IP Camera
User Manual

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 ② Time 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

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, Privacy Mask, Video Tampering, Exception, Alarm Input/Output, Audible alarm output and ROI.

- **Smart event**

Smart event include Intrusion Detection, Line Cross Detection, Loiter Detection and People Gather Detection.

- **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**
- **WIFI function**

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

- **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

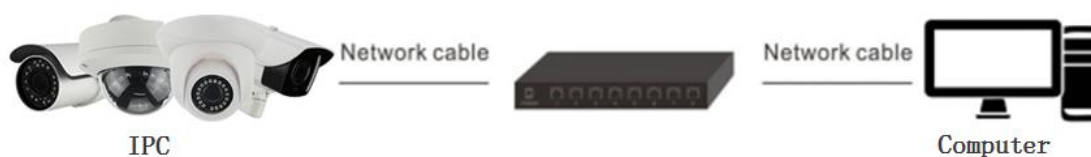Set IP camera over the LAN via a switch or a router as shown in Figure 2-2:

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 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:
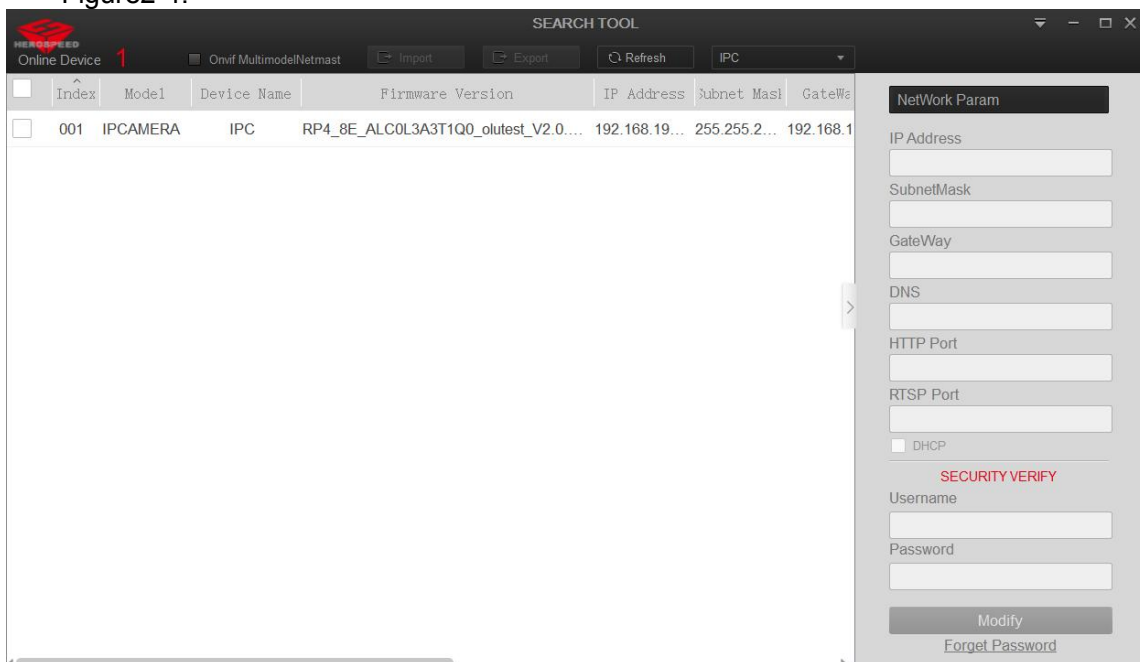

Figure 2-4

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

Step 2： 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 3： 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. The default administrator user name is "admin", and password is "admin". And you are highly recommended to "Modify" the initial password after your first login.
- To access the IPC of different subnets, set the gateway of the IP camera after login. For details, see 7.3.1 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.

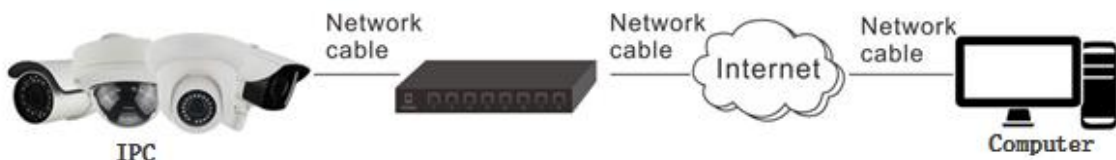➢ **The router is connected to the IP camera as shown in Figure 2-5:**

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.
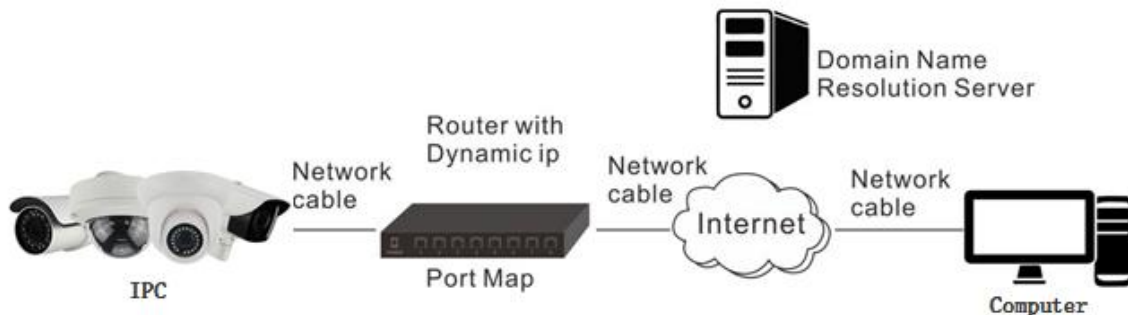
> ## Normal Domain Name Resolution as shown in Figure 2-7:

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 8.3.2.

Step 3: Visit the camera via the applied domain name.
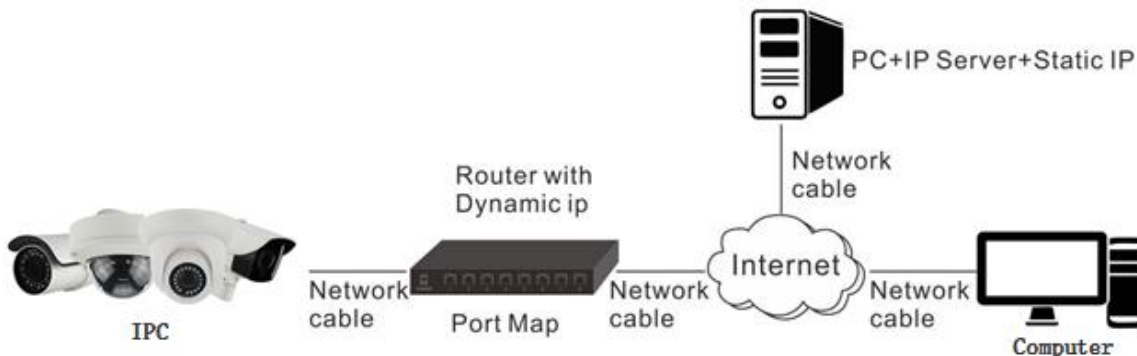
> ## Private Domain Name Resolution, as shown in Figure 2-8:

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 8.3.2.

Chapter 3 Access to the IPC by Client Software

The iVMS320 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 client software are shown in Figure 3-1.
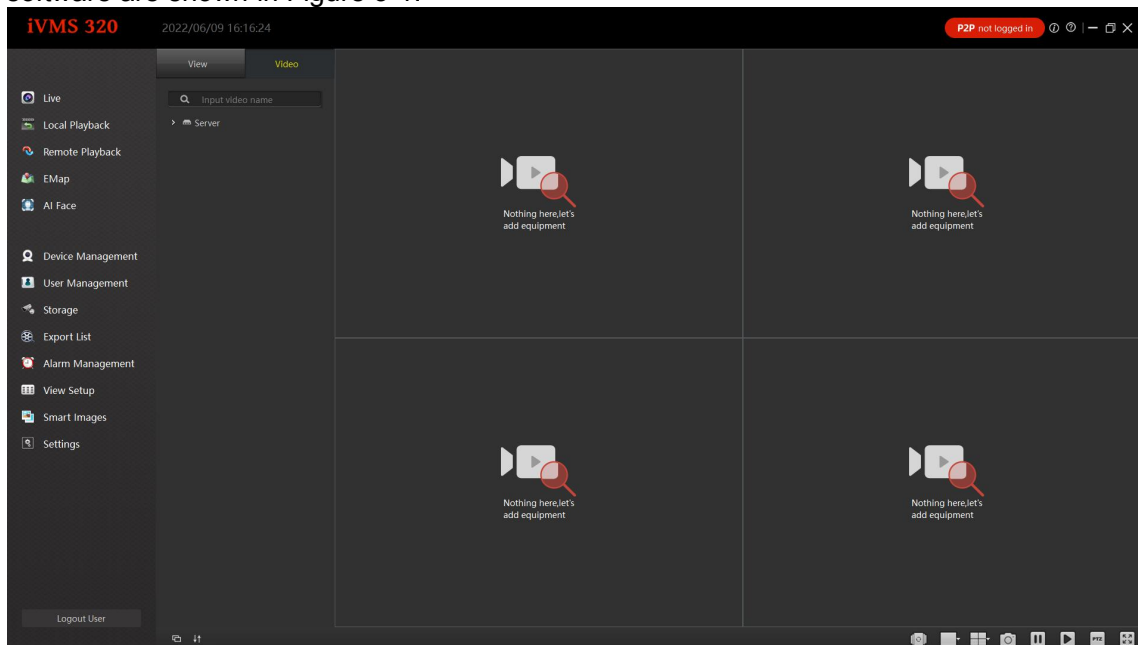
Figure 3-1

NOTE

- For detailed information about the software, please refer to the user manual of the iVMS 320 Client Software.

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.
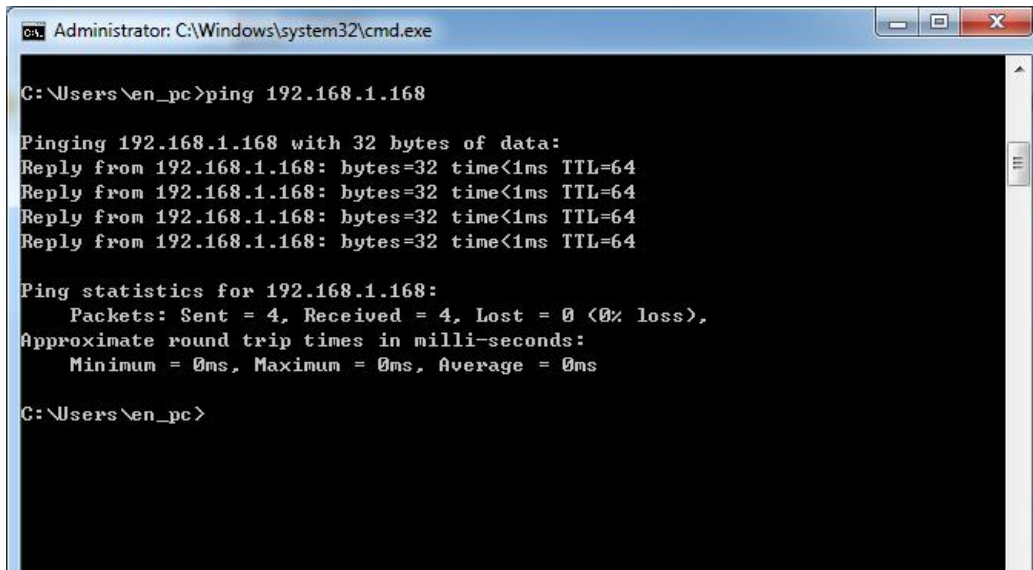
Figure 4-1

4.2 Login and Exit

4.2.1 Login

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 login interface, as shown in Figure 4-2.
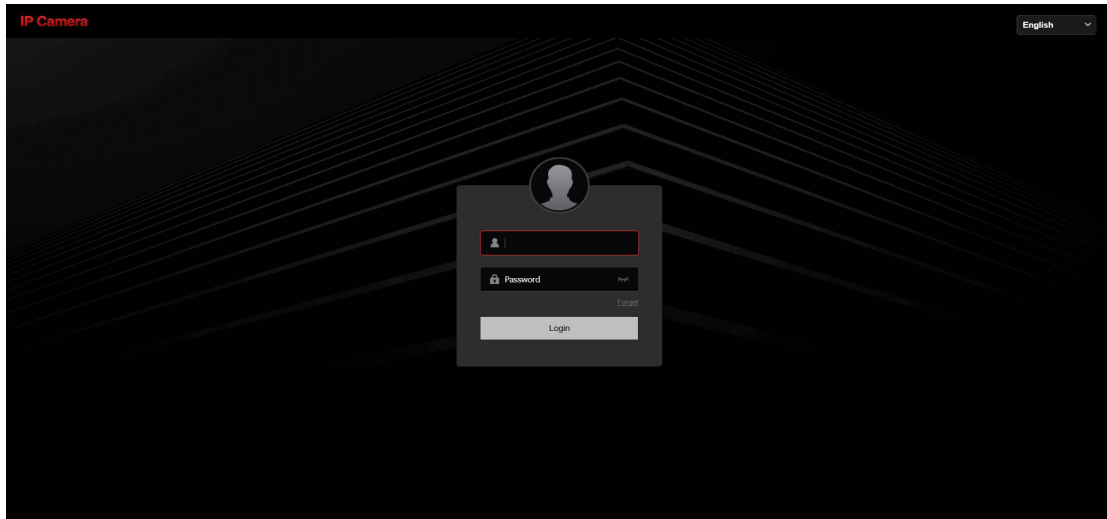
Figure 4-2

Select system language (Simplified Chinese, Traditional Chinese, English, Russian, Korean, Polish, French, Japanese, Spanish, Portuguese, Italian, Hebrew, Turkish, Bulgarian, Arabic, German, Dutch, Czech, Vietnamese are supported), enter the username (default is "admin") and password (default is "admin"): 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, the interface prompts to change the password, as shown in Figure 4-3:
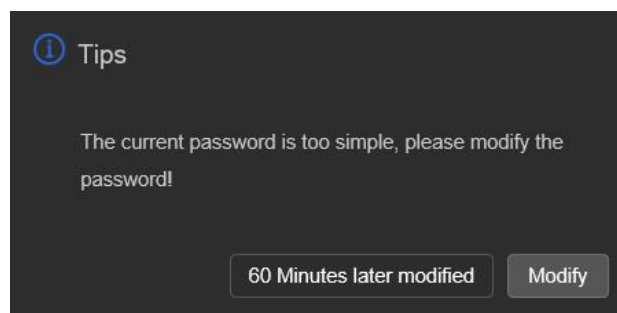
Figure 4-3

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

Figure 4-4

To change your password, follow these steps:

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

Step 2: Set security questions 1, 2, and 3 and enter the answers.

Step 3: Click "key export" to save the key file to your computer.

Step 4: Click "Save" 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 the initial password "admin", each time you log in, you will be prompted to change the password. You can select "After 60 Minutes later

modified". After 60 minutes, the interface will automatically pop up the password modification interface.
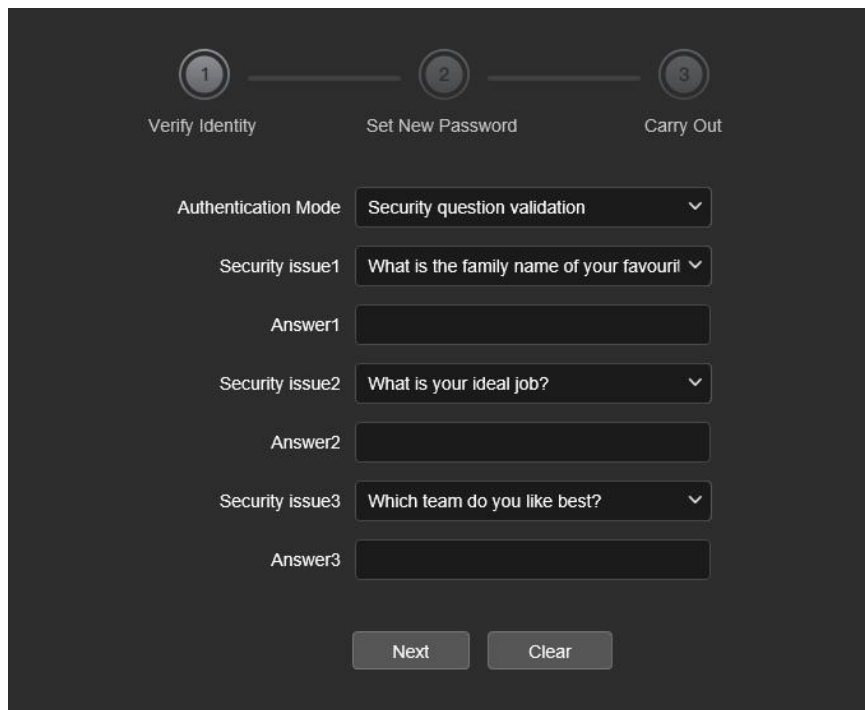
4.2.3 Forget password

When you forget your password, you can reset the password in two ways: security question verification and security key verification.

Security question verification

Step 1: On the login interface, click "Forget".

Step 2: Select the verification method as "Security question validation" (as shown in Figure 4-5 ①), enter the answers to security questions 1, 2, and 3, and click "Next"

Figure 4-5 ①

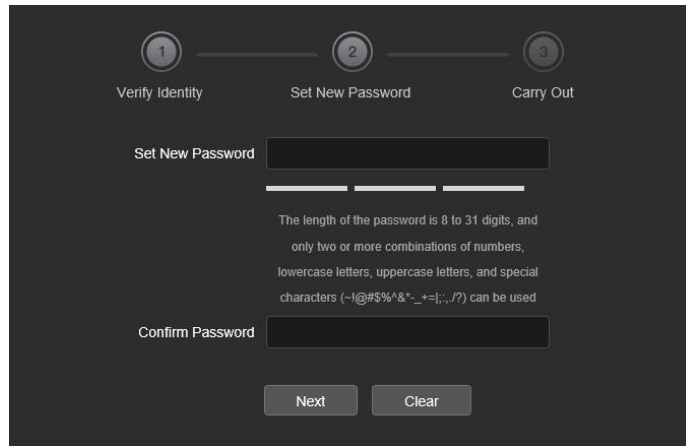**Step 3:** Enter the new password and confirm the password (as shown in Figure 4-5 ②), and click "Next".

