 1: In the main interface, click "Configuration →Network → Basic Settings → DDNS" to enter the DDNS function settings interface, as shown in Figure 8-4-4:

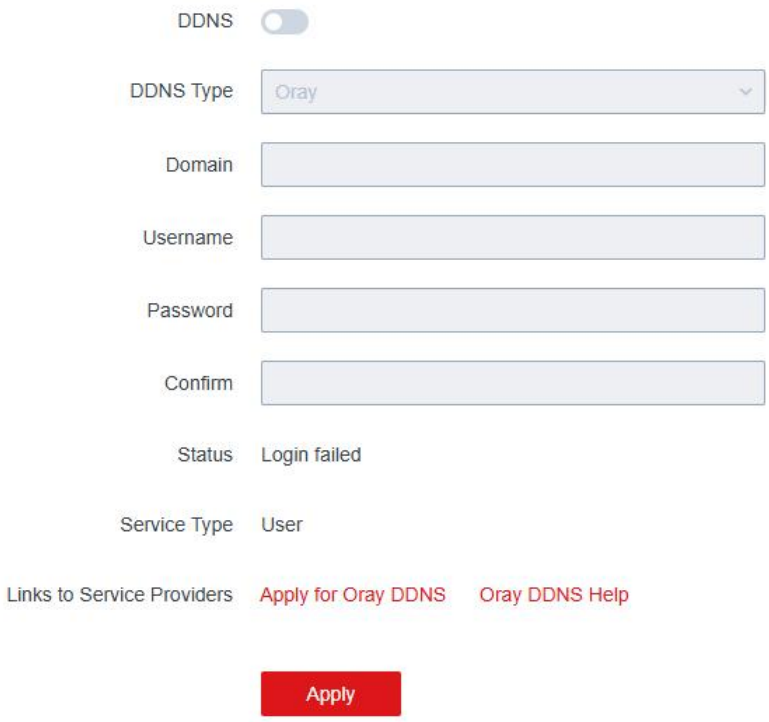


Figure 8-4-4

Steps 2: Enable DDNS, select the DDNS type, and enter the username, password, and site name .

Steps 3: Click "Apply" to save the configuration.

Steps 4: Enter the domain name in the PC web browser and press "Enter". If you can display the web interface of the device, the configuration is successful. If it is not displayed, the configuration fails.

【DDNS】Enable / disable DDNS function.

【DDNS Type】Choose the type of Oray, NO-IP, Dyn, Planet Dynamic DNS and Planet Easy DDNS five types.

【Domain】The input selection type corresponds to the successful domain name.

【User Name】The input selection type corresponds to the registered account.

【Password】The input selection type corresponds to the registration password.

【Confirm】Re-enter the password, this password and DDNS password.

【Status】Shows whether the current device is set up DDNS successfully.

【Service Type】Displays the type of user name.

【Links to service providers】Show service provider information.

NOTE

- Access via DDNS domain requires IPC to be accessible to the Internet.

④ PPPoE

PPPoE(Point-to-Point Protocol over Ethernet) is one of the ways in which IPC devices access the network. After obtaining the PPPoE user name and password provided by the Internet Service Provider, you can establish a network connection through PPPoE dialup. After the connection is successful, the IPC automatically obtains a dynamic IP address of the WAN.

The specific operation steps are as follows:

Step 1: In the main menu, click "Configuration →Network → Basic Settings →PPPoE" to enter PPPoE to set the interface, as shown in Figure 8-4-5.

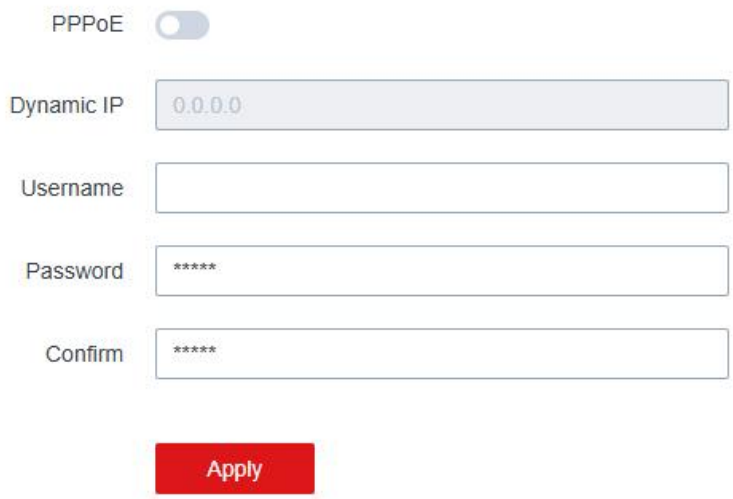


Figure 8-4-5

Steps 2: Click " " to open PPPoE, input the device dynamic IP user name, and password of the PPPoE.

Steps 3: Click "Apply" to save the configuration.

【PPPoE】 Turn on/off the device PPPoE function.

【User Name】 The PPPoE user name provided by the ISP (Internet Service Provider).

【Password】 The password corresponding to the user name.

【Confirm】Re-enter the password.

NOTE

After completing the setting, the device will automatically dial after restarting. After successful dialing, the network information can be displayed in the network status, and users can access the device through the IP address.

⑤ FTP

Set the FTP (File Transfer Protocol) server, you can store the alarm picture to the FTP server.

Prerequisites

You need to purchase or download the FTP service tool and install the software on your PC.

The steps to configure FTP are as follows:

Step 1: In the main interface, click "Configuration → Network → Basic Setting → FTP" to enter the FTP server settings interface, as shown in Figure 8-4-6.

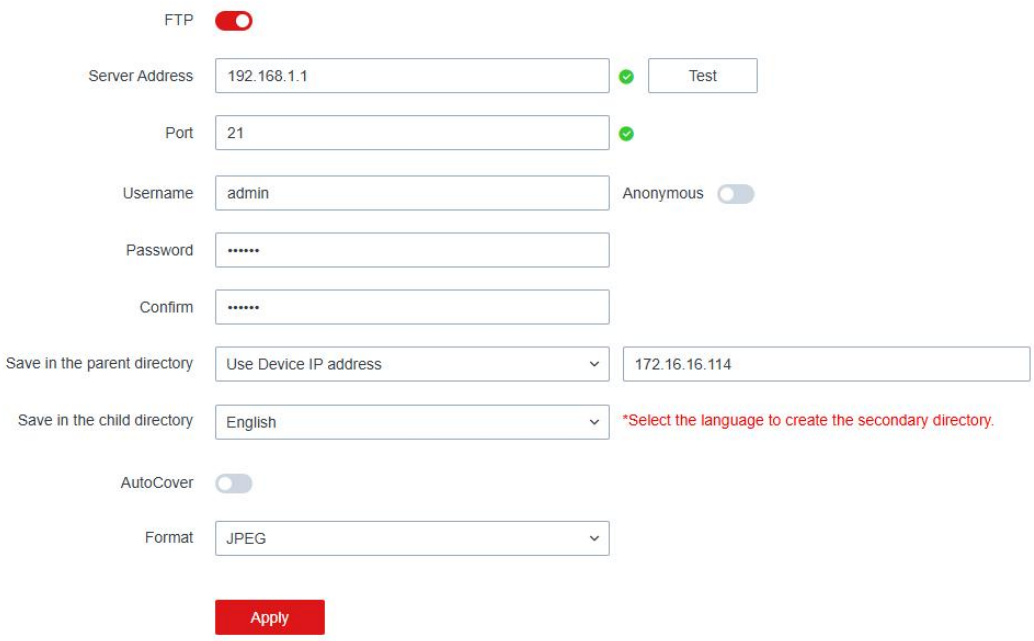


Figure 8-4-6

Step 2: Enter the server address, port, user name, password, confirm the password, save in the parent directory, save in the child directory, check "Auto Cover", and select the upload FTP server image format JPEG.

Step 3: Click "Apply" to save the configuration.

Step 4: Click "Test" to confirm whether the network connection and FTP configuration are correct.

【FTP Server】Fill in the FTP server address.

【Test】Enter the FTP server information and click "Test" to confirm the correctness of all input information and whether the device and server are connected properly.

【Port】Fill in the FTP server port number.

【User Name】Fill in the FTP server username.

【Password】Fill in the FTP server password.

【Confirm】Fill in the FTP server password.

【Save in the parent directory】Automatically create a level-1 directory under the FTP storage path.

【Save in the child directory】Create a secondary directory under the FTP primary directory.

NOTE

- To create an FTP user, you need to set the FTP folder write permission, otherwise the image will not be uploaded successfully.
- If the test fails, please recheck the network or FTP configuration.
- When you select "Use OSD" for the parent directory, the FTP server must support UTF-8 encoding.
- Select "Use device IP address" or "Custom" for the parent directory. When the child directory is in Chinese, the FTP server must support UTF-8 encoding.

⑥ SNMP

Before setting SNMP parameters, the user needs to have an SNMP server, and ensure that the SNMP server is configured with relevant parameters and can work normally.
IPC supports three simple network management protocol versions, V1, V2 and V3. The network management protocol is selected according to the SNMP server-side protocol version. By configuring the SNMP protocol, the device parameters can be obtained and the alarm exception information of the device can be received.
After enabling the SNMP function of the device, set "Read SNMP Community" and "Write SNMP Community", and then set the Trap address, the device can send alarm and abnormal information to the management station, and can receive device information by setting the Trap port.
The specific operation steps are as follows:
On the main interface, click "Configuration → Network → Basic Settings → SNMP" to enter the SNMP configuration interface, as shown in Figure 8-4-7 below:
After selecting "SNMP" to enable the SNMP function of the device, select the SNMP version, such as V3, you can set the parameter information of V3 ("SNMP Port", "Read SNMP Community", "Write SNMP Community", "Trap Address", etc.), the device can send alarm and abnormal information to the management station, and can receive device information by setting the Trap port. After setting the parameters, click "Apply".

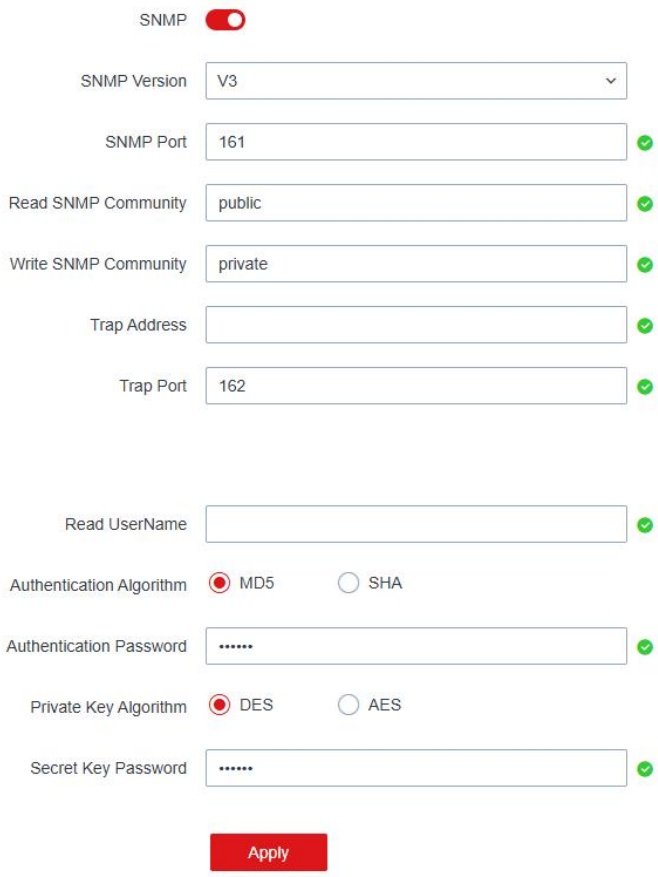


Figure 8-4-7

⑦ Other

In the main interface, click "Configuration →Network → Basic Settings → Other" to enter the Video Password Authentication interface, as shown in Figure 8-4-8.



Figure 8-4-8

【Video Password Authentication】 After opening, encrypt all the devices and platforms connected to the camera video, and connect to the IPC video by entering the correct username and password.

【P2P Encryption Enable】 When enabled, the stream between the camera and the App

is encrypted.

NOTE

- AL platform devices do not support enable P2P encryption .

⑧ QoS

In the main interface, click "Configuration →Network → Basic Settings → QoS" to enter the QoS interface, as shown in Figure 8-4-9.

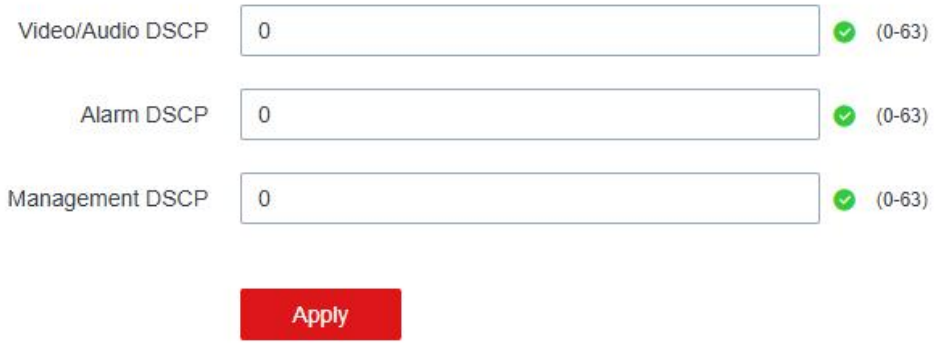


Figure 8-4-9

Configuring QoS service quality can effectively solve the problems of network delay and network congestion. It supports setting the QoS classification standards "Video/Audio DSCP", "Alarm DSCP" and "Management DSCP" respectively. The value range is 0-63, and the default value is 0. The larger the value, the higher the transmission service quality will be provided in the case of network congestion, ensuring the priority processing and real-time performance of data.

NOTE

The QoS function requires support from network devices (such as routers) on the transmission path.

⑨ 802.1X

In the main interface, click "Configuration →Network → Basic Settings → 802.1X" to enter the 802.1X interface, as shown in Figure 8-4-10.

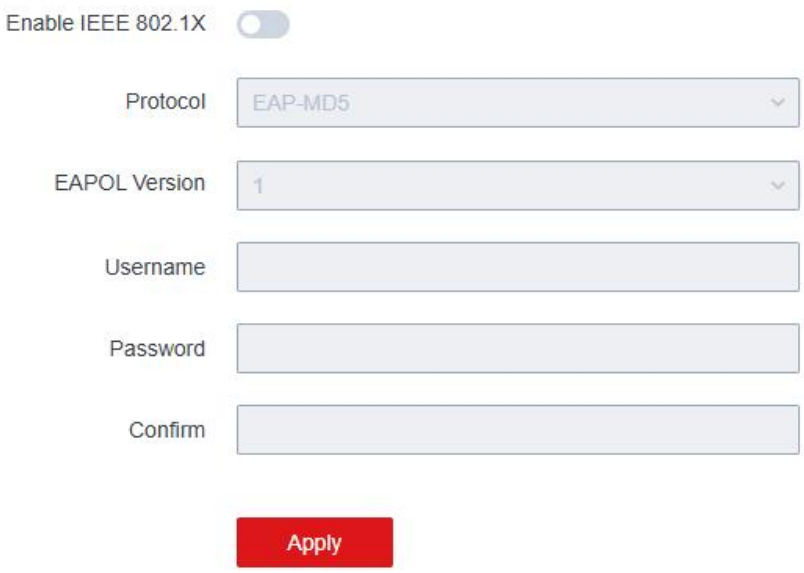


Figure 8-4-10

【Enable IEEE802.1X】Enable/disable IEEE802.1X.

【Protocol】Configure the protocol type. The default value is "EAP-MD5". "EAP-LEAP" is optional

【EAPOL Version】Configure EAPOL version, default is 1, optional 2.

【User Name】Configure the user name for connecting to the device.

【Password】Configure the password for connecting to the device.

【Confirm】Re-enter password.

NOTE

The configuration protocol can be used to authenticate the user rights of the connected device.

⑩ RS485

By configuring the parameters of the RS-485 serial port, the interface is matched. Please set the baud rate, data bit and other information of the interface according to the actual environment. RS-485 serial port parameters Select the decoder type and configure the decoder address according to actual needs.

In the main interface, click "Configuration →Network → Basic Settings → RS485" to enter the RS485 interface, as shown in Figure 8-4-11.

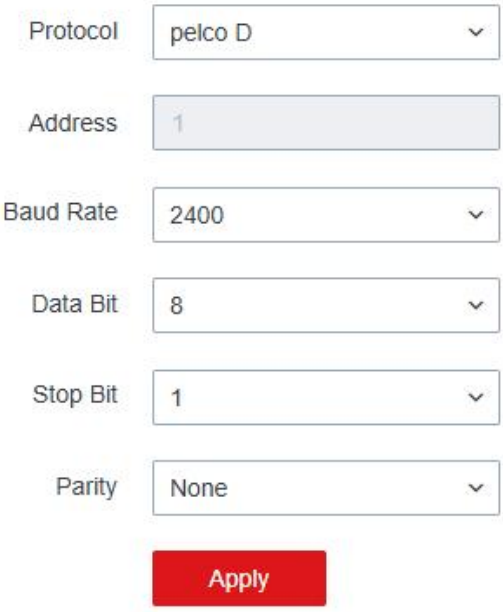


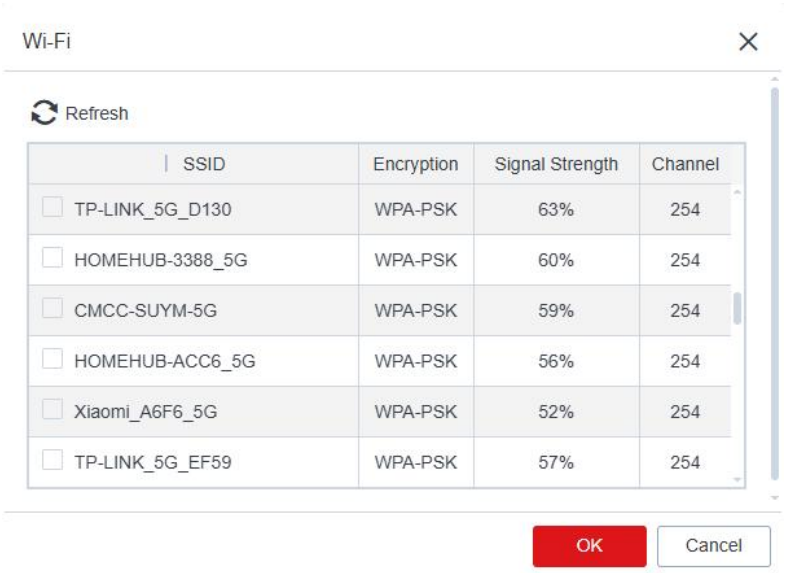
Figure 8-4-11

NOTE

The configuration protocol can be used to authenticate the user rights of the connected device.

⑪ Wi-Fi

In the main interface, click "Configuration → Network → Basic Configuration → Wi-Fi" to enter the Wi-Fi configuration interface. You can set this interface to connect the IPC to Wi-Fi, as shown in Figure 8-4-12.



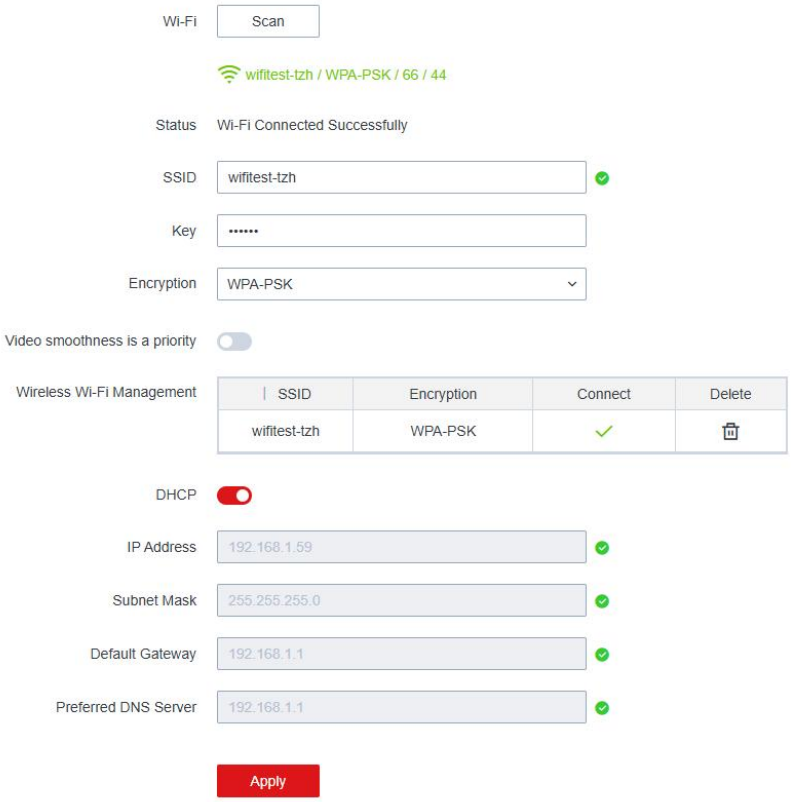


Figure 8-4-12

【Video smoothness is a priority】When enabled, the camera dynamically adjusts the bitrate and image quality, prioritizing smooth video transmission to minimize stutter caused by network fluctuations; when disabled, image quality is prioritized, making stutter or buffering more likely under poor network conditions.

【Wi-Fi Management】Wi-Fi IPC can remember the account that has connected to Wi-Fi, and enable the device to connect or delete the Wi-Fi account through wireless Wi-Fi management.

The steps for connecting IPC to Wi-Fi are as follows:

Step 1: Click the "Scan" button to search for nearby Wi-Fi hotspots that can be connected;

Step 2: Select the Wi-Fi to connect to and enter the Wi-Fi password in the key field;

Step 3: Turn on "Auto-acquire" and click "Apply".

NOTE

- Only cameras that support Wi-Fi function have Wi-Fi interface. Please refer to the actual camera for specific functions.
- When the camera is connected to Wi-Fi, you can also disable DHCP and manually enter and select the preferred DNS server IP address and default gateway of the same Wi-Fi network segment to set the camera Wi-Fi network information.
- Wi-Fi IPC can remember up to 3 connected Wi-Fi accounts.

⑫ Wi-Fi Hotspots

In the main interface, click "Configuration → Network → Basic Configuration → Wi-Fi Hotspots" to enter the Wi-Fi Hotspots interface. You can turn on and set the camera Wi-Fi hotspot. After setting, mobile phones and other devices can connect to the hotspot to access IPC. The Wi-Fi hotspot interface is shown in Figure 8-4-13.

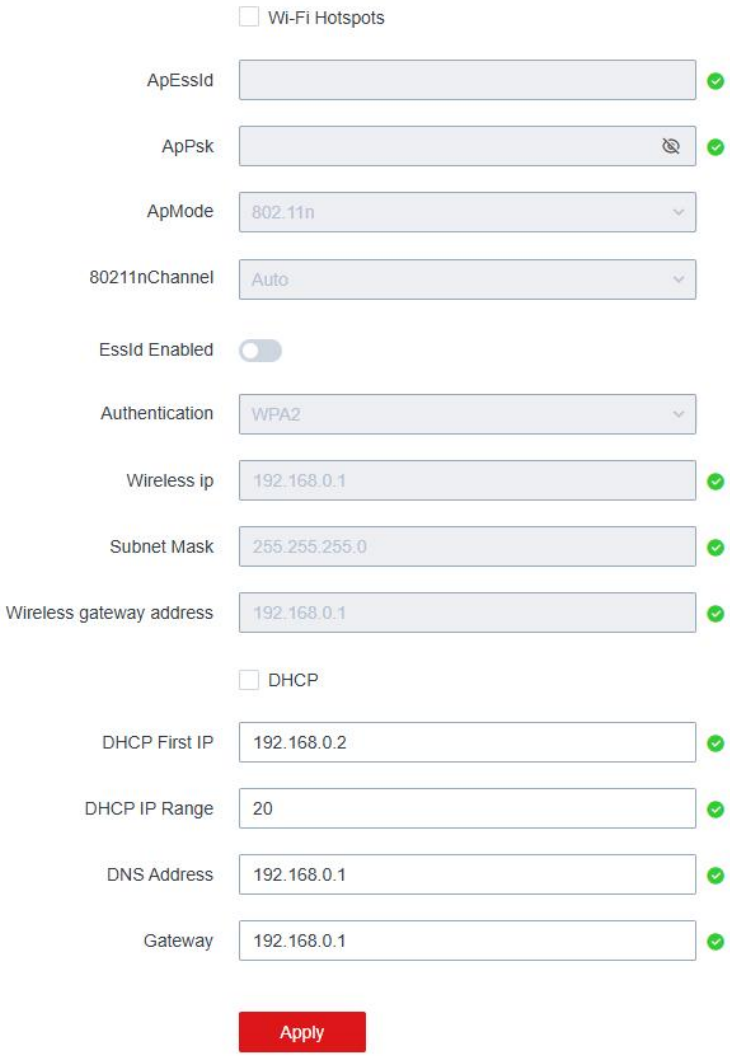


Figure 8-4-13

The steps to enable and set up the camera's Wi-Fi hotspot are as follows:
Step 1: Check "Wi-Fi Hotspot" to enable the hotspot function;
Step 2: Set the AP name, AP password, WiFi hotspot operating frequency band, authentication switch, authentication method, wireless IP, subnet mask and wireless gateway address;
Step 3: Click "Save" to complete the settings.

NOTE

- Only cameras that support Wi-Fi hotspot function have Wi-Fi Hotspot interface. Please refer to the actual camera for specific functions.

- When configuring the camera's Wi-Fi hotspot, you can also disable automatic acquisition and manually enter the starting address, allocation quantity, DNS address, and gateway information.
- When a wired connection is unavailable in the scene where your device is located, you can connect to the device through a WLAN hotspot.

⑬ RTMP

In the main interface, click "Configuration →Network → Basic Settings → RTMP" to enter the RTMP interface, as shown in Figure 8-4-14.

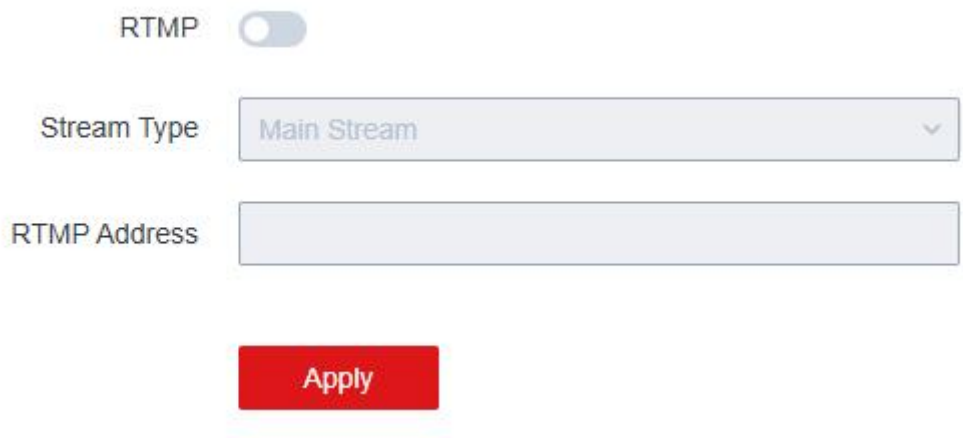


Figure 8-4-14

【RTMP】Enable/disable RTMP.

【Stream Type】Configure the stream type, the default is "main stream", "sub stream" is optional.

【RTMP Address】Configuring RTMP Address.

NOTE

By configuring the protocol, you can push the video stream to the corresponding RTMP address through the TCP-based streaming media transmission protocol.

⑭ RTCP

Devices rely on RTCP (Real-time Transport Control Protocol) to deliver packets in order to provide a reliable delivery mechanism and to provide flow control or congestion control services.

In the main interface, click "Configuration →Network → Basic Settings → RTCP" to enter the RTCP interface, as shown in Figure 8-4-15.



Figure 8-4-15

【Enable】Enable/disable RTCP.

8.4.2 P2P

① P2P

P2P is a private network penetration technology. It does not need to apply for a dynamic domain name, perform port mapping, or deploy a transit server. You can directly scan the QR code to download a mobile client. After registering an account, you can add and manage multiple IPC, NVR, XVR devices simultaneously on the mobile client.

You can add devices in the following two ways to manage multiple devices.

1) Scan the QR code for the mobile phone system, download the App and register the account. For details, see the App User Manual on the website.

2) Log on to the P2P platform, register an account, and add the device via the serial number.

The specific operation steps are as follows:

Step 1: In the main interface, click "Configuration →Network → P2P" to enter the P2P settings interface, as shown in Figure 8-4-16.

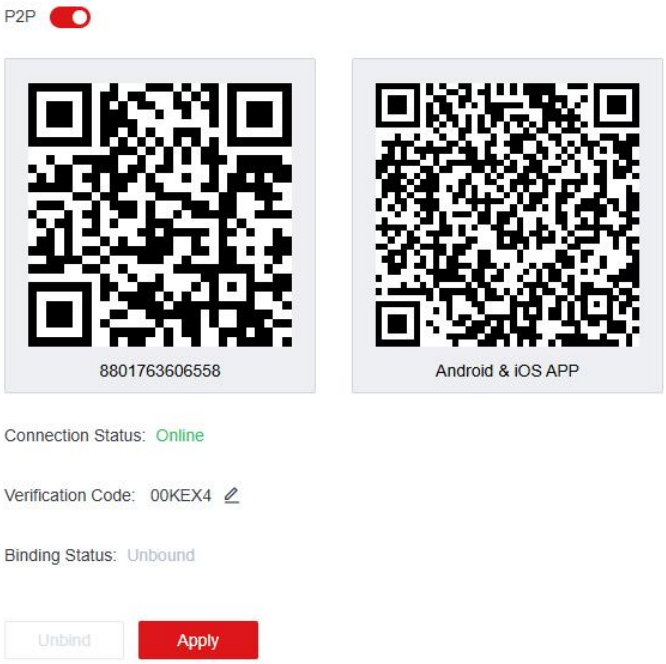


Figure 8-4-16

Step 2: Make sure that the IPC accesses the external network and click " " to open P2P.
Step 3: Click "Apply" to save the configuration.
Step 4: Refresh page, the status shows "Online". This indicates that P2P is enabled and can be used normally;If the device has not been added, the binding status is displayed as "Unbound".

App Client operation example
The following content is introduced by taking the operation of the mobile phone client (App) as an example. The steps are as follows:
Step 1: Use the Android or iOS phone to scan the corresponding QR code to download and install the App.
Step 2: Run the client and log in to the account (No account is required to register first).
Step 3: Add devices to the mobile client.

After login,Go to home page, click " " , select "SN Add(Recommend)", scan the SN QR code on the device or P2P interface, enter the device name, user name, password and verification code on label(CAPTCHA) after scan the QR code (the verification code printed on the label or view on P2P settings interface), select group, click "Add" .
Step 4: Live preview
After adding the device on the mobile client, the binding status on the device's P2P page will be displayed as "Bound";On the mobile client homepage, find the device you want to preview in real time, click the corresponding thumbnail, and start playing the real-time video.

You can also modify the verification code of the device. After modification, you can add the device in the mobile client with the new verification code. At the same time, in addition to checking the device binding status, you can also actively unbind the device. After unbinding, the manual client needs to re-add the device before it can be used normally.

NOTE

- The device P2P is enabled by default. To use this function, the device must be connected to the external network, and the connection status is displayed as “P2P connection successful”. Otherwise, it will not work properly.
- If the P2P page verification code is modified, it will be inconsistent with the device label. If modified, the verification code displayed on the modified P2P page shall prevail.

8.4.3 Email

After setting the email information and enabling the alarm linkage email function, when the IPC triggers an alarm, the system sends an alarm email to the user mailbox.

The specific operation steps are as follows:

Step 1: In the main interface, click "Configuration →Network → Email" to enter the email settings interface, as shown in Figure 8-4-17.

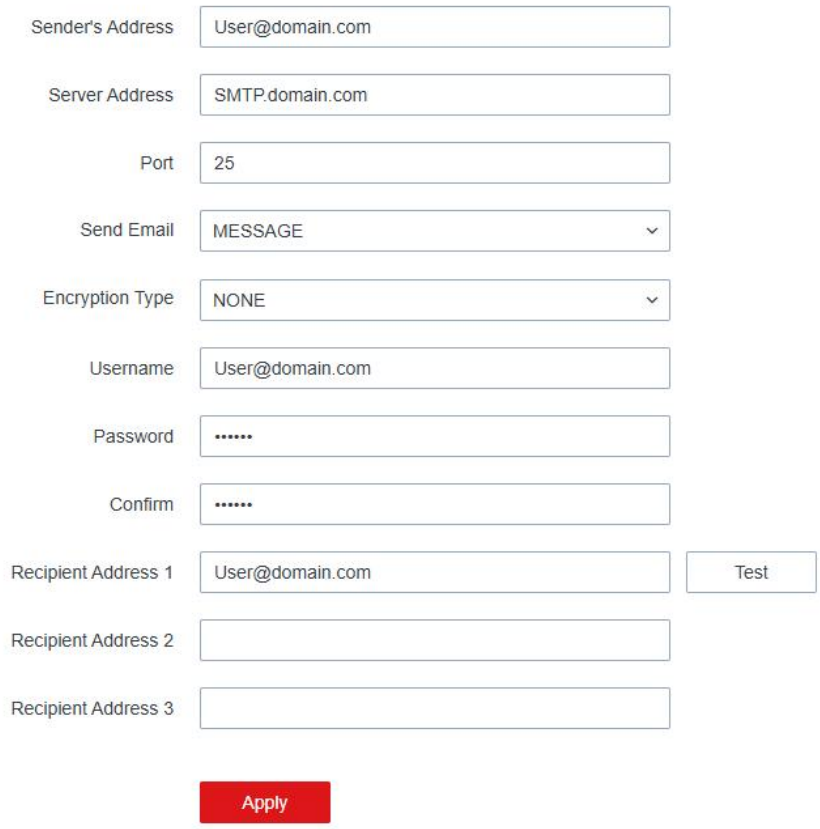


Figure 8-4-17

Step 2: Configure Sender's Address, Server Address, Port, Send Email, Encryption Type, User Name, Password, and Receiver.

Step 3: Click "Test" to confirm whether the network connection and SMTP configuration are correct.

Step 4: Click "Apply" to save the configuration.

NOTE：

Sender

【Sender's Address】Fill in the full address of the sender mailbox.

【Server Address】Fill in your email server address.

【Port】Fill in your email server port.

【Send Email】In the drop-down menu, select SMTP file format, JPEG image format and message for selection.

【Encryption Type】You can select the encryption type from the drop-down menu, supporting SSL, TLS or no encryption, to ensure that data is sent to the correct client and server.

【User Name】Fill in the send mailbox user name.

【Password】Fill in the send mailbox password.

【Confirm】Fill in the send mailbox password.

Receiver

【Receiver's Address 1, 2, 3】Fill in the full address of your inbox, here up to 3 inboxes, click on the completion of the completion of the "Test" to ensure that all the correctness of the input information and network connectivity of the camera.

8.5 Video and Audio

In the main interface, click "Configuration → Video and Audio" to enter the video and audio configuration interface, where you can set the device video, audio and other functions.

8.5.1 Video

In the main interface click "Configuration → Video and Audio → Video" into the video configuration interface, where you can set the profile, stream type, encoding and other video parameters, as shown in Figure 8-5-1.

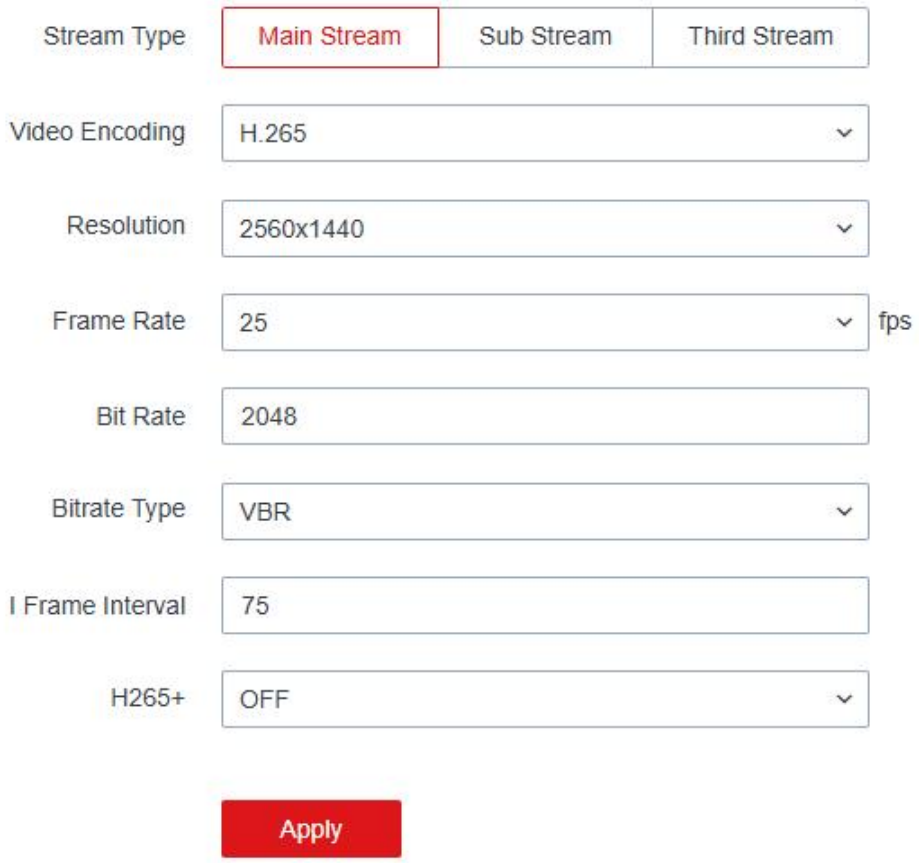


Figure 8-5-1

【Stream Type】Default is the Main Stream, you can select Sub Stream or Tri-Stream.

【Profile】Default is the Main Profile, you can select Basic Profile or High Profile.

【Video Encoding】Switch the encoding method in the drop-down menu.

【Resolution】Switch the output resolution in the drop-down menu.

【Frame Rate】Set the frame rate of the current output video of the device.
【Bit Rate】Support 64-12000kbps. The higher the bit rates the better video quality, but it occupy the greater network bandwidth and the greater the pressure transmission.
【Bitrate Type】 Switch the code rate output mode in the drop-down menu, fixed rate and variable rate.
【I-Frame Interval】IPC acquisition key frame interval, can be set 1-400ms.
【H265+/H264+】Turn on/off the camera H265+/H264+.
【Watermark】Turn on/off the watermark function. It can prevent the video from being tampered after it is turned on. After setting the "watermark name", use our "HSPlayer" player to check whether the video has been tampered with and the watermark information.
【Watermark name】Enter a watermark name.

NOTE

- Depending on the IPC function, device stream type, encoding, frame rate and other information in the drop-down menu options are also different.
- Only cameras that support the H264/H264+ function display Profile items on the video interface.
- When the frame rate is set too low, it will cause video carton, please be careful.
- The higher the bit rate, the greater the current network bandwidth and the greater the transmission pressure.
- Only cameras that support the H264+/H265+ function display H264+/H265+ on/off items on the video interface.
- When the camera turns the H265+/H264+ on or off, it takes 30-60 seconds. Please be patient.

8.5.2 Audio

In the main interface, click "Configuration → Video and Audio → Audio" to enter the audio configuration interface, where you can set the device audio input mode, select the audio code, set the input volume, as shown in Figure 8-5-2.

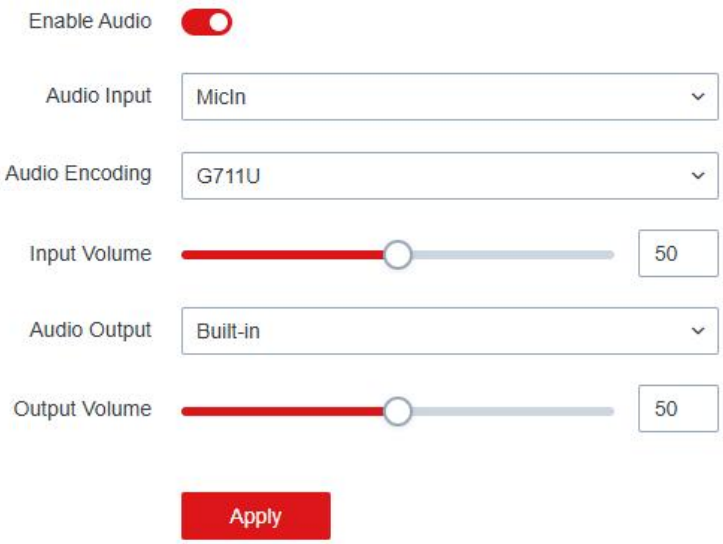


Figure 8-5-2

【Enable Audio】Turn on / off device audio input.
【Audio Input】Select the audio input method.
【Audio Encoding】Choose audio encoding, G711U/ G711A /AAC.
【Input Volume】Set the device input volume,the volume range is 0-100.
【Audio Output】Select the audio output method.
【Output Volume】Set the device output volume,the volume range is 0-100.

NOTE

- Depending on the IPC function, the configuration items on the audio configuration page will be different, and the options for audio input, encoding, audio output, etc. in the drop-down menu will also be different.

8.5.3 ROI

ROI is the area of interest setting, users can set the most concerned and most interested area in the video screen through this function, IPC will improve the video image quality of the corresponding area when video encoding, reduce the encoding quality of other areas, so as to highlight The image effect in the selected area.

The specific operation steps are as follows:

Step 1: In the main interface, click "Configuration → Video and Audio → ROI" to enter the ROI setting interface, as shown in Figure 8-5-3.

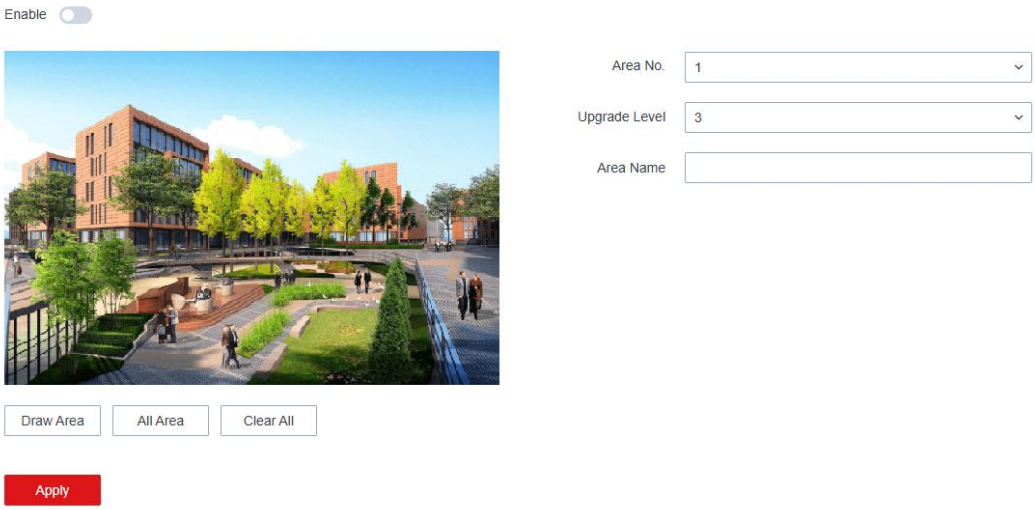


Figure 8-5-3

Step 2:

- 【Draw Area】 Move your mouse over the preview image, press and hold the left-mouse button to select the ROI area range, then release the left-mouse button. Click "Stop Drawing" to complete area drawing.
- 【All Area】 Click to automatically select the entire image area.
- 【Clear All】 Clears all areas of the drawing.
- 【Area No.】 Select the configured area. Up to three areas can be set.
- 【Upgrade Level】 The higher the value, the more obvious the improvement of video image quality in the corresponding area; the lower the value, the more obvious the quality reduction in the corresponding area.
- 【Area Name】 You can assign a mark to the configured area number. The area name will not be displayed on the live image.

Step 3: Click “Apply” to complete the ROI setting.

NOTE

- The ROI function depends on the specific model, and the ROI function is only supported under the H.264 or H.265 code. Other codes do not support the ROI function at this time.
- The ROI configuration is more effective when using a non-ROI frame rate setting is lower.

8.6 Image

In the main interface, click "Configuration → Image" to enter the image configuration interface, where you can set the device image and OSD text and other information.

8.6.1 Image

In the main interface, click "Configuration → Image → Image" to enter the image configuration interface, where you can adjust the related image parameters such as Image Adjustment, Exposure Settings, Day and Night Mode, White Balance, Video Adjustment, Image Enhancement and BackLight Settings, as shown in Figure 8-6-1.

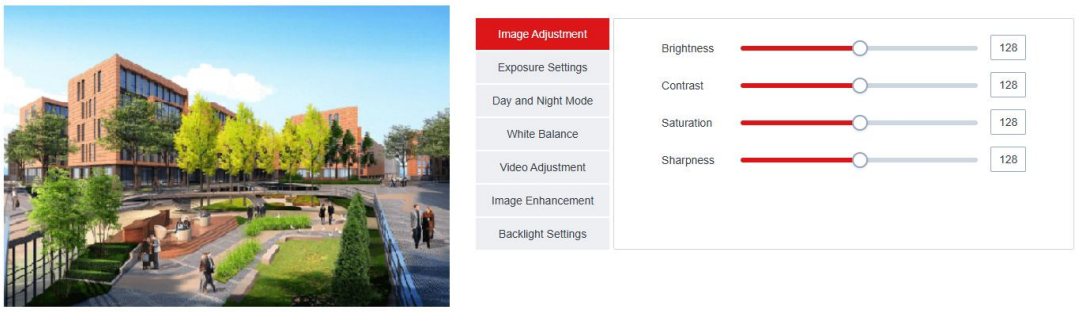


Figure 8-6-1

【Image Adjustment】You can input the value manually to set brightness, contrast, saturation, sharpness. These parameters shall be set according to the actual environment. The scope of valid values is from 0 to 255, you can drag the slider to set, and the default value is 128, as shown in Figure 8-6-2.



Figure 8-6-2

【Exposure Settings】You can see the Aperture Type of the camera, set the Exposure Settings according、Anti Flicker to actual needs, and automatically save after setting. As shown in Figure 8-6-3.

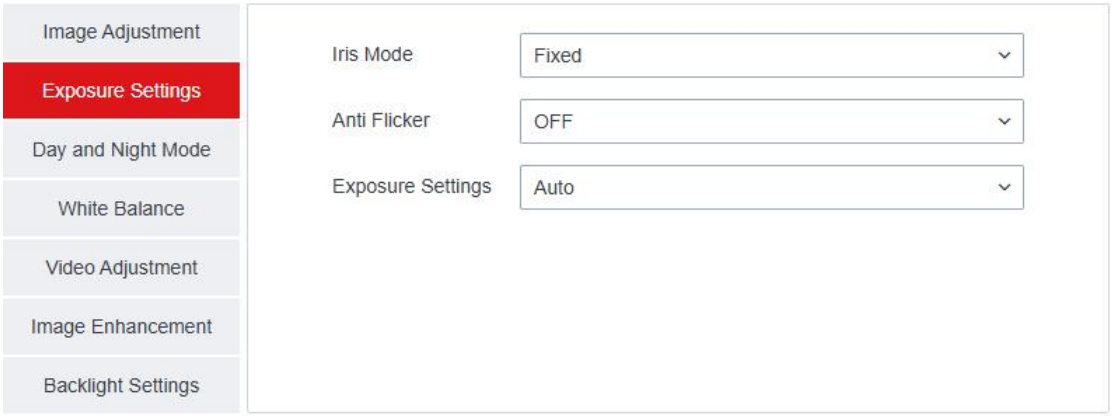


Figure 8-6-3

【Day and Night Mode】The fill light mode defaults to automatic, sensitivity is 3, filter time is 3 seconds, light brightness is 100, as shown in Figure 8-6-4. When the fill mode is "Auto", the device will turn on the fill light according to the actual environment. The user can switch the fill mode to "Day", "Night" and "Scheduled-Switch" according to the actual environment of the site, and switch the sensitivity and filter time of the device according to the fill mode.

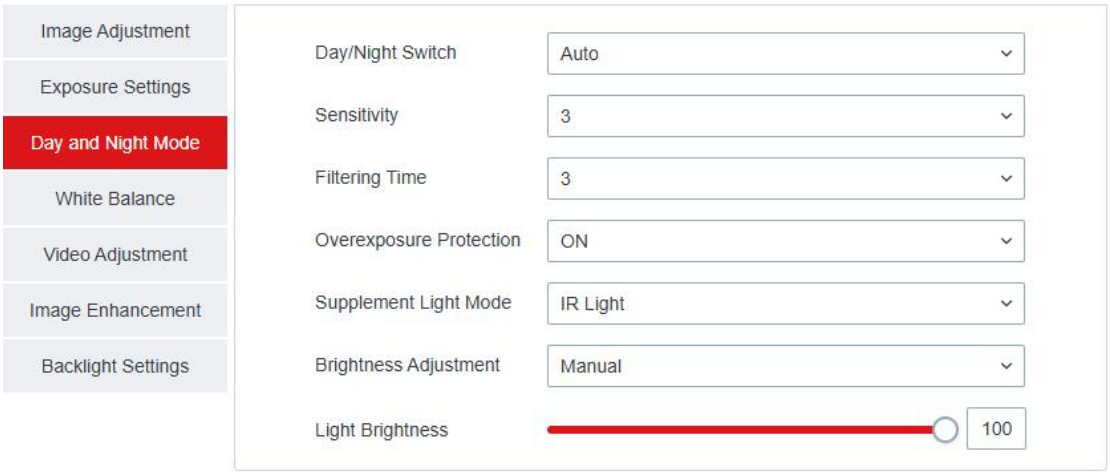


Figure 8-6-4

When the fill mode is "Scheduled-Switch", you can set the Dawn time and the Dark time (the start and end fill time) and the fill light brightness, as shown in Figure 8-6-5.

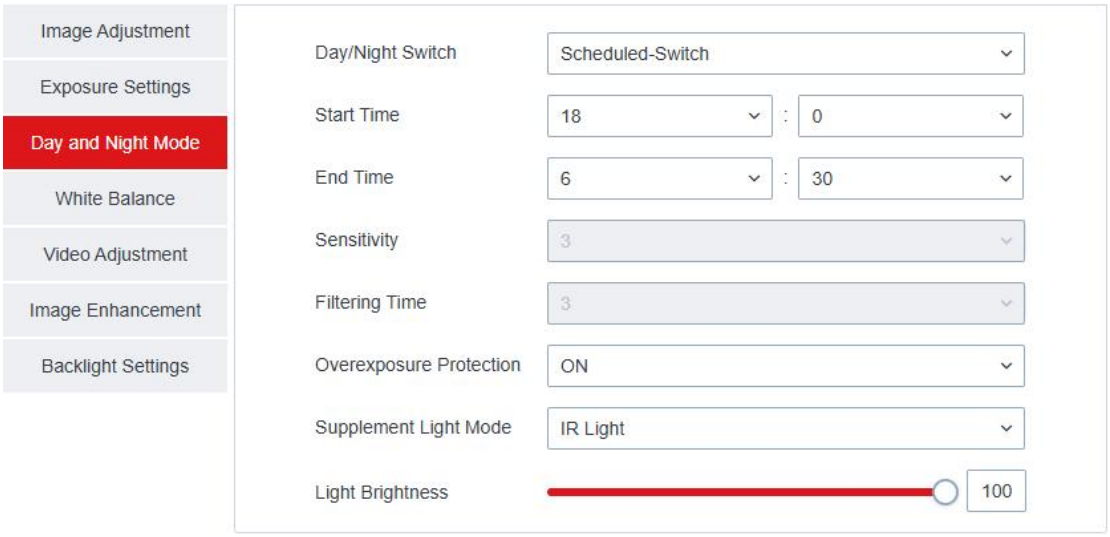


Figure 8-6-5

When the fill mode is "Day", the fill light of the device is always off, and the camera is in color mode.
When the fill mode is "Night", the fill light of the device is always on.

Filtering time: It is used to prevent the ambient light from getting better and the light is frequently turned on and off, and the filtering time is set. During this time period, the camera is not disturbed by ambient light.

Overexposure Protection: It is turned off by default. It can prevent overexposure in most scenes after turning it on.

Light brightness: It is used to adjust the brightness of the fill light, and the adjustable range is 0-100.

Supplement Light Mode: Depending on the capabilities of the device, it can support three modes: IR Light, Warm Light, and Intelligent.
When the fill light mode is "IR Light", the device supports ir light fill light.
When the fill light mode is "Warm Light", the device supports warm light fill light.
When the fill light mode is "Intelligent," the device defaults to ir light. Users can configure "Human," "Vehicle," and "Non-Motorized Vehicle" as detection targets ("Human" is the default, but can be selected simultaneously). Upon detecting a configured target, the device will automatically activate the warm light supplementary lighting. A delay time (the duration for which the warm light is on) can also be configured.

【White Balance】Default AWB1, switchable Manual, Fluorescent Lamp, Warm Light, Natural Light, there are six types of automatic white balance, which can meet the needs of customers in different scenarios.As shown in Figure 8-6-6.

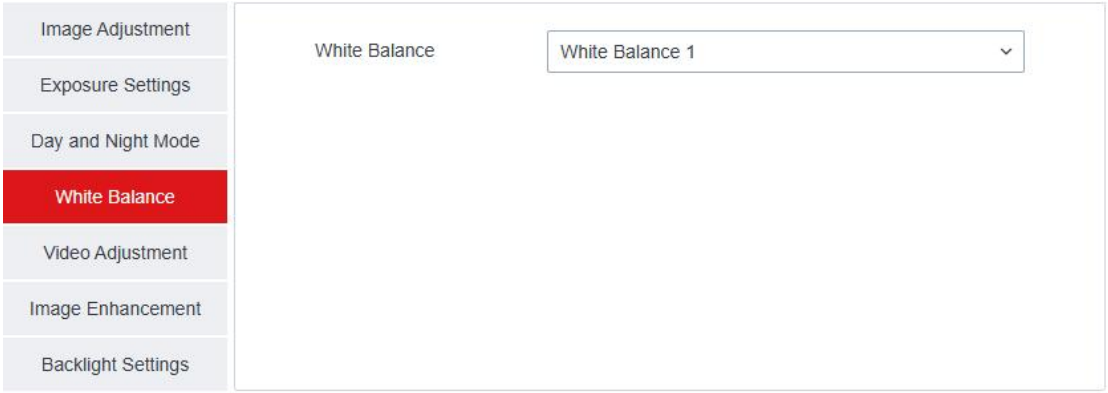


Figure 8-6-6

White balance 1, White balance 2: Both are in automatic mode; "White Balance 2" has a wider white balance range than "White Balance 1."

Manual: It is support Red, Blue gain adjustable, adjust the range (0-255).

Fluorescent Lamp: This preset adapts to fluorescent-lamp light sources, and the image tone leans toward blue.

Warm Light: This preset adapts to warm-lamp light sources, and the image tone leans toward red.

Natural Light: This preset adapts to natural-light environments, and its imaging performance is similar to the auto white-balance mode.

【Video Adjustment】Here you can turn on Mirror, Corridor Mode,and set the Video Format, as shown in Figure 8-6-7.

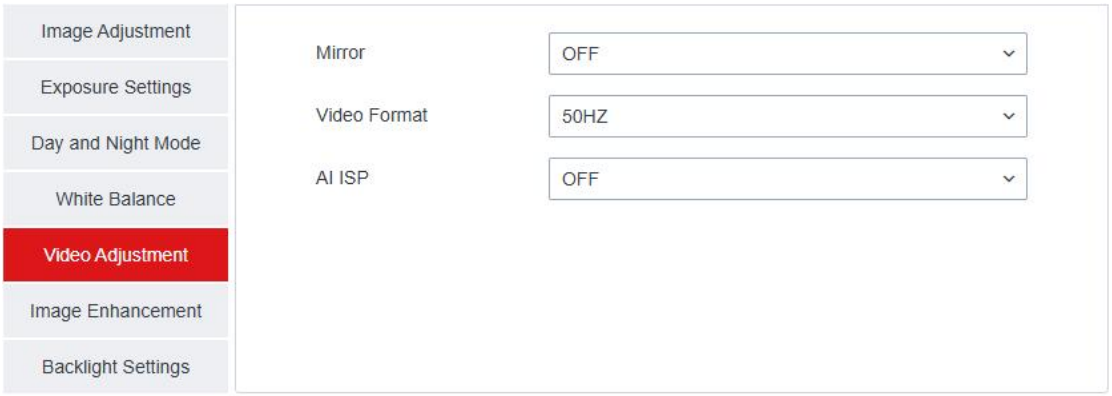


Figure 8-6-7

Mirror: The default is Off, you can switch Level, Vertical, Both, when the device video image is reversed, through the menu to flip the image.

Corridor Pattern: The default is Off, open the corridor mode, you can choose to preview the interface rotated 90 degrees and 270 degrees.

Video Format: The default setting is PAL (50HZ) shipment,you can switch in the drop-down menu NTSC(60HZ),switching the video format requires restarting the device to take effect.

AI ISP: You can turn on and off the AI ISP function according to the actual scenario. For devices that support the AI ISP function, it is turned on by default.

【Image Enhancement】Here you can turn on WDR , Digital Noise Reduction , Distortion Correction , Defog Mode , as shown in Figure 8-6-8.

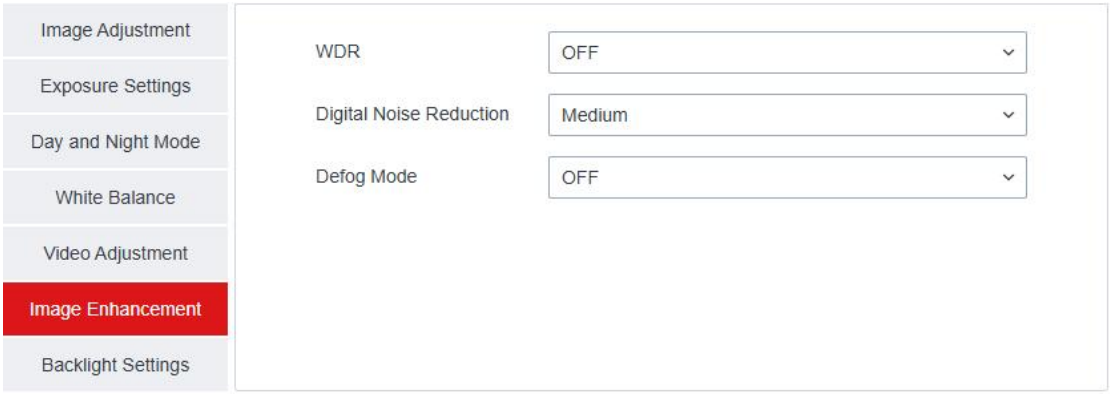


Figure 8-6-8

WDR： The default is Shut Down, you can switch in the drop-down menu Low, Mid, High.
Digital Noise Reduction： The default is Shut Down, you can switch in the drop-down menu Low, Mid, High.
Distortion Correction： The default is Shut Down, you can switch in the drop-down menu turn on.
Defog Mode： The default is Shut Down, you can switch in the drop-down menu Low, Mid, High.

【Backlight Settings】It is used to set backlight compensation and strong light suppression. The default is off, it can be turned on manually, as shown in Figure 8-6-9.



Figure 8-6-9

BLC： It is off by default. once turned on, the intensity can be adjusted by dragging.
HLC： It is off by default; you can select to turn it on from the drop-down menu.

NOTE

- The camera image interface only displays the device support functions. The specific interface is subject to the actual product.
- WDR, BLC, and HLC are mutually exclusive. Turning on one of these functions will automatically turn off the other two functions.

8.6.2 OSD

The OSD is information displayed on the real-time monitoring screen. The name, date, and day of the IPC can be displayed on the monitor screen.
In the main interface, click "Configuration → Image → OSD" to enter the OSD configuration interface, where you can set the preview interface to display menu time, OSD text and other information, as shown in Figure 8-6-10.

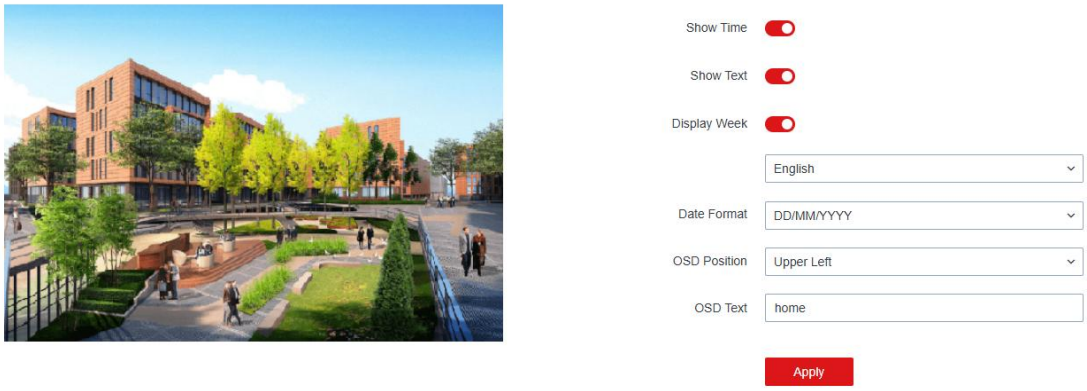


Figure 8-6-10

【Show Time】Turn on / off the preview interface time display.
【Show Text】Turn on / off the preview interface OSD text display.
【Display week】Turn on/off the time display in the preview interface, you can choose "English" or "Chinese".
【Date Format】Set the preview interface to display the date format, default day / month / year, switchable month / day / year and year / month / day options.
【OSD Position】This sets the position of the time or OSD text displayed in the preview interface. The default is the top left, which can be switched to the bottom left by pulling down the dropdown menu. Alternatively, you can drag the preview window to any position.
【OSD Text】Enter the preview interface to display text information, such as hall elevator, hall door and other equipment location information.

8.6.3 Privacy Mask

Privacy occlusion is a privacy protection feature that blocks the privacy of the surveillance screen from being viewed and recorded.
In the main interface, click "Configuration → Image → Privacy Mask" to enter the privacy mask settings interface. As shown in Figure 8-6-11.

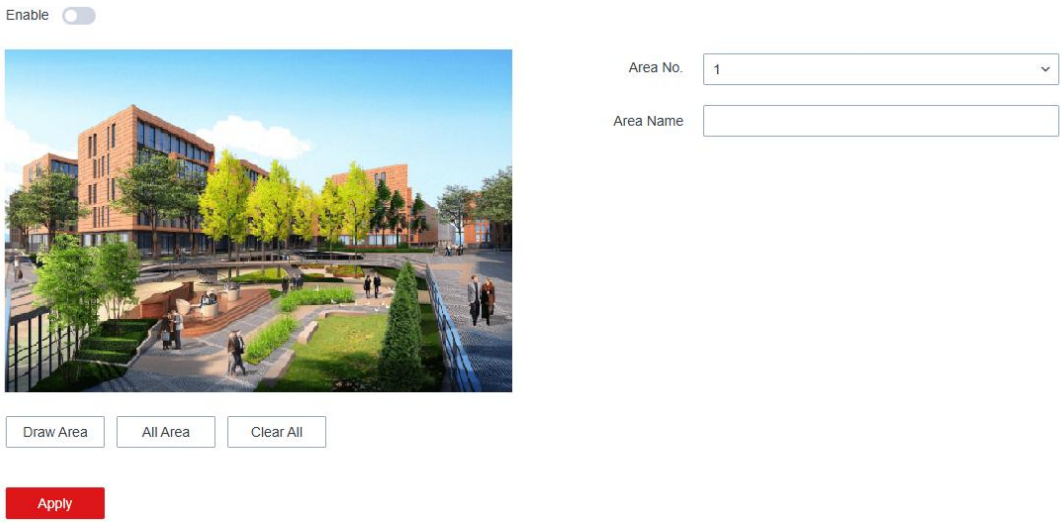


Figure 8-6-11

The detailed setup steps are as follows.

Step 1: Basic Settings: Enable Privacy Masking to activate the privacy masking function of the network camera.

Step 2: Select and configure the privacy mask area. Click "Apply" to complete the area configuration.

- 【Draw Area】 Move your mouse over the preview image, press and hold the left- mouse button to select the privacy- mask area range, then release the left- mouse button. Click "Stop Drawing" to complete area drawing.
- 【All Area】 Click to automatically select the entire image area.
- 【Clear All】 Clears all areas of the drawing.
- 【Area No.】 Select the configured area. Up to three areas can be set.
- 【Area Name】 You can assign a mark to the configured area number. The area name will not be displayed on the live image.

Step 3: Click “Apply” to complete the Privacy Mask setting.

8.7 Event

In the main interface, click "Configuration → Event" to enter the event configuration interface,including Basic Event and Smart Event.

8.7.1 Basic Event

In the Basic Event interface, you can set the device's Motion Detection, Video Tampering, Alarm Input, Alarm Output, Exception, Audible alarm output, and other events.

① Motion

The motion detection function is used to detect whether there is a moving object in a certain area within a certain period of time. When there is a moving object, the IPC will

alarm according to the setting.

The specific operation steps are as follows:

Step 1: In the main interface click on the "Configuration → Event → Basic Event → Motion" to enter the motion detection settings interface, as shown in Figure 8-7-1.

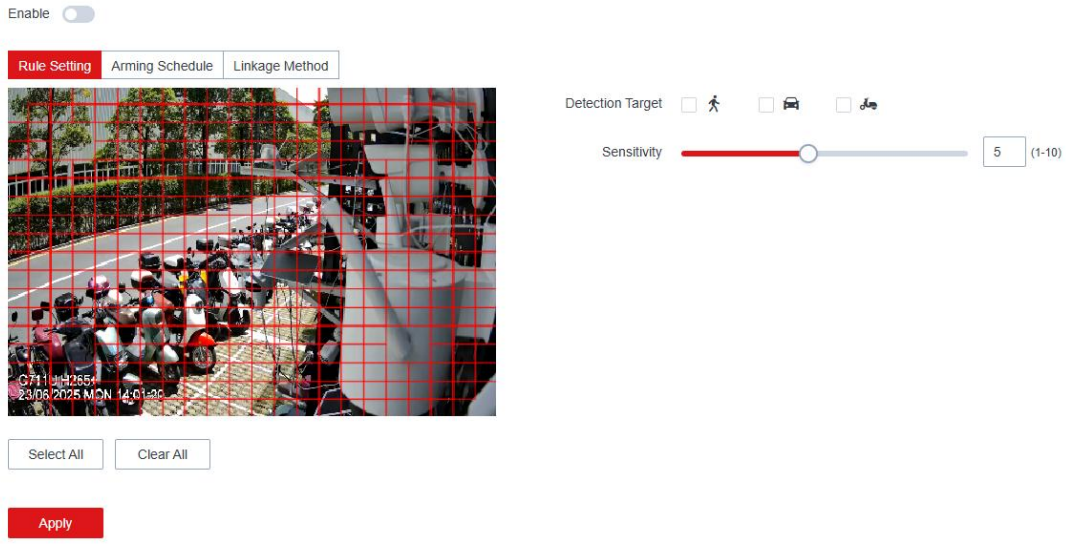


Figure 8-7-1

Step 2: Click "Enable" to turn on the motion detection alarm.