Figure 4-5 ②

Step 4: Click "Re-login" to return to the login interface (as shown in Figure 4-5 ③).

Figure 4-5 ③

Security Key verification

Step 1: On the login interface, click "Forget".

Step 2: Select the verification method as "Security Key Verification" (as shown in Figure

4-6 ①), and click "Import" to import the key file exported when the password is modified;

Figure 4-6 ①

Step 3: Enter the new password and confirm the password (as shown in Figure 4-6 ②),

and click "Next".

Figure 4-6 ②

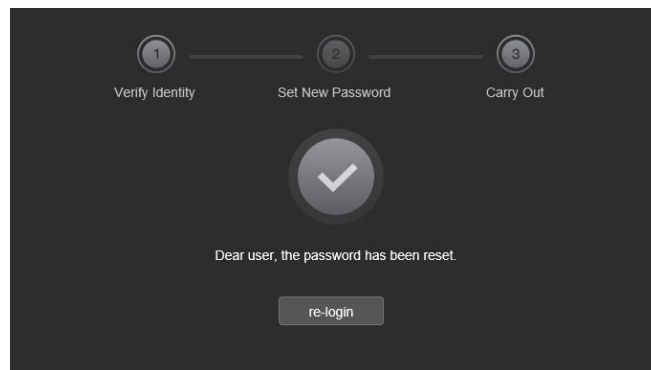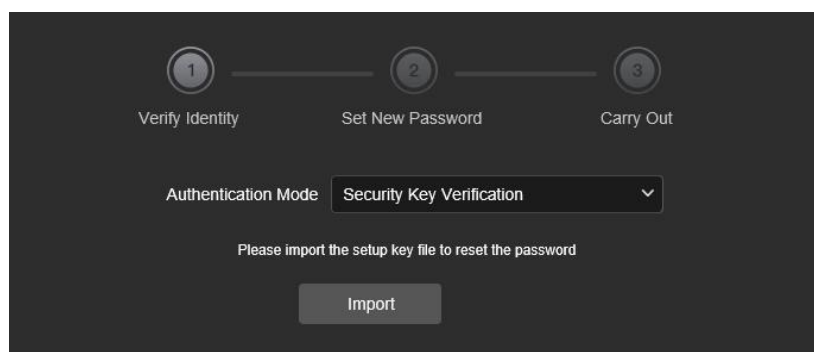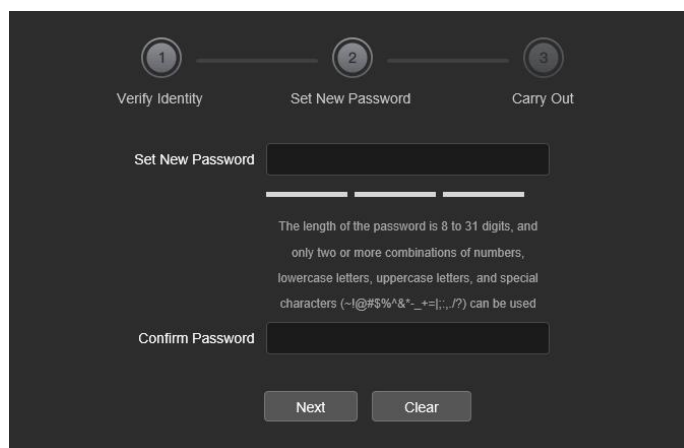**Step 4:** Click "Re-login" to return to the login interface (as shown in Figure 4-6 ③).
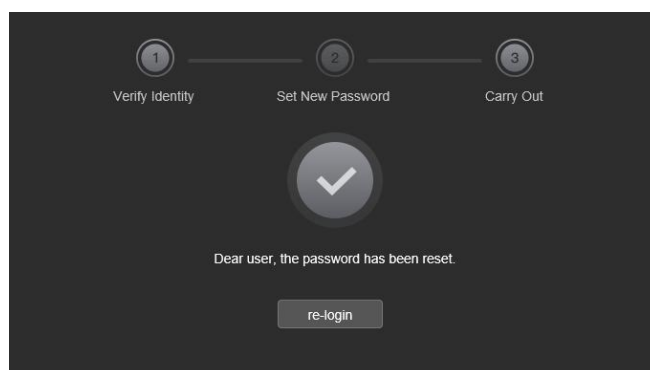

Figure 4-6 ③

 NOTE

● When selecting "Security question validation", enter the correct answers to 2 questions to enter the "Set New Password" interface and proceed to the next step.
● When setting a new password, you must set at least 8 digits and contain both letters and numbers to set it successfully.
● An IPC key file can be used multiple times to reset the password if you forget 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 IE browser or 360 browser, you need to download and install the controls after login.
- The plugin of smart IP camera is "LsIPCPlugin".

Open Internet Explorer and log in to IPC to enter the preview interface, as shown in Figure 4-7.
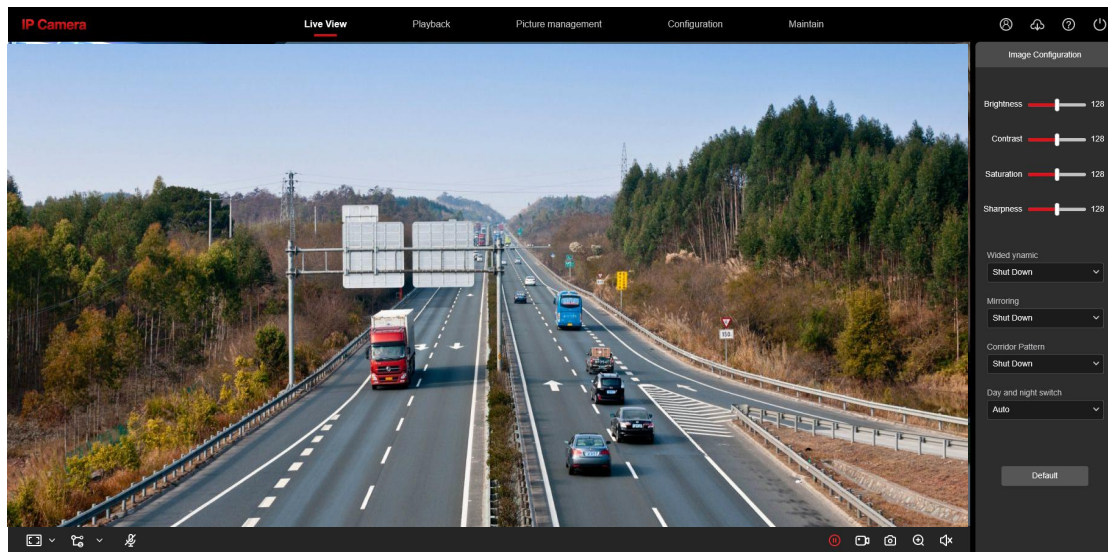
Figure 4-7

Click "Download plugin" in the upper right corner, select the control storage path, click "Download", close the IE browser, click "Open", select "English" → "OK" → "Next" →

"Next" → "Next" → "Install" → "Finish" in Figure 4-8 (①、②、③、④、⑤、⑥) to
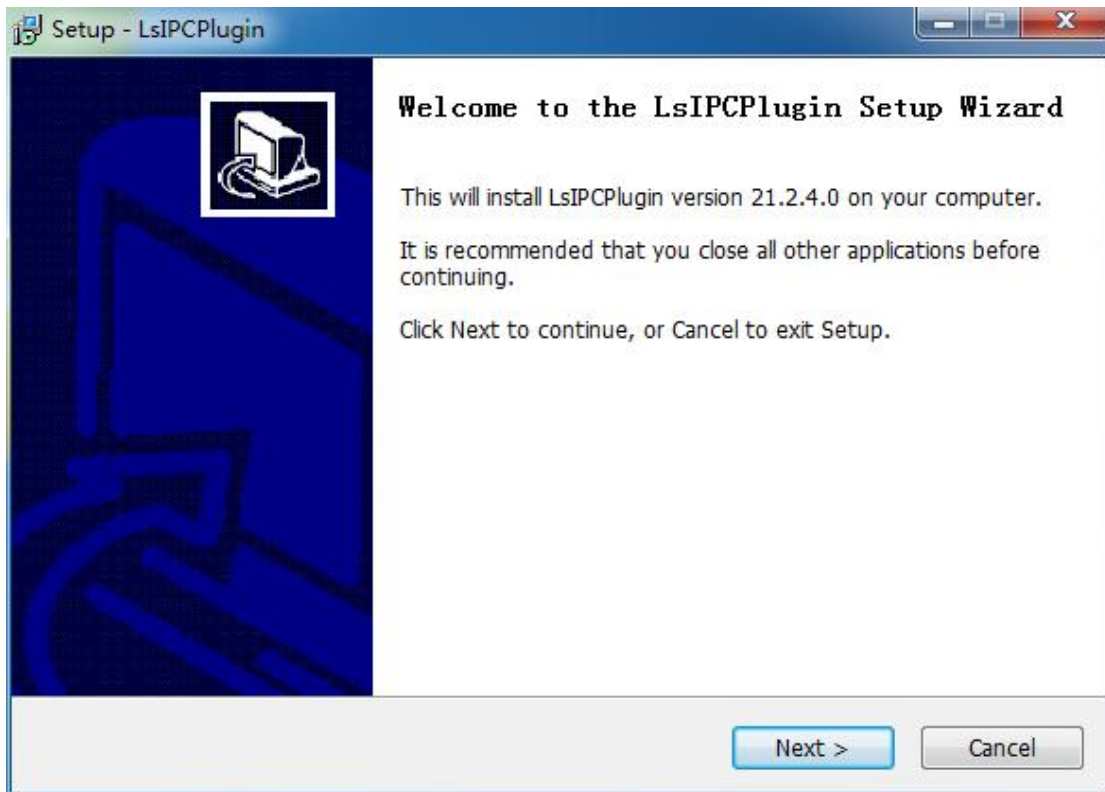
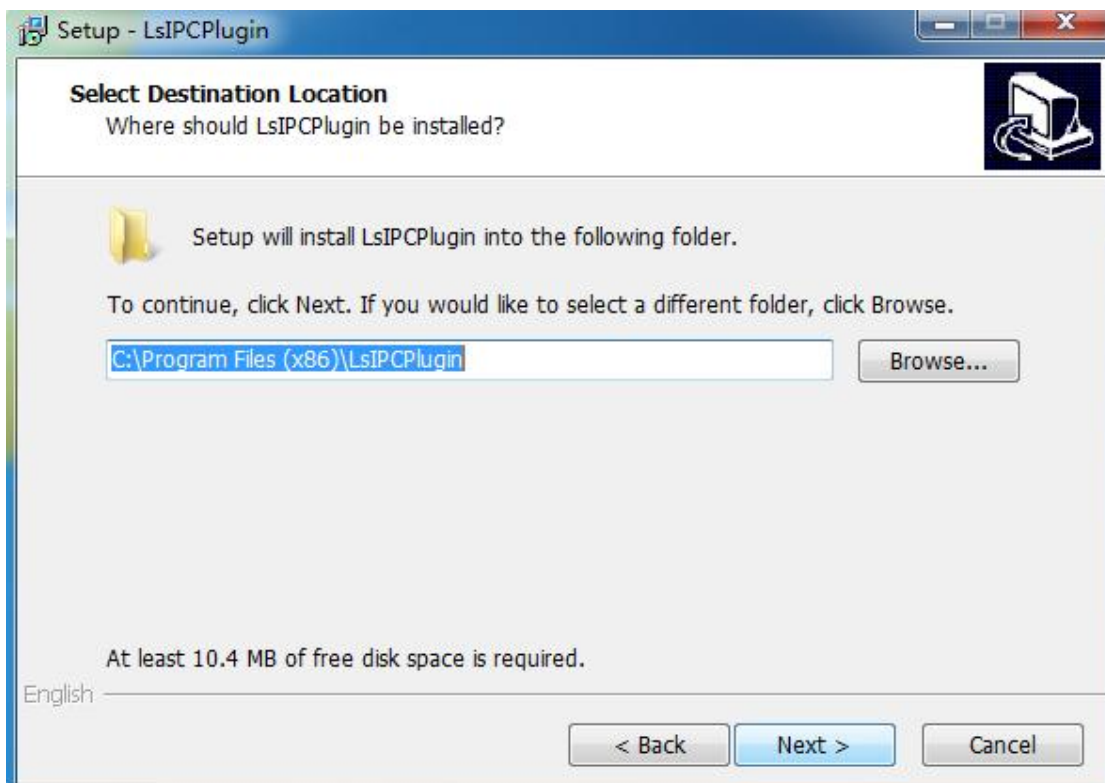complete the installation:

Figure 4-8 ①

Figure 4-3 ②
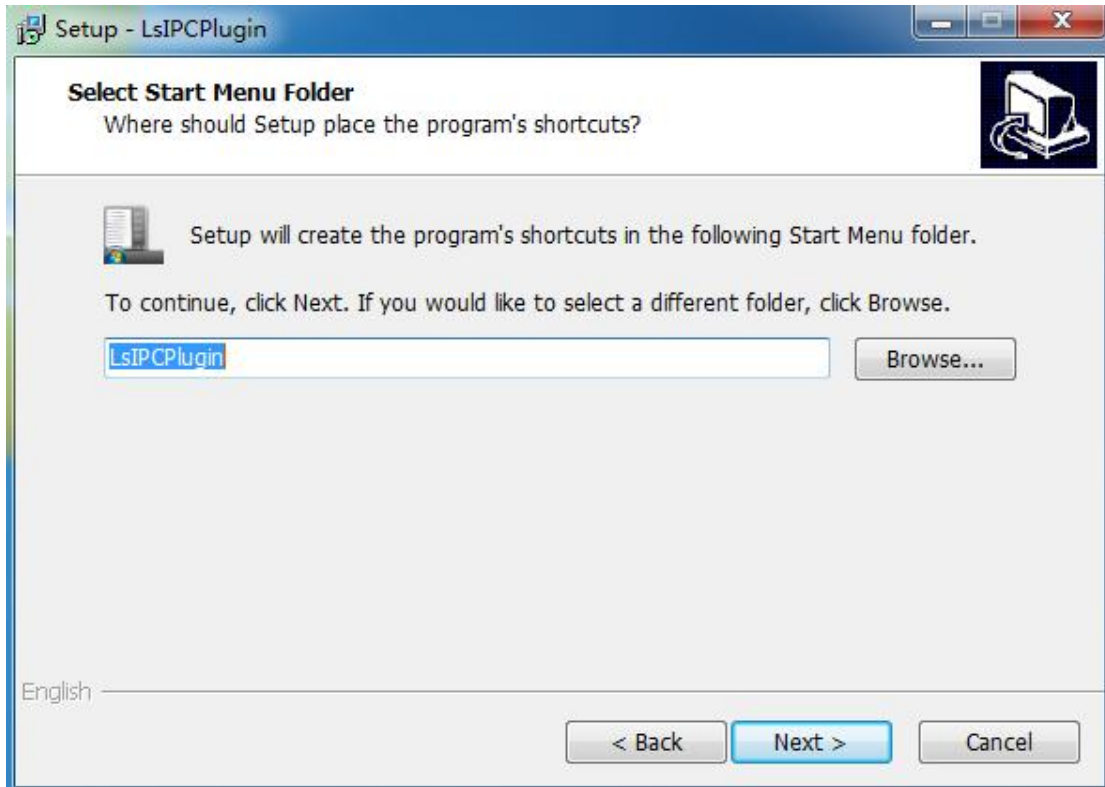
Figure 4-3 ③
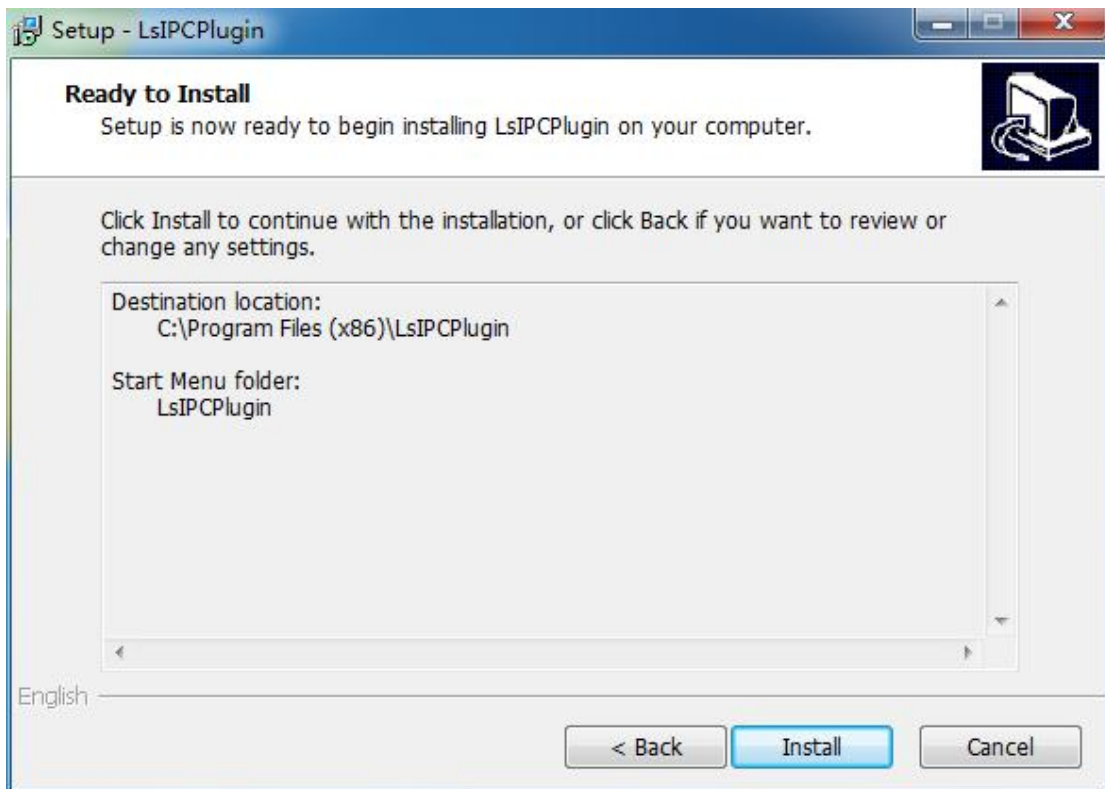
Figure 4-3 ④
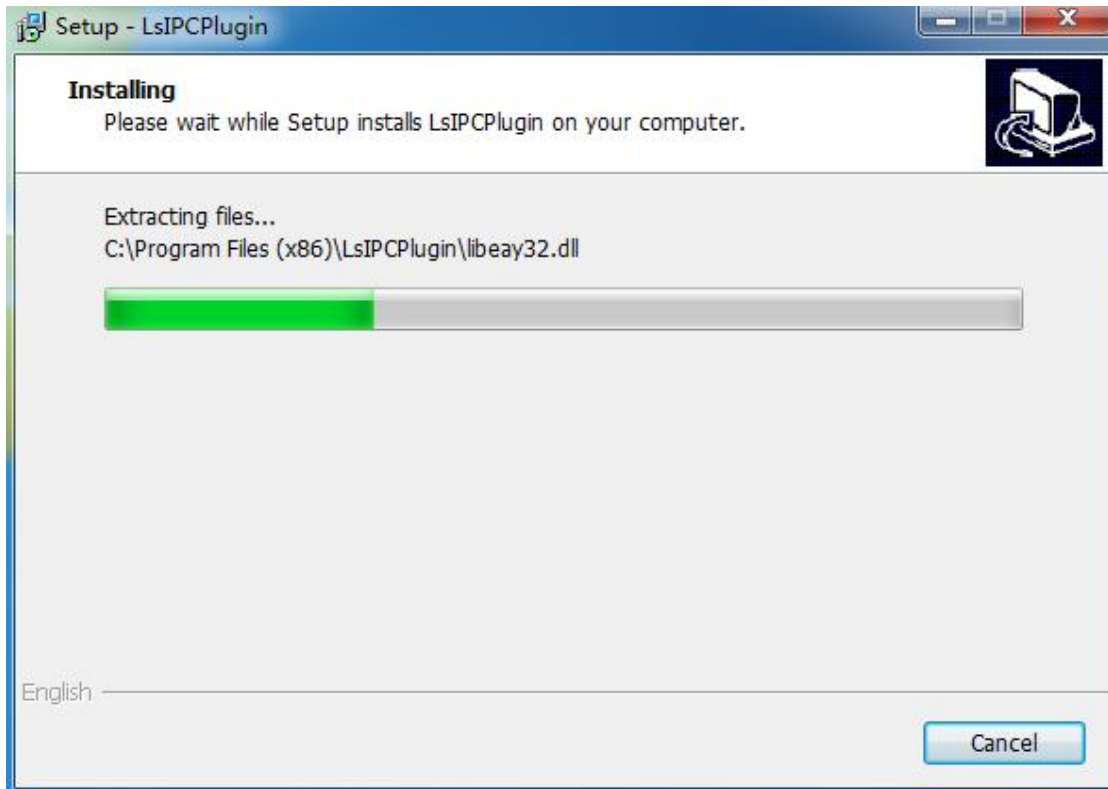
Figure 4-3 ⑤