Step 3: Select the area to set the detection target,motion detection sensitivity, click "Apply".

【Select All】Motion detection range to monitor all of the area, which Consists of 396(22*18) small squares.

【Manually draw the alarm area】Move the mouse to the preview screen, click the left mouse button to select the range of motion detection, release the left mouse button to complete the alarm area selection. A camera can select multiple motion detection zones at the same time.

【Clear All】Clearing all the motion detecting area that selected currently.

【Detection Target】Set the target to be detected, supports Human, Vehicle and Non-Motor Vehicle, Human is selected by default.

【Sensitivity】The default is 5, can switch the range of 1-10. The larger the value, the easier the device will trigger an alarm.

Step 4: Set the arming schedule.

As shown in Figure 8-7-2, you can view, edit, and delete the arming time of motion detection. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.

– After setting, click "Apply" to complete the setting of the arming time.

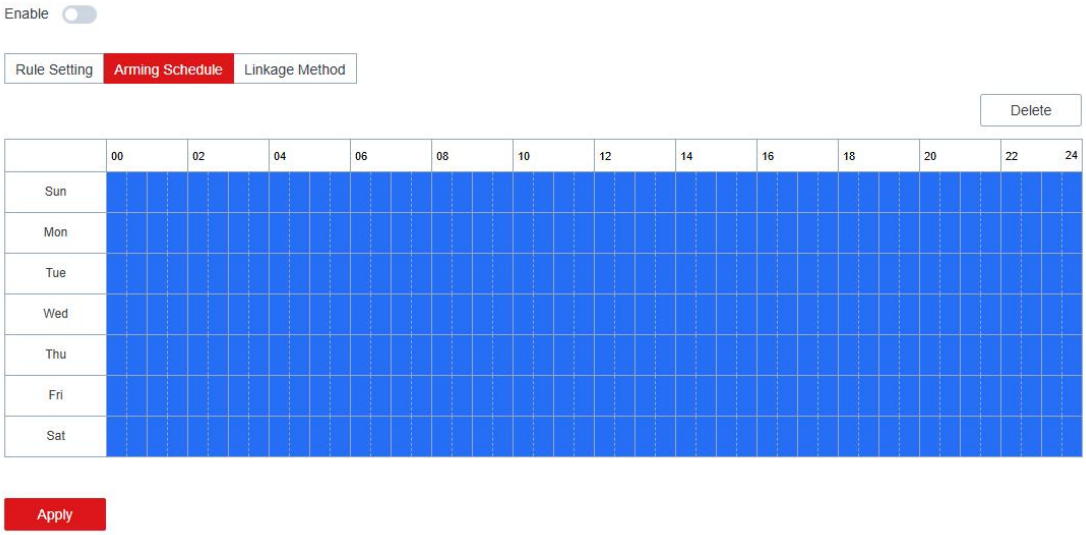


Figure 8-7-2

NOTE

- When the arming time is set, there can be no overlap between any two time periods.

Step 5: Set the linkage method.

Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via Cloud, Light Warning,Sound Alarm) and linkage alarm output(IO Output), as shown in Figure 8-7-3.

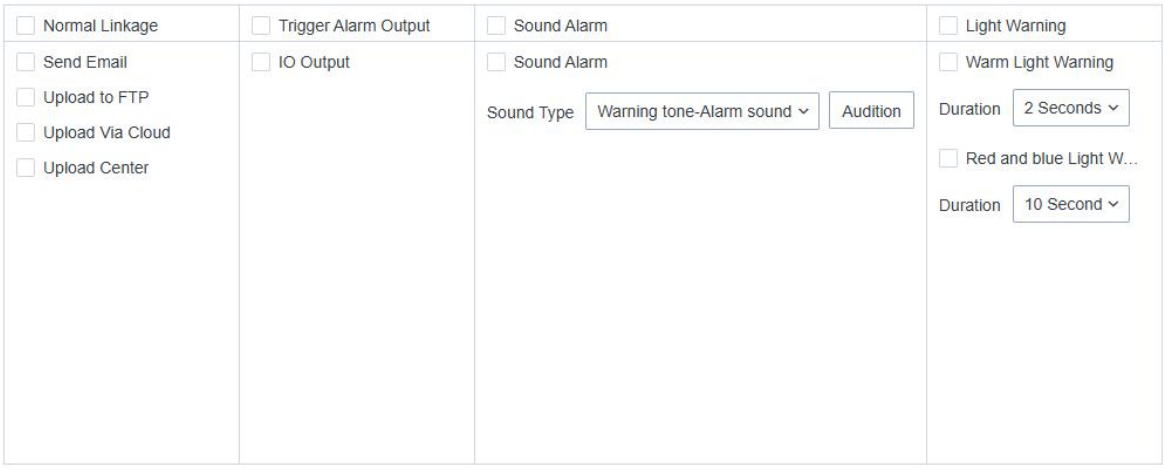


Figure 8-7-3

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.
【Light Warning】After selection, the device will link the alarm light to flash.
【IO Output】Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.
【Sound Alarm】After selection, the device will emit an alarm sound when alarming.

NOTE

- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.

②Video Tampering

The video tampering alarm function is used to detect whether a monitoring area is blocked by human factors and other factors during a certain period of time. When the area of the device is blocked, the IPC will alarm according to the settings. When the video tampering alarm is generated, the video tampering cause can be quickly discharged and the monitoring screen can be restored.

The specific operation steps are as follows:

Step 1: In the main interface click on the "configuration → Event → Basic Event → Video Tampering" to enter the video tampering settings interface, as shown in Figure 8-7-4.

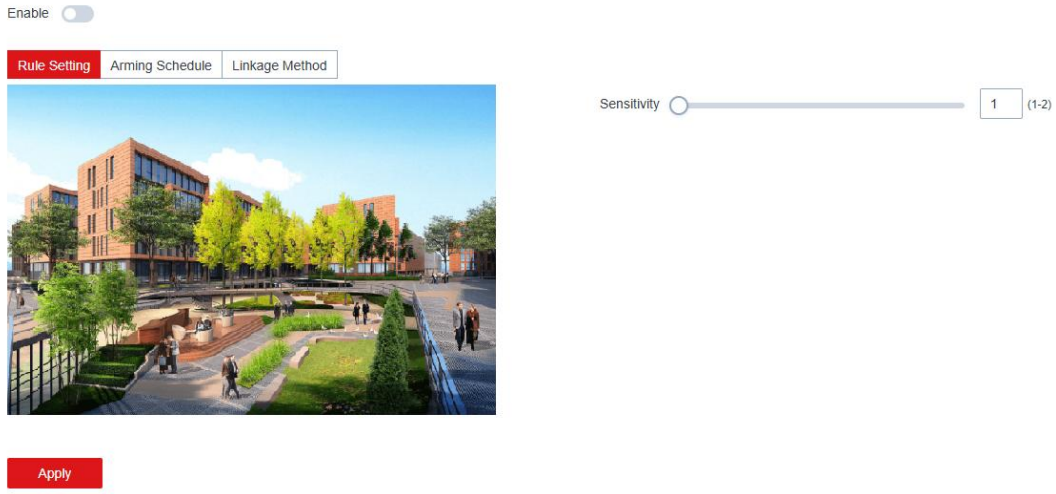


Figure 8-7-4

Step 2: Click "Enable" to turn on the video tampering alarm.
Step 3: Select the area to set the video tampering sensitivity, click "Apply".
【Draw Area】Move the mouse to the preview screen, click the left mouse button to select the range of motion detection, release the left mouse button, draw a 4-sided area, support dragging to adjust the position of the 4-sided area, dragging the vertex to adjust the size of the 4-sided area,click “Stop Drawing” to complete the alarm area selection.

【Clear All】Clearing all the video tempering area that selected currently.
【Sensitivity】The default is 1, can switch the range of 1-2, the greater the value of the more sensitive equipment alarm.

Step 4: Set the arming schedule.

As shown in Figure 8-7-5, you can view, edit, and delete the arming time of the video tampering.The default is 0 arming 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.

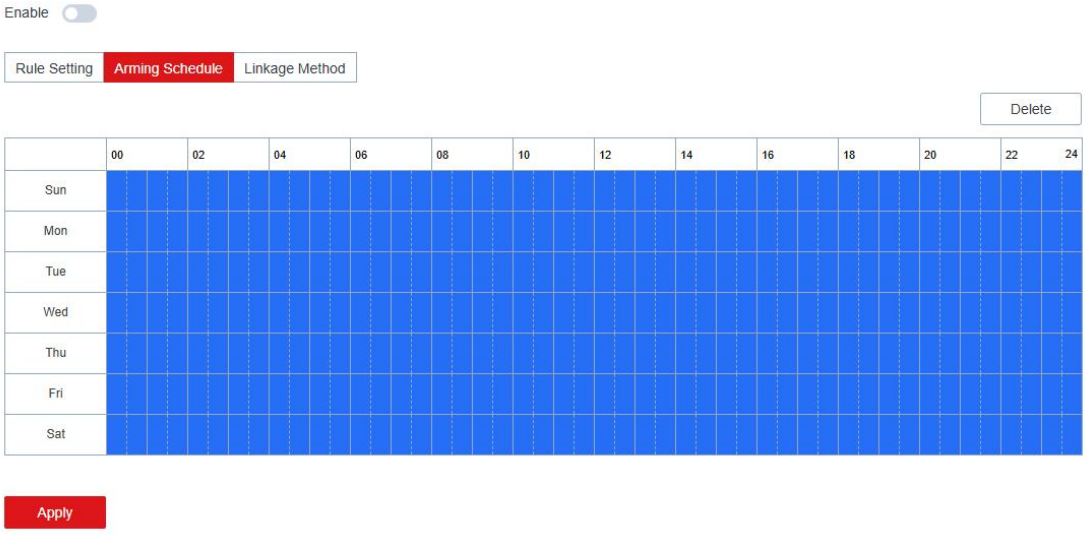


Figure 8-7-5

NOTE

- When the arming time is set, there can be no overlap between any two time periods.

Step 5: Set the linkage method.

Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via Cloud, Light Warning,Sound Alarm) and linkage alarm output(IO Output), as shown in Figure 8-7-6.

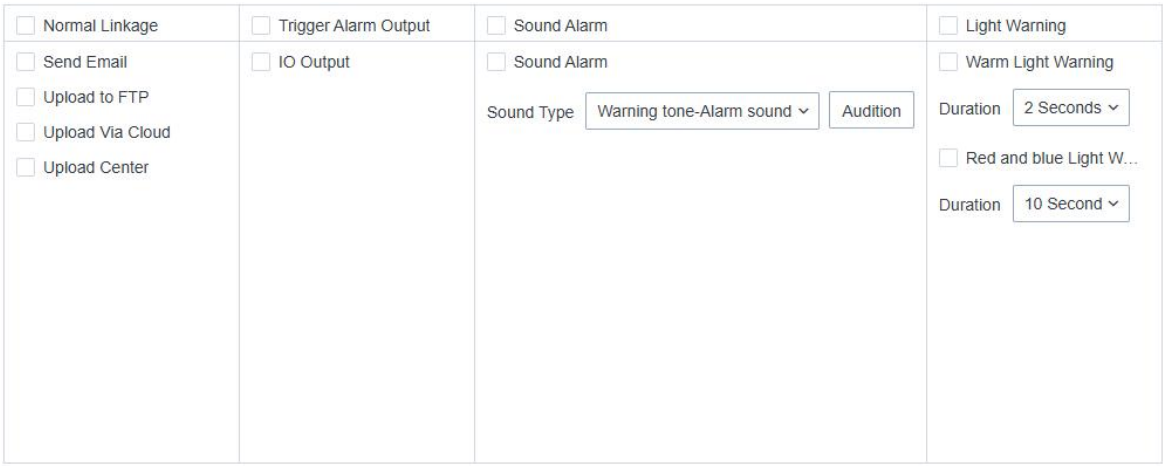


Figure 8-7-6

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.

【Light Warning】After selection, the device will link the alarm light to flash.

【IO Output】Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.

【Sound Alarm】After selection, the device will emit an alarm sound when alarming.

NOTE

- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.

③Alarm Input

Prerequisites

Before configuration, the device needs to be connected to the alarm input device. By configuring the alarm input, the alarm signal received by the alarm input device can be passed to the IPC for further processing.

The specific operation steps are as follows:

Step 1: In the main interface click on the "configuration → Event → Basic Event → Alarm Input" to enter the Alarming Input settings interface.

Step 2: Select the alarm input and alarm type(Normally open, Normally closed).

Step 3: Set the arming schedule.

As shown in Figure 8-7-7, you can view, edit, and delete the arming time of the alarm input. The default is 0 arming 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.

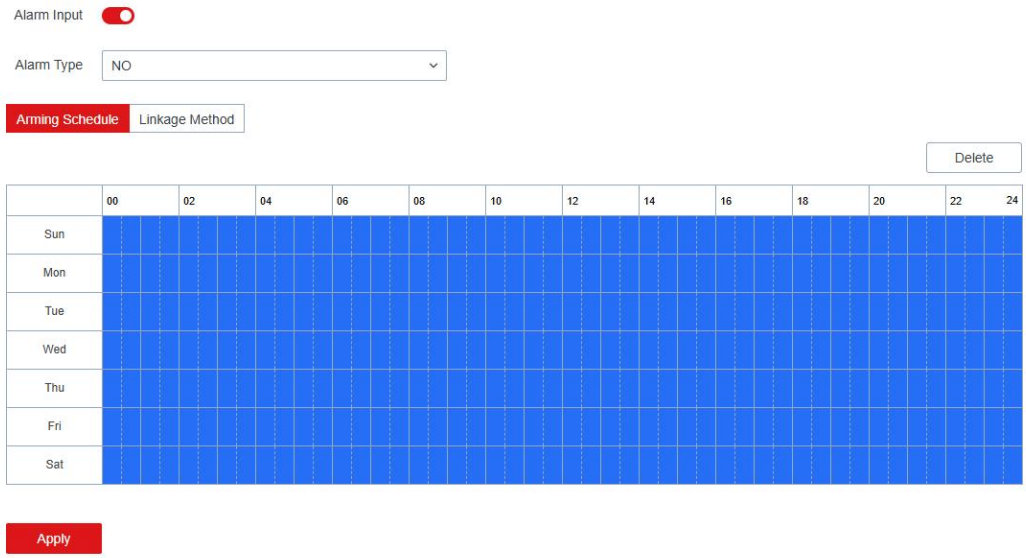


Figure 8-7-7

Step 4: Set the linkage method.

Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via Cloud, Light Warning,Sound Alarm) and linkage alarm output(IO Output), as shown in Figure 8-7-8.

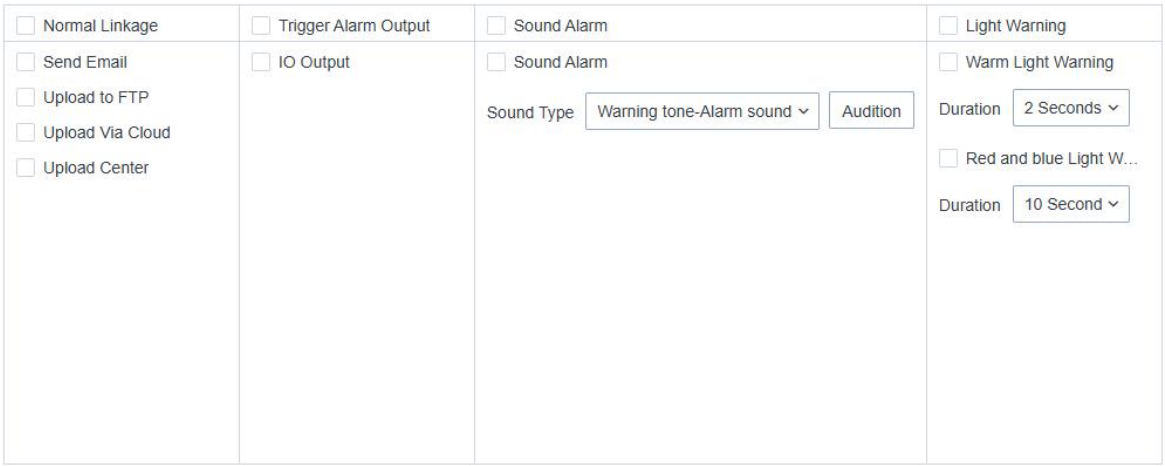


Figure 8-7-8

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.
【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.
【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.
【Light Warning】After selection, the device will link the alarm light to flash.
【IO Output】Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.
【Sound Alarm】After selection, the device will emit an alarm sound when alarming.

NOTE

- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.

④ Alarm Output

Prerequisites

Before configuration, the device needs to be connected to the alarm output device. By configuring the alarm output, the alarm signal received by the alarm input device can be passed to the IPC for further processing.

The specific operation steps are as follows:

Step 1: In the main interface click on the "configuration → Event → Basic Event → Alarm Output" to enter the Alarming Output settings interface.
Step 2: Set the duration.
Step 3: Set the arming schedule.
As shown in Figure 8-7-9, you can view, edit, and delete the arming time of the alarm input. The default is 0 arming 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.

Step 4: Click "Apply" to complete the setting of the arming time.

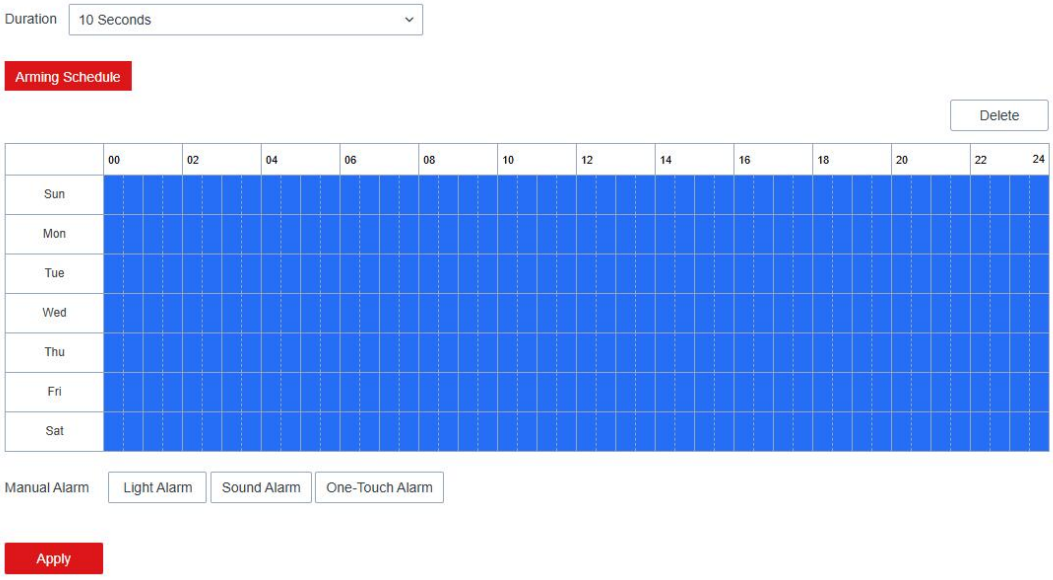


Figure 8-7-9

【Manual alarm】Manually triggering the alarm output devices on the device's own light, sound, and alarm output interfaces will trigger an alarm only once.

⑤ Abnormality Settings

Abnormal alarm types include "Network Broken", "IP Address Conflicted", "Disk Abnormality" and "Disk Full". When an abnormal event occurs during the operation of the IPC, the system executes the alarm linkage action."Disk Abnormality" and "Disk Full" support Normal Linkage.

The specific operation steps are as follows:

Step 1: In the main interface, click "Configuration → Event → Basic Event → Abnormality Settings" to enter the exception settings interface, as shown in Figure 8-7-10.

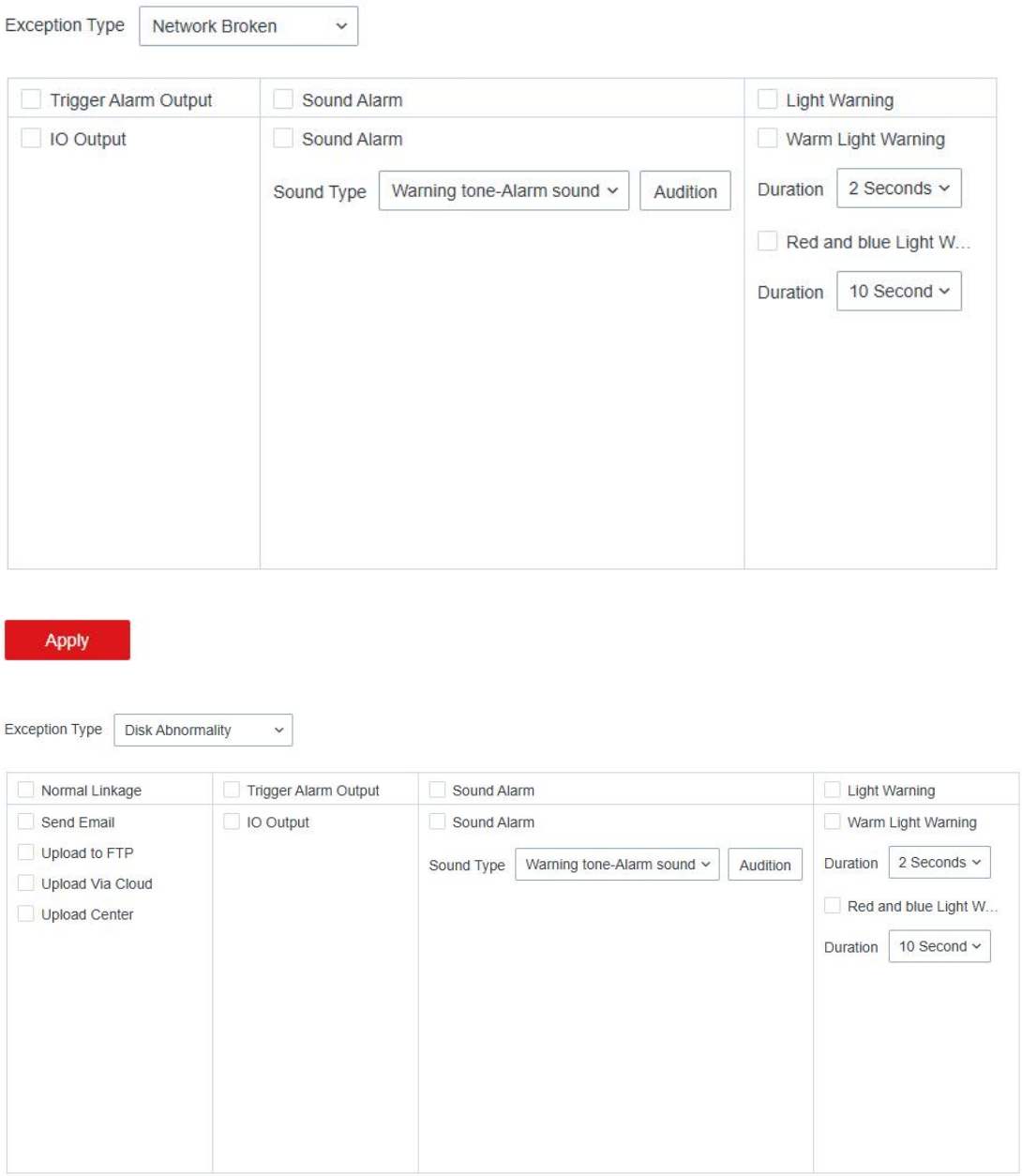


Figure 8-7-10

Step 2: Select the exception type and set the alarm output method.

Step 3: Click on the “Apply” after completing the settings.

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.

【IO Output】Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.

【Sound Alarm】After selection, the device will emit an alarm sound when alarming.
【Light Warning】After selection, the device will link the alarm light to flash.

⑥Sound Alarm

After configuring the sound alarm, when the event is triggered, the speaker on the device can be linked to alarm.

The specific operation steps are as follows:

Step 1: In the main interface, click "Configuration → Event → Basic Event → Sound Alarm" to enter the Sound Alarm setting interface, as shown in Figure 8-7-11.

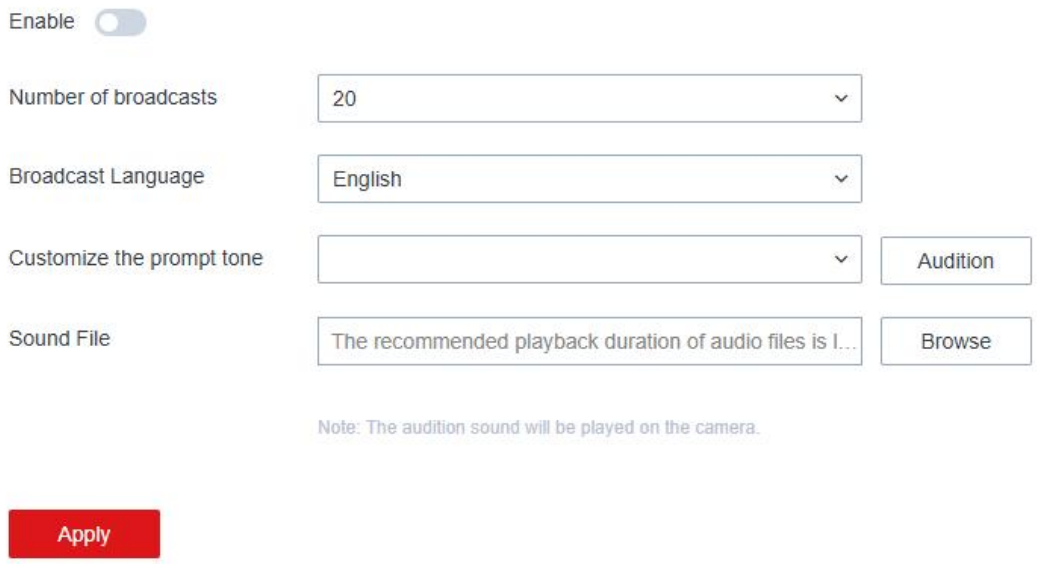


Figure 8-7-11

Step 2: Click "Enable"to turn on the sound alarm.

Step 3: Set number of broadcasts: default 3, optional 1-20.

Step 4: Set the broadcast language, you can choose Chinese and English.

Step 5: You can customize the upload of sound files, you need to select Custom in the sound type, and then select your own sound file to upload (Only supports one sound file, G711U,mp3,wav format are supported, File size less than 100K, -3dB, the recommended file broadcast time is less than 12S, and then you can lisen the uploaded custom audio file in the camera).

Step 6: Click “Apply” to complete the sound alarm setting.

NOTE

- Some cameras do not support the Sound Alarm. The specific interface is subject to the actual product.
- Custom audio files must be -3dB, otherwise there is a risk of burning the speakers.

⑦Alarm Server

After configuring the alarm server, when an event is triggered, the alarm event and screenshot can be sent to the set target IP or domain name.

The specific operation steps are as follows:

Step 1: On the main interface, click “Configuration → Event → Common Event → Alarm Server” to enter the alarm server interface, as shown in Figure 8-7-12 below.

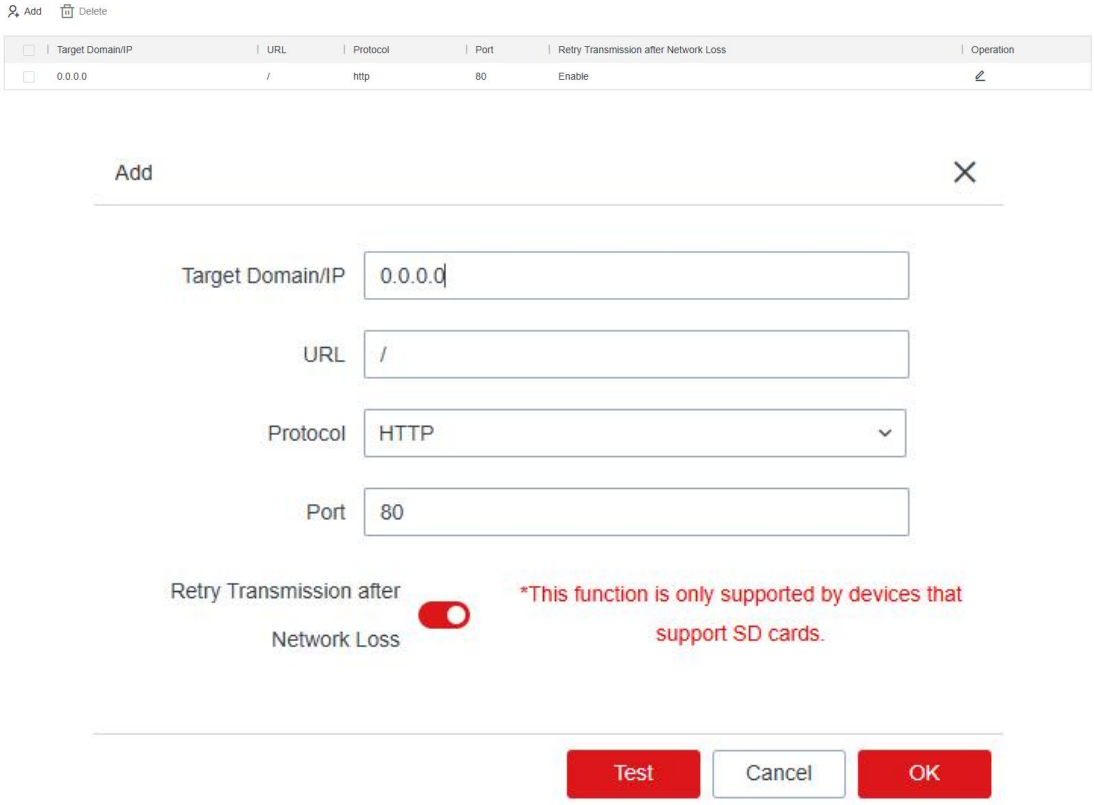


Figure 8-7-12

Step 2: Click " Add " and enter the relevant information in the pop-up window for adding an alarm server.

【Target Destination/IP】 defaults to 0.0.0.0. Enter the IP address or domain name of the corresponding alarm server according to your needs.

【URL】 defaults to /. Enter the URL according to your needs.

【Protocol】defaults to HTTP, with HTTPS optional. Configure the protocol type based on the server's support.

【Port】The default port is 80. Depending on the selected protocol type, the default port is displayed. The default port for HTTPS protocol is 443. Customers are supported to customize the port according to actual conditions.

【Retry Transmission after Network Loss】 is enabled by default but can be disabled. When enabled, data will be automatically cached to the SD card when the device network experiences an anomaly. When the device network is restored, the cached data will be uploaded.

Step 3: Click "Test" to test the validity of the added alarm server.

Step 4: Click "OK" to complete the alarm server addition.

Step 5: Click "" to edit the added alarm server information.

Step 6: Click " 删除 " to delete the added alarm server.

NOTE

- The offline resume function requires a device that supports SD cards, and the SD card must be formatted before using the offline resume function for the first time.
- Supports up to 3 servers, supports different ports on the same server, but does not support the same port on the same server.

⑧ Sound Detection

Enable and configure sound detection. When the volume changes by more than a certain value or the volume itself exceeds the set threshold, an alarm event will be generated and a linkage alarm will be triggered based on the judgment result.

The specific operation steps are as follows:

Step 1: On the main interface, click "Configuration → Events → Common Events → Sound Detection" to enter the sound detection interface, as shown in Figure 8-7-13 below.



Figure 8-7-13

Step 2: Check "Enable" to enable sound detection.

Step 3: Configure the sound detection settings. Once completed, click "Apply" below.

【Detection Type】Abrupt Change(default), Sudden Rise, Sudden Drop , Threshold.

【Difference】The difference between two volume levels. Integer value between 10-400, default 100. This setting is available when the detection type is Steep Rise, Steep Fall, or Sudden Change.

【Threshold】An alarm is generated when the volume exceeds the limit. Integer value

between 0-400, default 200. This setting is available when the detection type is Threshold.
【Relative Sound Intensity Progress Chart】Supports a graphical display of relative sound intensity, allowing customers to more intuitively see sound changes. The vertical sound intensity bar refreshes in real time and moves from right to left. Click "ON" or "Stop" to advance or pause the progress bar. A gray vertical line indicates relative sound intensity, while a red vertical line indicates that the sound meets the alarm reporting conditions, triggering a sound detection alarm.
【Vernier】Drag the vernier to measure the real-time volume.

Step 4: Set the arming schedule.

As shown in Figure 8-7-14. You can view, edit, and delete the arming time of the intrusion detection. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.



Figure 8-7-14

NOTE

- When the arming time is set, there can be no overlap between any two time periods.

Step 6: Set the linkage method as needed.

Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via Cloud, Light Warning) and trigger alarm output(IO Output), as shown in Figure 8-7-15.