Figure 4-3 ⑥

⚠️**Notice**
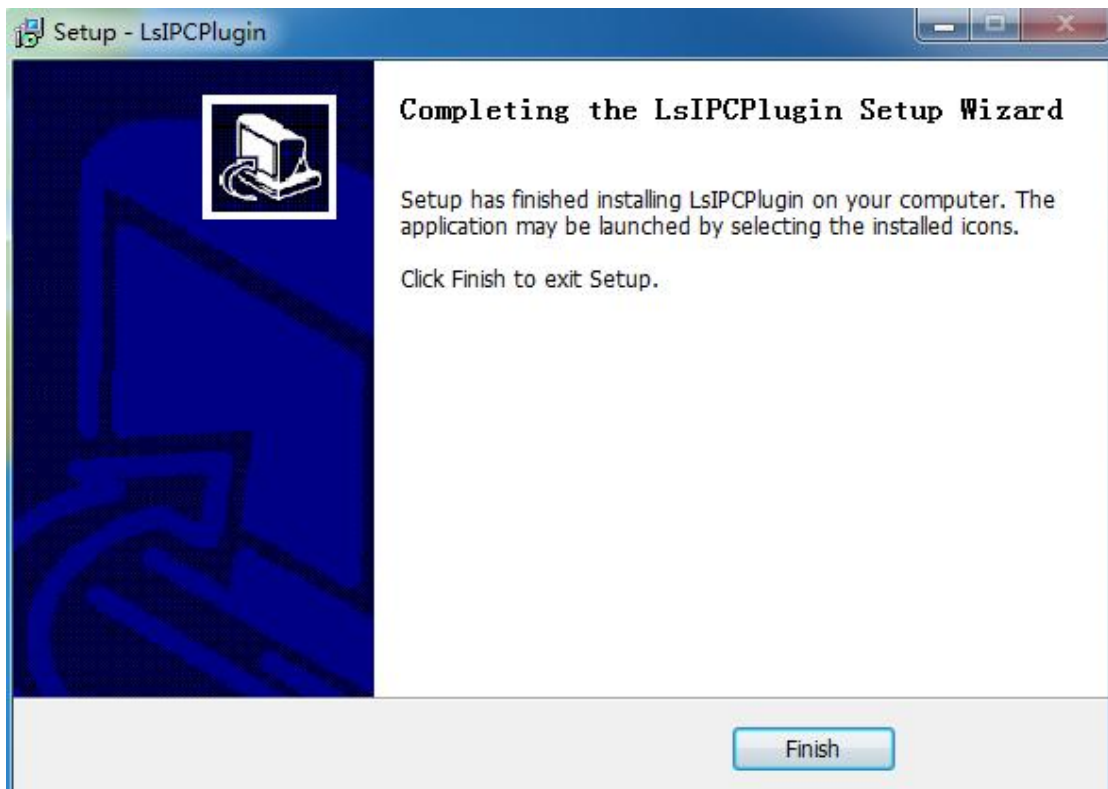
If the system prompt "installation failure", please uncheck the "cancel protection mode" in the setting safety of "Internet options" and enter the "custom level" ActiveX control Settings as show in Figure 4-4, and reinstall LsIPCPlugin after save settings.
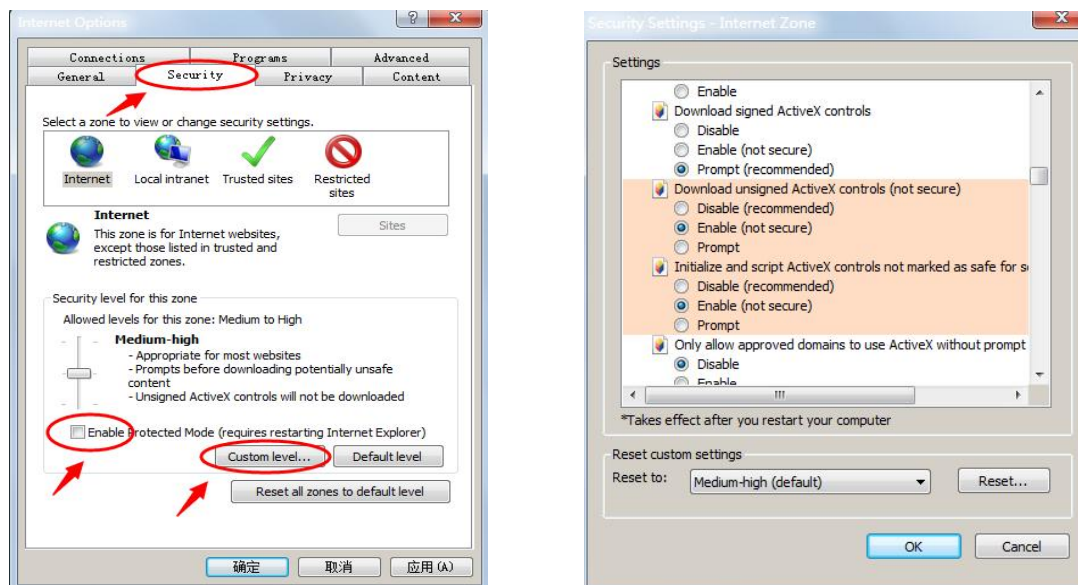
Figure 4-9

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 4-10:
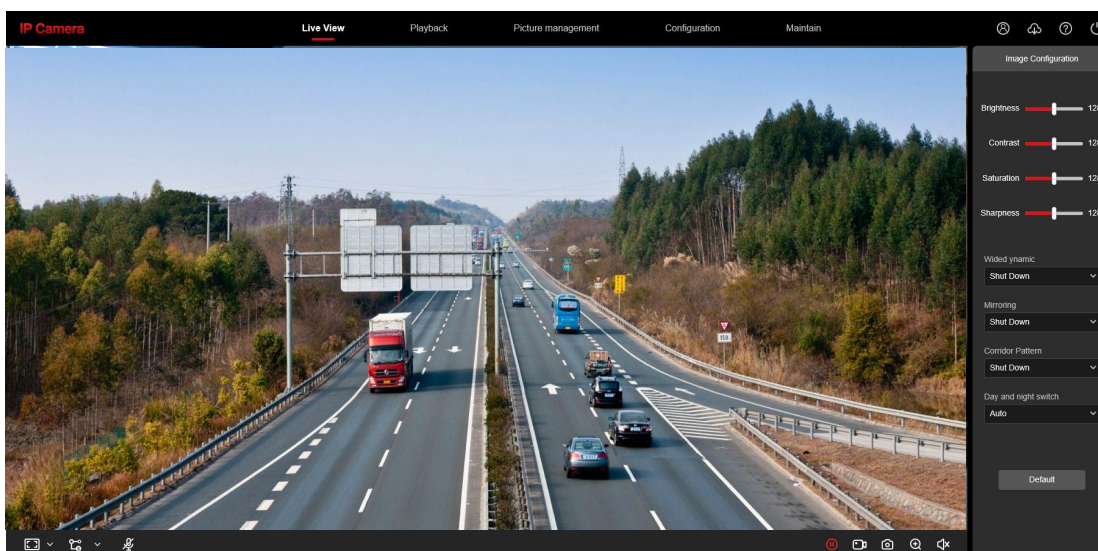
Figure 4-10

【Live View】 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**】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.

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

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

NOTE

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

Chapter 5 Live preview

5.1 Live preview

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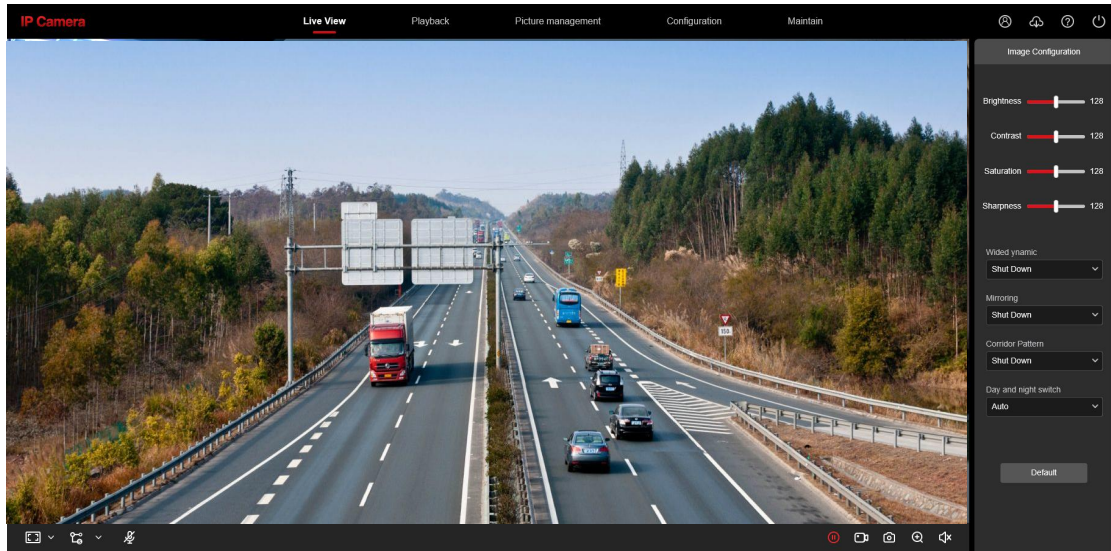
Figure 5-1

【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
4:3	The window size is 4:3.
1:1	The preview screen is displayed in its original size.
16:9	The window size is 16:9.
⟦ ⟧	Self-adaptive window size.
⟲M ⟲S ⟲3	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

Table 5-1

Chapter 6 Playback

In the main interface, click "**Playback**" 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, External Alarm, Vehicle Detection, Area Intrusion,Line Cross Detection,Loiter Detection,Personnel Gathering), click "**Search**" 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.

【Play/Stop】After searching for the video, click "▶" to start playing the video. At this time, the button becomes "⏸" 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.

【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. You can also adjust the volume by dragging the volume.

【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:
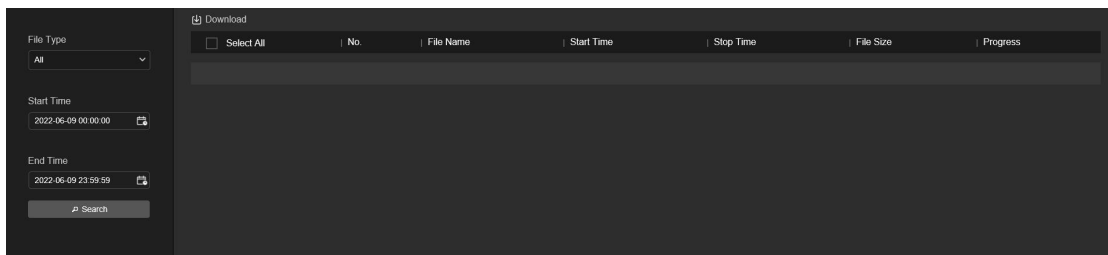
Figure 6-2

【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" → "Save", set the download file storage path, the file starts to download, and wait for the download progress to complete.

👉 **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.
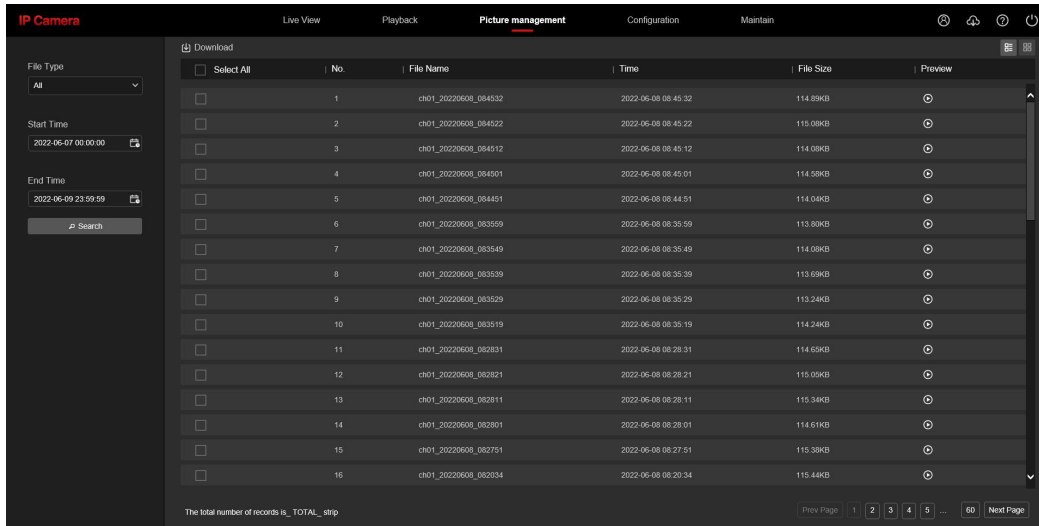
Figure 7-1

【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 Local Configuration

In the main interface, click "Configuration → Local Configuration" 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 8-1.
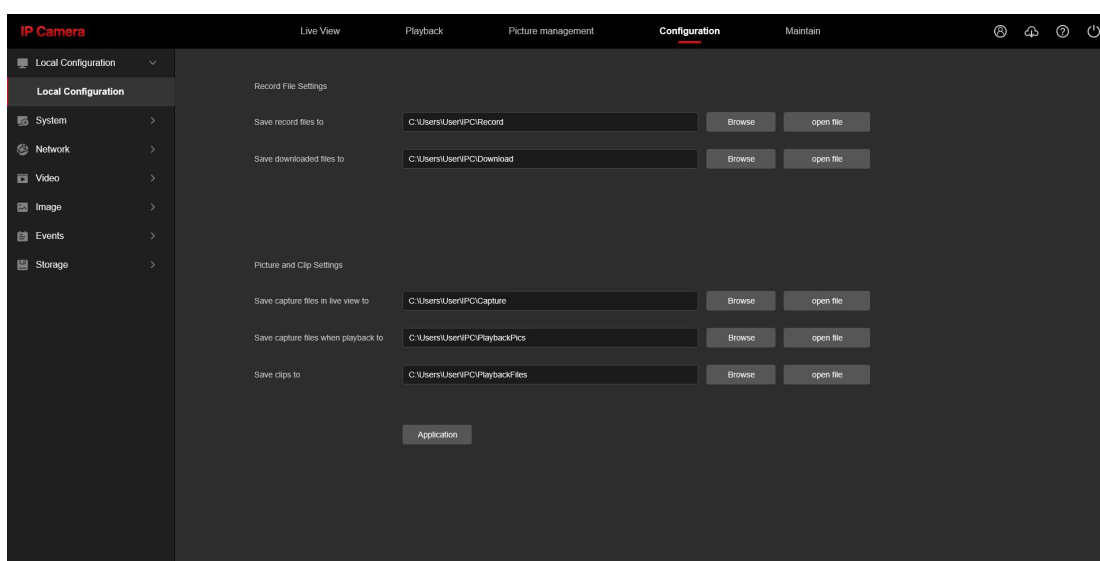
Figure 8-1

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

【Record Path of Live View】 Set the saving path for the manually recorded video files.

【Download Path of Playback】 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.

【Snapshot Path of Live View】 Set the saving path of the manually captured pictures in live view mode.

【Snapshot Path of Playback】 Set the saving path of the captured pictures in playback mode.

【Record Path of Playback】 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 cannot support local configuration.

8.2 System

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

8.2.1 System Configuration

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

① **Time Setting**

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 8-2.
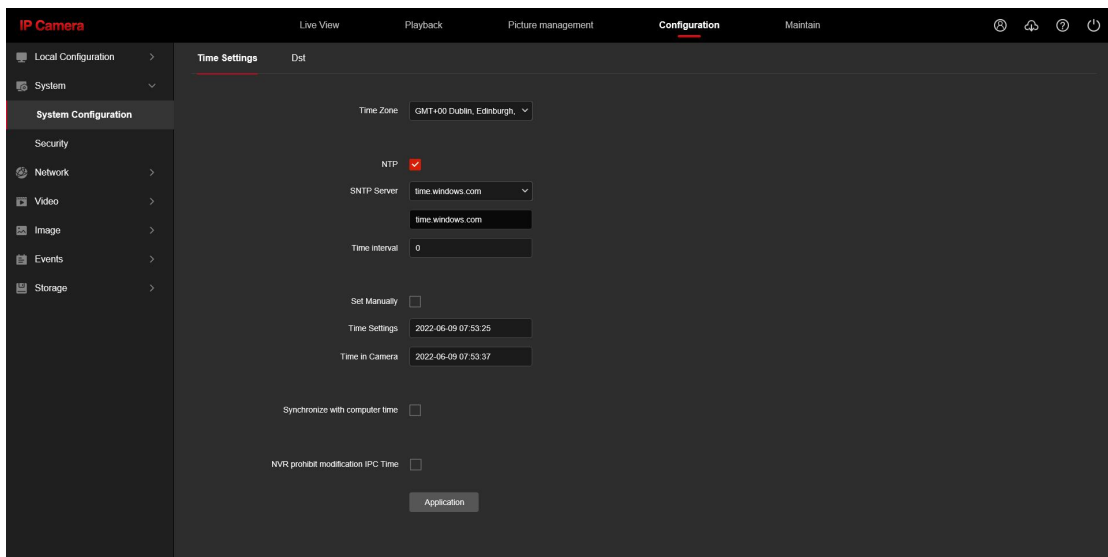
Figure 8-2

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

【Time in Camera】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 "Application" after completing the settings.

【SNTP Sever】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 "Customize".

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

【Set Manually】Setting the IPC 's date and time manually. Click on the "Application" after completing the settings.
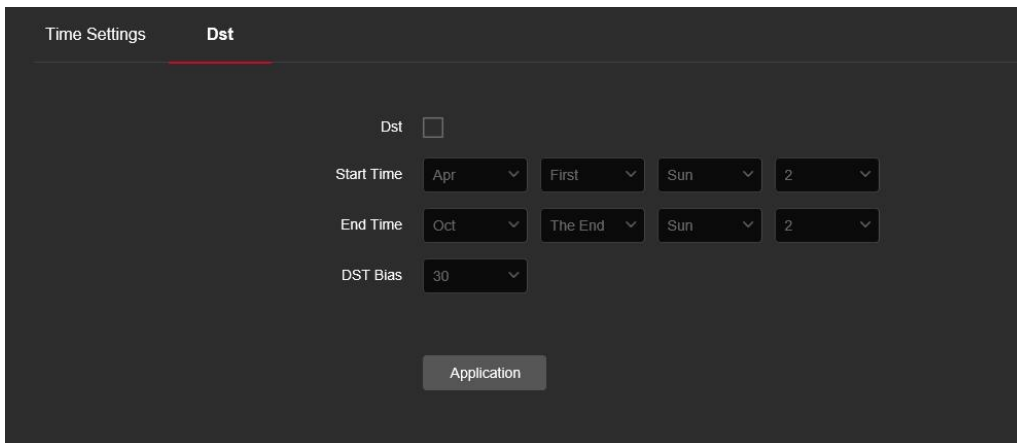
【Synchronize with computer time】The IPC will synchronize with the computer time and

date that your connect currently. Click on the "Application" after completing the settings. 【NVR prohibit modification IPC time】The IPC time will be not affected by the backend storage devices (such as NVR and XVR, etc.) after check this option. The IPC＇s time will be running according to the user 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.
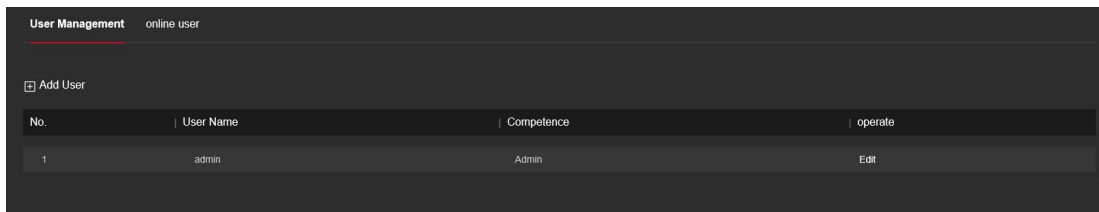
Figure 8-3

8.2.2 Security

In the main interface, click "Configuration → System → Security" to enter the user management settings interface, where you can add, edit, delete the user, you can also query the current user information. The current user for the administrator "admin", the user can actually need other users; you can create up to 10 users, as shown in Figure 8-4.
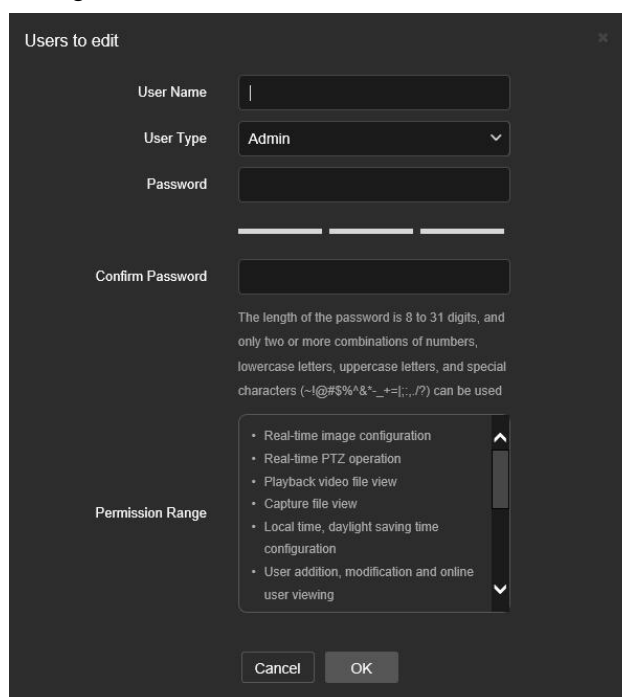
Figure 8-4

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 8-5.

Figure 8-5

![CAUTIONS symbol] **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 symbol] **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).
  Viewer -- only preview permission.
- When setting the IP camera password, the password length is 8-31 characters and must contain numbers and letters.

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 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.

② **First modified (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 the old password(Default password is "admin") and enter the new password in the Password and Confirm Password fields.
Step 3: Select security questions 1, 2, 3 and set the corresponding answers, and click "key export" to export the key file to your computer.
Step 4: Click "OK" to complete the password modification.

③ **Modify the (admin user) password again**

Step 1: In the user list, click the "Edit" button after the admin user to enter the user interface.
Step 2: Enter the old password, and 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 the initial password "admin", each time you log in, you will be prompted to change the password. You can select "Modify after 60 mins". After 60 minutes, the interface will automatically pop up the password modification interface.
- When modifying the administrator password, after setting the security question, click "Browse" to select the path, and click "Export" to export the key file, so that the password can be reset when the password is 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 importing the key.
- 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.

④ **Edit the User (new user)**

Step 1: In the user list, select the user to be modified, and click "Edit" 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.

⑤ **Delete Users**

Step 1: Click to select the user you want to delete and click "Delete".
Step 2: Click "OK" on the pop-up dialogue box to delete the user.

8.3 Network

8.3.1 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 Setup → TCP / IP" to enter the TCP / IP interface, as shown in Figure 8-6 ①.
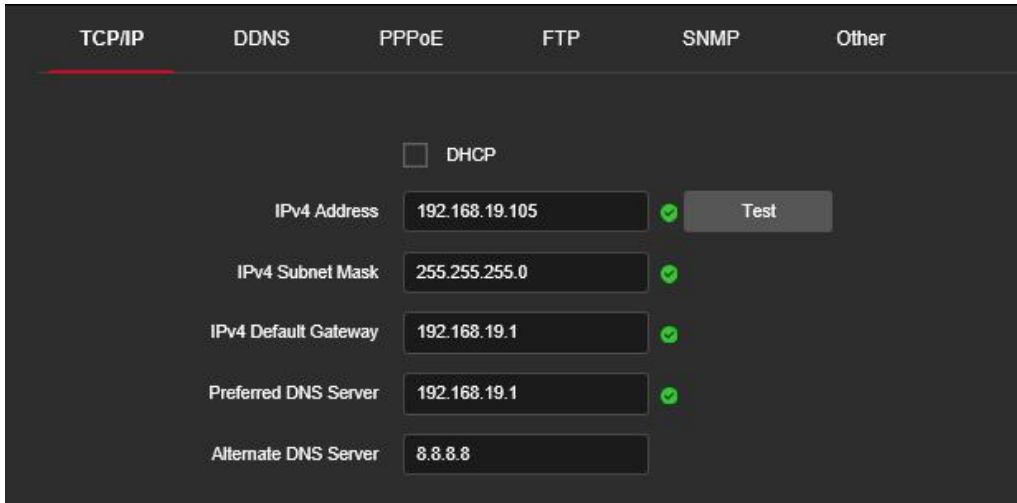
Figure 8-6 ①

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 "Application" to save the configuration.

Port

In the main interface, click "Configuration → Network → Basic Setup → 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), BITVISION port(default is 6000), the protocol port has the ONVIF port (default is 8999). As shown in Figure 8-6 ②.
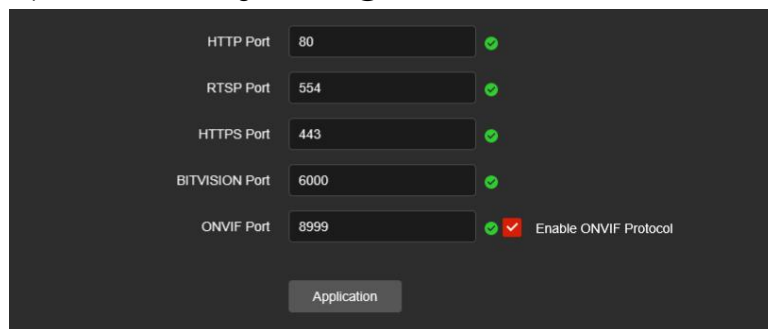
Figure 8-6 ②

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

【ONVIF Port】When the IPC access to ONVIF agreement with the back-end equipment, the need to enable ONVIF protocol; the ONVIF protocol is enabled.

 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 BITVISION port.

② 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 configuration → DDNS" to enter the DDNS function settings interface, as shown in Figure 8-7:

Figure 8-7

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

Steps 3: Click "Application" 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.

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

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

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

【Confirm Password】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.

③ 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 configuration → PPPoE" to enter PPPoE to set the interface, as shown in Figure 8-8.

Figure 8-8

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.

 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.

④ **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.

 NOTE

● To create an FTP user, you need to set the FTP folder write permission, otherwise the image will not be uploaded successfully.

The steps to configure FTP are as follows:

Step 1: In the main interface, click "Configuration → Network → Basic configuration → FTP" to enter the FTP server settings interface, as shown in Figure 8-9.

Figure 8-9

Step 2: Enter the server address, port, user name, password, confirm the password, storage first level directory, storage secondary directory, check "Auto Cover", and select the upload FTP server image format JPEG.

Step 3: Click "Application" to save the configuration.
Step 4: Click "Test" to confirm whether the network connection and FTP configuration are correct.

☞ **NOTE**

● If the test fails, please recheck the network or FTP configuration.

【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 Password】Fill in the FTP server password.
【Storage first level directory】Automatically create a level-1 directory under the FTP storage path.
【Storage secondary directory】Create a secondary directory under the FTP primary directory.

⑤ **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 community name" and "Write community name", 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 configuration → SNMP" to enter the SNMP configuration interface, as shown in Figure 8-10 below:
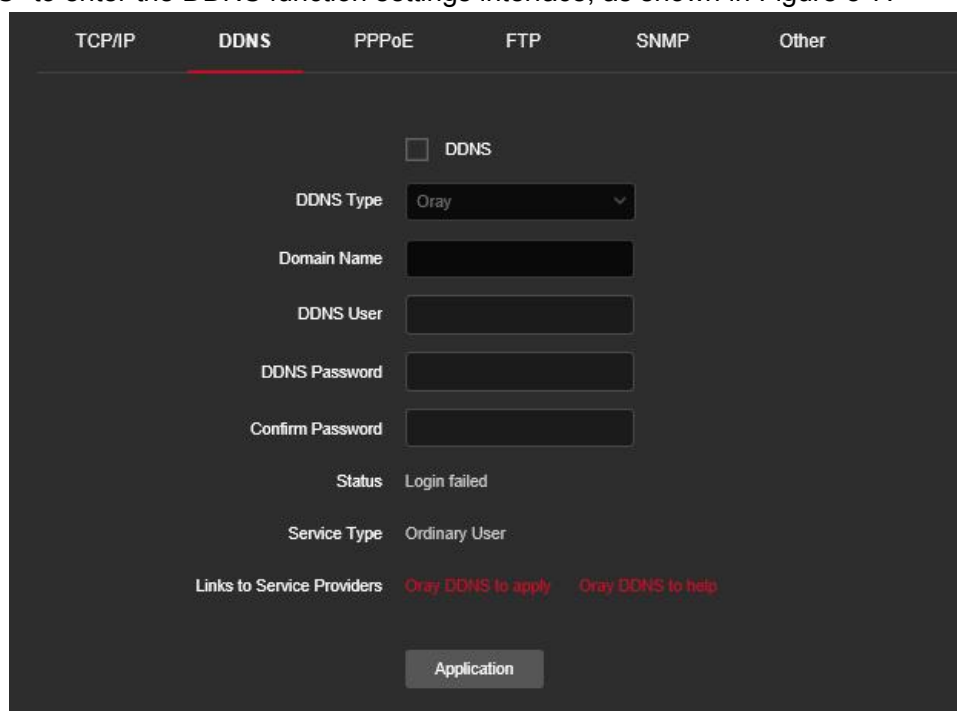After selecting "SNMP" to enable the SNMP function of the device, select the SNMP version, such as V3, you can set the parameter information of V3 ("SNMP Port", "Read community name", "Write community name", "Trap Address", etc.), the device can send alarm and abnormal information to the management station, and can receive device information by setting the Trap port. After setting the parameters, click "Application".
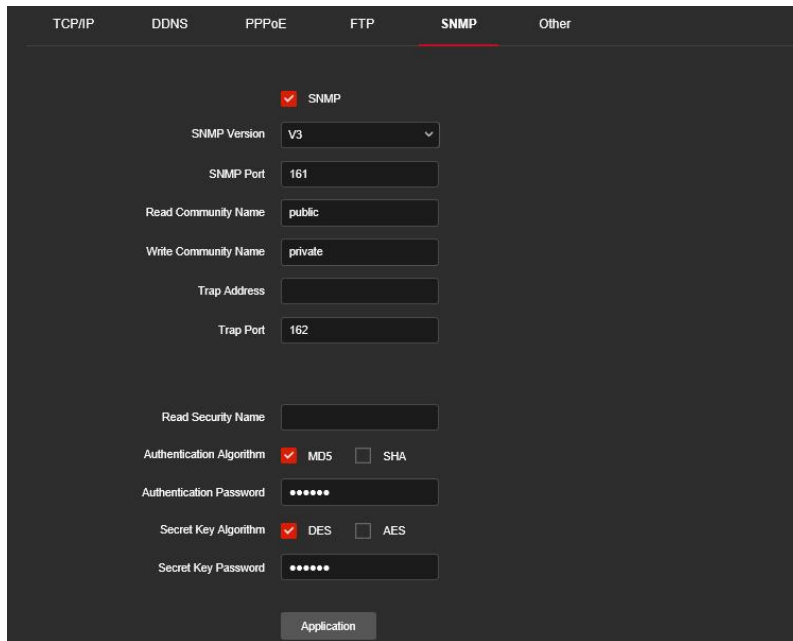
Figure 8-10

⑥ **Other**

In the main interface, click "Configuration →Network → Basic configuration → Other" to enter the Video Password Authentication interface, as shown in Figure 8-11.
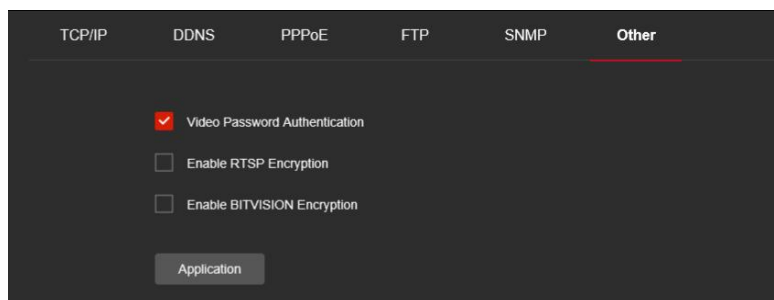
Figure 8-11

【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.

【Enable RTSP Encryption】 When enabled, the RTSP stream of the camera is encrypted.

【Enable BITVISION Encryption】 When enabled, the stream between the camera and the BitVision App is encrypted.

NOTE

● AL platform devices do not support enable BITIVISION encryption .

8.3.2 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.

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.

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 8-12.

Figure 8-12

Step 2: Make sure that the IPC accesses the external network and click "☐" to open P2P.

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

Step 4: Refresh page, the status shows "Connection successful". This indicates that P2P is enabled and can be used normally.

App Client operation example

The following content is introduced by taking the operation of the mobile phone client (BitVision 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 BitVision 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, click "Device manage" , " ➕ " and " Add device" , select "SN Add", enter the device user name, password and verification code after scan the QR code (the verification code printed on the label), click "Add" to set device NOTE and group, click "Done" after add successfully.
Step 4: Live preview

Select "Real time" and " " to enter the device list in the main interface, select the touching pen and the channel to be previewed in the group, you will see the live video after click " Done ".

② IPEYE
In the main interface, click "Configuration →Network → P2P → IPEYE" to enter the IPEYE interface.   After IPEYE is enabled, you can add the device to the IPEYE account

at https://www.ipeye.ru/ View IPC real-time audio / video, as shown in Figure 8-13 ①.