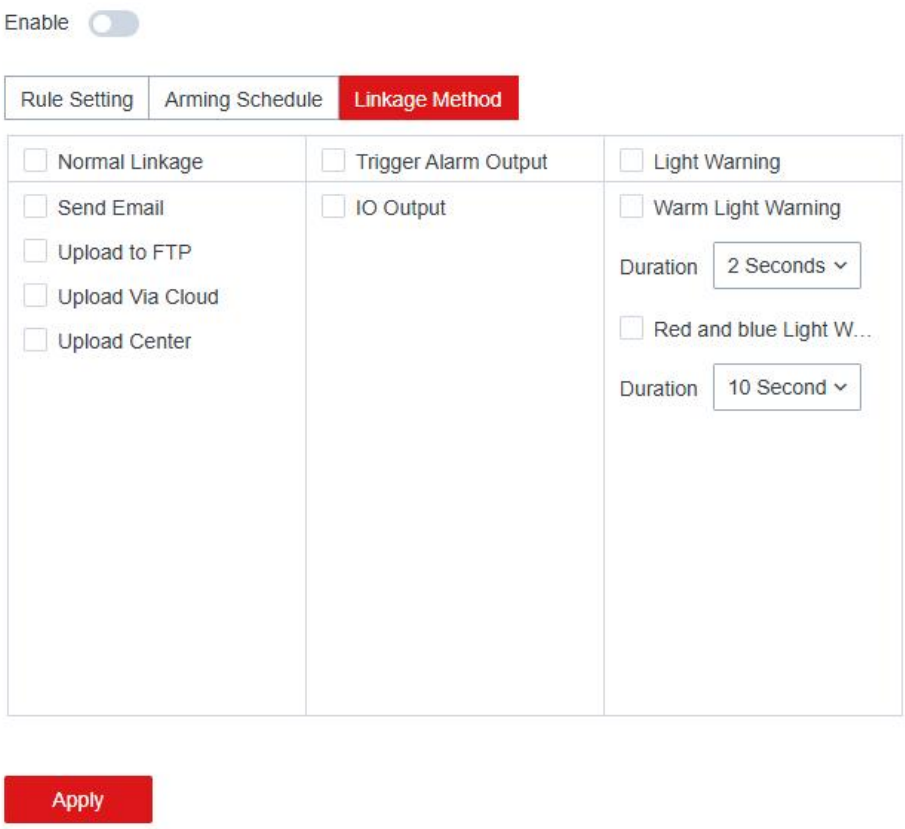


Figure 8-7-15

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.

【Light Warning】After selection, the device will link the alarm light to flash.

【IO Output】Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.

NOTE

- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.

⑨Scene Change

Enable and configure scene change detection. When the camera scene changes, an alarm event can be generated, and a linked alarm can be triggered based on the judgment result.

The specific operation steps are as follows:

Step 1: On the main interface, click "Configuration → Events → Common Events → Scene Change" to enter the scene change interface, as shown in Figure 8-7-16 below.

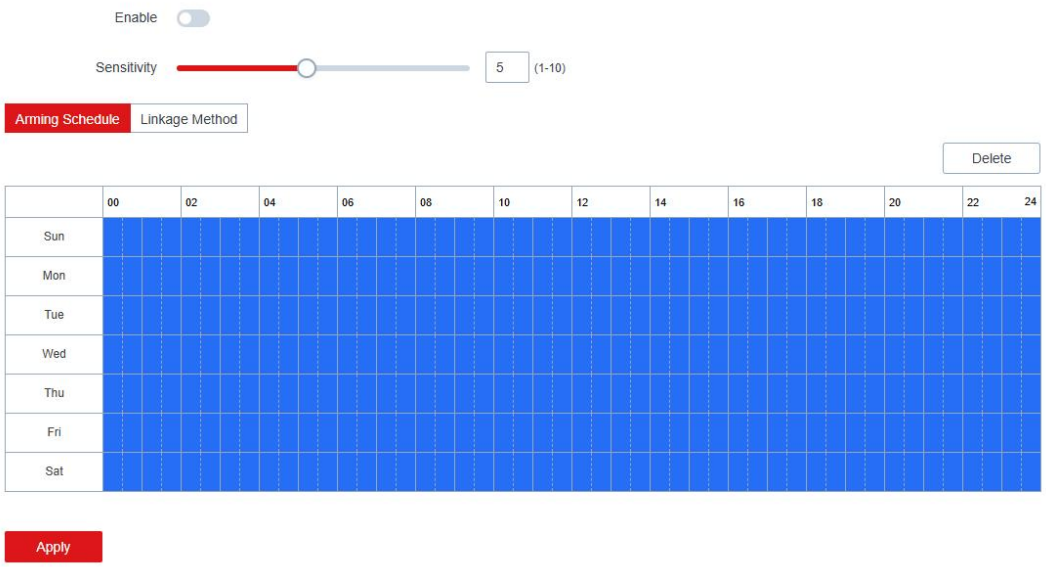


Figure 8-7-16

Step 2: Check "Enable" to enable scene change detection.

Step 3: Configure scene change sensitivity settings from 1 to 10, with a default value of 5. Higher values result in greater sensitivity to scene changes, making it easier to trigger alarms, but also reducing detection accuracy.

Step 4: Set the arming schedule.

As shown in Figure 8-7-17. You can view, edit, and delete the arming time of the intrusion detection. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.

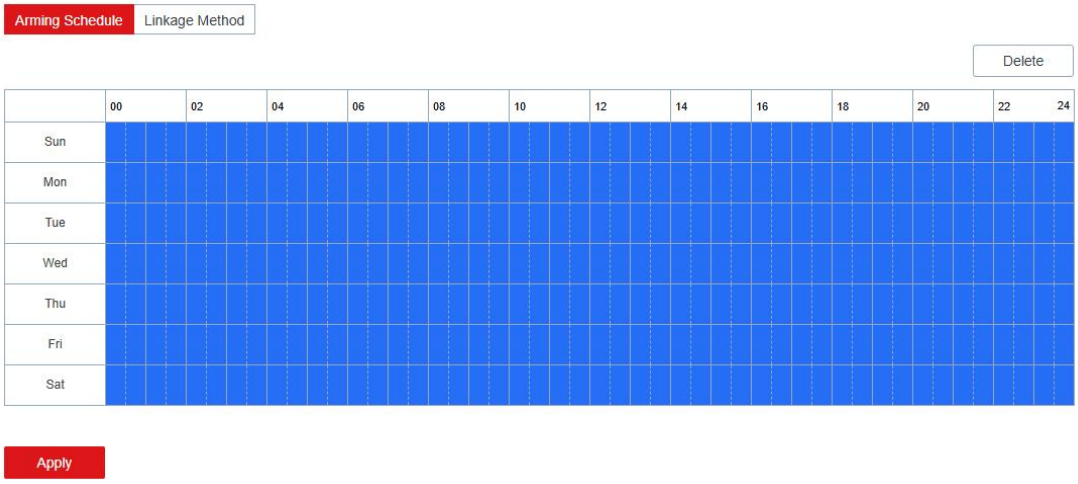


Figure 8-7-17

NOTE

- When the arming time is set, there can be no overlap between any two time periods.

Step 6: Set the linkage method as needed.

Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via Cloud, Light Warning,Sound Alarm) and trigger alarm output(IO Output), as shown in Figure 8-7-18.

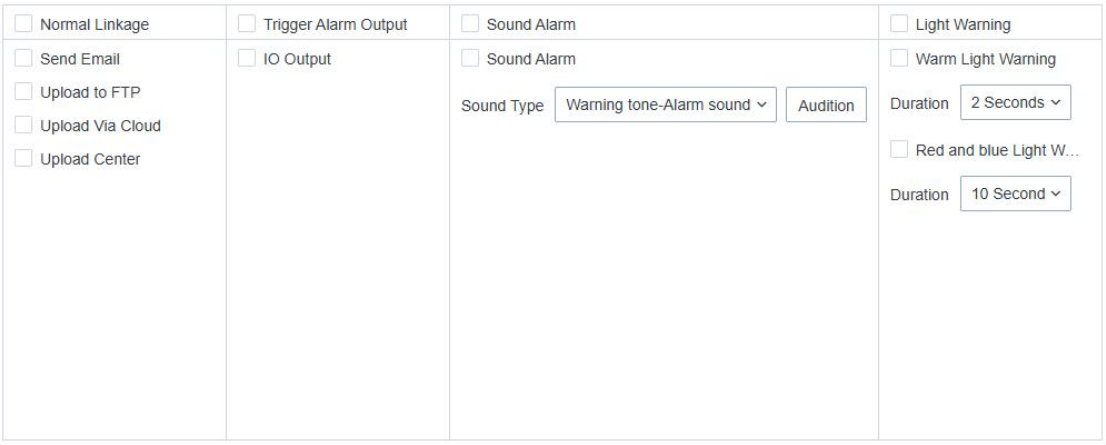


Figure 8-7-18

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.

【Light Warning】After selection, the device will link the alarm light to flash.

【IO Output】Select and the IO output port is connected to the alarm device. During the

alarm, the device will link the device to alarm.

【Sound Alarm】After selection, the device will emit an alarm sound when alarming.

NOTE

- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.

8.6.2 Smart Event

① Intrusion

The area intrusion detection is used to detect whether there is a target intrusion in the video setting area, and the alarm is linked according to the judgment result.

The specific operation steps are as follows:

Step 1: In the main interface click on the "Configuration → Event → Smart Event→ Intrusion" to enter the Intrusion Detection settings interface, as shown in Figure 8-7-19.

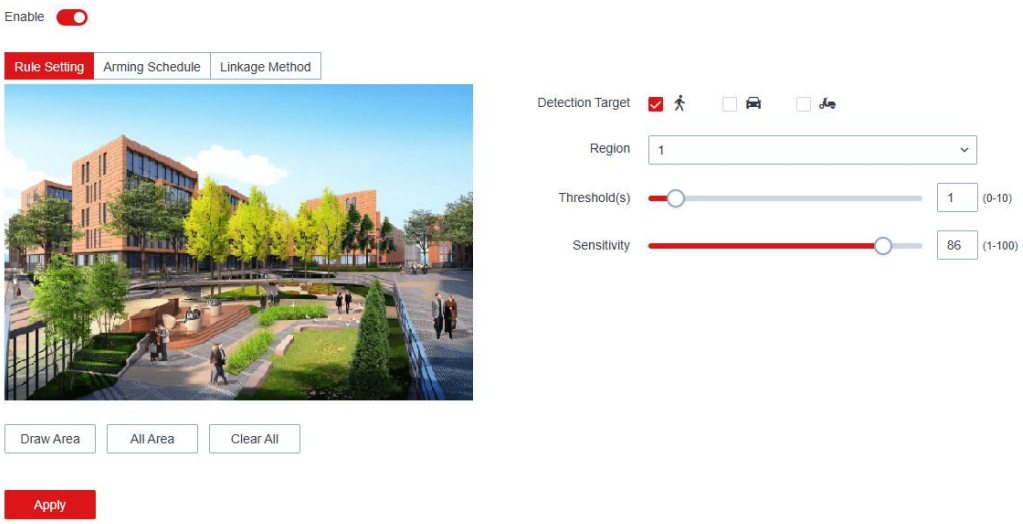


Figure 8-7-19

Step 2: Check "Enable" to enable intrusion detection.

Step 3: Select "Region": The system supports setting up to 4 warn region. After selecting a warn region, you need to make the following settings. After setting, please click "Apply".

【Draw Area】Click “Draw Area”, move the mouse to the preview screen and click the left mouse button in sequence to draw the endpoints of the 4-8 polygon warning area, right-click to end the polygon drawing, and support dragging polygon vertices to adjust the area size, drag the entire polygon to adjust the overall area position.

【All Area】When need all areas to be detected, click "All Area" to automatically select all areas.

【Clear All】Used to delete the selected alert area.

【Detection Target】Set the target to be detected, supports Human, Vehicle and

Non-Motor Vehicle, Human is selected by default.

【Threshold(s)】Indicates that the target enters the alert zone and continues to stay for this time to generate an alarm. If set to 5s, the target intrusion area will trigger an alarm after 5s.

【Sensitivity】Used to set the sensitivity of detected area intrusion. The default is 50. Drag the progress bar or enter the value directly in the value box to modify the sensitivity. The greater the sensitivity, the easier it is to trigger an alarm.

Step 4: When you need to set other Warn Region, repeat step 3 to complete the setup.

Step 5: Set the arming schedule.

As shown in Figure 8-7-20. You can view, edit, and delete the arming time of the intrusion detection. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.



Figure 8-7-20

NOTE

- When the arming time is set, there can be no overlap between any two time periods.

Step 6: Set the linkage method as needed.

Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via Cloud, Light Warning,Sound Alarm) and trigger alarm output(IO Output), as shown in Figure 8-7-21.

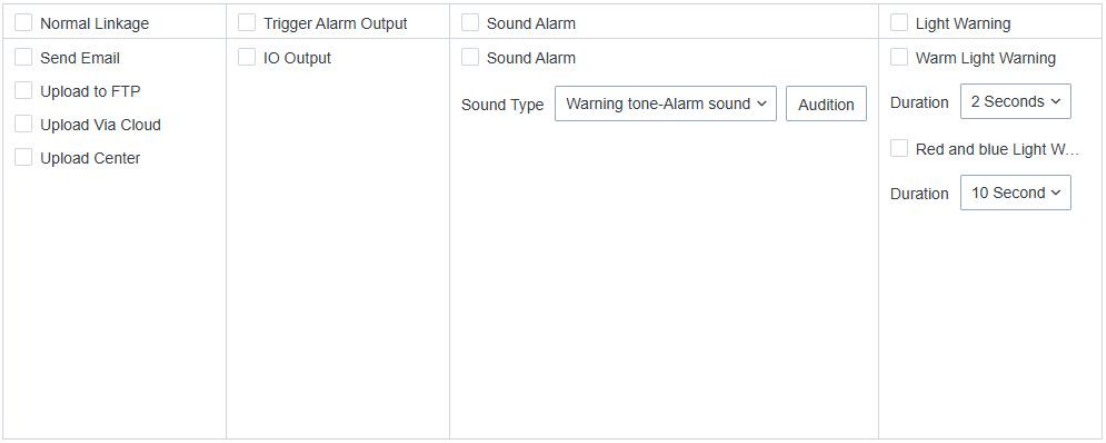


Figure 8-7-21

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.

【Light Warning】After selection, the device will link the alarm light to flash.

【IO Output】Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.

【Sound Alarm】After selection, the device will emit an alarm sound when alarming.

NOTE

- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.

② Enter Area

The entry area is used to detect whether the target entering the set area from outside the set area, and the alarm is linked according to the judgment result.

The specific operation steps are as follows:

Step 1: In the main interface click on the "Configuration → Event → Smart Event→ Enter Area" to enter the Enter Area Detection settings interface, as shown in Figure 8-7-22.

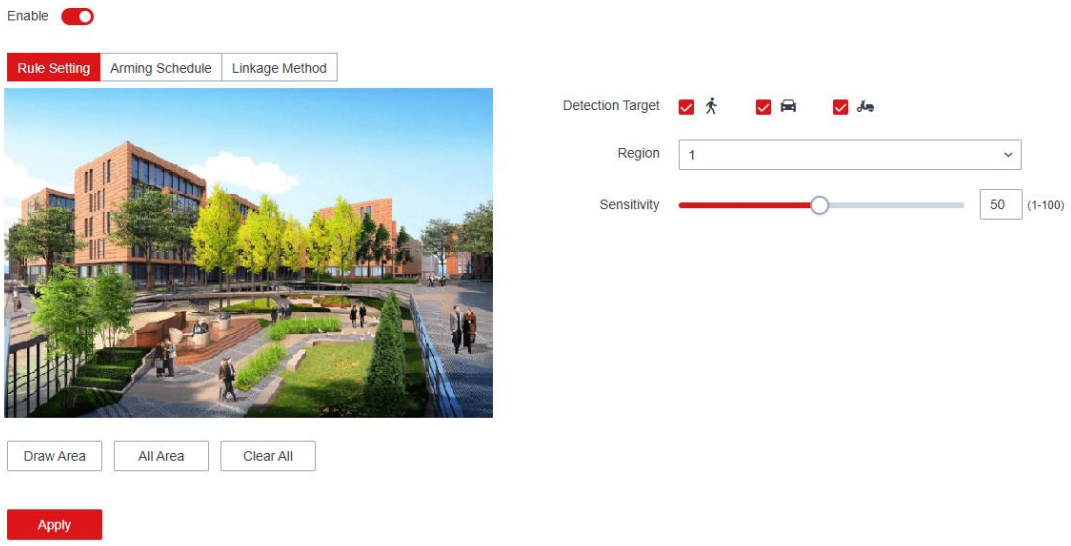


Figure 8-7-22

Step 2: Check "Enable" to enable enter area detection.

Step 3: Select "Region": The system supports setting up to 4 warn region. After selecting a warn region, you need to make the following settings. After setting, please click "Apply".

【Draw Area】Click “Draw Area”, move the mouse to the preview screen and click the left mouse button in sequence to draw the endpoints of the 4-8 polygon warning area, right-click to end the polygon drawing, and support dragging polygon vertices to adjust the area size, drag the entire polygon to adjust the overall area position.

【All Area】When need all areas to be detected, click "All Area" to automatically select all areas.

【Clear All】Used to delete the selected alert area.

【Detection Target】Set the target to be detected, supports Human, Vehicle and Non-Motor Vehicle, Human is selected by default.

【Sensitivity】Used to set the sensitivity of detected enter area. The default is 50. Drag the progress bar or enter the value directly in the value box to modify the sensitivity. The greater the sensitivity, the easier it is to trigger an alarm.

Step 4: When you need to set other Warn Region, repeat step 3 to complete the setup.

Step 5: Set the arming schedule.

As shown in Figure 8-7-23. You can view, edit, and delete the arming time of the enter area detection. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.

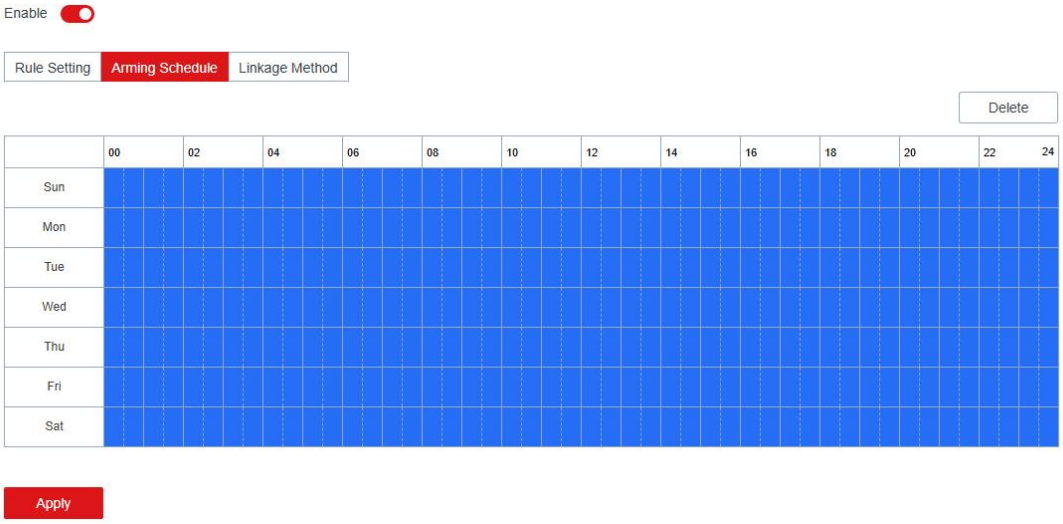


Figure 8-7-23

NOTE

- When the arming time is set, there can be no overlap between any two time periods.

Step 6: Set the linkage method as needed.

Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via Cloud, Light Warning,Sound Alarm) and trigger alarm output(IO Output), as shown in Figure 8-7-24.

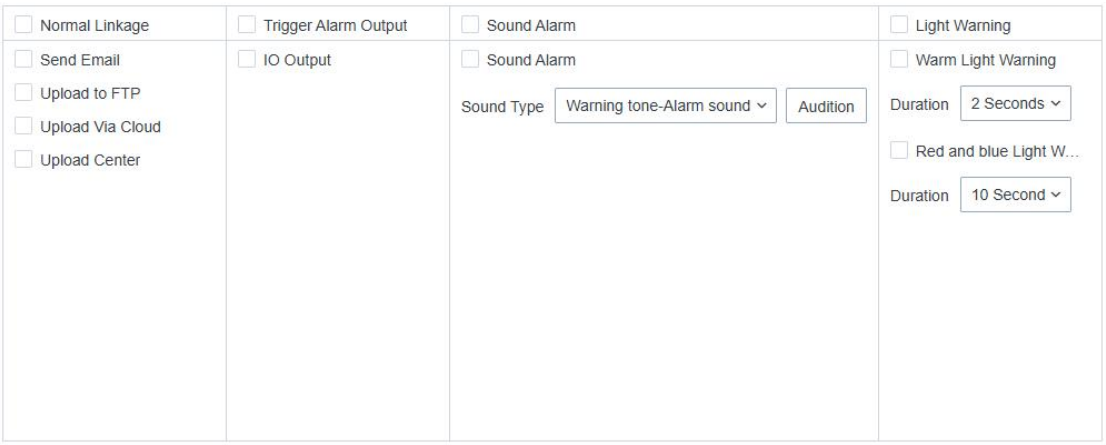


Figure 8-7-24

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.

【Light Warning】After selection, the device will link the alarm light to flash.

【IO Output】Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.
【Sound Alarm】After selection, the device will emit an alarm sound when alarming.

NOTE

- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.

③ Leave Area

The leave area is used to detect whether there is a target leaving the set area in the video setting area. When it reaches the set area, and the alarm is linked according to the judgment result.

The specific operation steps are as follows:

Step 1: In the main interface click on the "Configuration → Event → Smart Event→ Leave Area" to enter the Leave Area Detection settings interface, as shown in Figure 8-7-25.

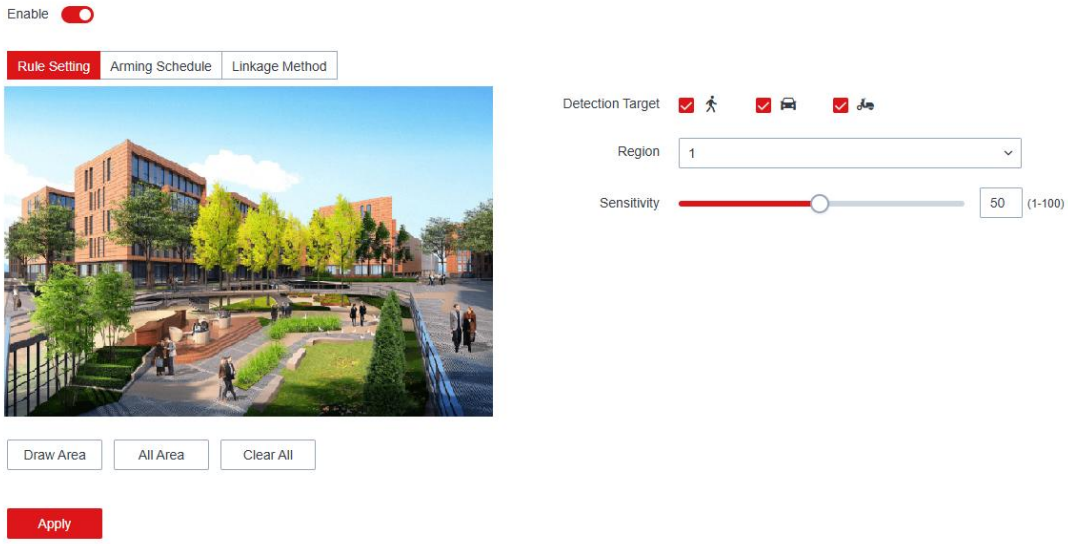


Figure 8-7-25

Step 2: Check "Enable" to enable leave area detection.

Step 3: Select "Region": The system supports setting up to 4 warn region. After selecting a warn region, you need to make the following settings. After setting, please click "Apply".

【Draw Area】Click “Draw Area”, move the mouse to the preview screen and click the left mouse button in sequence to draw the endpoints of the 4-8 polygon warning area, right-click to end the polygon drawing, and support dragging polygon vertices to adjust the area size, drag the entire polygon to adjust the overall area position.

【All Area】When need all areas to be detected, click "All Area" to automatically select all areas.

【Clear All】Used to delete the selected alert area.

【Detection Target】Set the target to be detected, supports Human, Vehicle and Non-Motor Vehicle, Human is selected by default.

【Time threshold(s)】Indicates that the target enters the alert zone and continues to stay for this time to generate an alarm. If set to 5s, the target intrusion area will trigger an alarm after 5s.

【Sensitivity】Used to set the sensitivity of detected leave area. The default is 50. Drag the progress bar or enter the value directly in the value box to modify the sensitivity. The greater the sensitivity, the easier it is to trigger an alarm.

Step 4: When you need to set other Warn Region, repeat step 3 to complete the setup.

Step 5: Set the arming schedule.

As shown in Figure 8-7-26. You can view, edit, and delete the arming time of the leave area detection. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.

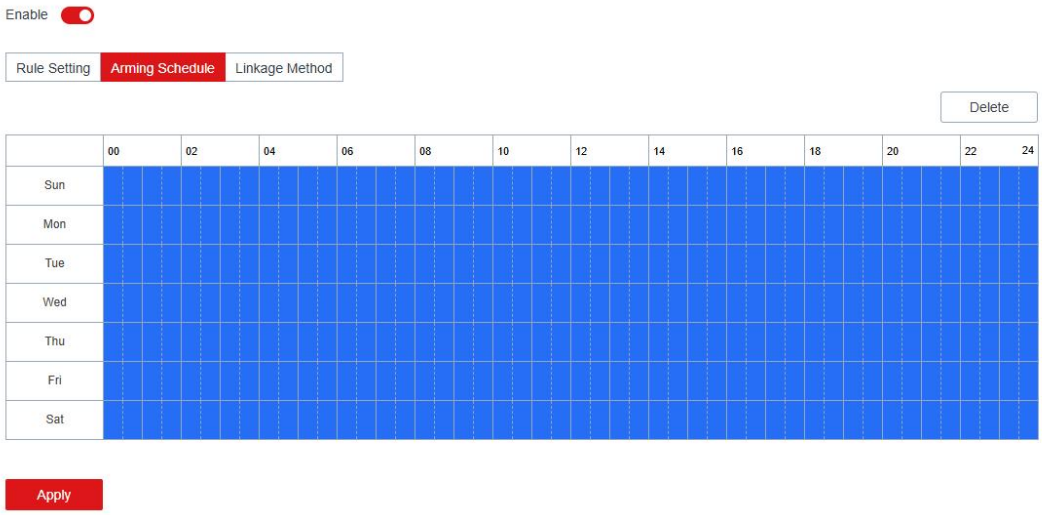


Figure 8-7-26

NOTE

- When the arming time is set, there can be no overlap between any two time periods.

Step 6: Set the linkage method as needed.

Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via Cloud, Light Warning,Sound Alarm) and trigger alarm output(IO Output), as shown in Figure 8-7-27.

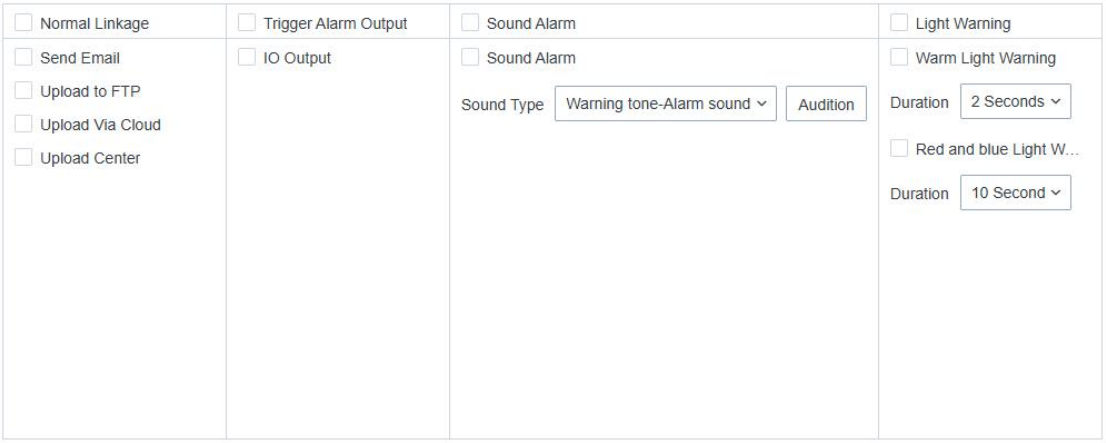


Figure 8-7-27

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.

【Light Warning】After selection, the device will link the alarm light to flash.

【IO Output】Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.

【Sound Alarm】After selection, the device will emit an alarm sound when alarming.

NOTE

- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.

④ Line Crossing Detection

The line crossing detection function is used to detect whether there is a target in the video that crosses the set warning surface, and the alarm is linked according to the judgment result.

The specific operation steps are as follows:

Step 1: In the main interface click on the "Configuration → Event → Smart Event → Line Crossing Detection" to enter the Line Crossing Detection settings interface, as shown in Figure 8-7-28.

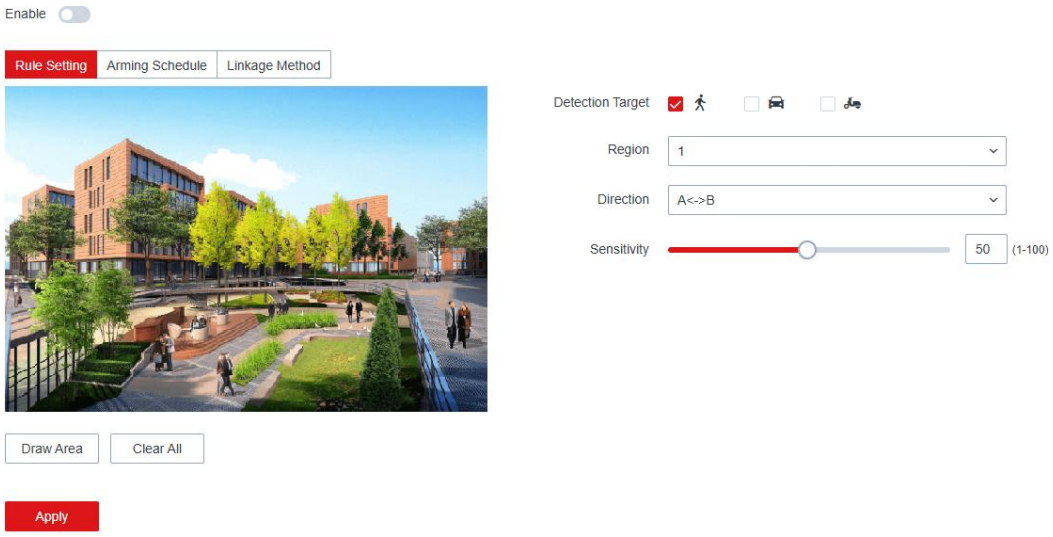


Figure 8-7-28

Step 2: Check "Enable" to enable line crossing detection.

Step 3: Select "Region": The system supports setting up to 4 warn line. After selecting a warn line, you need to make the following settings. After setting, please click "Apply" below.

【Draw Area】Click "Draw Area" and a line segment with an arrow will appear on the screen. Click on the line segment, click and drag one of the endpoints to modify the length of the line segment; or click and drag the position of the line segment with the arrow in the picture to complete the drawing of a warning surface.

【Clear All】Used to delete the selected alert area.

【Detection Target】Set the target to be detected, supports Human, Vehicle and Non-Motor Vehicle, Human is selected by default.

【Direction】There are three options: "A<->B", "A->B", and "B->A", indicating the direction in which the object crosses the interface to trigger an alarm. "A->B" means that the alarm will be triggered when the object crosses from A to B; "B->A" means that the alarm will be triggered when the object crosses from B to A; "A<->B" means that the object crosses from A to B, or from B to B, the alarm is triggered, that is, the alarm is triggered in both directions.

【Sensitivity】Used to set the sensitivity for detecting line crossing; the default value is 50.. Drag the progress bar or enter the value directly in the value box to modify the sensitivity. The greater the sensitivity, the easier it is to trigger an alarm.

Step 4: When you need to set other Warn Line, repeat step 3 to complete the setup.

Step 5: Set the arming schedule.

As shown in Figure 8-7-29. You can view, edit, and delete the arming time of the Line Cross detection. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the

arming schedule.

- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.

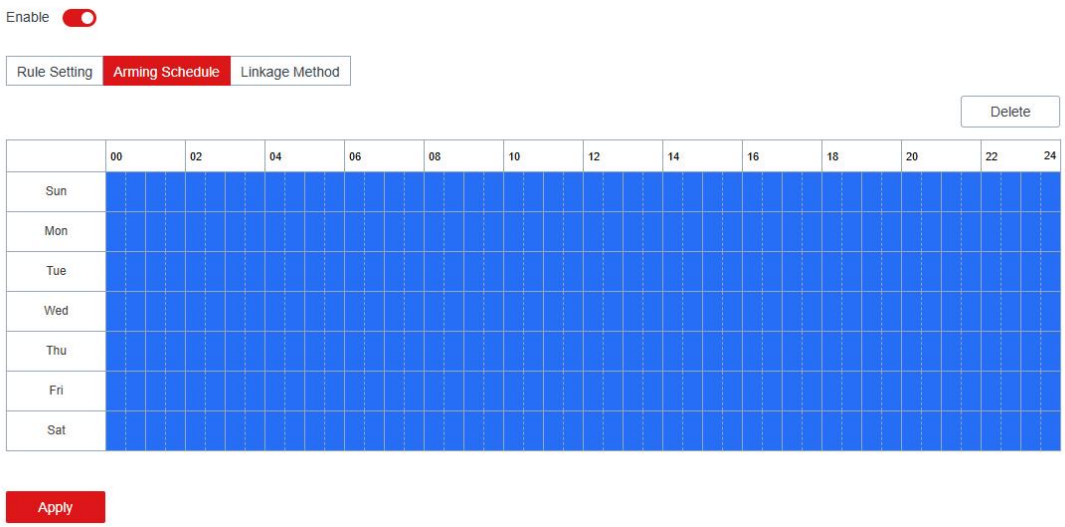


Figure 8-7-29

NOTE

- When the arming time is set, there can be no overlap between any two time periods.

Step 6: Set the linkage method as needed.

Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via Cloud, Light Warning,Sound Alarm) and trigger alarm output(IO Output), as shown in Figure 8-7-30.

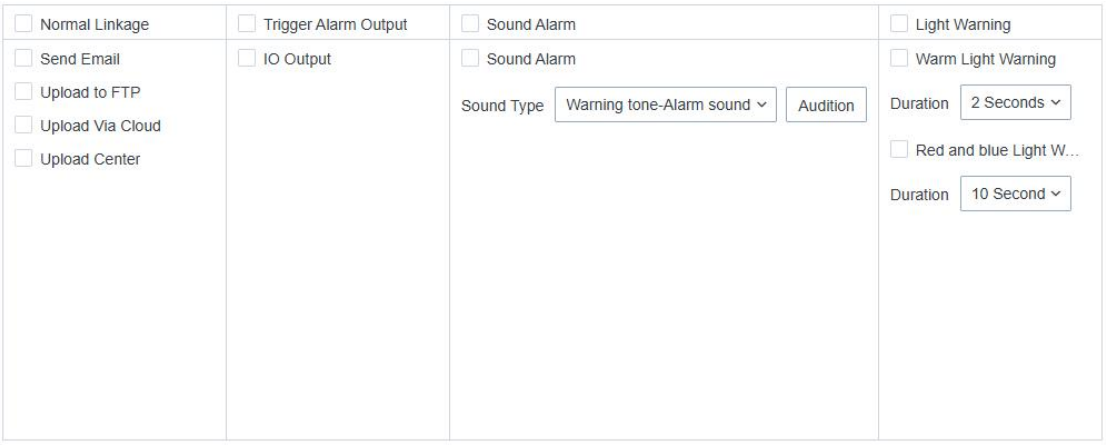


Figure 8-7-30

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.
【Light Warning】After selection, the device will link the alarm light to flash.
【IO Output】Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.
【Sound Alarm】After selection, the device will emit an alarm sound when alarming.

NOTE

- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.

⑤ Loitering Detection

The loitering detection function is used to detect that the target stays within the set area for more than the set time threshold, and then alarms according to the judgment result.
The specific operation steps are as follows:
Step 1: In the main interface click on the "Configuration → Event → Smart Event → Loitering Detection" to enter the Loitering Detection settings interface, as shown in Figure 8-7-31.

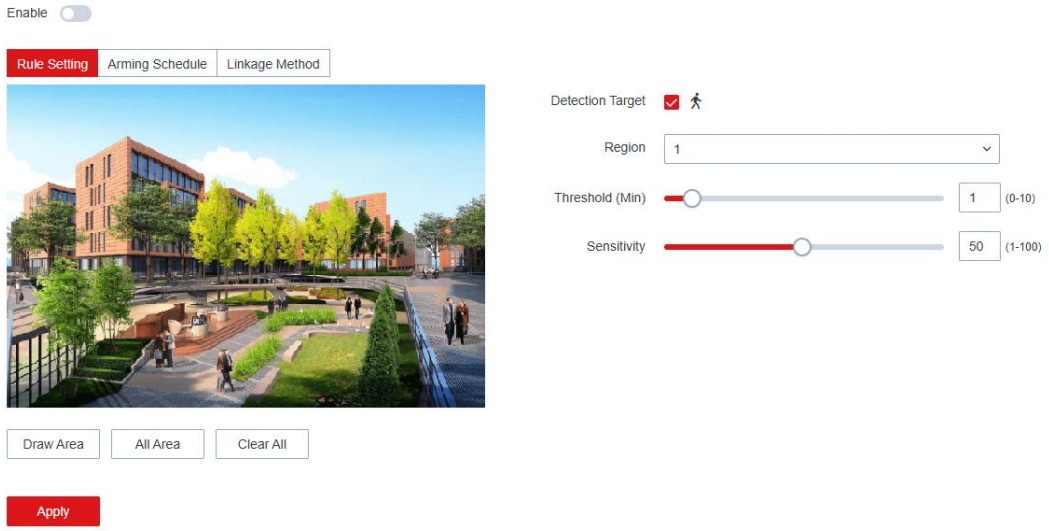


Figure 8-7-31

Step 2: Check "Enable" to enable loitering detection.
Step 3: Select "Region": The system supports setting up to 4 warn region. After selecting a warn region, you need to make the following settings. After setting, please click "Apply" below.
【Draw Area】Click “Draw Area”, move the mouse to the preview screen and click the left mouse button in sequence to draw the endpoints of the 4-8 polygon warning area, right-click to end the polygon drawing, and support dragging polygon vertices to adjust the

area size, drag the entire polygon to adjust the overall area position.

【All Area】When need all areas to be detected, click "All Area" to automatically select all areas.

【Clear All】Used to delete the selected alert area.

【Detection Target】Set the target to be detected, supports Human, Human is selected by default.

【Time threshold(min)】Indicates that the target generates an alarm after continuous movement in the detection area. The larger the time threshold, the longer the target continues to move in the detection area to trigger an alarm.

【Sensitivity】This setting determines the sensitivity for detecting loitering; the default value is 50. Drag the progress bar or enter the value directly in the value box to modify the sensitivity. The greater the sensitivity, the easier it is to trigger an alarm.

Step 4: When you need to set other Warn Region, repeat step 3 to complete the setup.

Step 5: Set the arming schedule.

As shown in Figure 8-7-32. You can view, edit, and delete the arming time of the Loiter detection. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.

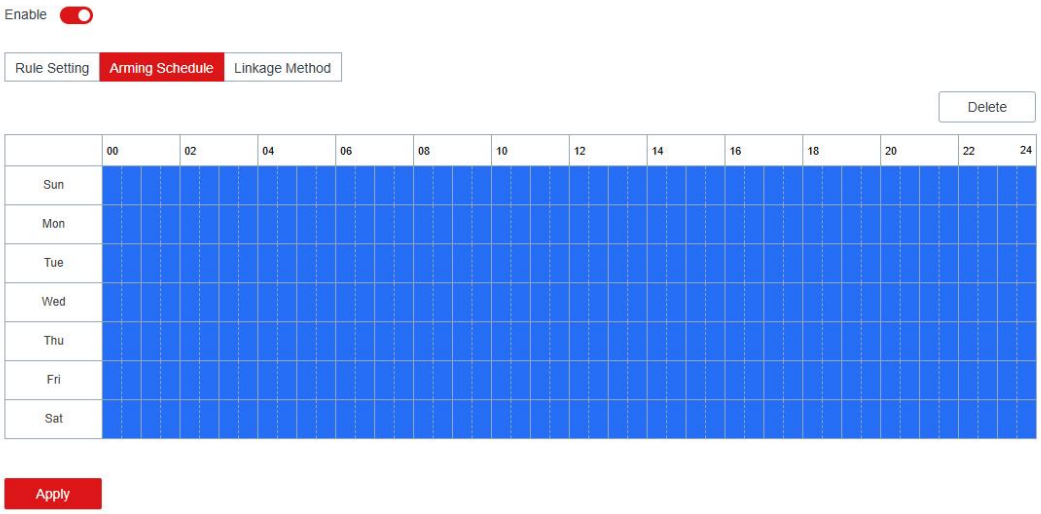


Figure 8-7-32

NOTE

- When the arming time is set, there can be no overlap between any two time periods.

Step 6: Set the linkage method as needed.

Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via

Cloud, Light Warning,Sound Alarm) and trigger alarm output(IO Output), as shown in Figure 8-7-33.

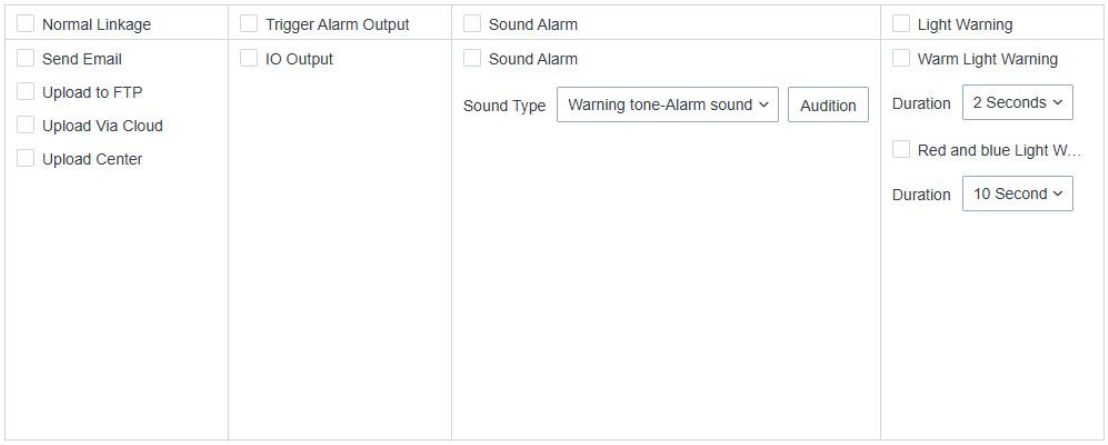


Figure 8-7-33

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.

【Light Warning】After selection, the device will link the alarm light to flash.

【IO Output】Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.

【Sound Alarm】After selection, the device will emit an alarm sound when alarming.

NOTE

- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.

⑥ People Gathering

The people gathering detection function is used to detect that the density of the personnel in the set area exceeds the set threshold, and the alarm is linked according to the judgment result.

The specific operation steps are as follows:

Step 1: In the main interface click on the "Configuration → Event → Smart Event → People Gathering" to enter the People Gather Detection settings interface, as shown in Figure 8-7-34.

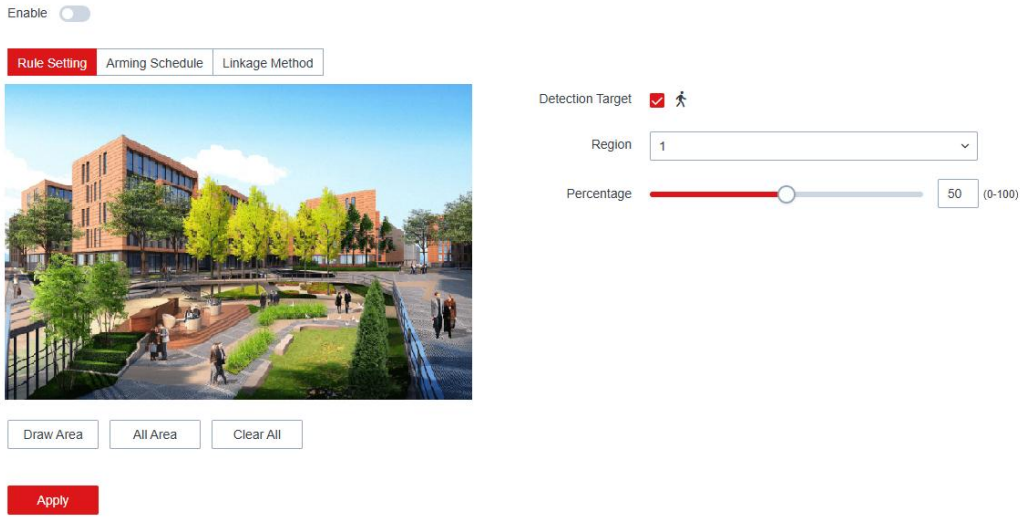


Figure 8-7-34

Step 2: Check "Enable" to enable people gathering detection.

Step 3: Select "Region": The system supports setting up to 4 warn region. After selecting a warn region, you need to make the following settings. After setting, please click "Save" below.

【Draw Area】Click “Draw Area”, move the mouse to the preview screen and click the left mouse button in sequence to draw the endpoints of the 4-8 polygon warning area, right-click to end the polygon drawing, and support dragging polygon vertices to adjust the area size, drag the entire polygon to adjust the overall area position.

【All Area】When need all areas to be detected, click "All Area" to automatically select all areas.

【Clear All】Used to delete the selected alert area.

【Detection Target】Set the target to be detected, supports Human and Vehicle, Human is selected by default.

【Percentage】Indicates the proportion of personnel in the entire alert area. When the proportion of personnel exceeds the set percentage, the system will generate an alarm. The percentage is 50% by default. The larger the value, the more people can be accommodated in the alert area, and the less likely it is to trigger an alarm.

Step 4: When you need to set other Warn Region, repeat step 3 to complete the setup.

Step 5: Set the arming schedule.

As shown in Figure 8-7-35. You can view, edit, and delete the arming time of the People gather detection. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.

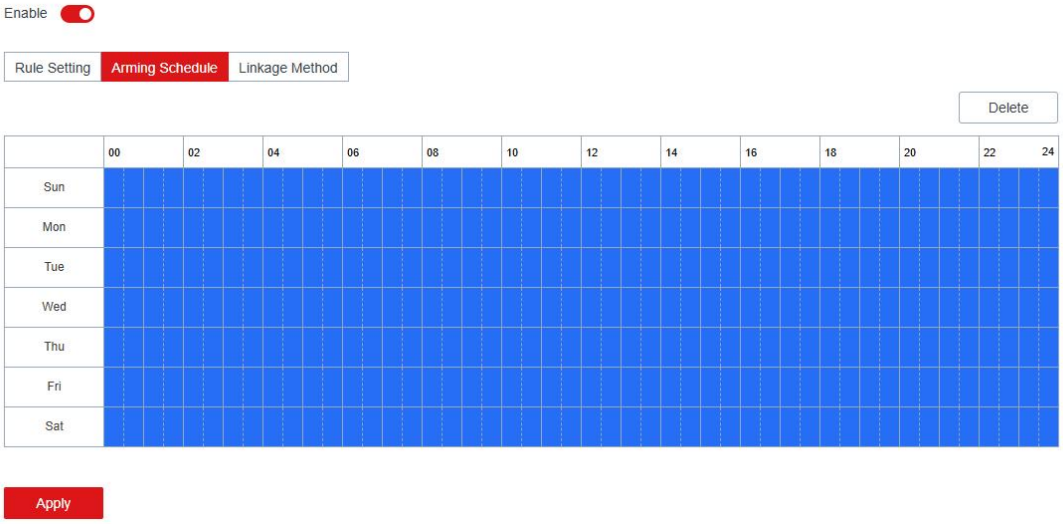


Figure 8-7-35

NOTE

- When the arming time is set, there can be no overlap between any two time periods.

Step 6: Set the linkage method as needed.

Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via Cloud, Light Warning,Sound Alarm) and trigger alarm output(IO Output), as shown in Figure 8-7-36.

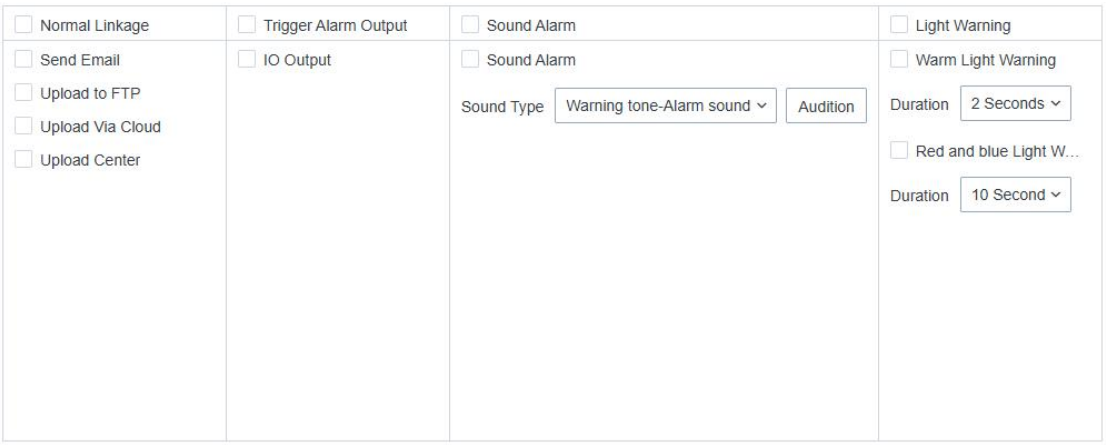


Figure 8-7-36

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.

【Light Warning】After selection, the device will link the alarm light to flash.

【IO Output】Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.
【Sound Alarm】After selection, the device will emit an alarm sound when alarming.

NOTE

- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.

⑦ Face Detection

Face detection is used to detect whether a face is detected in the set area, and the alarm is linked according to the judgment result.

The specific operation steps are as follows:

Step 1: In the main interface click on the "Configuration → Event → Smart Event → Face Detection" to enter the Face Detection settings interface, as shown in Figure 8-7-37.

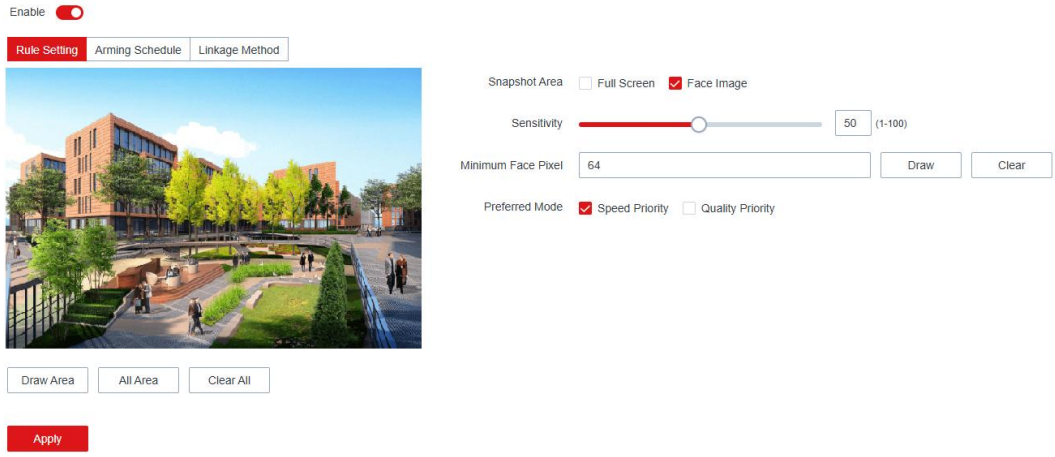


Figure 8-7-37

Step 2: Check "Enable" to enable Face detection.

Step 3: Select "Region": The system supports setting up to 1 warn region. After selecting a warn region, you need to make the following settings. After setting, please click "Save" below.

【Draw Area】Click “Draw Area”, move the mouse to the preview screen and click the left mouse button in sequence to draw the endpoints of the 4-8 polygon warning area, right-click to end the polygon drawing, and support dragging polygon vertices to adjust the area size, drag the entire polygon to adjust the overall area position.

【All Area】When need all areas to be detected, click "All Area" to automatically select all areas.

【Clear All】Used to delete the selected alert area.

【Snapshot Area】Set the capture area, the default is "Full Screen", "Face Image" is optional.

【Sensitivity】This setting determines the sensitivity for detecting faces; the default value is 50.. Drag the progress bar or enter the value directly in the value box to modify the

sensitivity. The greater the sensitivity, the easier it is to trigger an alarm.

【Minimum face Pixel】This setting determines the minimum width of a face in pixels. The default value is 64 (minimum), and the maximum is the entire image. Users can directly input the pixel width or set the minimum face width by drawing directly, depending on the specific scenario.

【Preferred Mode】This setting determines the preferred mode for face detection (algorithm push mode). The default is “Speed Priority” (prioritizes detection speed). “Quality Priority” is optional (prioritizes face quality).

Step 4: Set the arming schedule.

As shown in Figure 8-7-38. You can view, edit, and delete the arming time of the face detection. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.

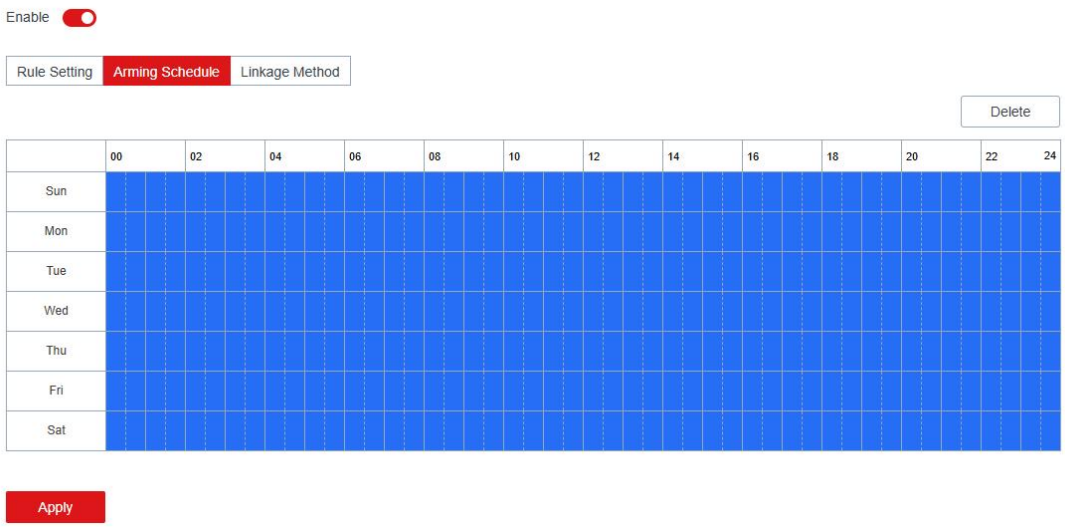


Figure 8-7-38

NOTE

- When the arming time is set, there can be no overlap between any two time periods.

Step 6: Set the linkage method as needed.

Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via Cloud) , as shown in Figure 8-7-39.

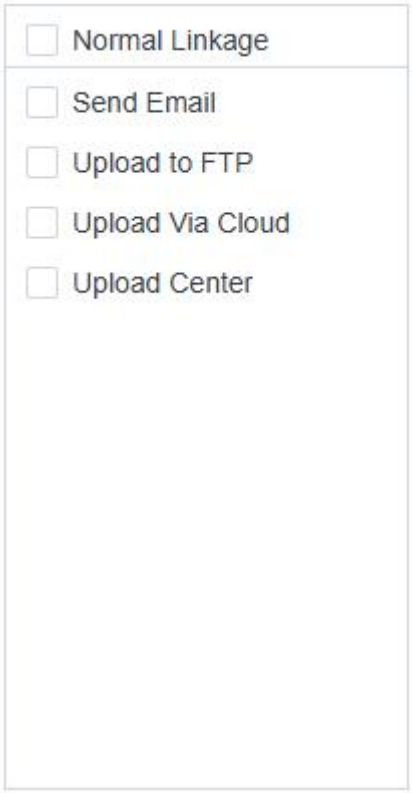


Figure 8-7-39

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.

NOTE

- The configuration items supported by face detection on different devices may vary. Please refer to the actual device for the specific interface.
- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.

⑧Illegal Parking

Illegal parking detection is used to detect whether there is illegal parking in the video setting area. If a vehicle or a vehicle with an unauthorized license plate enters the designated area and remains there for more than a set time threshold, an alarm will be triggered based on the judgment result.

The specific operation steps are as follows:

Step 1: In the main interface click on the "Configuration → Event → Smart Event→ Illegal Parking" to enter the illegal parking settings interface, as shown in Figure 8-7-40.

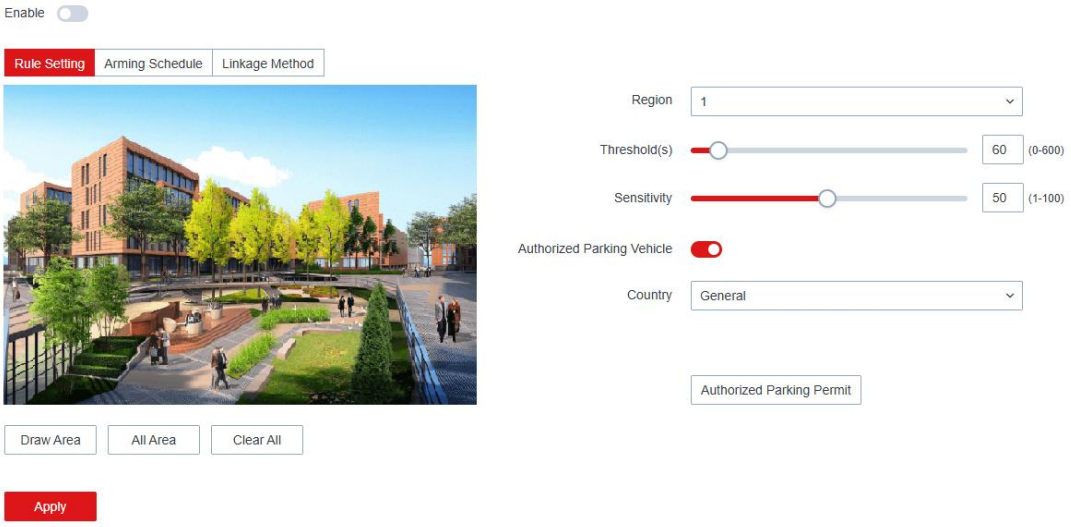


Figure 8-7-40

Step 2: Check "Enable" to enable illegal parking detection.

Step 3: Select "Region": The system supports setting up to 4 warn region. After selecting a warn region, you need to make the following settings. After setting, please click "Apply".

【Draw Area】Click “Draw Area”, move the mouse to the preview screen and click the left mouse button in sequence to draw the endpoints of the 4-8 polygon warning area, right-click to end the polygon drawing, and support dragging polygon vertices to adjust the area size, drag the entire polygon to adjust the overall area position.

【All Area】When need all areas to be detected, click "All Area" to automatically select all areas.

【Clear All】Used to delete the selected alert area.

【Threshold(s)】Indicates that the target enters the alert zone and continues to stay for this time to generate an alarm. If set to 60s, the target intrusion area will trigger an alarm after 60s.

【Sensitivity】Used to set the sensitivity of detected illegal parking. The default is 50. Drag the progress bar or enter the value directly in the value box to modify the sensitivity. The greater the sensitivity, the easier it is to trigger an alarm.

【Authorized Parking Vehicle】It is off by default; turning it on allows you to record parking permits.

【Country】After enabling permitted parking, you can configure the country and filter license plates according to national rules to improve the license plate recognition rate.

【Authorized Parking Permit】Click and add, modify, or delete license plates in the pop-up license plate information window. License plates listed in the "Permitted Parking" sign will be allowed to park; parking with other license plate numbers will trigger an alarm.

Step 4: When you need to set other Warn Region, repeat step 3 to complete the setup.

Step 5: Set the arming schedule.

As shown in Figure 8-7-41. You can view, edit, and delete the arming time of the illegal parking detection. The default is to arm the alarm 24 hours a day. You can adjust the

arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.

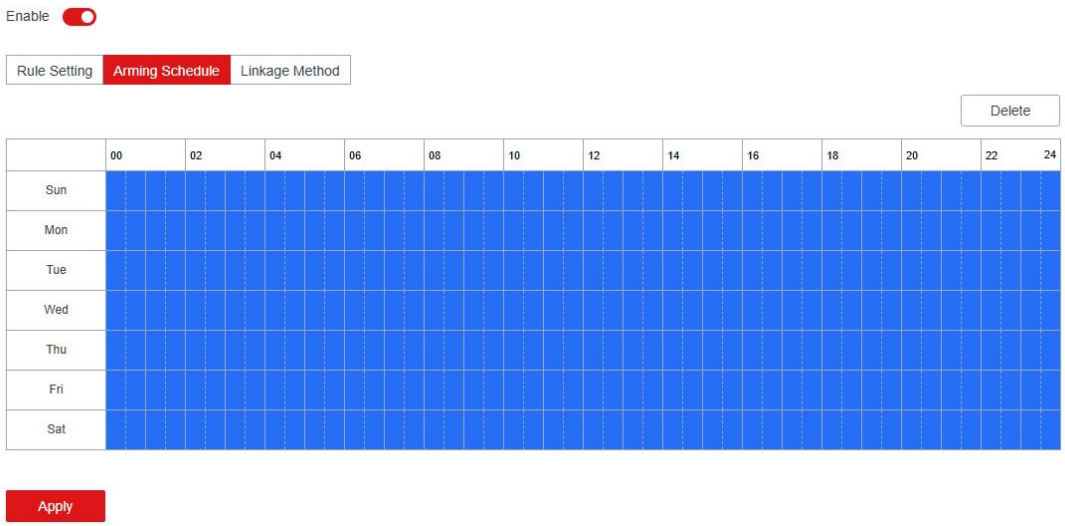


Figure 8-7-41

NOTE

- When the arming time is set, there can be no overlap between any two time periods.

Step 6: Set the linkage method as needed.

Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via Cloud, Light Warning,Sound Alarm) and trigger alarm output(IO Output), as shown in Figure 8-7-42.

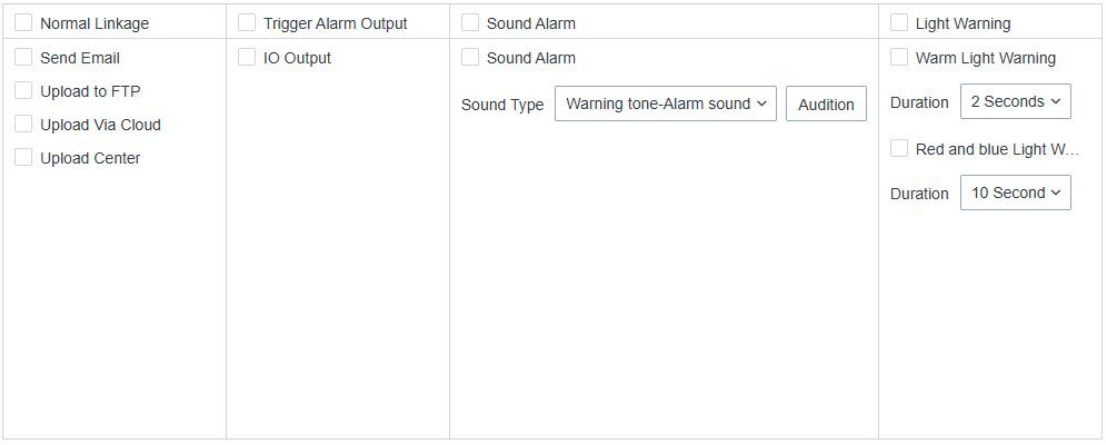


Figure 8-7-42

【Send Email】Select and the system is configured with SMTP, the alarm information will

be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.

【Light Warning】After selection, the device will link the alarm light to flash.

【IO Output】Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.

【Sound Alarm】After selection, the device will emit an alarm sound when alarming.

NOTE

- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.
- The configuration for detecting illegal parking may vary depending on the device; please refer to the actual product for the specific interface.

⑨Line Crossing Count

The line crossing counting is used to count the number of people crossing the line in the set warning area according to the set entry direction, and to determine whether to trigger an alarm based on the set alarm number threshold. The alarm is triggered based on the judgment result.

The specific operation steps are as follows:

Step 1: In the main interface click on the "Configuration → Event → Smart Event→ Line Crossing Count" to enter the Line Crossing Count settings interface, as shown in Figure 8-7-43.

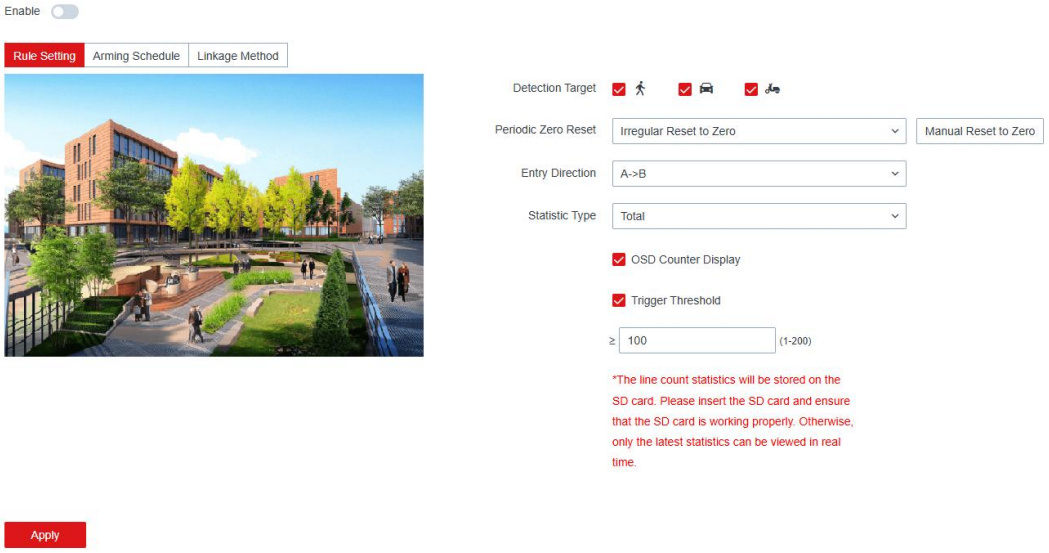


Figure 8-7-43

Step 2: Check "Enable" to enable line crossing counting.

Step 3: The default detection is for the entire area, and there is no need to configure the warning area. You can set it according to the detection target, entry direction, statistical type, etc.After setting, please click "Apply".

【Detection Target】Set the target to be detected, supports Human, Vehicle and Non-Motor Vehicle, Human is selected by default.

【Periodic Zero Reset】Set and operate scheduled and manual clears for count statistics.

【Entry Direction】 Set the entry direction, supporting A->B (default) and B->A. A direction detection line is also displayed on the interface; you can drag the vertex to adjust the detection line's position and length. "A->B" indicates an entry when the target crosses the line from A to B, and a departure when it crosses the line from B to A; "B->A" indicates an entry when the target crosses the line from B to A, and a departure when it crosses the line from B to A.