P2P	**IPEYE**
	☐ Enable IPEYE
	Note: IPEYE only supports H264 encoding
	Application
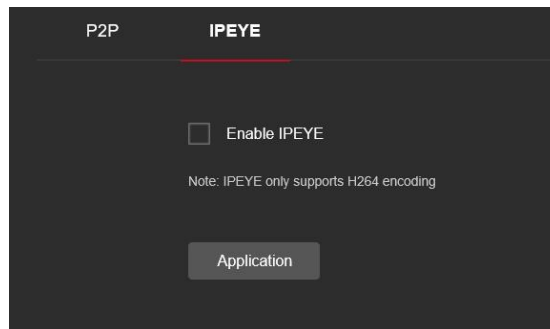
Figure 8-13 ①

The steps to monitor the audio and video in real time at https://www.ipeye.ru/ are as follows:
Step 1: Enter IPEYE interface, enable IPEYE enable, refresh the interface, and the

interface displays IPEYE Client address as shown in Figure 8-13 ②.
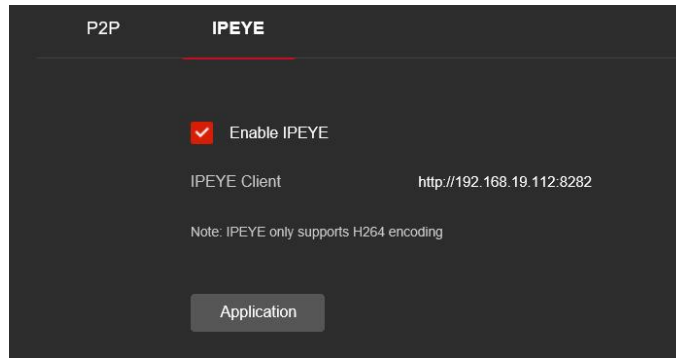
Figure 8-13 ②

Step 2: Log in to IPEYE Client "http://192.168.19.112:8282", enter IPEYE login account & password, IPC user name & password, click "Confirm" to add the device, as shown in Figure 8-14 ③.

Figure 8-13 ③

Step 3: Log in to "https://www.ipeye.ru/" and enter the IPEYE device list to view the newly added device name as "cloud_xxxxx". Click "Play" to view the device real-time monitoring video. The list of IPEYE devices is shown in Figure 8-13 ④.
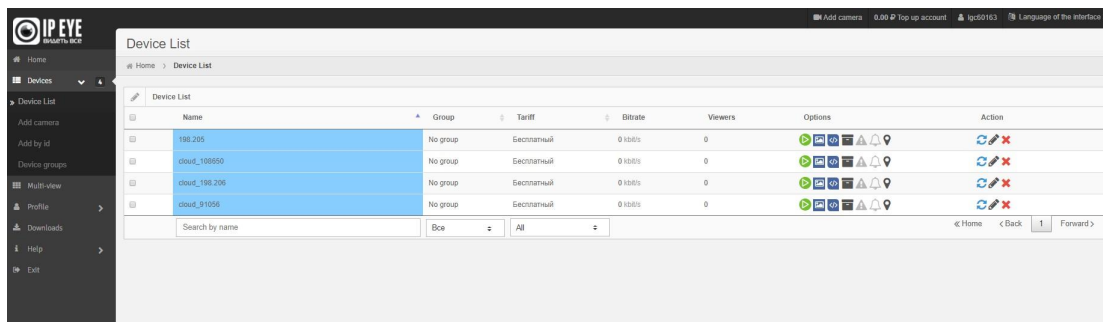
Figure 8-13 ④

NOTE：

● Some cameras do not support the IPEYE function. The specific interface is subject to the actual product.

8.3.3 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 8-14.
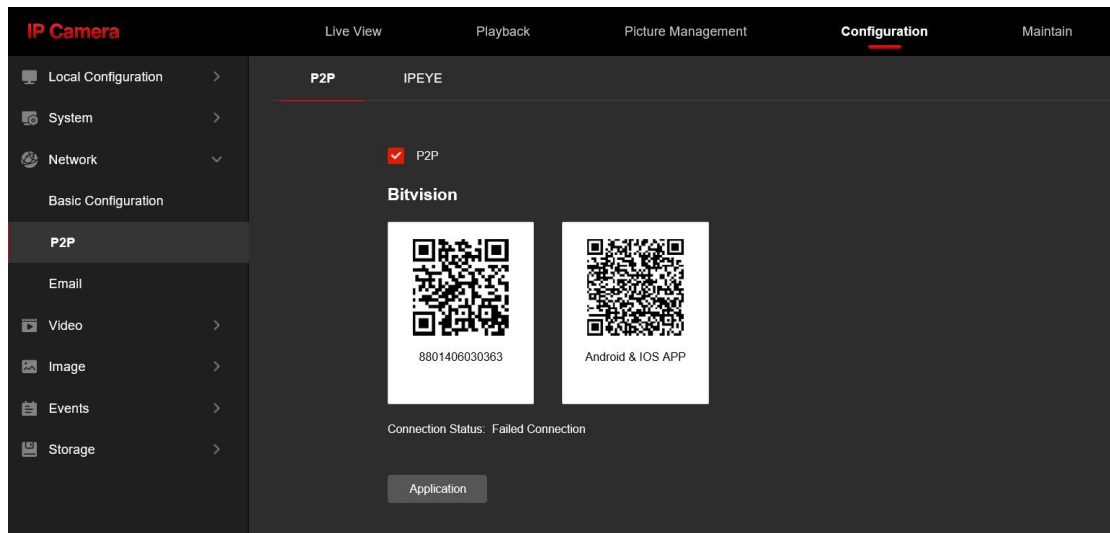
Figure 8-14

Step 2: Configure Sender, SMTP Server, Port, User Name, Password, and Receiver.

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

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

NOTE：

Sender

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

【SMTP Server】Fill in your email server address.

【Port】Fill in your email server port.

【Upload Via SMTP】In the drop-down menu, select SMTP file format, JPEG image format, AVI video and message for selection.

【My Server Requires Authentication】When enabled, the server and user are authenticated to ensure that the 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 Password】Fill in the send mailbox password.

Receiver

【Email 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.

8.4 Video

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

8.4.1 Video

In the main interface click "configuration → video → video" into the video configuration interface, where you can set the IPC device name, stream type, encoding and other video parameters, as shown in Figure 8-15.

Figure 8-15

【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.

【Framerate】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.

【Rate Control】　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 1-5s.

【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

- Different IPC, 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.

8.4.2 Audio

In the main interface, click "Configuration → Video → 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 8-16.
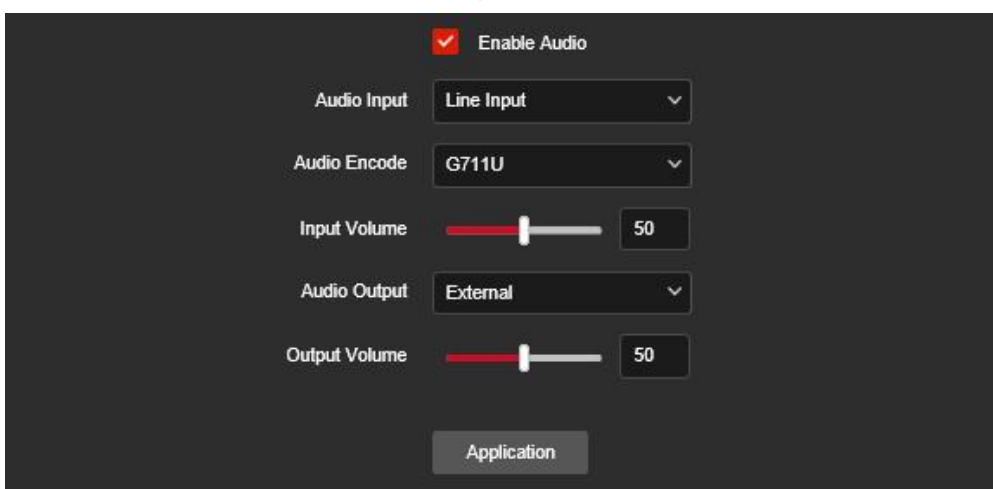
Figure 8-16

【Enable Audio】Turn on / off device audio input.
【Audio Input】Select the audio input method.
【Audio Encode】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.

8.5 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.

8.5.1 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 switch, White Balance, Video Adjustment, Image Enhancement and BackLight Settings, as shown in Figure 8-17.
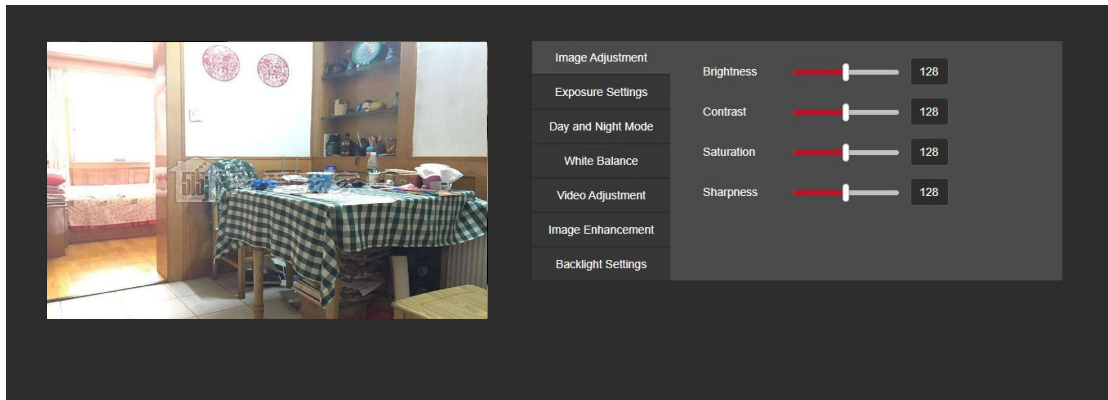
Figure 8-17

【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 8-18.
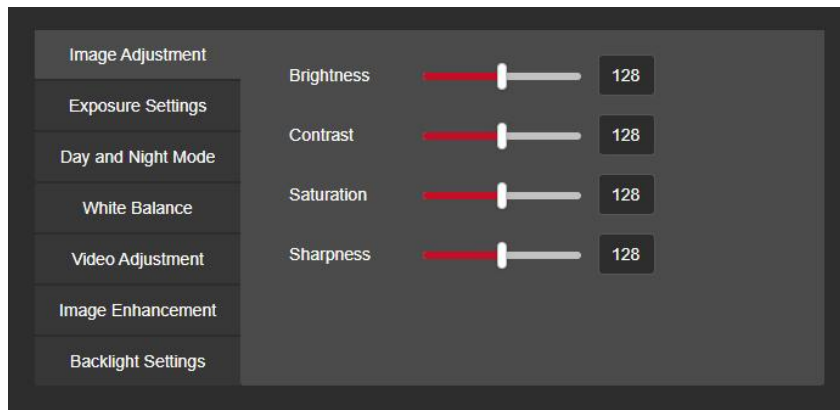
Figure 8-18

【Exposure settings】You can see the Aperture Type of the camera, set the Exposure Time according to actual needs, and automatically save after setting. As shown in Figure 8-19.
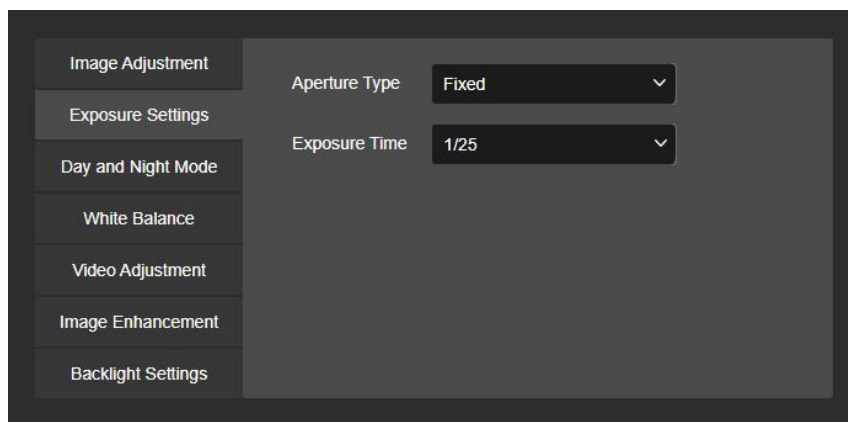
Figure 8-19

【Day and night switch】The fill light mode defaults to automatic, sensitivity is 3, filter time is 3 seconds, light mode is manual, light brightness is 100, as shown in Figure 8-20 ①.

When the fill mode is "Automatic", the device will turn on the fill light according to the actual environment. The user can switch the fill mode to "Daytime ", "Night" and "Time" according to the actual environment of the site, and switch the sensitivity and filter time of the device according to the fill mode.
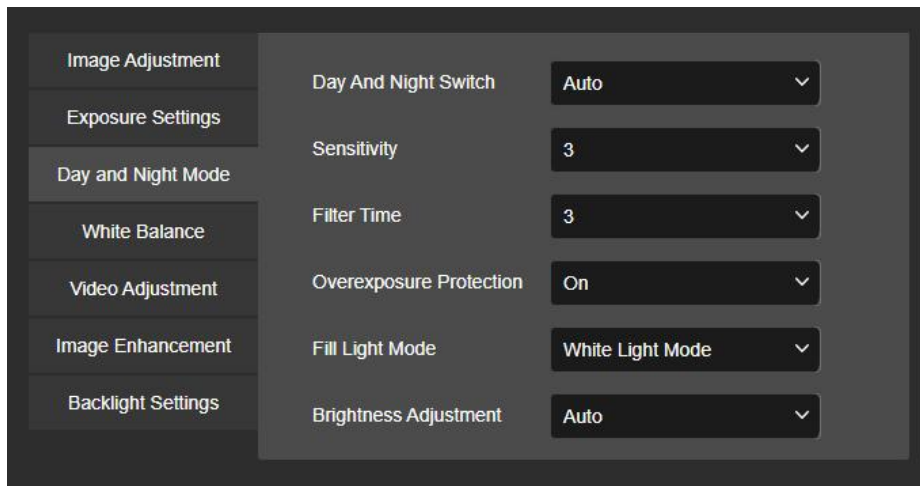
Figure 8-20 ①

- When the fill mode is "Time", 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 8-20 ②.
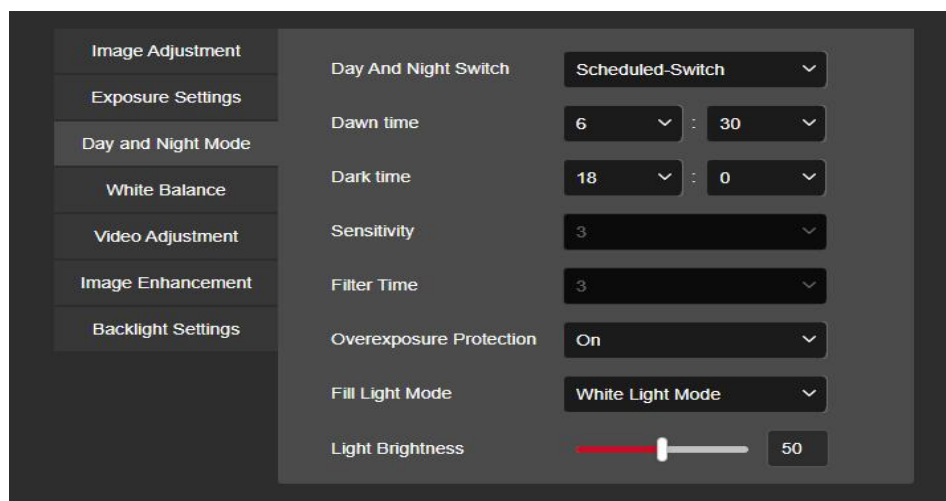
Figure 8-20 ②

- 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.

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

【White balance】Default auto, switchable Manual,there are two types of automatic white balance, which can meet the needs of customers in different scenarios.As shown in Figure 8-21.
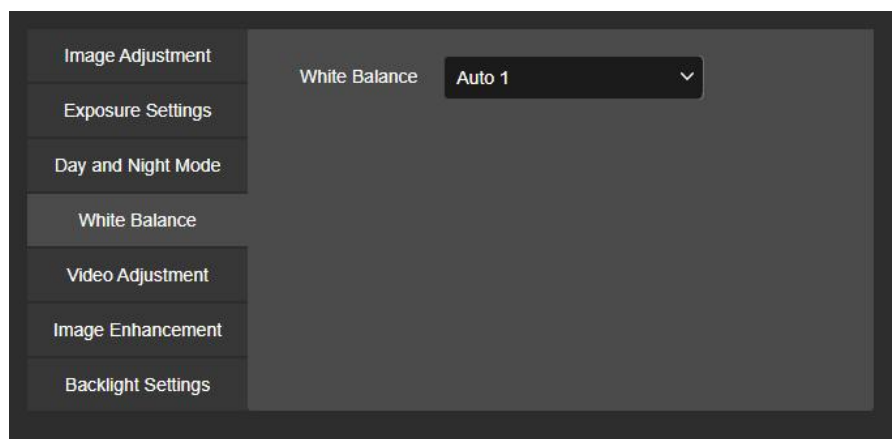
Figure 8-21

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

【Video adjustment】Here you can turn on Mirroring,Corridor Mode,and set the Video Format, as shown in Figure 8-22.
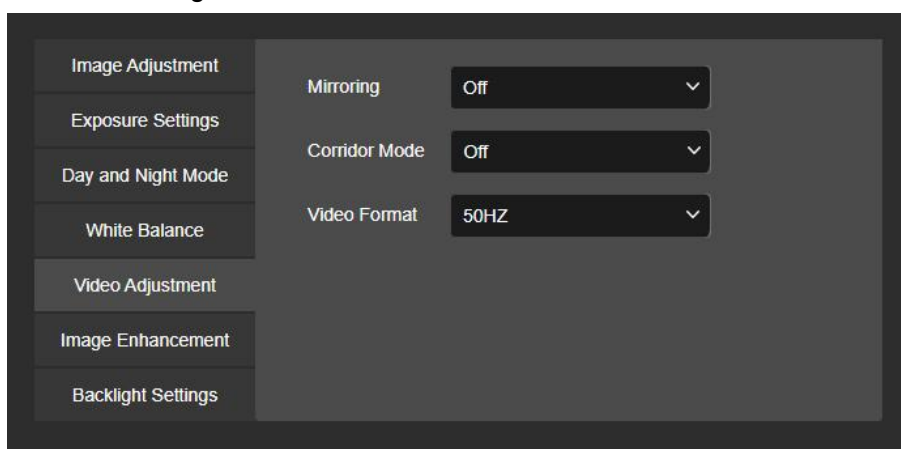
Figure 8-22

Mirroring: 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.