【Statistics Type】 Set the statistics type, supporting Total, Entry (default), and Exit.

【OSD Counter Display】 Enables or disables the count overlay OSD. (Off by default.) When enabled, the count result is displayed in the upper right corner of the video.

【Tigger Threshold】 Set the alarm threshold; exceeding this threshold triggers an alarm.

Step 4: Set the arming schedule.

As shown in Figure 8-7-44. You can view, edit, and delete the arming time of the line cross counting. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.

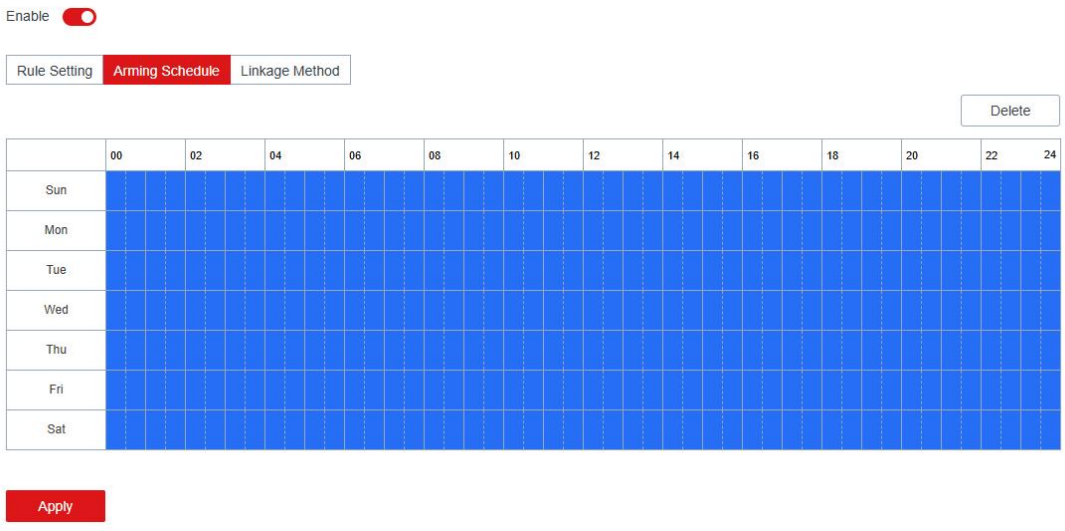


Figure 8-7-44

NOTE

- When the arming time is set, there can be no overlap between any two time periods.

Step 5: Set the linkage method as needed.

Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via Cloud, Light Warning,Sound Alarm) and trigger alarm output(IO Output), as shown in Figure 8-7-45.

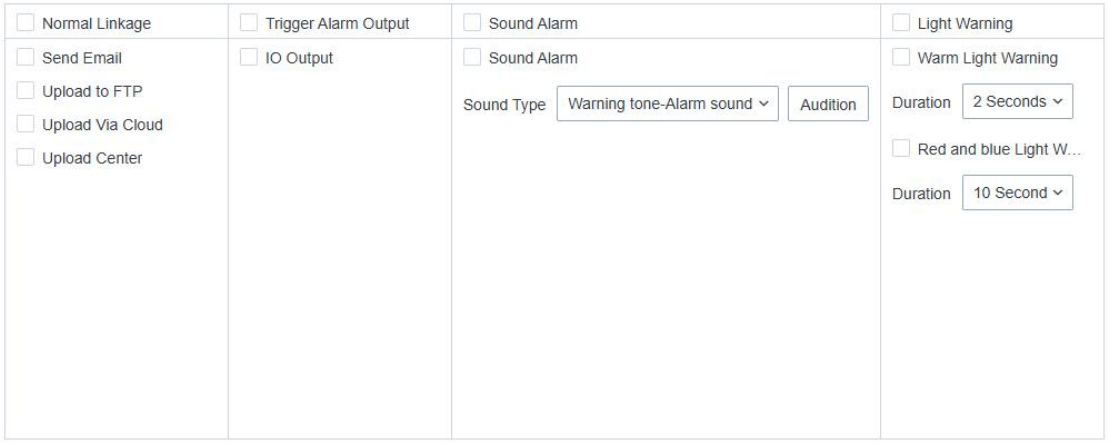


Figure 8-7-45

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.

【Light Warning】After selection, the device will link the alarm light to flash.

【IO Output】Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.

【Sound Alarm】After selection, the device will emit an alarm sound when alarming.

NOTE

- Only devices that support SD cards and ensure that the SD card is in normal use can support the storage of line-crossing statistical data. Otherwise, only real-time data viewing is supported. The SD card must be formatted before using the line-crossing counting function for the first time.
- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.

⑩ License Plate Detection

License Plate detection is used to detect whether a license plate is detected in the set area, and the alarm is linked according to the judgment result.

The specific operation steps are as follows:

Step 1: In the main interface click on the "Configuration → Event → Smart Event → License Plate Detection" to enter the License Plate Detection settings interface, as shown in Figure 8-7-46.

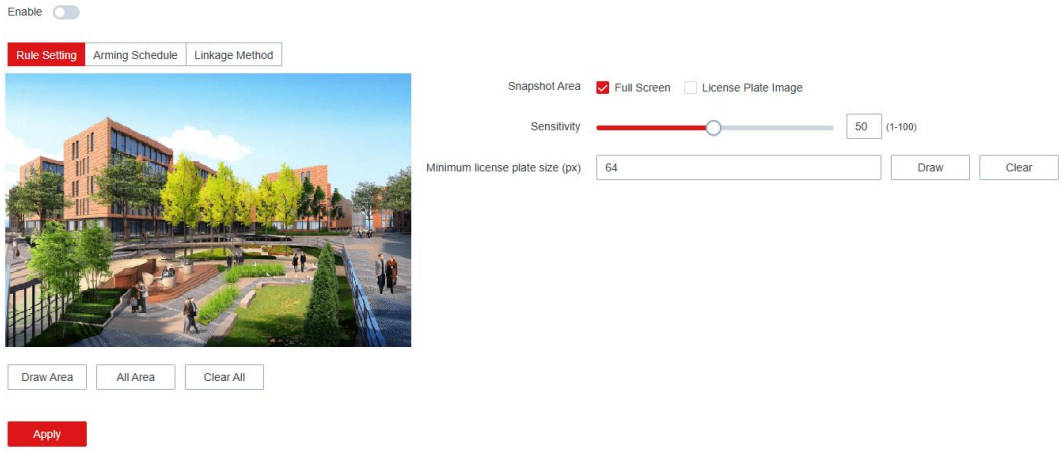


Figure 8-7-46

Step 2: Check "Enable" to enable license plate detection.

Step 3: Select "Region": The system supports setting up to 1 warn region. After selecting a warn region, you need to make the following settings. After setting, please click "Save" below.

【Draw Area】Click “Draw Area”, move the mouse to the preview screen and click the left mouse button in sequence to draw the endpoints of the 4-8 polygon warning area, right-click to end the polygon drawing, and support dragging polygon vertices to adjust the area size, drag the entire polygon to adjust the overall area position.

【All Area】When need all areas to be detected, click "All Area" to automatically select all areas.

【Clear All】Used to delete the selected alert area.

【Snapshot Area】Set the capture area, the default is "Full Screen", "License Plate Image" is optional.

【Sensitivity】This setting determines the sensitivity for detecting license plates; the default value is 50. Drag the progress bar or enter the value directly in the value box to modify the sensitivity. The greater the sensitivity, the easier it is to trigger an alarm.

【Minimum License Plate Size(px)】This setting specifies the minimum width of the license plate in pixels. The default value is 64 (minimum), and the maximum is the entire image. Users can directly input the pixel width or set the minimum license plate width by drawing it directly, depending on the actual scenario.

Step 4: Set the arming schedule.

As shown in Figure 8-7-47. You can view, edit, and delete the arming time of the license plate detection. The default is to arm the alarm 24 hours a day. You can adjust the arming

time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.

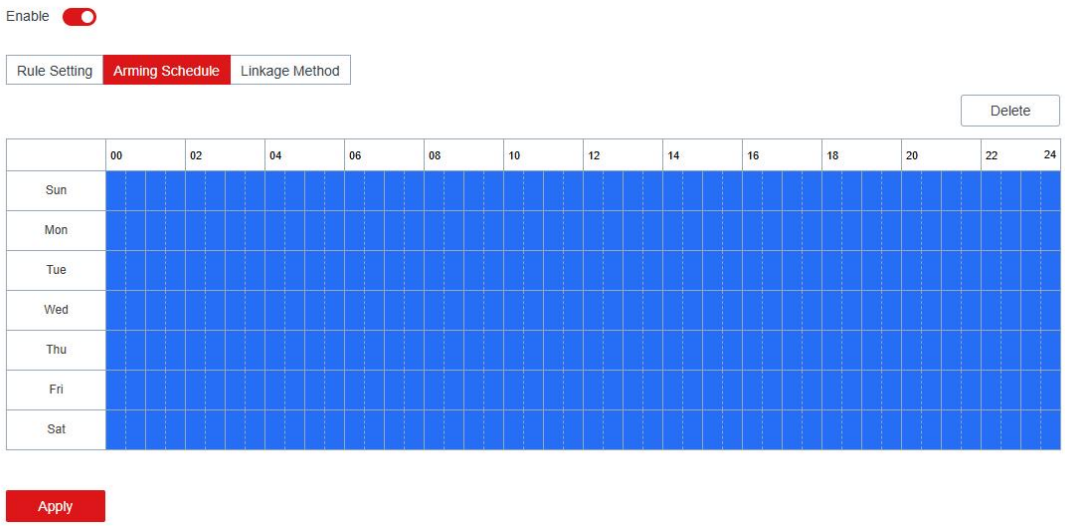


Figure 8-7-47

NOTE

- When the arming time is set, there can be no overlap between any two time periods.

Step 6: Set the linkage method as needed.

Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via Cloud) , as shown in Figure 8-7-48.

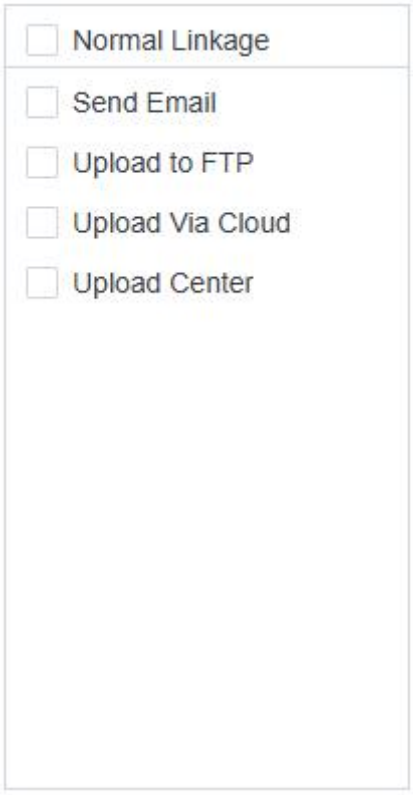


Figure 8-7-48

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.

NOTE

- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.

⑪ Abandoned Object Detection

Object Dependency Detection is used to detect whether there are any objects left in a designated video area, and to trigger an alarm based on the detection result.

The specific operation steps are as follows:

Step 1: In the main interface click on the "Configuration → Event → Smart Event→ Abandoned Object Detection" to enter the Abandoned Object Detection settings interface, as shown in Figure 8-7-49.

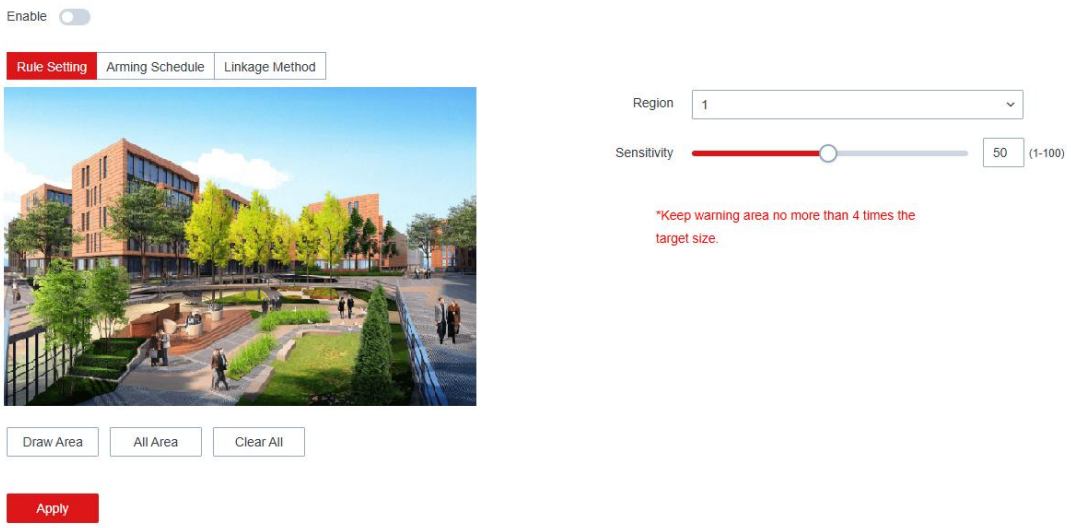


Figure 8-7-49

Step 2: Check "Enable" to enable abandoned object detection.

Step 3: Select "Region": The system supports setting up to 4 warn region. After selecting a warn region, you need to make the following settings. After setting, please click "Apply".

【Draw Area】Click “Draw Area”, move the mouse to the preview screen and click the left mouse button in sequence to draw the endpoints of the 4-8 polygon warning area, right-click to end the polygon drawing, and support dragging polygon vertices to adjust the area size, drag the entire polygon to adjust the overall area position.

【All Area】When need all areas to be detected, click "All Area" to automatically select all areas.

【Clear All】Used to delete the selected alert area.

【Sensitivity】This setting determines the sensitivity for detecting items left behind; the default value is 50. Drag the progress bar or enter the value directly in the value box to modify the sensitivity. The greater the sensitivity, the easier it is to trigger an alarm.

Step 4: When you need to set other Warn Region, repeat step 3 to complete the setup.

Step 5: Set the arming schedule.

As shown in Figure 8-7-50. You can view, edit, and delete the arming time of the abandoned object detection. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.

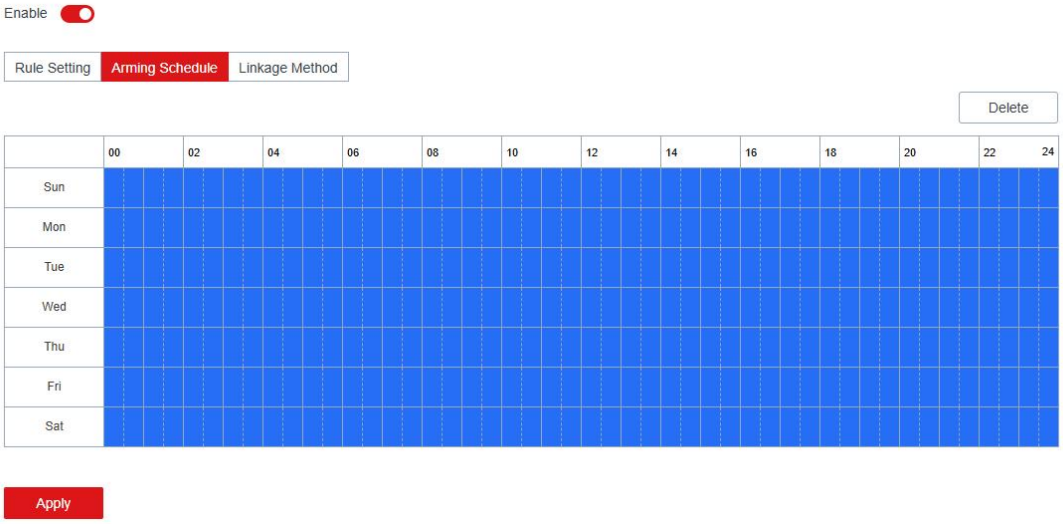


Figure 8-7-50

NOTE

- When the arming time is set, there can be no overlap between any two time periods.

Step 6: Set the linkage method as needed.

Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via Cloud, Light Warning,Sound Alarm) and trigger alarm output(IO Output), as shown in Figure 8-7-51.

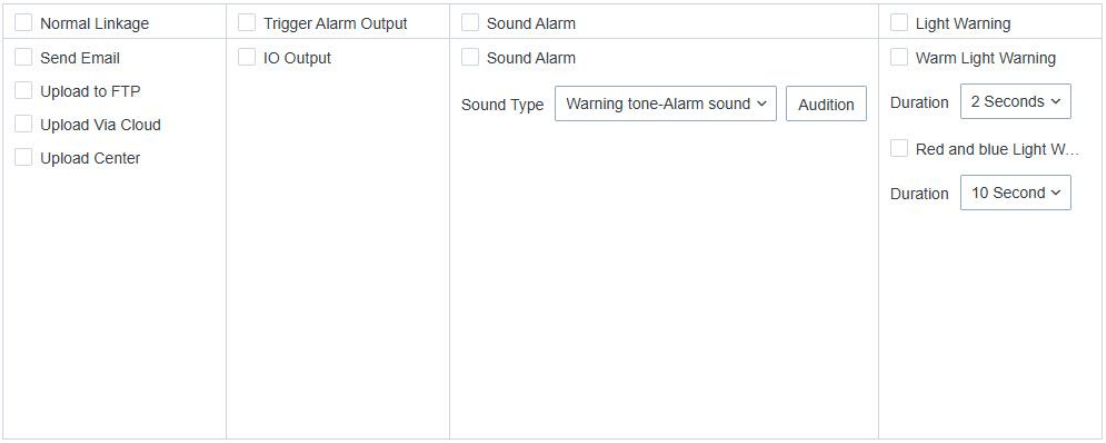


Figure 8-7-51

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.

【Light Warning】After selection, the device will link the alarm light to flash.

【IO Output】Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.
【Sound Alarm】After selection, the device will emit an alarm sound when alarming.

NOTE

- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.
- Keep warning area no more than 4 times the target size.

⑫ Moving Object Detection

Moving Object Detection is used to detect whether a target item is moved within a designated video area, and determines whether to trigger an alarm based on a set time threshold.

The specific operation steps are as follows:

Step 1: In the main interface click on the "Configuration → Event → Smart Event→ Moving Object Detection" to enter the Moving Object Detection settings interface, as shown in Figure 8-7-52.

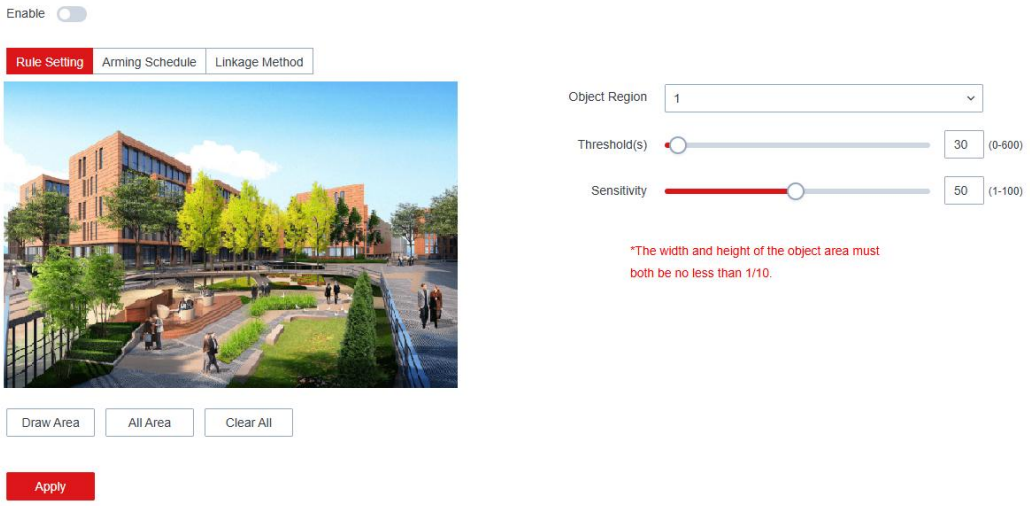


Figure 8-7-52

Step 2: Check "Enable" to enable moving object detection.

Step 3: Select "Object Region": The system supports setting up to 4 object region. After selecting a object region, you need to make the following settings. After setting, please click "Apply".

【Draw Area】Click “Draw Area”, move the mouse to the preview screen and click the left mouse button in sequence to draw the endpoints of the 4-8 polygon object area, right-click to end the polygon drawing, and support dragging polygon vertices to adjust the area size, drag the entire polygon to adjust the overall area position.

【All Area】When need all areas to be detected, click "All Area" to automatically select all

areas.

【Clear All】Used to delete the selected alert area.

【Threshold(s)】This indicates the time elapsed after the target item has been moved before an alarm is triggered. For example, setting it to 60 seconds means the alarm will be triggered 60 seconds after the target item has been moved.

【Sensitivity】This setting determines the sensitivity for detecting item movement; the default value is 50.Drag the progress bar or enter the value directly in the value box to modify the sensitivity. The greater the sensitivity, the easier it is to trigger an alarm.

Step 4: When you need to set other Object Region, repeat step 3 to complete the setup.

Step 5: Set the arming schedule.

As shown in Figure 8-7-53. You can view, edit, and delete the arming time of the moving object detection. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.

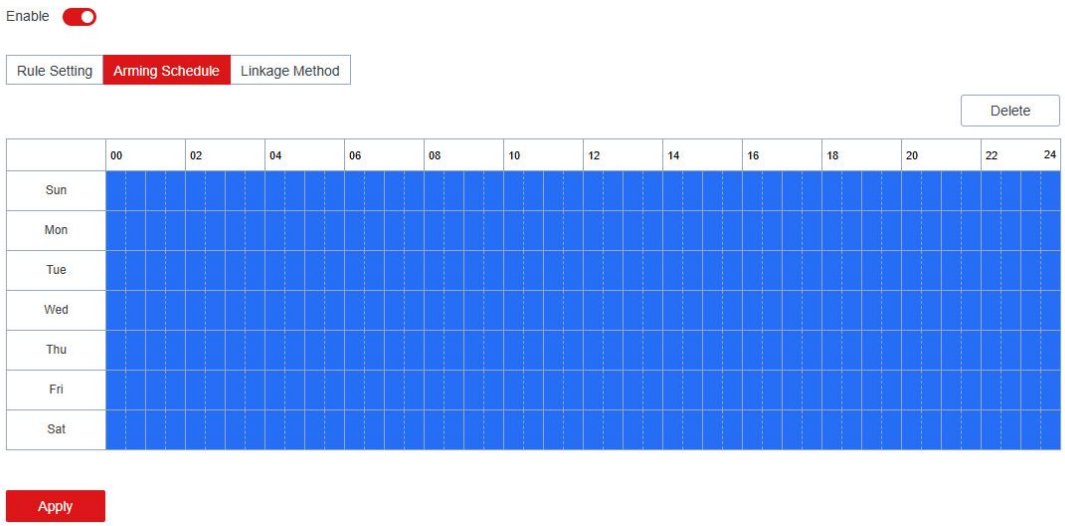


Figure 8-7-53

NOTE

- When the arming time is set, there can be no overlap between any two time periods.

Step 6: Set the linkage method as needed.

Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via Cloud, Light Warning,Sound Alarm) and trigger alarm output(IO Output), as shown in Figure 8-7-54.

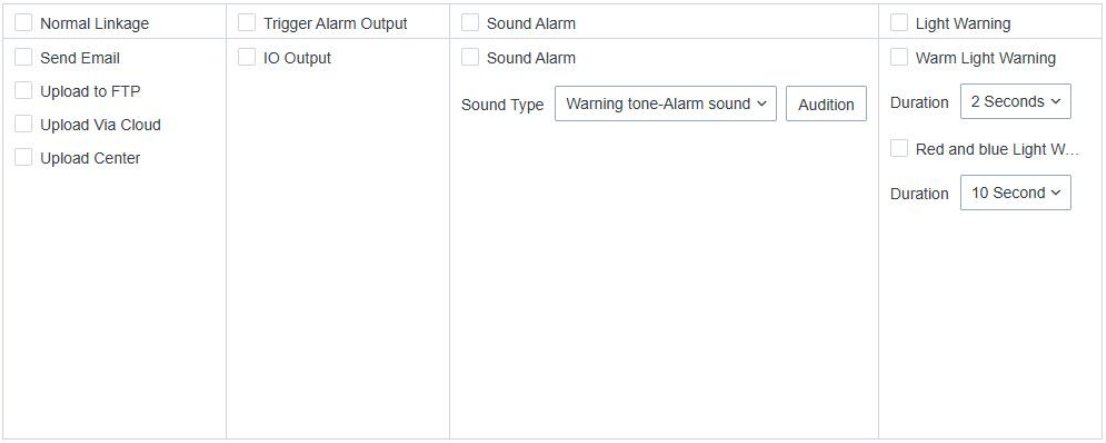


Figure 8-7-54

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.

【Light Warning】After selection, the device will link the alarm light to flash.

【IO Output】Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.

【Sound Alarm】After selection, the device will emit an alarm sound when alarming.

NOTE

- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.
- The width and height of the object area must both be no less than 1/10..

⑬ Heatmap

It supports configuration of heatmaps, ultimately enabling the detection and statistical analysis of traffic volume in different areas and the display of the heatmap using different colors.

The specific operation steps are as follows:

Step 1: In the main interface click on the "Configuration → Event → Smart Event→ Heatmap" to enter the Heatmap settings interface, as shown in Figure 8-7-55.

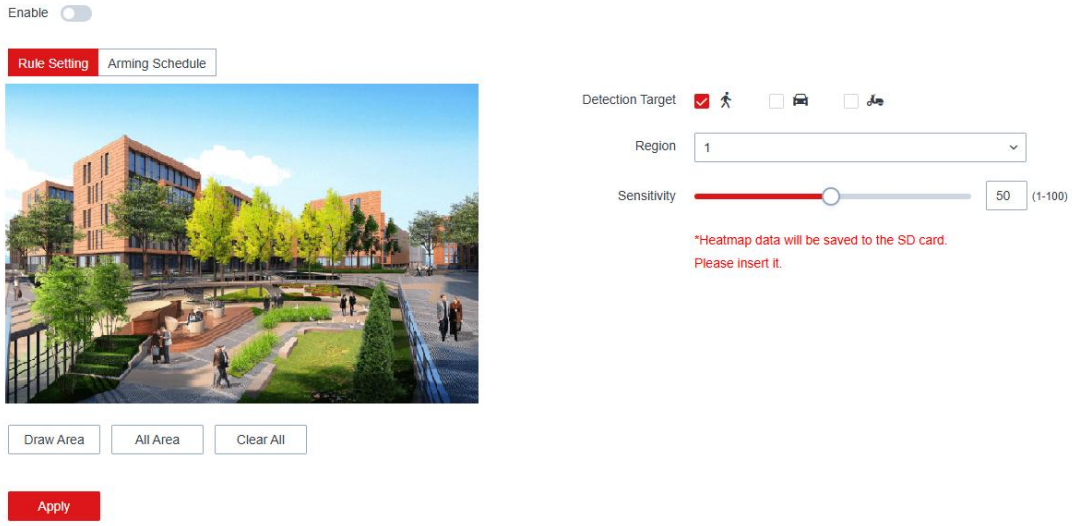


Figure 8-7-55

Step 2: Check "Enable" to enable the heatmap statistics function.

Step 3: Select "Region": The system supports setting up to 4 warn region. After selecting a warn region, you need to make the following settings. After setting, please click "Apply".

【Draw Area】Click “Draw Area”, move the mouse to the preview screen and click the left mouse button in sequence to draw the endpoints of the 4-8 polygon warning area, right-click to end the polygon drawing, and support dragging polygon vertices to adjust the area size, drag the entire polygon to adjust the overall area position.

【All Area】When need all areas to be detected, click "All Area" to automatically select all areas.

【Clear All】Used to delete the selected alert area.

【Detection Target】Set the target to be detected, supports Human, Vehicle and Non-Motor Vehicle, Human is selected by default.

【Sensitivity】Used to set the sensitivity of heatmap statistics. The default is 50. Drag the progress bar or enter the value directly in the value box to modify the sensitivity. A higher sensitivity makes it easier to trigger traffic heatmap statistics.

Step 4: When you need to set other Warn Region, repeat step 3 to complete the setup.

Step 5: Set the arming schedule.

As shown in Figure 8-7-56. You can view, edit, and delete the arming time of the heatmap statistics. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.

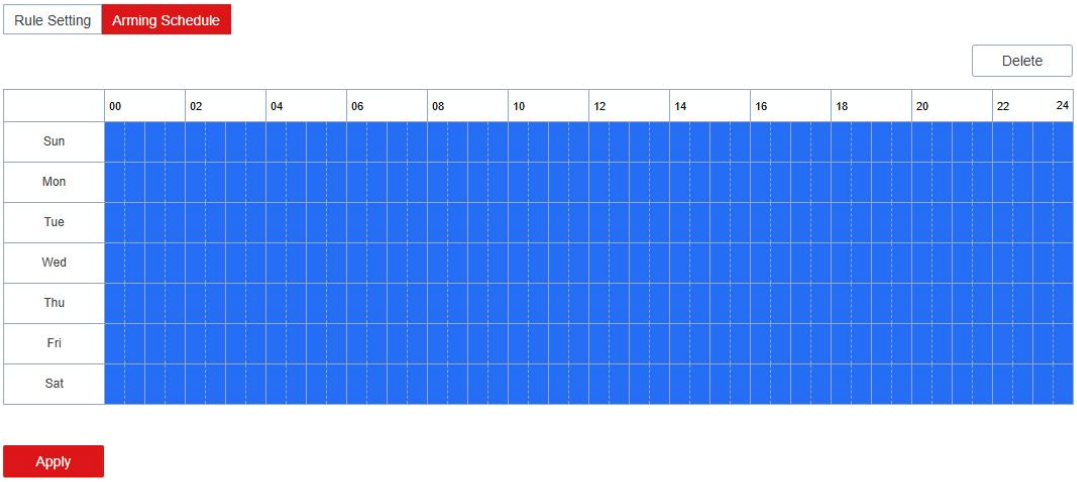


Figure 8-7-56

NOTE

- When the arming time is set, there can be no overlap between any two time periods.
- Heatmap data will be saved to the SD card. Please insert it.

⑭Video Structured Analytics

Video structured analytics is used to automatically extract relevant structured video data based on a set area, detection target, and sensitivity. It supports sending this data to various endpoints (NVR, APP, VMS), which can then display and apply it according to their business needs. Disabling video structuring prevents the IPC from performing any structured data extraction, thus saving IPC resources.

The specific setting steps are as follows:

Step 1: On the main interface, click "Configuration → Event → Smart Event → Video Structured Analytics" to enter the video structured analytics configuration interface, as shown in Figure 8-7-57.

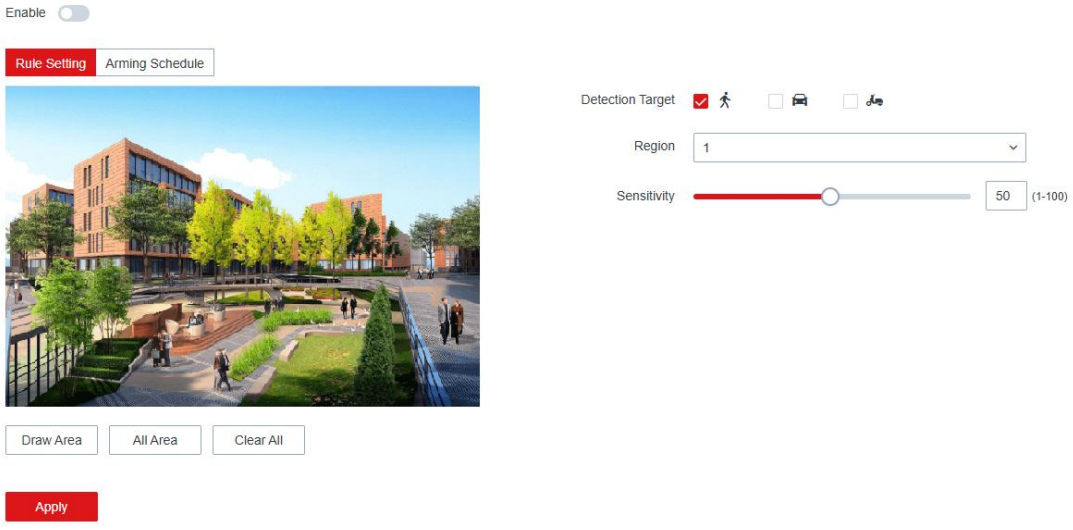


Figure 8-7-57

Step 2: Check "Enable" to enable the video structured analytics function.

Step 3: Select "Area Settings": The system supports setting up to 4 alert zones. After selecting an alert zone, you need to make the following settings. Once you are finished, please click "Apply" below.

【Draw area】 Click "Draw area", move the mouse to the preview screen and click the left mouse button to draw a 4-8 polygon area, right-click to end the polygon area drawing, and then click anywhere in the preview interface to complete the area drawing. It supports one-click selection of all areas, supports dragging the vertices of the 4-8 polygon, adjusting the detection area, and supports dragging the position of the moving area.

【Clear All】 Used to clear the areas already drawn on the guard zone.

【Detection Target】 Set the target to be detected, supports Human, Vehicle and Non-Motor Vehicle, Human is selected by default.

【Sensitivity】 This setting adjusts the detection sensitivity, which defaults to 50. Drag the progress bar or enter a value directly in the value box to modify the sensitivity. A higher sensitivity makes detection easier.

Step 4: When you need to set other Warn Region, repeat step 3 to complete the setup.