【Image enhancement】Here you can turn on WDR,DNR Mode,Distortion,Defog Mode, as shown in Figure 8-23.
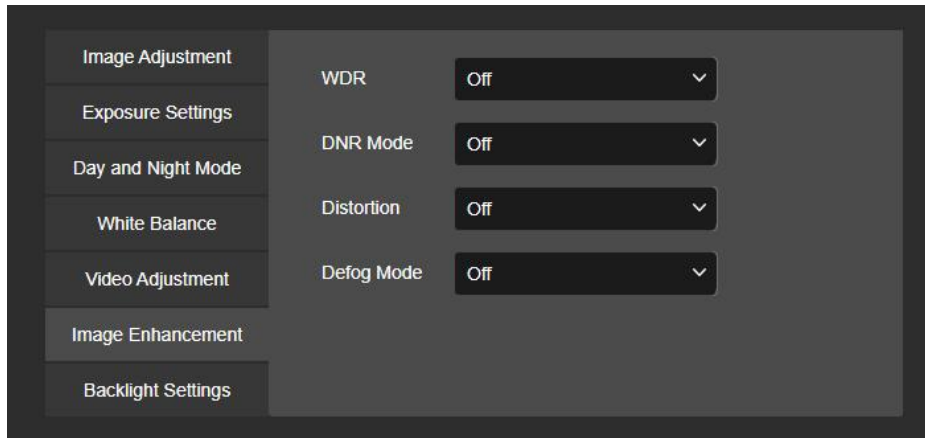
Figure 8-23

WDR：The default is Shut Down, you can switch in the drop-down menu Low, Mid, High.

DNR Mode：The default is Shut Down, you can switch in the drop-down menu Low, Mid, High.

Distortion：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 8-24.
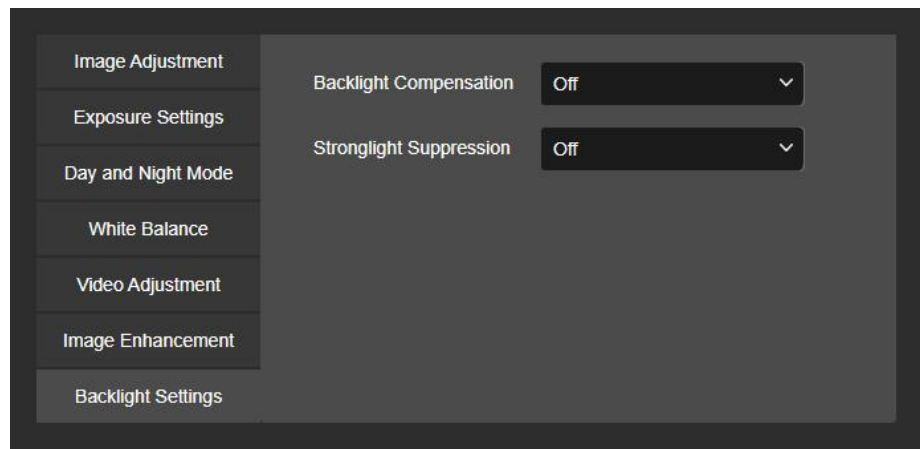
Figure 8-24

 NOTE

- The camera image interface only displays the device support functions. The specific interface is subject to the actual product.
- Wide dynamic, backlight compensation, and strong light suppression are mutually exclusive. Turning on one of these functions will automatically turn off the other two functions.

8.5.2 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 8-25.
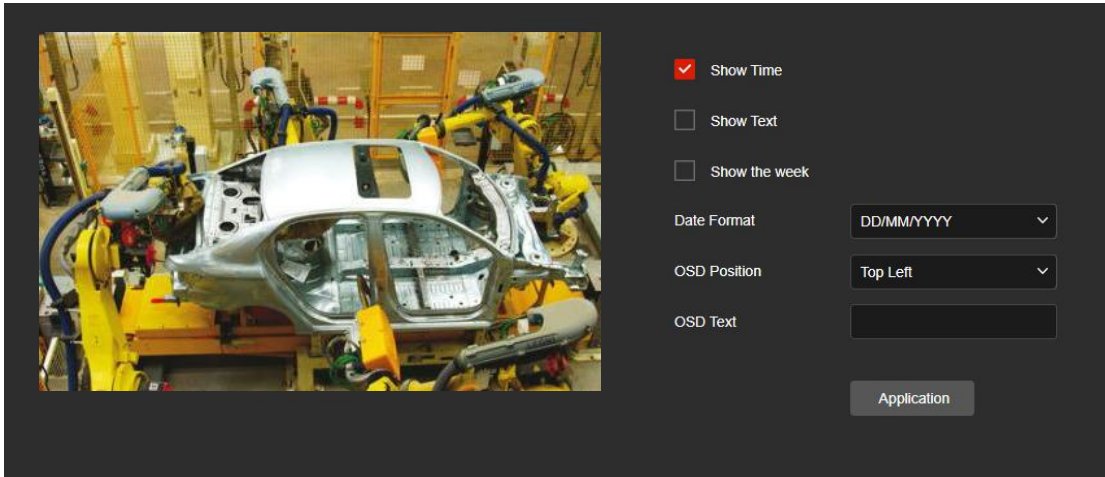
Figure 8-25

【Time】Turn on / off the preview interface time display.

【Text】Turn on / off the preview interface OSD text display.

【Show the 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】Set the preview interface to display the time or OSD text position, the default is the Top_Left, you can switch the Bottom_Left.

【OSD Text】Enter the preview interface to display text information, such as hall elevator, hall door and other equipment location information.

8.6 Events

In the main interface, click "Configuration → Events" to enter the event configuration interface,including common events and Smart events.

8.6.1 Ordinary Event

In the Ordinary event interface, you can set the device's Motion Detection, Privacy Mask, Video Tampering, Alarm Input, Alarm Output, Exception, Audible alarm output, ROI, and other events.

① **Motion Detection**

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 → Events → Ordinary Events →Motion Detection" to enter the motion detection settings interface, as shown in Figure 8-26.

Figure 8-26

Step 2: Click "Enable" or "Detect human movement only" to turn on the motion detection alarm.

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

【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.

【Sensitivity】The default is 5, can switch the range of 0-10. The larger the value, the

easier the device will trigger an alarm.

Step 4: Set the arming schedule.

As shown in Figure 8-27, 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 fill in the start time and end time, set up and click "Application". If you need to delete the time period, click the "Delete" button and then reset the time period.

-   Method 2: Click the arming time period, two arrows will be displayed at both ends of the time period. Move the adjustment arrow left or right to adjust the arming time.

-   You can set up more than one time period for up to 8 time periods.

-   After the day of deployment time is set, if the other time also need to set the same arming time, click the right side of the timeline "⊟" copy button, in the "copy to" interface check the "Select　All" or a day, then Click "OK".

-   After setting, click "Application" to complete the setting of the arming time.

Figure 8-27

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(Upload Via SMTP, Upload Via FTP, Upload Via Cloud, Flash Warning,Sound Alarm) and linkage alarm output(IO Output), as shown in Figure 8-28.

Figure 8-28

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

【Upload Via 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.

【Flash 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 **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 → Event → Ordinary Events→ Privacy Mask" to enter the privacy mask settings interface. As shown in Figure 8-29.
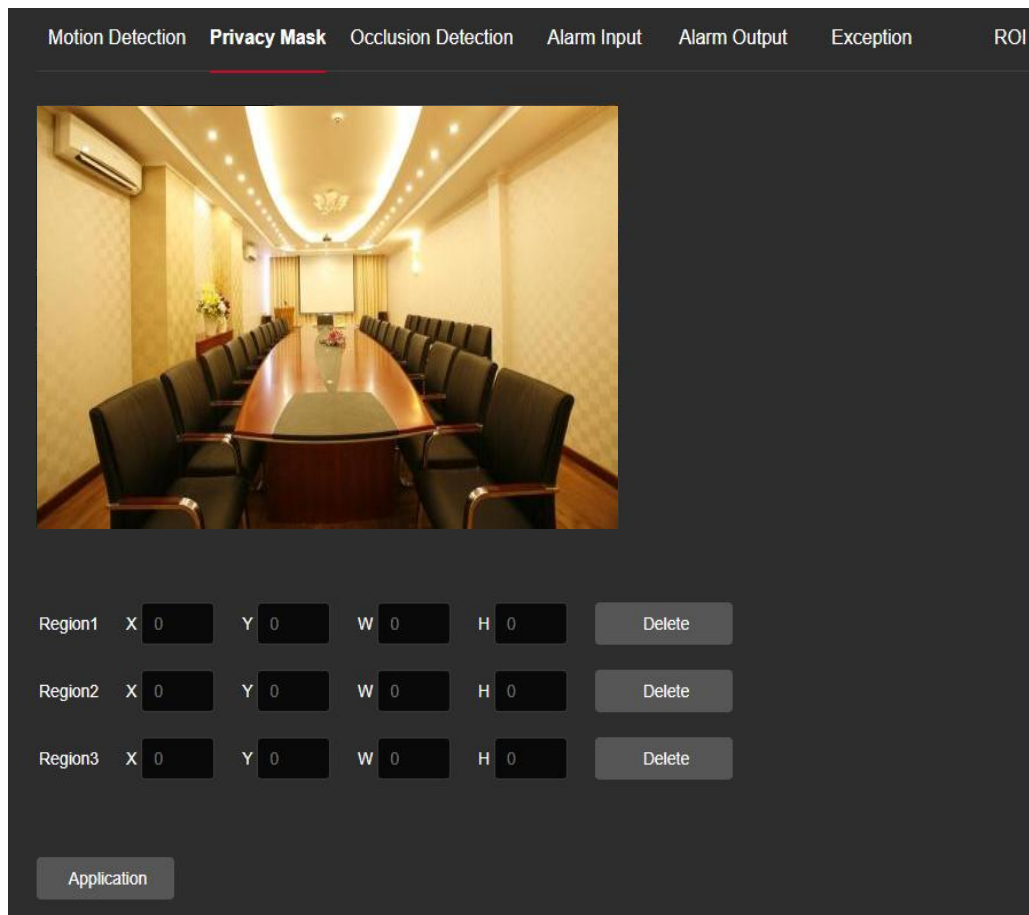
Figure 8-29

Here you can choose up to 3 occlusion areas. Hold down the left mouse button and drag to select the area in the area. Region 1、Region 2、Region 3 bellow will show the corresponding coordinates, width, and height of the region .If you want to delete a region, click on the corresponding "Delete" button. Click on the "Application" after completing the setting.

③ **Occlision Detection**

The occlusion 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 occlusion alarm is generated, the occlusion alarm 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 → Events → Ordinary Events→ Occlision Detection" to enter the video tampering settings interface, as shown in Figure 8-30.
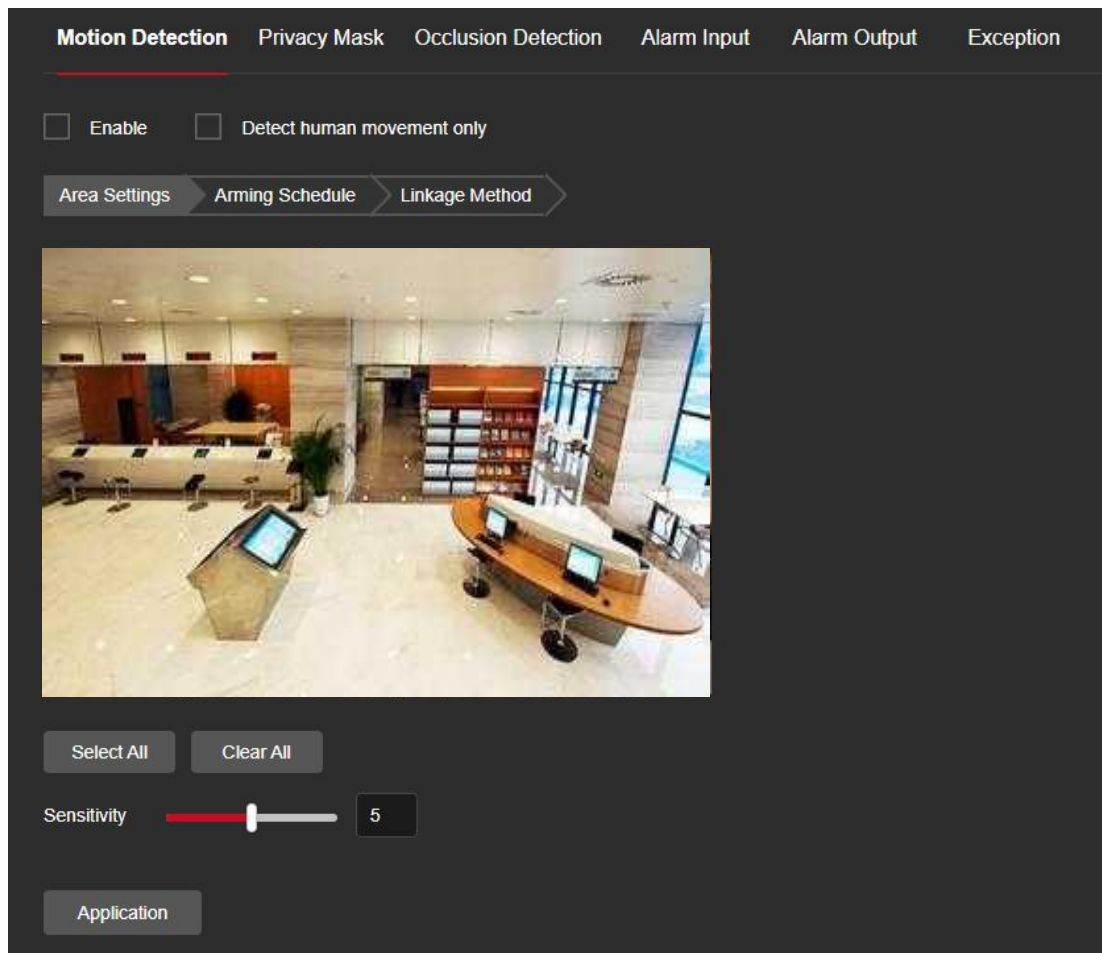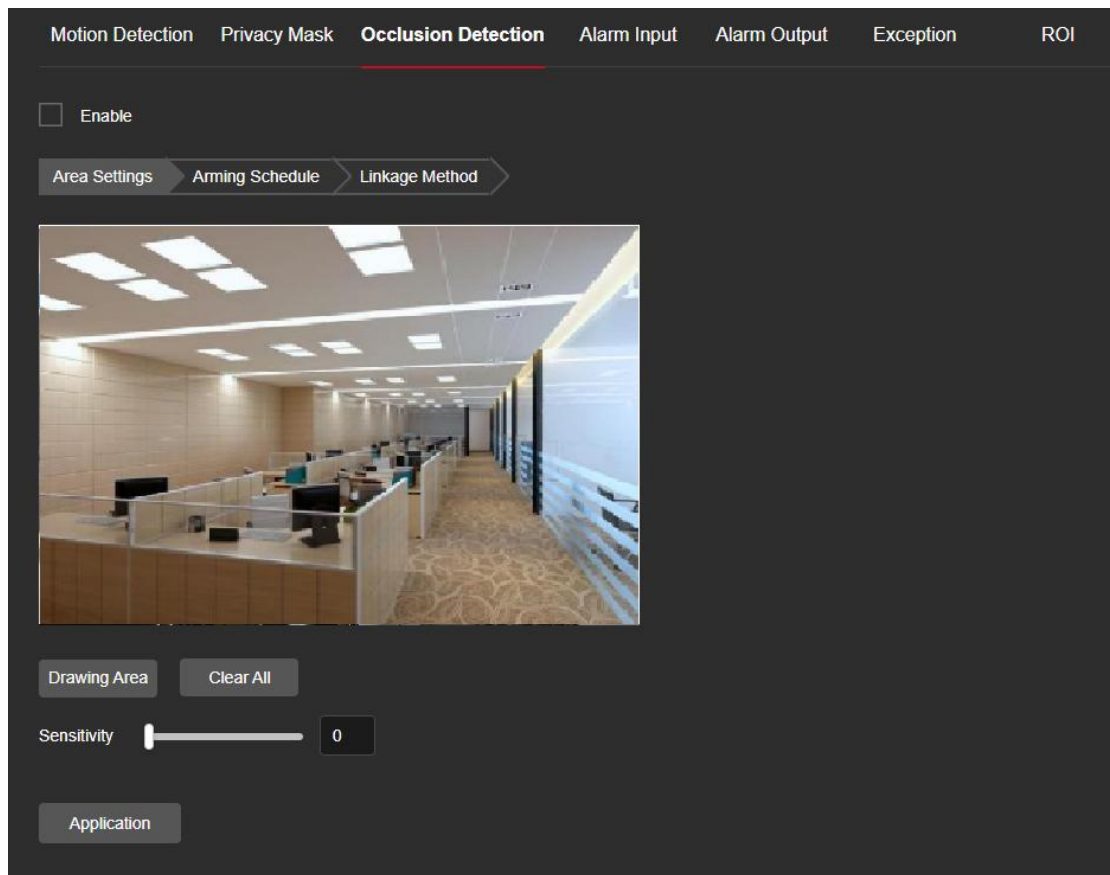
Figure 8-30

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

Step 3: Select the area to set the video tampering sensitivity, click "Application".

【Drawing 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, click "Stop Drawing" to complete the alarm area selection.

【Clear All】Clearing all the video tempering area that selected currently.

【Sensitivity】The default is 0, can switch the range of 0-2, the greater the value of the more sensitive equipment alarm.

Step 4: Set the arming schedule.

As shown in Figure 8-31, 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 fill in the start time and end time, set up and click "Save". If you need to delete the time period, click the "Delete" button and then reset the time period.

- Method 2: Click the arming time period, two arrows will be displayed at both ends of the time period. Move the adjustment arrow left or right to adjust the arming time.