Step 5: Set the arming schedule.

As shown in Figure 8-7-58. You can view, edit, and delete the arming time of the heatmap statistics. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.

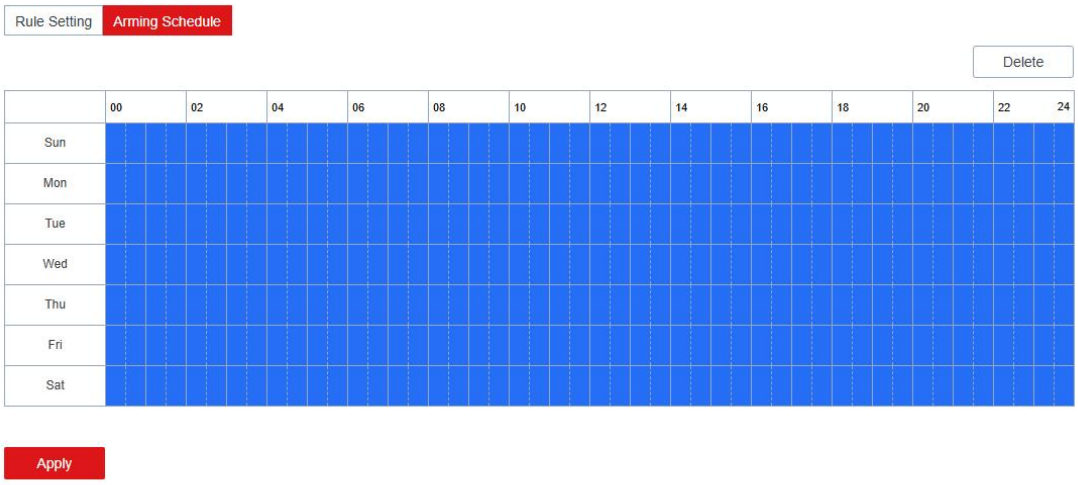


Figure 8-7-58

NOTE

- When the arming time is set, there can be no overlap between any two time periods.

⑮ Fireworks Detection

Fireworks detection is used to detect smoke (smoke or fire) in an area and automatically trigger an alarm.

The specific setting steps are as follows:

Step 1: On the main interface, click "Configuration → Event → Smart Event → Fireworks Detection" to enter the fireworks detection configuration interface, as shown in Figure 8-7-59.

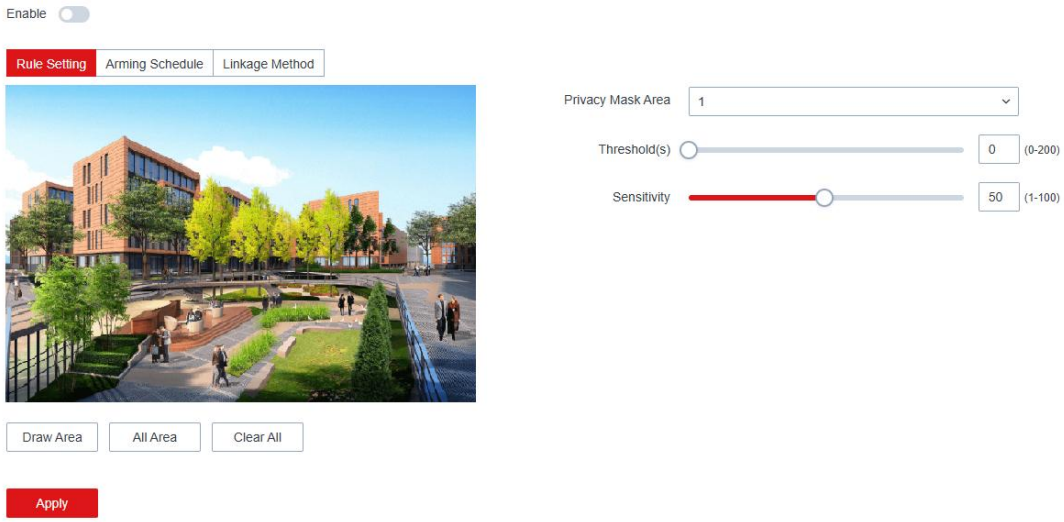


Figure 8-7-59

Step 2: Check "Enable" to turn on the smoke detection function.

Step 3: Select "Area Settings": The system supports setting up to 4 shielded areas. These shielded areas will not be used for smoke and fire detection. After selecting a shielded area, you need to make the following settings. Once finished, please click "Apply" below.

【Draw Area】 Click “Draw Area”, hold down the left mouse button and drag to draw the masked area. You can also drag and move the area position; one-click selection of the entire area is also supported.

【Clear All】 Used to clear the areas already drawn on the guard zone.

【Threshold(s)】Set a time threshold, indicating that the corresponding alarm event will only be triggered after the detected smoke and fire reaches the set time threshold. For example, setting it to 5 seconds means that the alarm will be triggered 5 seconds after smoke and fire are detected.

【Sensitivity】 This setting adjusts the detection sensitivity, which defaults to 50. Drag the progress bar or enter a value directly in the value box to modify the sensitivity. A higher sensitivity makes detection easier.

Step 4: When you need to set other Warn Region, repeat step 3 to complete the setup.

Step 5: Set the arming schedule.

As shown in Figure 8-7-60. You can view, edit, and delete the arming time of the heatmap statistics. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.

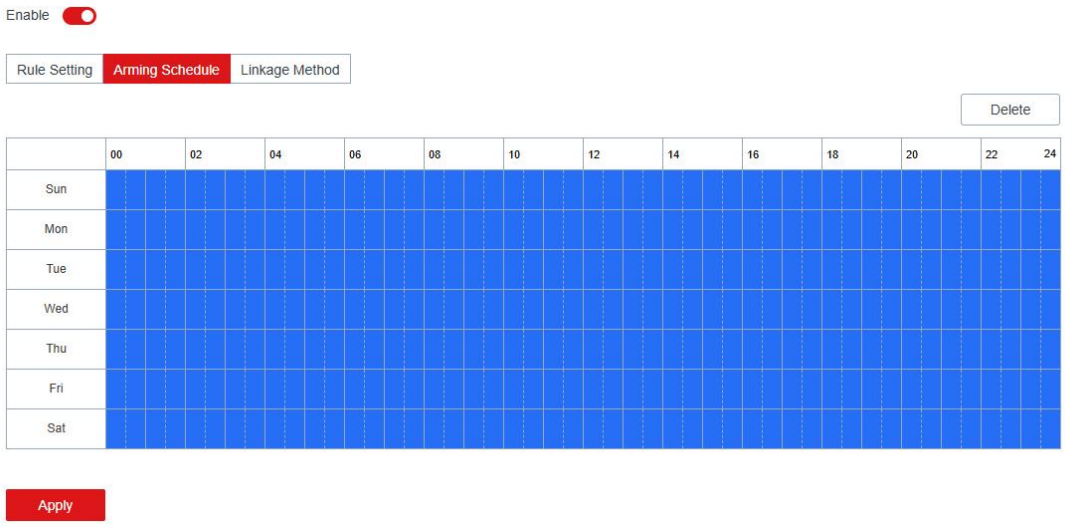


Figure 8-7-60

NOTE

- When the arming time is set, there can be no overlap between any two time periods.

Step 6: Set the linkage method as needed.

Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via Cloud, Light Warning,Sound Alarm) and trigger alarm output(IO Output), as shown in Figure 8-7-61.

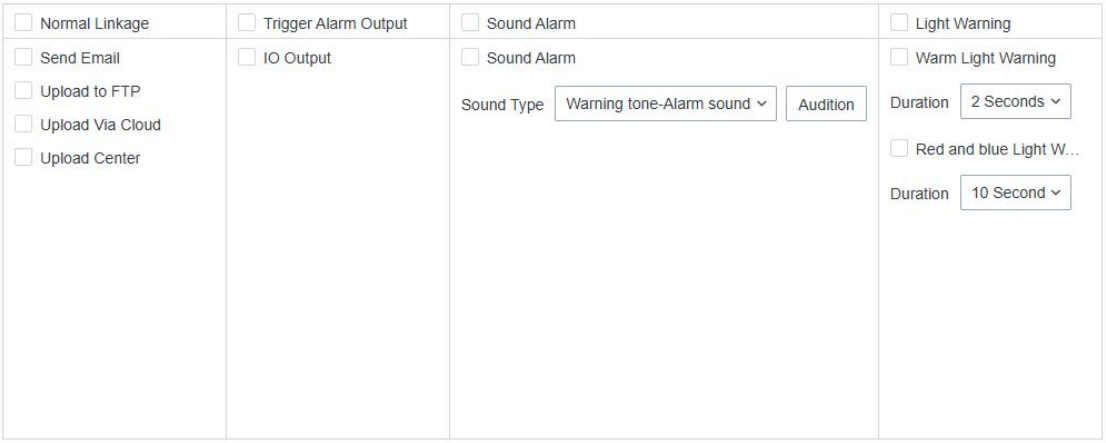


Figure 8-7-61

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.

【Light Warning】After selection, the device will link the alarm light to flash.

【IO Output】Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.

【Sound Alarm】After selection, the device will emit an alarm sound when alarming.

NOTE

- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.

8.7.3 One-Key Disarm

One-key disarming means that users can set disarming modes and disarming linkage items for all alarm events that have been set, so as to cancel linkage and set linkage mode in the set alarm events at one time.

Step 1: In the main interface click on the "Configuration → Event → One-Key Disarm" to enter the One-Key Disarm settings interface, as shown in Figure 8-7-60.

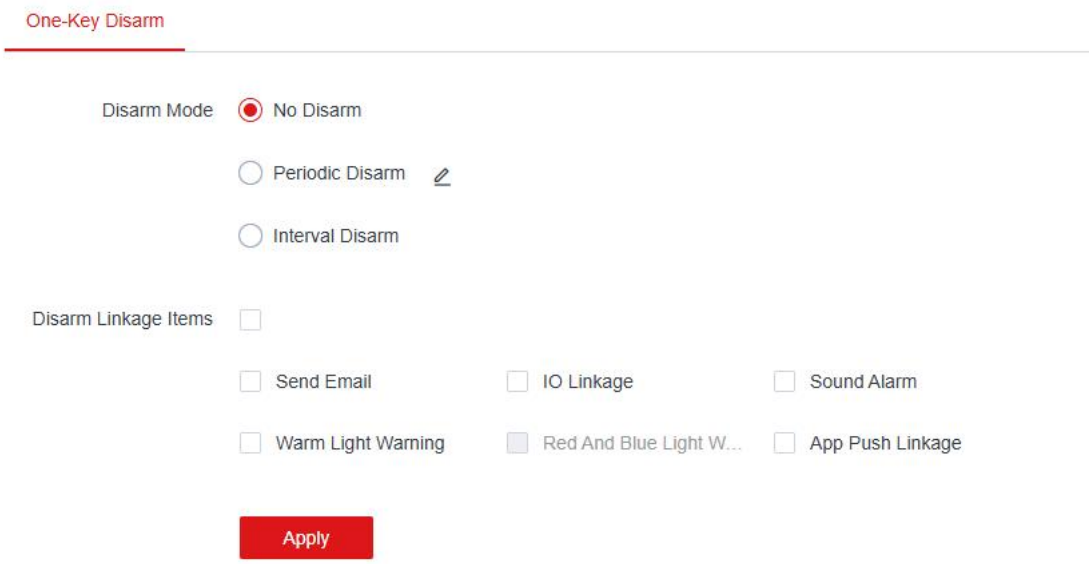


Figure 8-7-60

Step 2: Check to set the disarm mode, choose one of the three, cannot support both at the same time.

【No Disarm】By default, the alarm is not disarmed and the alarm is responded to according to the alarm area, arming time and linkage mode configured by the user in the alarm event.

【Periodic Disarm】Check the periodic disarming checkbox, click the "" icon button to open the time configuration window, and set the disarming time. After completing the setting, click "Apply" to perform periodic disarming operations according to the set disarming time. Automatic disarming will be performed during the set time period (according to the disarming linkage item, the corresponding enabled alarm event linkage mode will be canceled), and automatic deployment will be performed during the unset time period (according to the disarming linkage item, the corresponding enabled alarm event linkage mode will be set).

【Interval Disarm】Check the zone disarming, set the start time (date and specific time) and end time (date and specific time), click "Apply", and perform a single scheduled disarming operation according to the set time period. Automatic disarming will be performed during the time period (according to the disarming linkage item, the corresponding enabled alarm event linkage mode will be canceled), and automatic arming will be performed after the end time (according to the disarming linkage item, the corresponding enabled alarm event linkage mode will be set).

Step 3: Set the disarm linkage items. Customers can check the linkage items that need to be disarmed or not according to actual needs. The linkage items include: email linkage, IO output, sound alarm, warm light warning, red and blue light warning, and APP alarm push.

NOTE

- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.

8.7.4 Statistical Analysis

In the statistical analysis interface, various statistical data can be queried, counted, and exported, making it easier for users to manage statistical data.

① Line Crossing Statistics

The line statistics interface can count, view, download and export the line counting data stored in the IPC memory card.

On the main interface, click "Configuration → Event → Statistical Analysis → Line Crossing Statistics" to enter the Line Crossing Statistics interface, as shown in Figure 8-7-61 below.

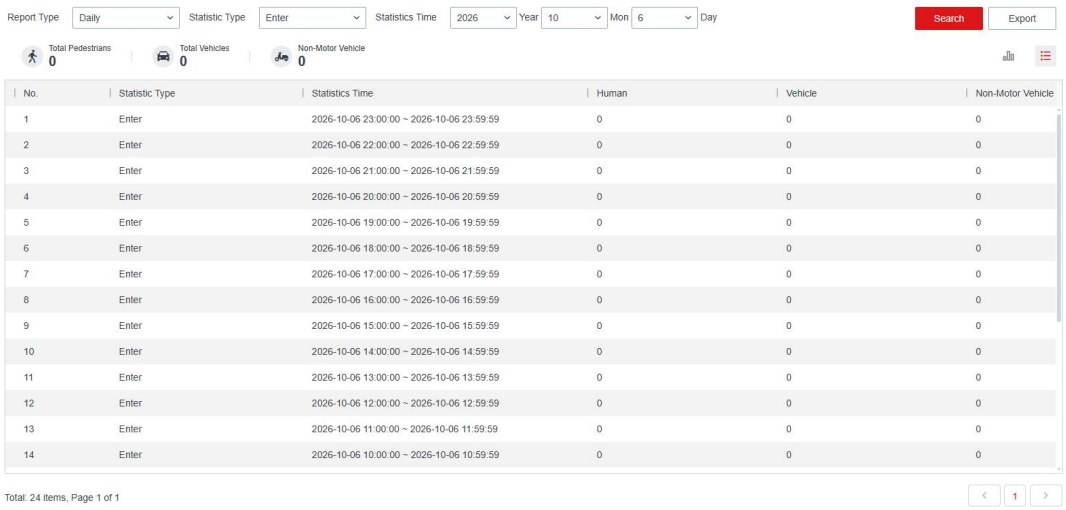


Figure 8-7-61

【Search】 Query the corresponding line-crossing count data based on the specified report type, statistics type, and statistical time.

【Export】 Click "

" to export the queried data. The exported file format is .csv.

【Display】 The default list display format is "". If desired, click "" to display the data in icon format.

NOTE

- The line crossing count are for data stored in the SD card. When the line crossing count is turned on, you need to ensure that the device supports the SD card and the SD card is in normal use, otherwise the statistics query cannot be normal.

② Heatmap

The heatmap statistics interface can statistically analyze the traffic heat data stored on the IPC memory card and display the heatmap using different colors.。
On the main interface, click "Configuration → Event → Statistical Analysis → Line Crossing Statistics" to enter the Line Crossing Statistics interface, as shown in Figure 8-7-62 below:

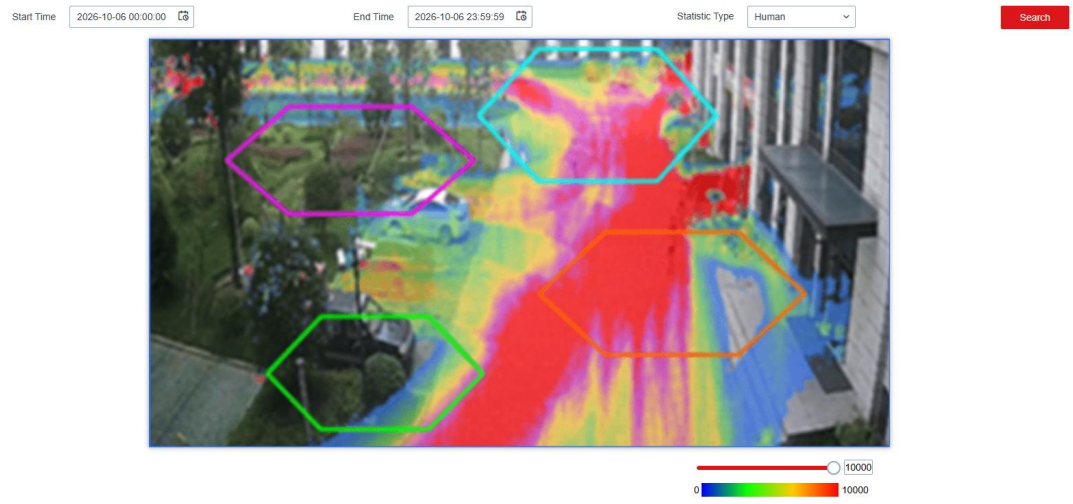


Figure 8-7-62

【Statistics】Based on the set start time, end time, and statistical type, query and statistically analyze the corresponding traffic popularity data, obtain the latest frame of the current real-time video, and display the heatmap using different colors.
【Example of color gradient for heat level】Blue, green, yellow, and red gradient stripes.
【Maximum value of the color range for heat display】The color displayed corresponds to the maximum value within the set range. The minimum value is 1, and the maximum is 10000. The default range is 0-10000, meaning that the darkest red is used only when the value reaches 10000. Users can set the maximum value within the range according to their specific needs.

NOTE

- The search time granularity is 1 hour.
- Heatmap data will be saved to the SD card. Please insert it.

8.7.5 Face Recognition

It supports facial recognition comparison with imported facial image databases and triggers alarms based on the comparison results.

① Face Database

Supports configuration of a face image library for face image comparison during face recognition. Only administrators have permission to configure the face image library. On the main interface, click "Configuration → Event → Face Recognition → Face Database" to enter the Face Database interface, as shown in Figure 8-7-63 below：

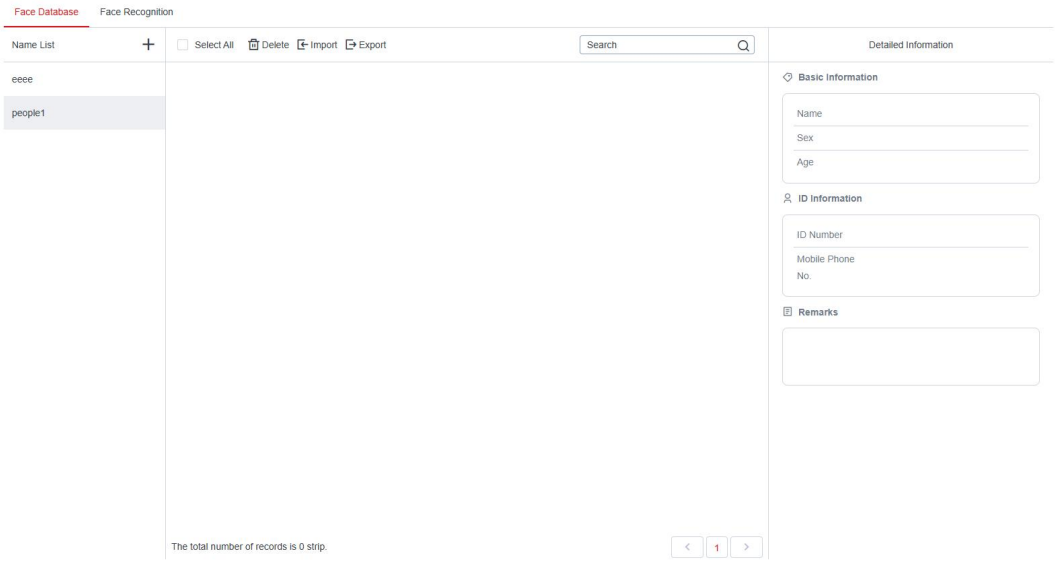


Figure 8-7-63

【Add】Click "+",enter a name for the database to add face images; up to 20 databases can be added.

【Edit】Select the list database you want to edit, and click "✎"to change the corresponding list database name.

【Delete】Select the list database you want to delete, and click "🗑" to delete the database.

【Image Import】Select the existing database and click "Import" to import face images.

【Image Export】Select the existing database, check the face images you want to export, and click "Export" to export the corresponding face images.

【Image Deletion】Click "🗑" on the corresponding face image, or select multiple face images and click " 🗑 Delete " to delete one or multiple face images.

【Fuzzy Search】Enter the name information of the face image in the search input box and

click " " to perform a fuzzy search.

【View Image Information】Select the face image for which you want to view detailed information, and the corresponding detailed information will be displayed on the right.

【Image Information Editing】Select the face image for which you want to edit details, click the " " icon on the image, and edit the relevant information in the pop-up details editing window. Save the image after you're done editing.

NOTE

- Imported image format requirements: JPG, JPEG, PNG, BMP; resolution: 64x64 pixels to 1920x1080 pixels; each image size less than 1MB; recommended size: 50KB.

② Face Recognition

It supports comparing captured facial images with faces in a pre-defined facial database and performing corresponding actions based on the set comparison type.

The specific operation steps are as follows:

Step 1: In the main interface click on the "Configuration → Event → Face Recognition →Face Recognition" to enter the Face Recognition settings interface, as shown in Figure 8-7-64：

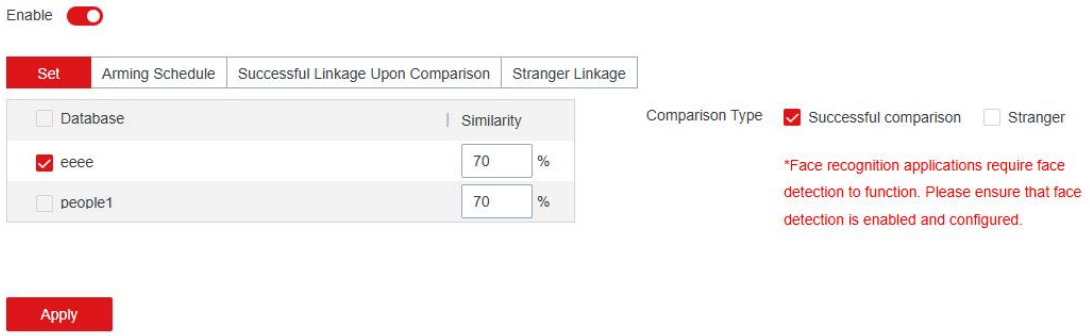


Figure 8-7-64

Step 2: Check "Enable" to enable face recognition；

Step 3: To set up face recognition rules, select "Set" .You can configure the comparison type, comparison library, and similarity score. After setting, please click "Apply" below.

【Comparison Type】: Choose between Default (match with selected library successful) or Stranger (match with selected library failed).

【Database】Users can select one or more face databases for comparison, depending on their needs.

【Similarity】A similarity threshold is set to adapt to different scenarios and improve the accuracy of the comparison. A higher similarity threshold results in a lower success rate of

matching the correct face from the face database, thus reducing the false alarm rate; conversely, a lower threshold increases the false alarm rate.

Step 4: Set the arming schedule.

As shown in Figure 8-7-65. You can view, edit, and delete the arming time of the face recognition. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.
- You can set up more than one time period for up to 8 time periods.
- After setting, click "Apply" to complete the setting of the arming time.

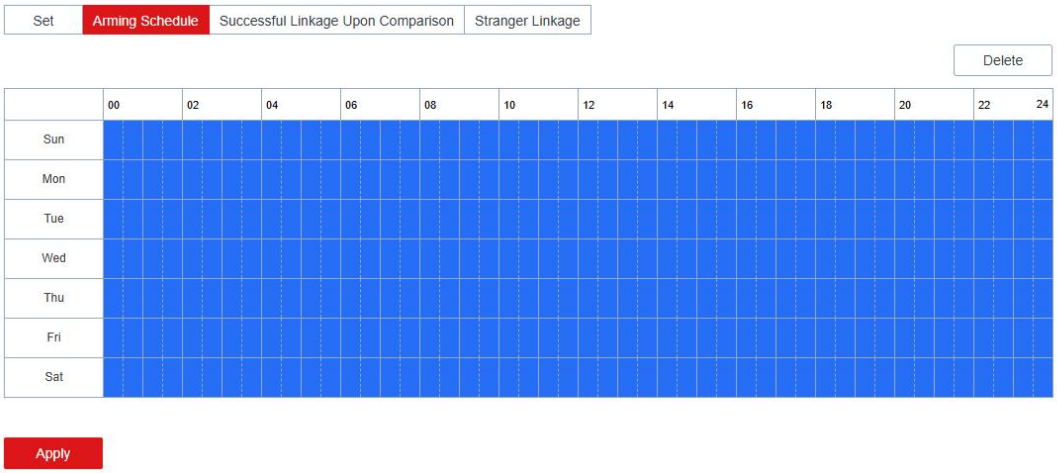


Figure 8-7-65

NOTE

- When the arming time is set, there can be no overlap between any two time periods.

Step 5: Set the linkage method as needed.

It supports setting corresponding linkage methods for different comparison types.Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via Cloud, Light Warning,Sound Alarm) and trigger alarm output(IO Output), as shown in Figure 8-7-66.

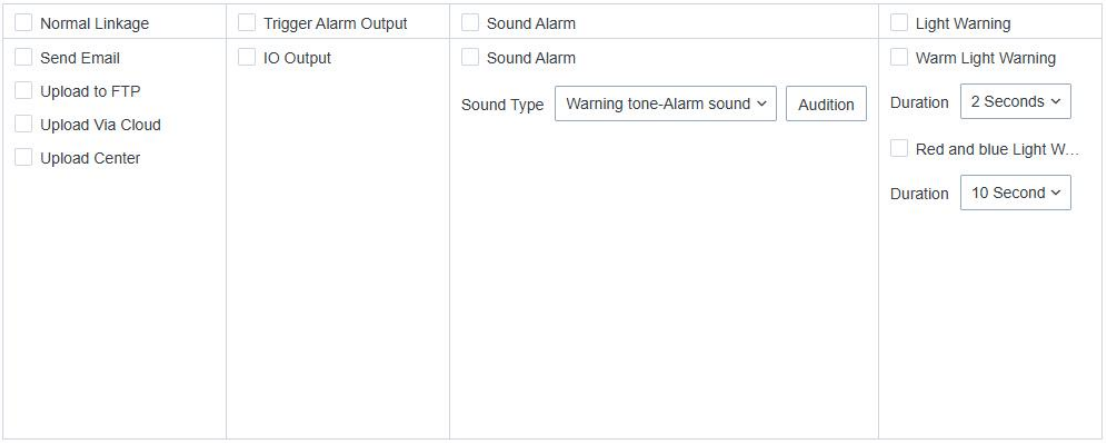


Figure 8-7-66

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.

【Light Warning】After selection, the device will link the alarm light to flash.

【IO Output】Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.

【Sound Alarm】After selection, the device will emit an alarm sound when alarming.

NOTE

- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.

8.7.6 License Plate Recognition

① License Plate Number

Supports license plate number database management for IPCs, including whitelists and blacklists, for license plate number comparison during license plate recognition. Only administrators have access to the license plate number database.

On the main interface, click "Configuration → Event → License Plate Recognition → License Plate Number" to enter the License Plate Number interface, as shown in Figure 8-7-67 below：

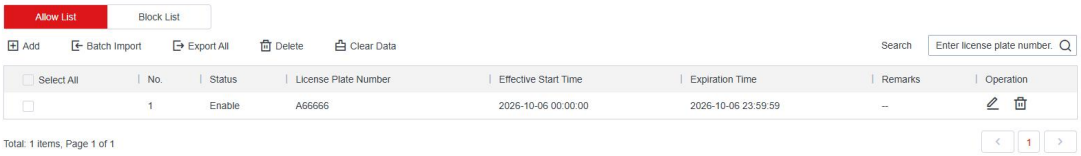


Figure 8-7-67

【Lists】License plate numbers are divided into whitelists and blacklists. Click to select the corresponding list database to add, modify, or delete license plate numbers in the whitelist or blacklist respectively.

【Add】Click "Add ",in the pop-up window for adding license plate numbers, enter the license plate number, set the valid start time and expiration time, and you can add the corresponding license plate number..

【Edit】In the operation bar for the license plate number record that needs to be edit, and click "to change the corresponding license plate number information.

【Delete】In the operation bar for the license plate number record that needs to be deleted, and click " " to delete the license plate number.

【Batch Import】Click " Batch Import " to download the corresponding template. After filling in the relevant license plate number information, select the file to import license plate numbers in batches.

【Batch Delete】In the list of license plate numbers, select the records you want to delete, and click " Delete " to perform batch deletion.

【Export All】Click " Export All " to export all license plate number information.

【Fuzzy Search】Enter the license plate number in the search input box and click " " to perform a fuzzy search.

【Clear Data】Click " Clear Data " to clear all license plate number records at once.

NOTE

- IThe allowlist and blocklist together support a total of 5,000 license plate numbers.
- For batch import, you need to download the import template first, fill in the relevant information according to the template, and then import.

② License Plate Recognition

It supports extracting license plate numbers from captured license plate images and comparing them with license plate numbers in a pre-defined license plate number database, and performing corresponding actions based on the set comparison type.

The specific operation steps are as follows:

Step 1: In the main interface click on the "Configuration → Event → License Plate Recognition→License Plate Recognition" to enter the License Plate Recognition settings interface, as shown in Figure 8-7-68：

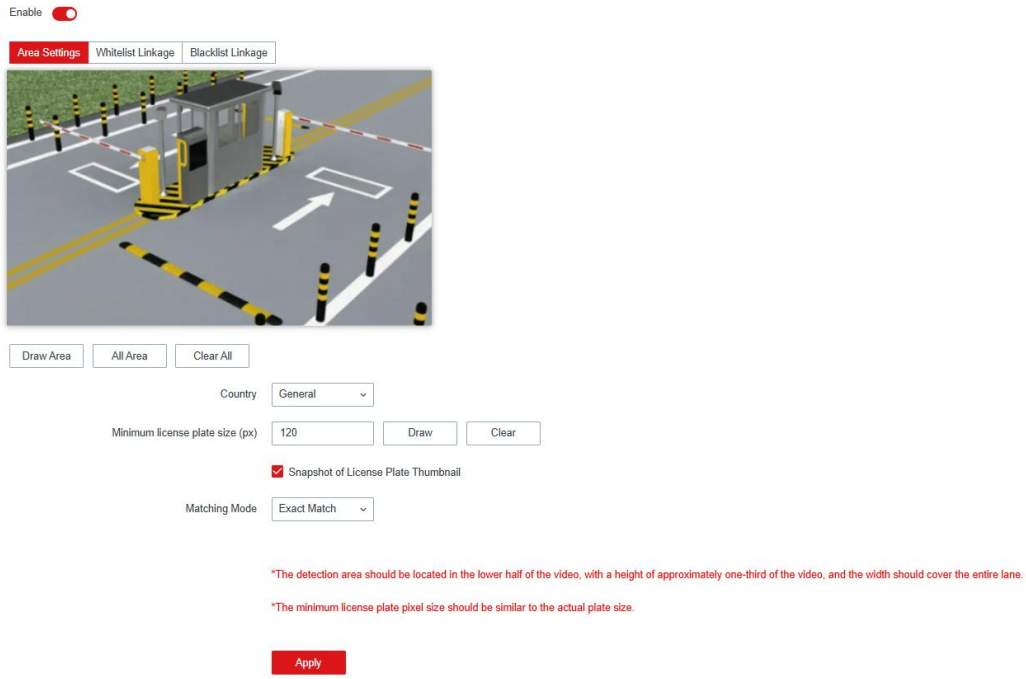


Figure 8-7-68

Step 2: Check "Enable" to enable license plate pecognition；

Step 3: To configure license plate recognition rules, select "Area Settings." This allows you to configure the detection area, country, minimum license plate size, and matching mode. Once you're finished setting up, click "Apply" below.

【Draw Area】Click “Draw Area”, move the mouse to the preview screen and click the left mouse button in sequence to draw the endpoints of the 4-8 polygon warning area, right-click to end the polygon drawing, and support dragging polygon vertices to adjust the area size, drag the entire polygon to adjust the overall area position.

【All Area】When need all areas to be detected, click "All Area" to automatically select all areas.

【Clear All】Used to delete the selected alert area.

【Country】This setting allows you to filter license plates based on their country of origin, improving recognition accuracy.

【Minimum license plate size】This setting specifies the minimum width of the license plate in pixels. The default value is 120 (minimum), and the maximum is the entire image. Users can directly input the pixel width or set the minimum license plate width by drawing it directly, depending on the actual scenario.

【Snapshot of License Plate Thumbnail】This setting determines whether to capture license plate images. Checking this box will capture an image of the license plate during

license plate recognition and display it in the corresponding window. Unchecking this box will neither capture nor display an image.

【Matching Mode】Used to set the matching mode. The default is exact matching, and fuzzy matching is optional. You can set the number of characters allowed to be mismatched, with a default of 1, 2, or 3. Fuzzy matching is performed based on the set number of characters allowed to be mismatched. Characters within the set number of mismatched characters can be identified and compared.

Step 5: Set the linkage method as needed.

It supports setting corresponding linkage methods for different comparison types.Alarm linkage methods include general linkage(Send Email, Upload to FTP, Upload Via Cloud, Light Warning,Sound Alarm) and trigger alarm output(IO Output), as shown in Figure 8-7-69.

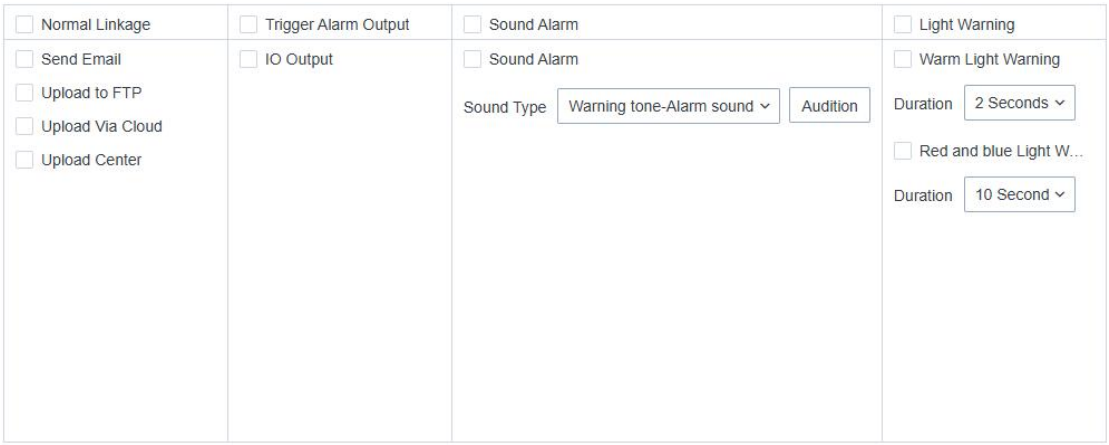


Figure 8-7-69

【Send Email】Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.

【Upload to FTP】Select and the system is configured with the FTP server, will send the alarm information to the FTP server.

【Upload Via Cloud】Select and the system is configured with the cloud server, will send the alarm information to the cloud account.

【Upload Center】 If selected and the system is configured with an alarm server, the alarm information will be sent to the alarm server when an alarm occurs.

【Light Warning】After selection, the device will link the alarm light to flash.

【IO Output】Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.

【Sound Alarm】After selection, the device will emit an alarm sound when alarming.

NOTE

- License plate recognition is mainly used for entrance and exit management (not involving toll collection).
- Different devices support different alarm linkage. The alarm linkage method is subject to the actual product.

③ Dual Camera Mode

Dual-camera mode can be configured, it is off by default, but can be adjusted according to the actual usage scenario.

On the main interface, click "Configuration → Event → License Plate Recognition → Dual Camera Mode" to enter the Dual Camera Mode interface, as shown in Figure 8-7-70 below：

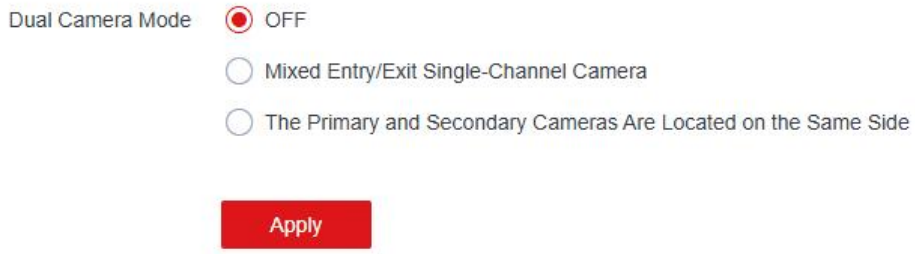


Figure 8-7-70

【OFF】Dual camera mode is off,the camera is used as a single camera.

【Mixed Entry/Exit Single-Channel Camera】This system is suitable for single-lane mixed-access entrances and exits. In use, one camera is required for entering vehicles, and another for exiting vehicles. Both cameras must support the single-lane mixed-access entrance/exit camera function. Once this function is enabled and configured, when the same vehicle passes through both cameras sequentially, one camera will prioritize capturing the passing vehicle, while the other camera will not capture it.

【Camera Mode】This is used to set whether this camera is the main camera or the secondary camera according to the actual usage scenario.

【Secondary Camera IP】Used to set the IP address of the secondary camera.

【Minimum Time Synchronization Interval】This setting determines the time interval for synchronization. The main camera synchronizes with the secondary camera according to the set time interval.

【The Primary and Secondary Cameras Are Located on the Same Side】Suitable for wide lane scenes, where the main camera and secondary camera simultaneously capture the same scene, and the main camera judges the shooting results.

【Camera Mode】This is used to set whether this camera is the main camera or the secondary camera according to the actual usage scenario.

【Secondary Camera IP】Used to set the IP address of the secondary camera.

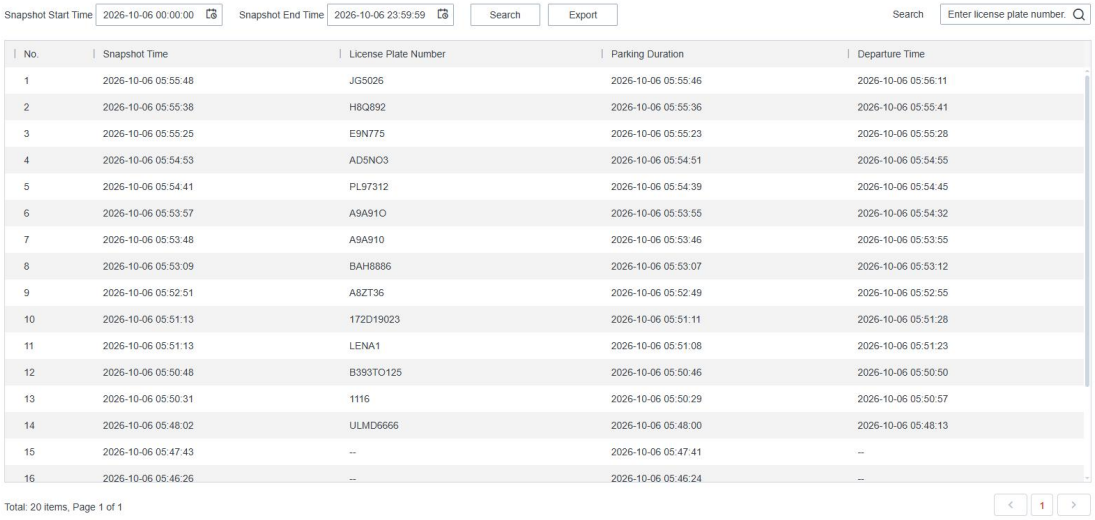
【Dual-Camera Snapshot Interval】Used to set the time interval for capturing license plates from the main camera and secondary camera.

【Minimum Time Synchronization Interval】This setting determines the time interval for synchronization. The main camera synchronizes with the secondary camera according to the set time interval.

8.7.7 Vehicle Record

① Illegal Parking

Supports viewing and exporting illegal parking record data stored on IPC.
On the main interface, click "Configuration → Event → Vehicle Record → Illegal Parking" to enter the Illegal Parking interface, as shown in Figure 8-7-71 below：



No.	Snapshot Time	License Plate Number	Parking Duration	Departure Time
1	2026-10-06 05:55:48	JG5026	2026-10-06 05:55:46	2026-10-06 05:56:11
2	2026-10-06 05:55:38	H8Q892	2026-10-06 05:55:36	2026-10-06 05:55:41
3	2026-10-06 05:55:25	E9N775	2026-10-06 05:55:23	2026-10-06 05:55:28
4	2026-10-06 05:54:53	AD5NO3	2026-10-06 05:54:51	2026-10-06 05:54:55
5	2026-10-06 05:54:41	PL97312	2026-10-06 05:54:39	2026-10-06 05:54:45
6	2026-10-06 05:53:57	A9A91O	2026-10-06 05:53:55	2026-10-06 05:54:32
7	2026-10-06 05:53:48	A9A910	2026-10-06 05:53:46	2026-10-06 05:53:55
8	2026-10-06 05:53:09	BAH8886	2026-10-06 05:53:07	2026-10-06 05:53:12
9	2026-10-06 05:52:51	A8ZT36	2026-10-06 05:52:49	2026-10-06 05:52:55
10	2026-10-06 05:51:13	172D19023	2026-10-06 05:51:11	2026-10-06 05:51:28
11	2026-10-06 05:51:13	LENA1	2026-10-06 05:51:08	2026-10-06 05:51:23
12	2026-10-06 05:50:48	B393TO125	2026-10-06 05:50:46	2026-10-06 05:50:50
13	2026-10-06 05:50:31	1116	2026-10-06 05:50:29	2026-10-06 05:50:57
14	2026-10-06 05:48:02	ULMD6666	2026-10-06 05:48:00	2026-10-06 05:48:13
15	2026-10-06 05:47:43	--	2026-10-06 05:47:41	--
16	2026-10-06 05:46:26	--	2026-10-06 05:46:24	--

Figure 8-7-71

【Search】Click to select the snapshot start time and snapshot end time, then click the "Search" button to query the corresponding illegal parking capture records.
【Fuzzy Search】If records have already been found using the time-based search filter, enter the specific license plate number in the license plate number input box and click "🔍" to perform a fuzzy search on the filtered records.

【Export】Based on the queried data, click "Export" button to export the data. The exported file format is .csv.

NOTE

- The exported files,file names and headers only support Chinese and English.

② License Plate Recognition

Supports viewing and exporting license plate recognition record data stored on the IPC..
On the main interface, click "Configuration → Event → Vehicle Record → License Plate Recognition" to enter theLicense Plate Recognition interface, as shown in Figure 8-7-72 below：

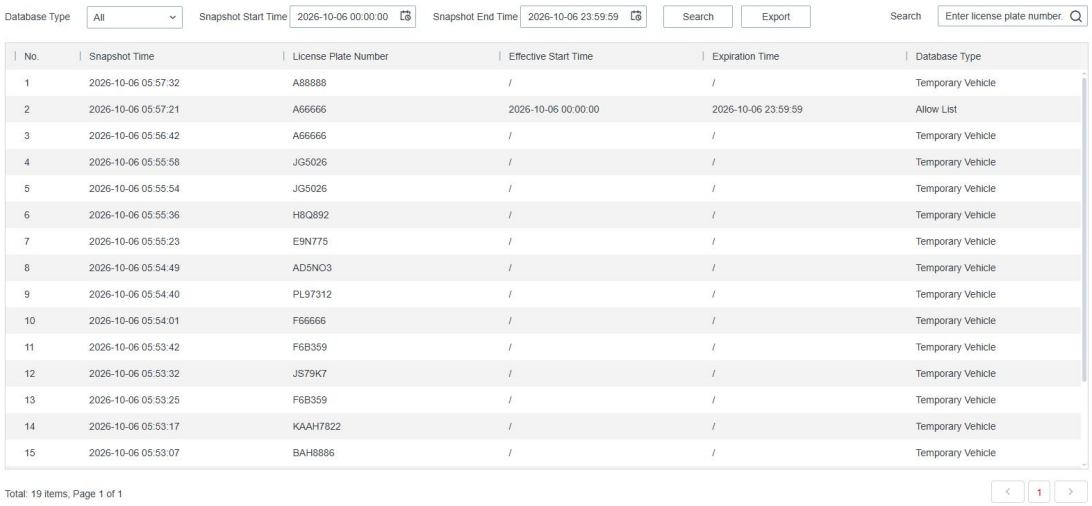


Figure 8-7-72

【Search】Click to select the database type, select the snapshot start time and snapshot end time, and click the "Search" button to query the corresponding license plate recognition capture records.

【Fuzzy Search】If records have already been found using the time-based search filter, enter the specific license plate number in the license plate number input box and click "🔍" to perform a fuzzy search on the filtered records.

【Export】Based on the queried data, click "Export" button to export the data. The exported file format is .csv.

NOTE

- The exported files,file names and headers only support Chinese and English.

8.8 Storage

8.8.1 Schedule Settings

① Record Schedule

The specific operation steps are as follows:

Step 1: In the main interface, click "Configuration → Storage → Schedule Settings → Record Schedule" to enter the recording setting interface, as shown in Figure 8-8-1.

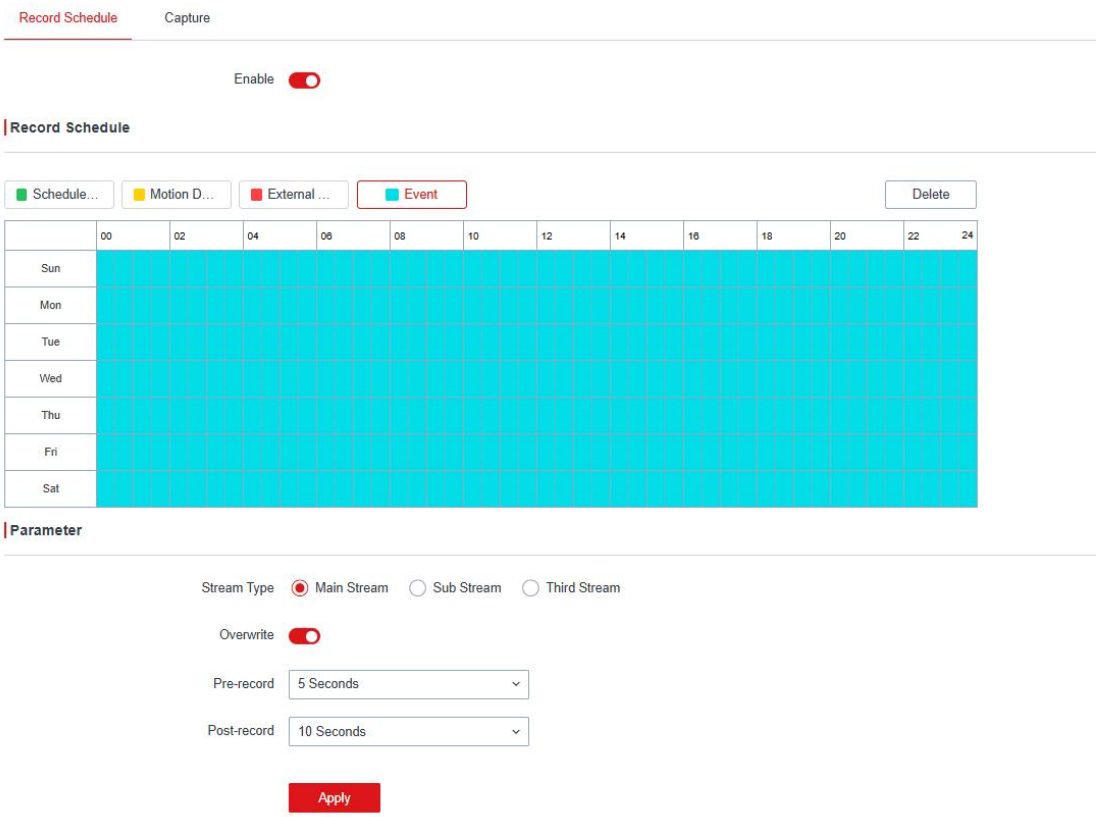


Figure 8-8-1

Step 2: To enable record, select the stream type (Main Stream, Sub Stream, Tri-Stream）.

Step 3: Configure the recording schedule time period corresponding to the recording type (scheduled recording, motion detection, external alarm, event).

- Method 1: Click the arming time period, manually enter the start time and end time, then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.
- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.

Step 4: Set the Pre-record and Post-record. You can set the Pre-recorded time (No Pre-record, 5S, 10s, 15s, 20s, 25s,30s) and Post-record (5s, 10s, 30s, 1min, 2min, 5min, 10min).

Step 5: Click "Apply" to complete the setting of the arming time.

NOTE

- You can set up more than one time period for up to 8 time periods.
- Tick "Select All" to enable 24/7 recording.
- No EMMC/TF card video recording function of the camera No EMMC/TF card management interface, please take the camera physical specific functions shall prevail.
- EMMC storage does not support time recording
- EMMC storage requires the camera to support EMMC hardware,please refer to the actual product.

- When the video type selects motion detection, alarm, the device will also perform scheduled recording while recording the selected recording type.
- The pre-record and post-record can be used for motion detection recording, alarm recording, motion detection and alarm recording.
- The content of the recording plan configuration items varies on different devices. Please refer to the actual device for the specific interface.

② Capture

The capture is used to set the camera capture schedule and capture parameters. After setting, the IP camera will capture images according to the settings. Users can enable scheduled capture in the capture parameter setting interface and set the capture plan according to actual needs.

The specific operation steps are as follows:

Step 1: In the main interface, click "Configuration → Storage → Schedule Settings → Capture" to enter the capture parameter setting interface, as shown in Figure 8-8-2.

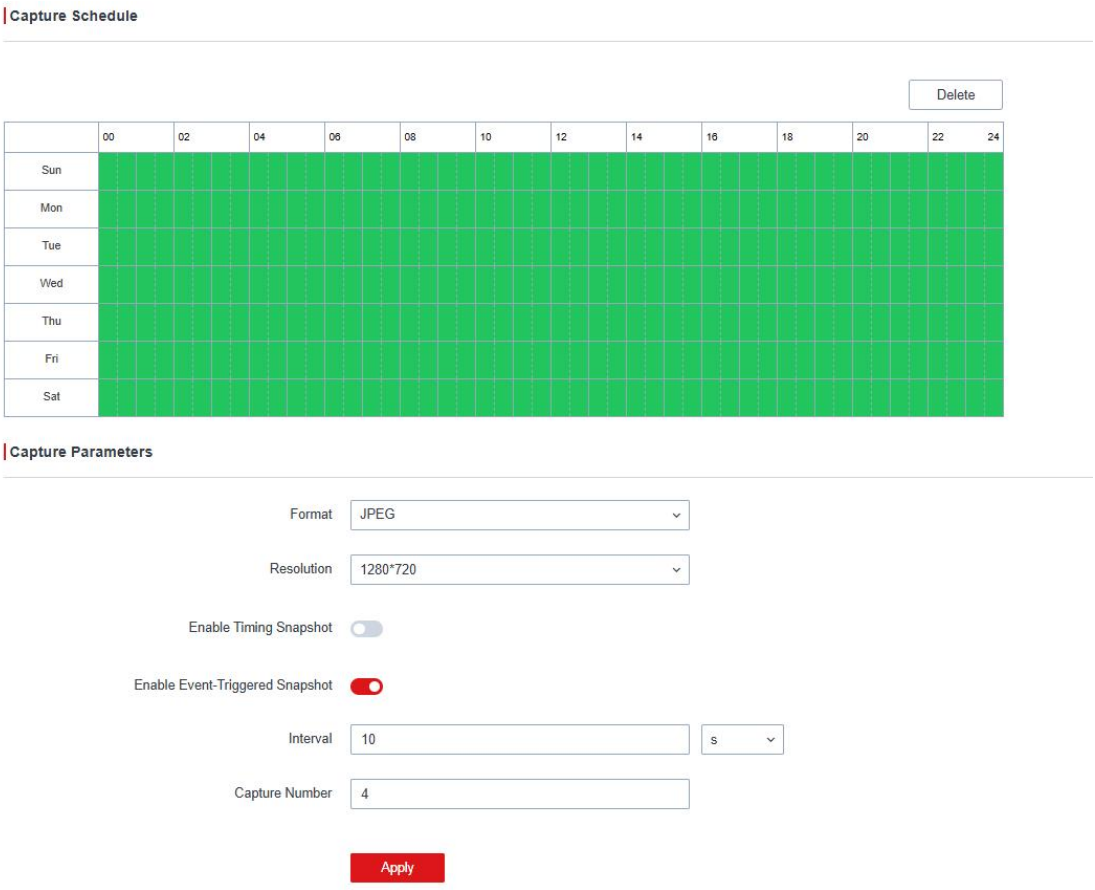


Figure 8-8-2

Step 2: Set the capture schedule.

– Method 1: Click the arming time period, manually enter the start time and end time,

then click "Save" after configuration. To delete this time period, click the "Delete" button before re-configuring the time period.

- Method 2: Press and hold the left-mouse button and drag on the time bar to set the arming schedule.

Step 3: Repeat **step 2** to set up a complete recording plan.

Step 4: Select options such as image format (JPEG), resolution, and picture quality under the capture parameters as required, and set up timing snapshot and event-triggered snapshot.

【Format】Support JPEG format.

【Resolution】The captured image resolution.

【Picture Quality】Three levels of "Low", "Midd" and "High" can be selected.

【Enable Timing Snapshot】During the set time period, grab a picture according to the set time interval.

【Interval】Please set the time interval of snapshot according to your needs.

【Capture Number】When an event triggers a snapshot, you can set the number of pictures captured by an event trigger.

Step 5: Click "Apply" to complete the settings.

NOTE

- You can set up more than one time period for up to 8 time periods.
- Tick "Select All" to enable 24/7 recording.
- No EMMC/TF card video recording function of the camera No EMMC/TF card management interface, please take the camera physical specific functions shall prevail.
- EMMC storage requires the camera to support EMMC hardware,please refer to the actual product.
- The arming time of the event snapshot needs to be configured in each event.
- The content of the capture parameter configuration items varies from device to device. Please refer to the actual device for the specific interface.

8.8.2 Storage management

① Storage

In the main interface, click "Configuration → Storage → Storage Management → Storage" to enter the storage management setting interface, where you can view the memory card capacity and status, and perform operations such as formatting and configuring the memory card, as shown in Figure 8-8-3 :

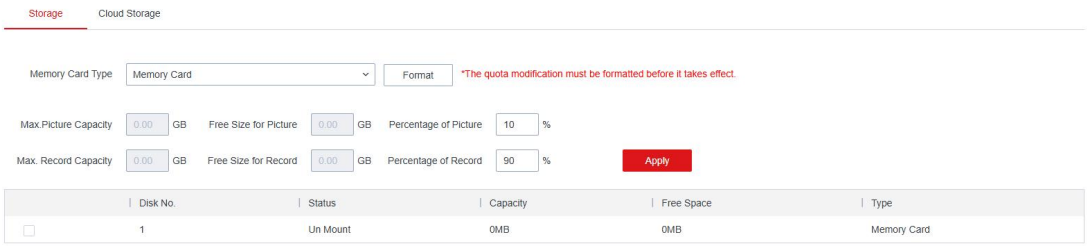


Figure 8-8-3

EMMC/SD card format steps are as follows：

Step 1: Select the disk to be formatted, click "Format".

Step 2: Click "OK".

Step 3: Wait for the format to complete the progress bar, formatting is complete, check the card information, Capacity =Free space, formatted successfully.

The steps to configure disk quota are as follows:

Step 1: Select the memory card.

Step 2: Set the disk quota, including parameters such as picture capacity and video capacity.

Step 3: Click "Save".

Step 4: Click "Format → OK" to complete the configuration of disk quota after formatting.

NOTE

- EMMC storage requires the camera to support EMMC hardware,please refer to the actual product.

② Cloud Storage

■ Cloud Storage

Set up cloud storage. When the device triggers an alarm, you can store the alarm picture taken by the device on a cloud server.

Prerequisites

1) You need to have a Google cloud storage account.

2) To use this function, the device must be connected to the external network, otherwise it will not work properly.

The specific operation steps are as follows:

Step 1: In the main interface, click "Configuration → Storage → Storage management → Cloud Storage" to enter the cloud storage configuration interface, as shown in Figure 8-8-4.

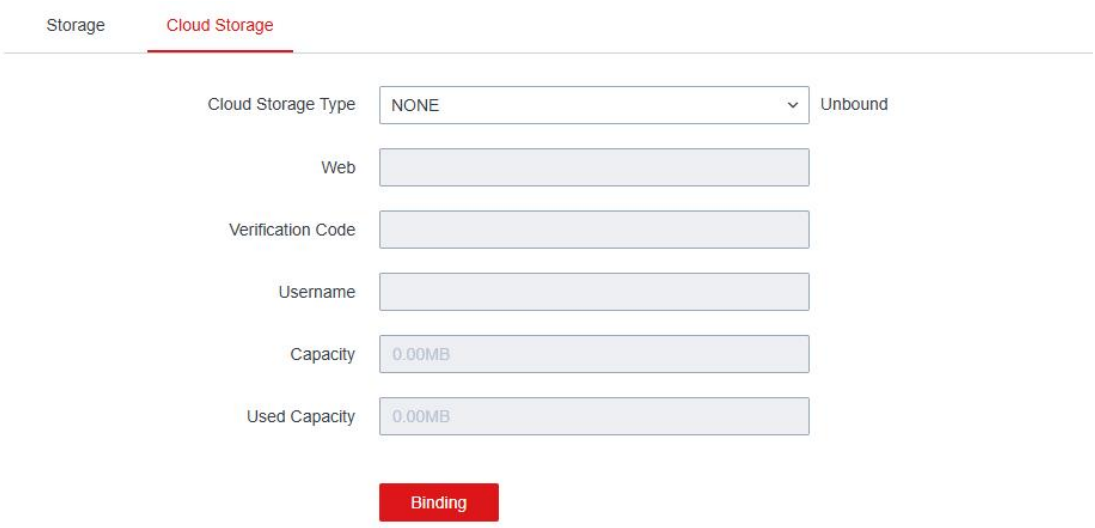


Figure 8-8-4

Step 2: Select the cloud storage type, such as "Google".

Step 3: Follow the prompts to log in to the website with a browser on the computer to obtain the "Verification Code".

Step 4: Enter the verification code in the "Verification code" field of the cloud storage interface.

Step 5: Click "Binding".

NOTE

- Cloud storage type only support google.
- The total capacity is the total capacity of the cloud disk owned by the current account. If you need to expand the capacity, you can log in to the corresponding website of the cloud disk to expand or purchase the capacity.

Chapter 9 Maintain

9.1 Device Information

In the Maintenance interface, click "Device Information" to enter the device information configuration interface, where you can view the basic information of the current device, as shown in Figure 9-1:



Figure 9-1

【Device Name】The name of the current IPC.
【Firmware Version】The current version of the IPC.
【Web Version】The current page version of the IPC.

NOTE

- Users can modify the device name according to actual needs.

9.2 Upgrade

In the Maintenance interface, click "Upgrade" to enter the device upgrade interface, where you can manual upgrade, online upgrade, as shown in Figure 9-2.



Figure 9-2

【Manual Upgrade】Clicking “Browse” to add upgrade file package, and upgrading the IPC program. (Please careful operation, the error of upgrade file will cause equipment system operate abnormally).

【Online Upgrade】With the device connected to the network, check the current version number and click "Check". If a newer update is available, click "Download". The device will then begin downloading the update. Once the download is complete, you can select the new firmware package to upgrade.

【Automatic Detection】With the device connected to the network, it will automatically detect if a new firmware update is available. If a new update is available, click "Download," and the device will begin downloading the update. Once the download is complete, you can select the new firmware package to upgrade.

9.3 Default

In the Maintenance interface, click "Default" to enter the device recovery default interface, where you can reset device parameters and reset all the parameters to the factory default, as shown in Figure 9-3.

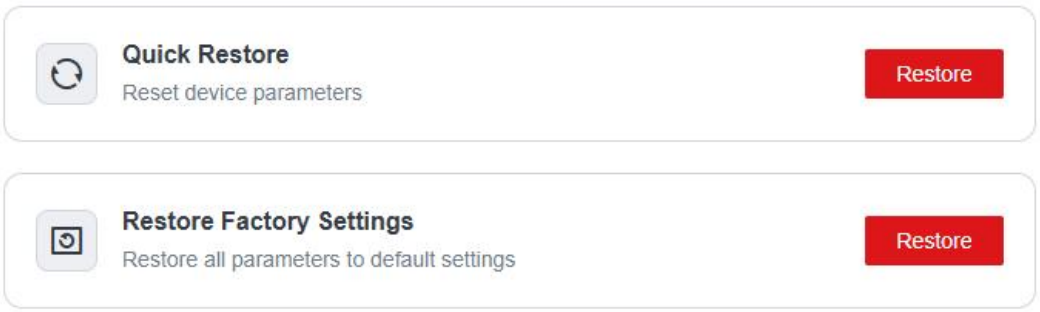


Figure 9-3

【Quick Restore】Clicking the "Restore" button under "Quick Restore" will restore all IPC settings except for network parameters, face image library, and user information to their

factory default settings.

【Restore Factory Settings】Click the "Restore" button under "Restore Factory Settings", All IPC parameter settings will be automatically restored to their factory default settings (please use this function with caution).

9.4 Auto Maintain

In the Maintenance interface, click "Auto Maintain" to enter the scheduled reboot settings interface, where you can set the time for the device to restart, set the restart "cycle" in the drop-down menu, for example, set "3:03 on the 3rd of each month" restart, click "Apply", IPC will be at 3 o'clock on the 3rd 3 times a reboot. As shown in Figure 9-4.



Figure 9-4

NOTE

- If used the default configuration to restart the device, in order to avoid overloading the server due to excessive device restarts at the same time, the background processing logic of the device is to restart randomly within 1 hour.

9.5 Import And Export

In the Maintenance interface, click "Import And Export" to enter the device parameters import and export interface, where you can export device parameters or import the parameters file to IPC , as shown in Figure 9-5.



Figure 9-5

9.6 Log

In the Maintenance interface click on the "Log" into the log search interface, where you can query the device alarm and all other relevant information. As shown in Figure 9-6.

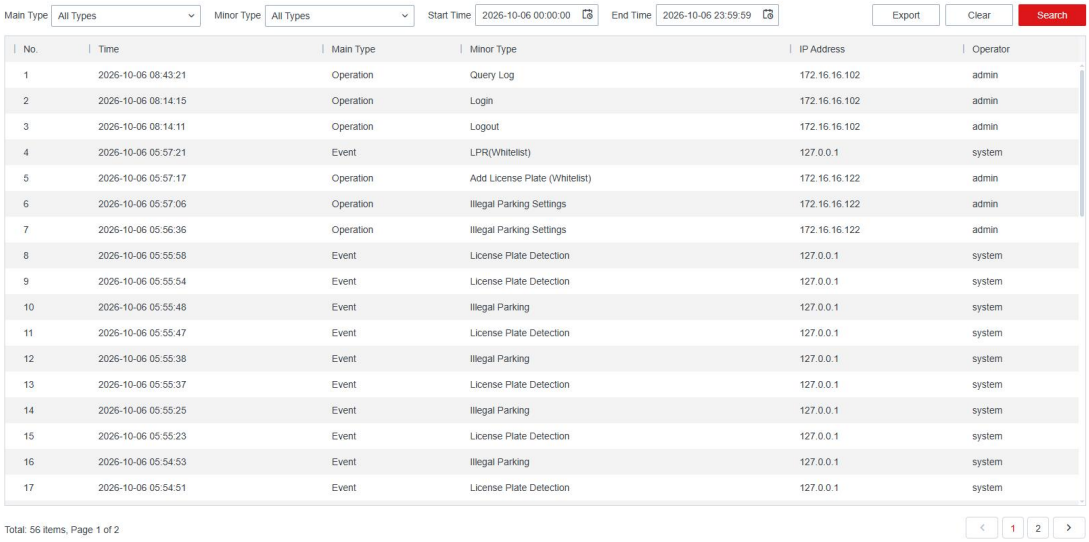


Figure 9-6

【Search】Set the main tpye,minor type and start time of the log query, click "Search", the log list shows the IPC execution record that meets the conditions.

【Clear】Clicking clear button to empty all logging.

【Export】Save the contents of the current log to the location you specified in txt format.

Chapter 10 Frequently Asked Questions

1.Why can not access the camera by Browser?

Answer: There maybe 4 reasons, Details are as follows:

a.The network unreasonable?

Solution: First you can connect network by PC, check the network cable if it is good. And check the network between the camera and the PC is good.

b.The IP address of the camera is occupied by other device or PC?

Solution: You can connect the camera with your PC directly, and modify the IP address or use the IP search tool.

c.The camera maybe in other network segment?

Solution: Check the IP address and net mask.

2. Why can not access the camera after update?

Answer: Clean browser cache.

Step: open IE, click “Tools” and select “Internet Options”, then you can see “Temporary Internet files” and click “Delete Files”, it will prompt a dialog you need to check “Delete all offline content” and click “OK”.

Also you can click “Start” and select “Run” then enter “cmd”, enter “arp -d” in “Command Prompt” interface. Re-access the camera.

3. Why cannot show the whole interface?

Answer: Close some options of IE.

Step: Open IE, click “View” and select “Toolbar”, close the “Favorites bar”, “Status bar” and “Command bar”.

4.Why POE IPC connection to POE switch does not work?

Answer: There maybe 5 reasons, Details are as follows:

a.Make sure that the IPC has POE function. If it cannot be confirmed, it can be confirmed by checking the PI number or disassembling the machine.

b.Use 8-core network cable, do not use 4-core network cable.

c.Check whether the function of the POE switch is normal.

d.The POE power supply protocol of IPC is inconsistent with the power supply protocol of the switch, and other switches can be replaced or the company's switches can be used for use.

e.The POE module of the IPC is damaged, replace the POE module.

5.Why IPC connection to NVR not working?

Answer: There maybe 2 reasons, Details are as follows:

a.The network segments of IPC and NVR are different?

Solution: Modify the values of the first three groups of the IP address of the IPC to be the same as the values of the first three groups of the IP address of the NVR, and modify the last group of numbers to different values.

b.IPC password has been changed?

Solution: Find the corresponding device on the NVR interface, click Edit, and then re-enter the correct IPC password.

6.Why IPC format the SD card, the normal capacity still cannot be recognized?

Answer: There maybe 2 reasons, Details are as follows:

a.SD card problem.

Solution: Use another SD card or another capacity SD card.

b.SD card has multiple partitions, causing IPC to fail to read normally.

Solution: Erase SD Card Partitions on Computer.