- You can set up more than one time period for up to 8 time periods.

- After the day of deployment time is set, if the other time also need to set the same arming time, click the right side of the timeline " " copy button, in the "copy to" interface check the "Select   All" or a day, then Click "OK".

‒ After setting, click "Application" to complete the setting of the arming time.

Figure 8-31

 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(Upload Via SMTP, Upload Via FTP, Upload Via Cloud, Flash Warning,Sound Alarm) and linkage alarm output(IO Output), as shown in Figure 8-32.
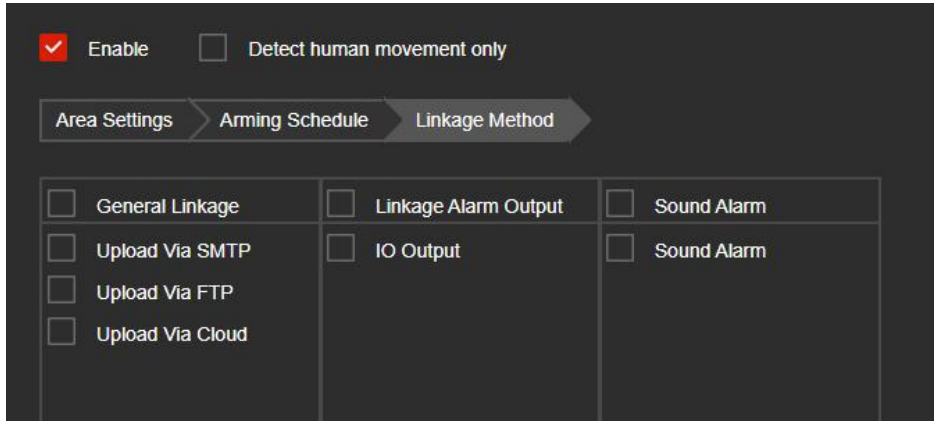

Figure 8-32

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

【Upload Via 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.

【Flash 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 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 → Events → Ordinary Events → 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 8-33, 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 fill in the start time and end time, set up and click "Save". If you need to delete the time period, click the "Delete" button and then reset the time period.

‒ Method 2: Click the arming time period, two arrows will be displayed at both ends of the time period. Move the adjustment arrow left or right to adjust the arming time.

‒ You can set up more than one time period for up to 8 time periods.

‒ After the day of deployment time is set, if the other time also need to set the same arming time, click the right side of the timeline "⊟" copy button, in the "copy to" interface check the "Select   All" or a day, then Click "OK".

‒ After setting, click "Application" to complete the setting of the arming time.

Figure 8-33

Step 4: Set the linkage method.

Alarm linkage methods include general linkage(Upload Via SMTP, Upload Via FTP, Upload Via Cloud,Flash Warning, Sound Alarm) and linkage alarm output(IO Output), as shown in Figure 8-34.
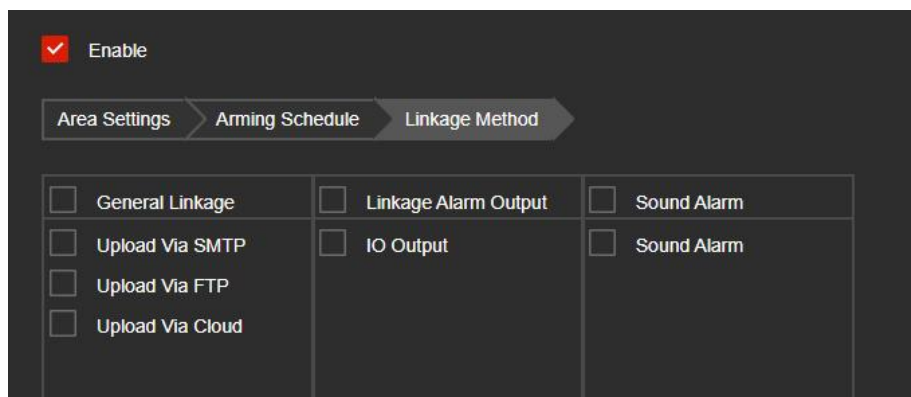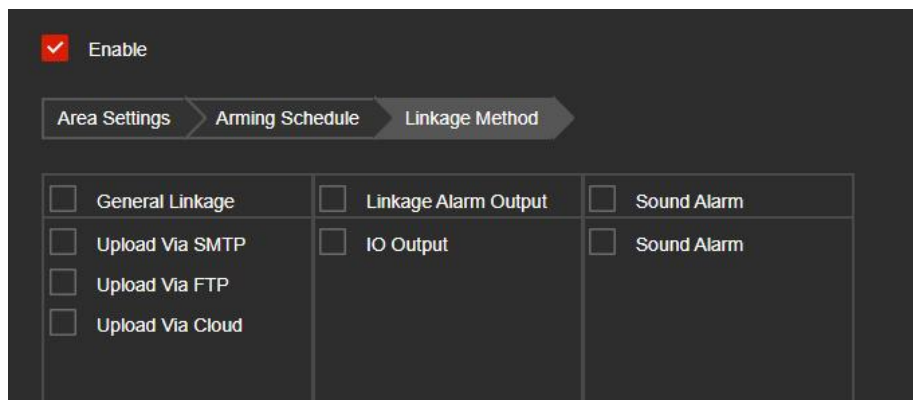

Figure 8-34

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

【Upload Via 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.

【Flash 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 **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 → Events → Ordinary Events→ Alarm Output" to enter the Alarming Output settings interface.

Step 2: Set the delay time.

Step 3: Set the arming schedule.

As shown in Figure 8-35, 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 fill in the start time and end time, set up and click "Save". If you need to delete the time period, click the "Delete" button and then reset the time period.

–   Method 2: Click the arming time period, two arrows will be displayed at both ends of the time period. Move the adjustment arrow left or right to adjust the arming time.

–   You can set up more than one time period for up to 8 time periods.

–   After the day of deployment time is set, if the other time also need to set the same

arming time, click the right side of the timeline "" copy button, in the "copy to"

interface check the "Select   All" or a day, then Click "OK".

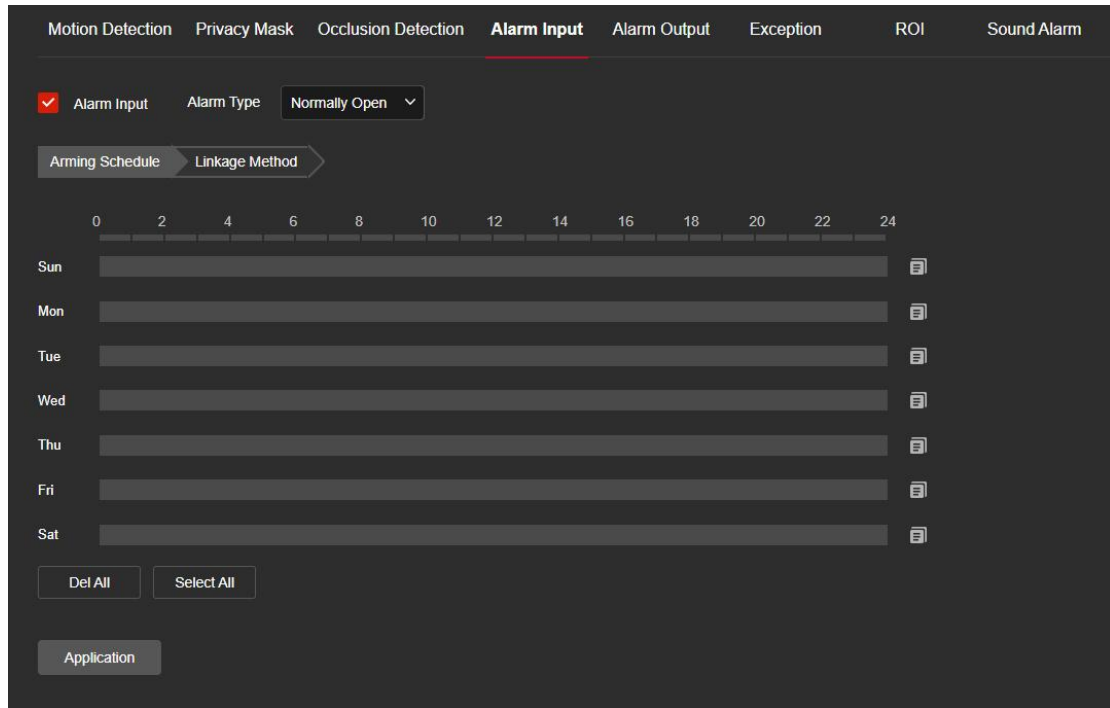**Step 4:** Click "Application" to complete the setting of the arming time.
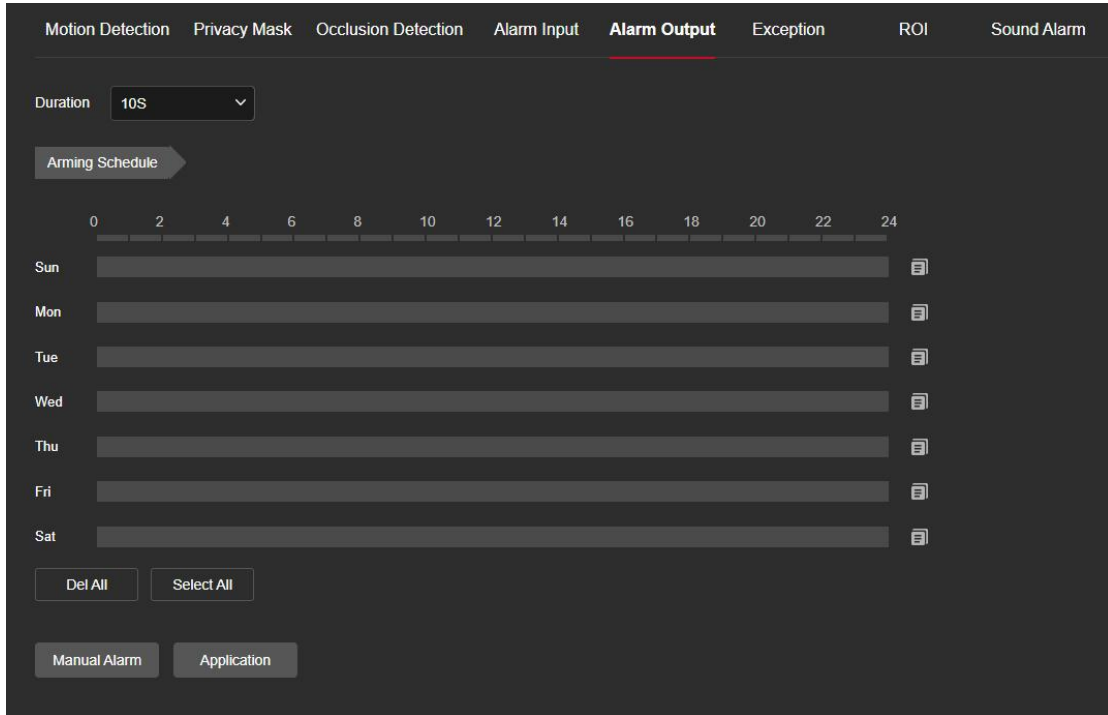
Figure 8-35

【Manual alarm】Manually control the alarm output device on the alarm output interface to link the alarm.

⑥ **Exception**

Set the alarm mode of abnormal events. When an abnormal event occurs during the operation of the IPC, the system executes the alarm linkage action.

The specific operation steps are as follows:

Step 1: In the main interface, click "Configuration → Events → Ordinary Events → Exception" to enter the exception settings interface, as shown in Figure 8-36.
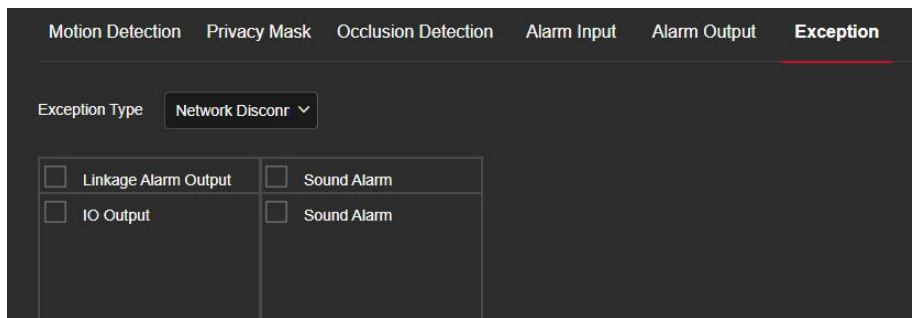
Figure 8-36

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

Step 3: Click on the "Application" after completing the settings.

【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.

⑦ **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 → Events → Ordinary Events → ROI" to enter the ROI setting interface, as shown in Figure 8-37.
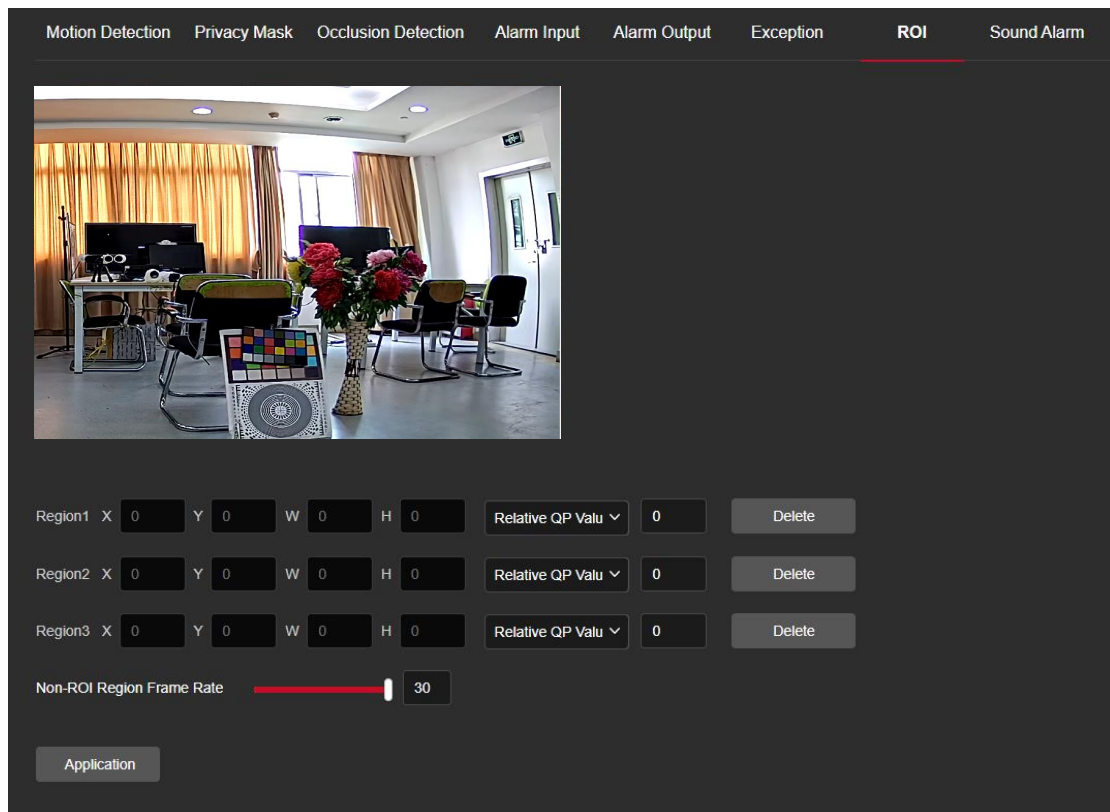
Figure 8-37

Step 2: 【Region Settings】Move the mouse to the preview screen, hold down the left mouse button to select the ROI area range, and release the left mouse button to complete the area drawing. You can also enter the X, Y, W, and H corresponding positions in the corresponding area to set the area.

Step 3: 【Set "Relative QP value" or "Absolute QP value"】Select "Relative QP value" or "Absolute QP value" in the corresponding area position and enter the corresponding value.

Step 4: Slide the scroll bar to set the frame rate of the Non-ROI region.

Step 5: Click "Application" 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.
- Click 【Delete】 in the corresponding setting area to delete the corresponding ROI area.

⑧ **Sound 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 → Events → Ordinary Events → Sound Alarm" to enter the Sound Alarm setting interface, as shown in Figure 8-38.


| Motion Detection | Privacy Mask | Occlusion Detection | Alarm Input | Alarm Output | Exception | ROI | **Sound Alarm** |

☐ Enable

Sound Type   Private sphere ▾   Audition

Delay Time   5 ▾   (s)

Broadcast Language   English ▾

Sound File   File size cannot exceed100K，Only audio files in …   Browse

Note: The audition sound will be played on the camera

Application
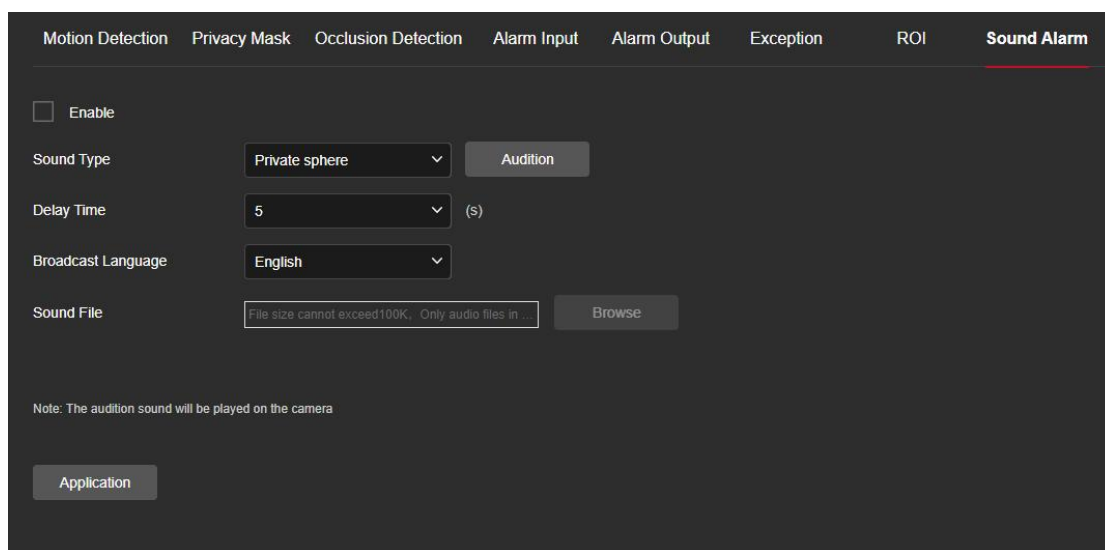
Figure 8-38

Step 2: Click "Enable"to turn on the sound alarm.Configure the alarm sound type of the camera, you can choose private area, warning area, surveillance area, welcome, deep water warning, dangerous area, valuables, high altitude warning, custom.

Step 3: Set delay time: default 5S, optional 10S, 20S, 30S.

Step 4: Set the alarm 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,the file size cannot exceed 100K, only G711U format is supported).

NOTE

- Some cameras do not support the Sound Alarm. The specific interface is subject to the actual product.

8.6.2 Smart Event

① **Intrusion Detection**

The area intrusion detection is used to detect whether a somebody enters the set area 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 → Events → Smart Event→ Intrusion Detection" to enter the Intrusion Detection settings interface, as shown in Figure 8-39.
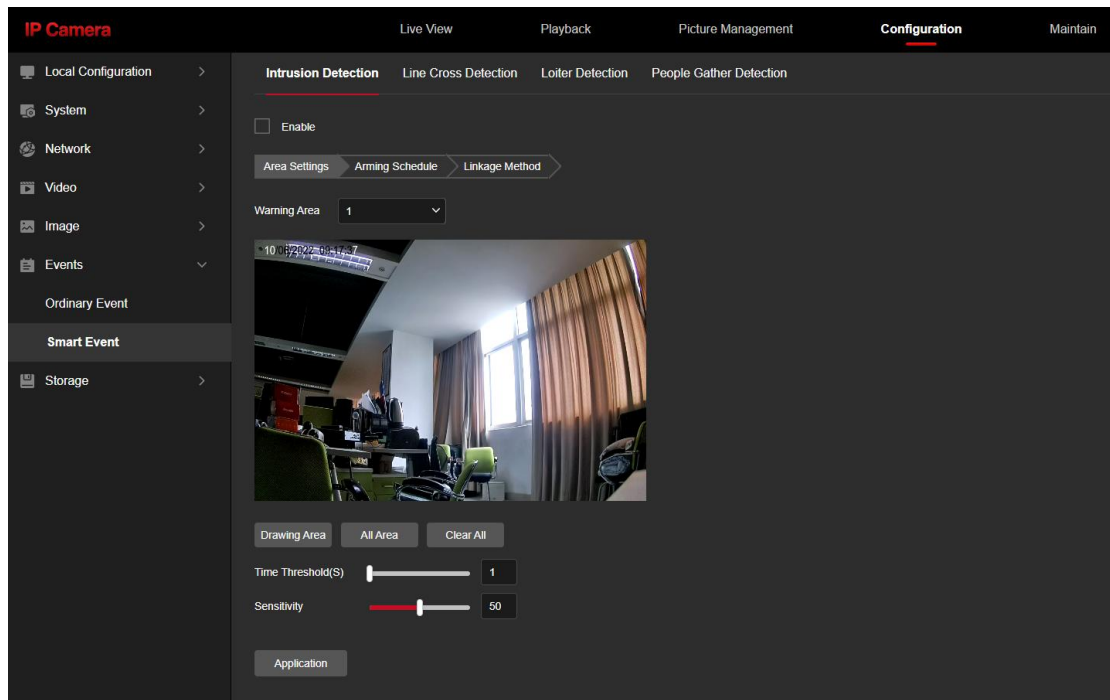
Figure 8-39

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

Step 3: Select "Warn 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".

【Drawing Area】Click "Drawing　Area", move the mouse to the preview screen, click the left mouse button and draw the endpoint of the quadrilateral guard area, then click the preview interface to complete the area drawing.

【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.

【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 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 8-40. 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 fill in the start time and end time, set up and click "Application". If you need to delete the time period, click the "Delete" button and then reset the time period.

‒   Method 2: Click the time of deployment, the time period will display two circles at both ends, the mouse moves to the circle, and move the adjustment arrow left and right to adjust the arming time.

‒   You can set up more than one time period for up to 8 time periods.

‒   After the day of deployment time is set, if the other time also need to set the same

arming time, click the right side of the timeline " 🗐 " copy button, in the "copy to"

interface check the "Select All" or a day, then Click "OK".

‒   After setting, click "Application" to complete the setting of the arming time.

Figure 8-40

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(Upload Via SMTP, Upload Via FTP, Upload Via Cloud, Flash Warning,Sound Alarm) and linkage alarm output(IO Output), as shown in Figure 8-41.
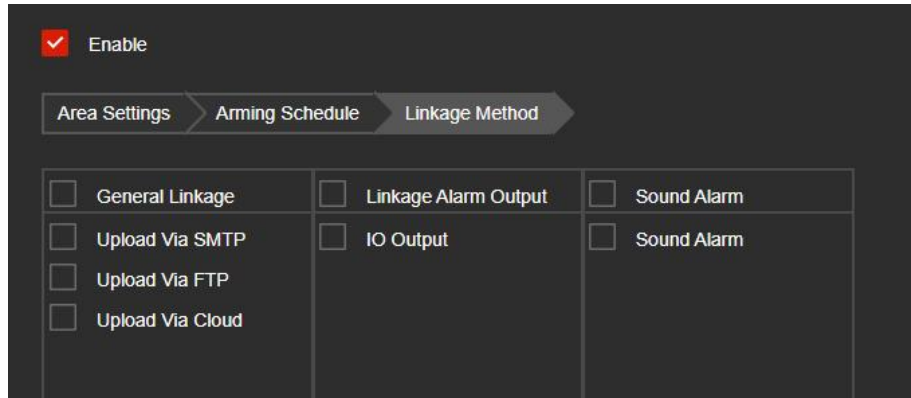
Figure 8-41

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

【Upload Via 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.

【Flash 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 Line Cross Detection

The line cross detection function is used to detect whether there is an object 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 → Events → Smart Event → Line Cross Detection" to enter the Line Cross Detection settings interface, as shown in Figure 8-42.
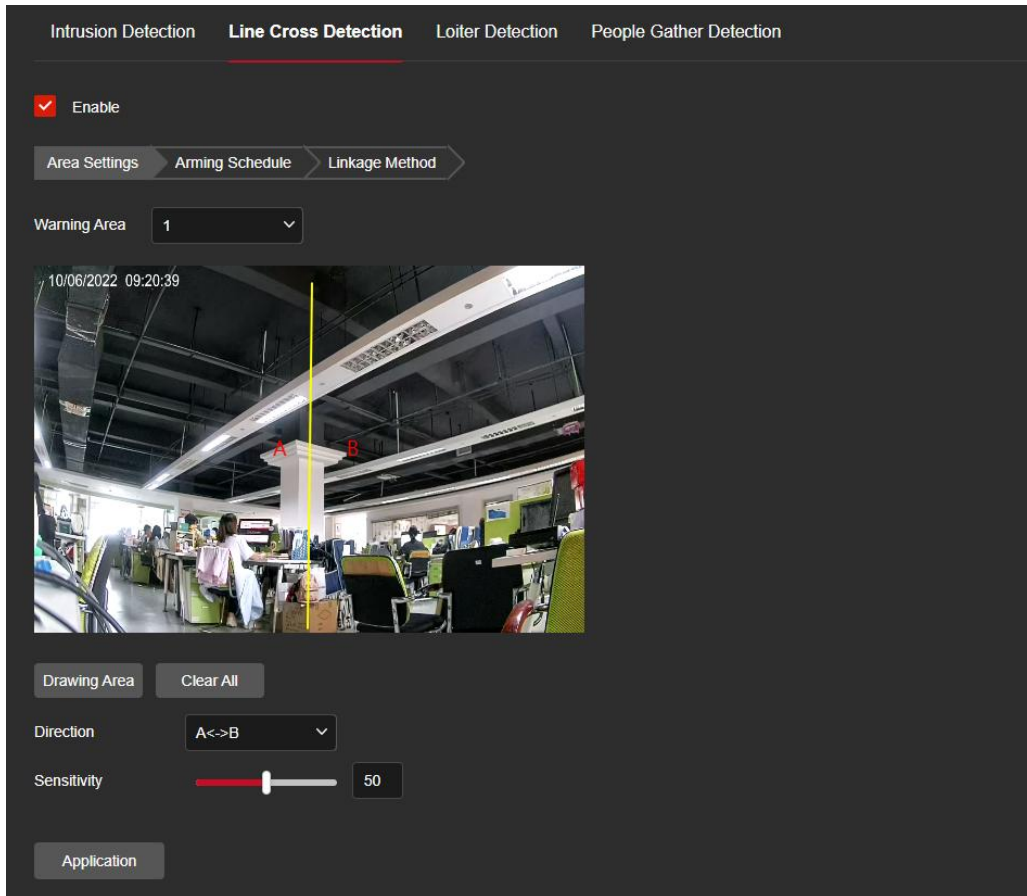
Figure 8-42

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

Step 3: Select "Warn Line": 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 "Save" below.

【Warn Line】Click "Drawing   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.

【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 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 Line, repeat step 3 to complete the setup.

Step 5: Set the arming schedule.

As shown in Figure 8-43. 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 fill in the start time and end time, set up and click "Save". If you need to delete the time period, click the "Delete" button and then reset the time period.

‒ Method 2: Click the time of deployment, the time period will display two circles at both ends, the mouse moves to the circle, and move the adjustment arrow left and right to adjust the arming time.

‒ You can set up more than one time period for up to 8 time periods.

‒ After the day of deployment time is set, if the other time also need to set the same arming time, click the right side of the timeline "▤" copy button, in the "copy to" interface check the "Select All" or a day, then Click "OK".

‒ After setting, click "Application" to complete the setting of the arming time.

Intrusion Detection	**Line Cross Detection**	Loiter Detection	People Gather Detection

✔ Enable

Area Settings ▶ Arming Schedule ▶ Linkage Method

```
     0    2    4    6    8   10   12   14   16   18   20   22   24
Sun  ████████████████████████████████████████████████████████  ▤
Mon  ████████████████████████████████████████████████████████  ▤
Tue  ████████████████████████████████████████████████████████  ▤
Wed  ████████████████████████████████████████████████████████  ▤
Thu  ████████████████████████████████████████████████████████  ▤
Fri  ████████████████████████████████████████████████████████  ▤
Sat  ████████████████████████████████████████████████████████  ▤
```
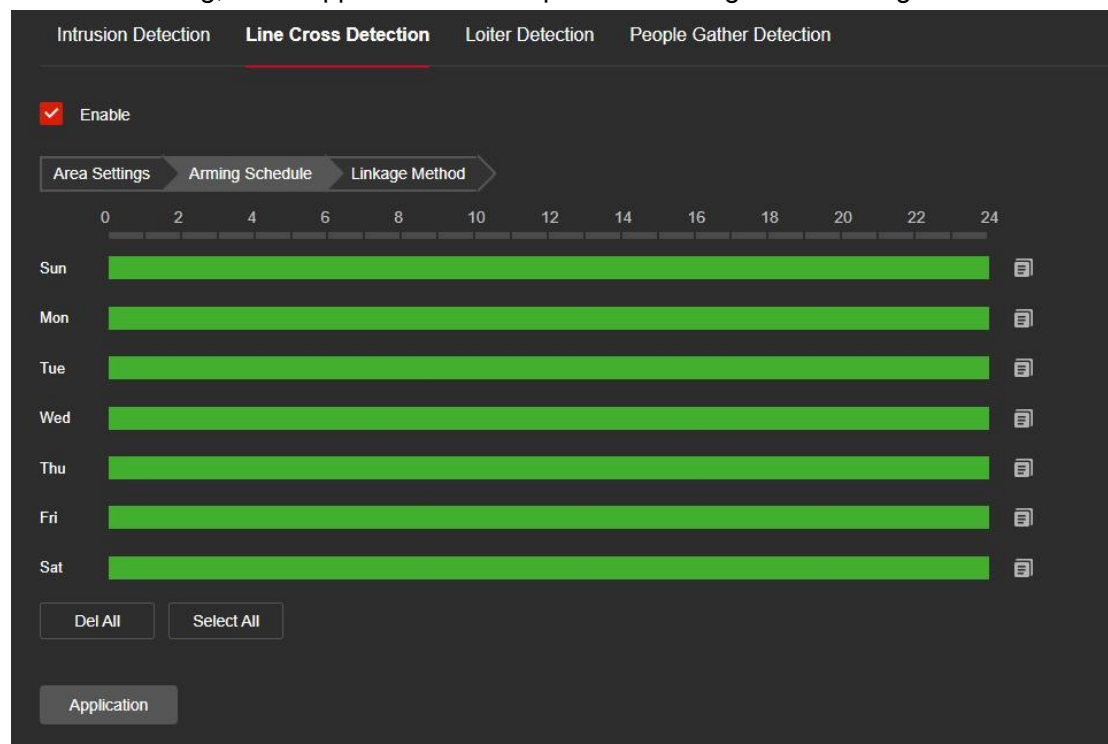
Del All	Select All

Application

Figure 8-43

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(Upload Via SMTP, Upload Via FTP, Upload Via Cloud, Flash Warning,Sound Alarm) and linkage alarm output(IO Output), as shown in Figure 8-44.
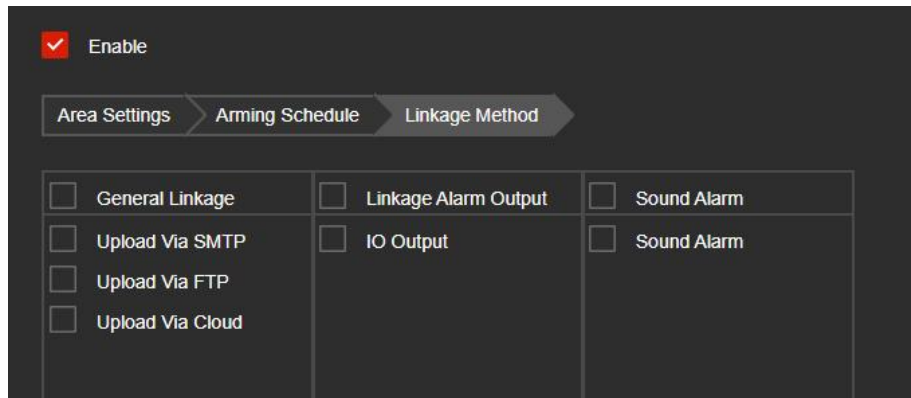
Figure 8-44

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

【Upload Via 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.

【Flash 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 **Loiter Detection**

The loiter 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 → Events → Smart Event → Loiter Detection" to enter the Loiter Detection settings interface, as shown in Figure 8-45.
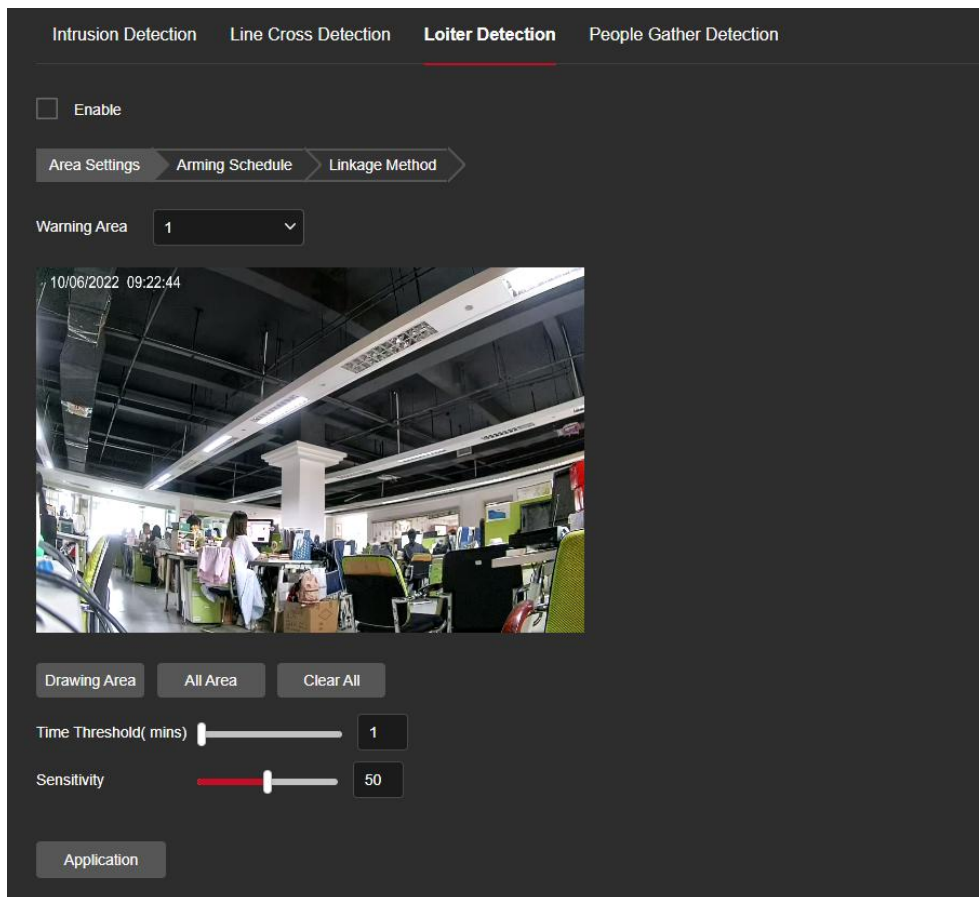
Figure 8-45

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

Step 3: Select "Warn 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.

【Drawing Area】Click "Drawing Area", move the mouse to the preview screen, click the left mouse button and draw the endpoint of the quadrilateral guard area, then click the preview interface to complete the area drawing.

【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.

【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】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 8-46. 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 fill in the start time and end time, set up and click "Application". If you need to delete the time period, click the "Delete" button and then reset the time period.
- Method 2: Click the time of deployment, the time period will display two circles at both ends, the mouse moves to the circle, and move the adjustment arrow left and right to adjust the arming time.
- You can set up more than one time period for up to 8 time periods.
- After the day of deployment time is set, if the other time also need to set the same arming time, click the right side of the timeline "▤" copy button, in the "copy to" interface check the "Select All" or a day, then Click "OK".
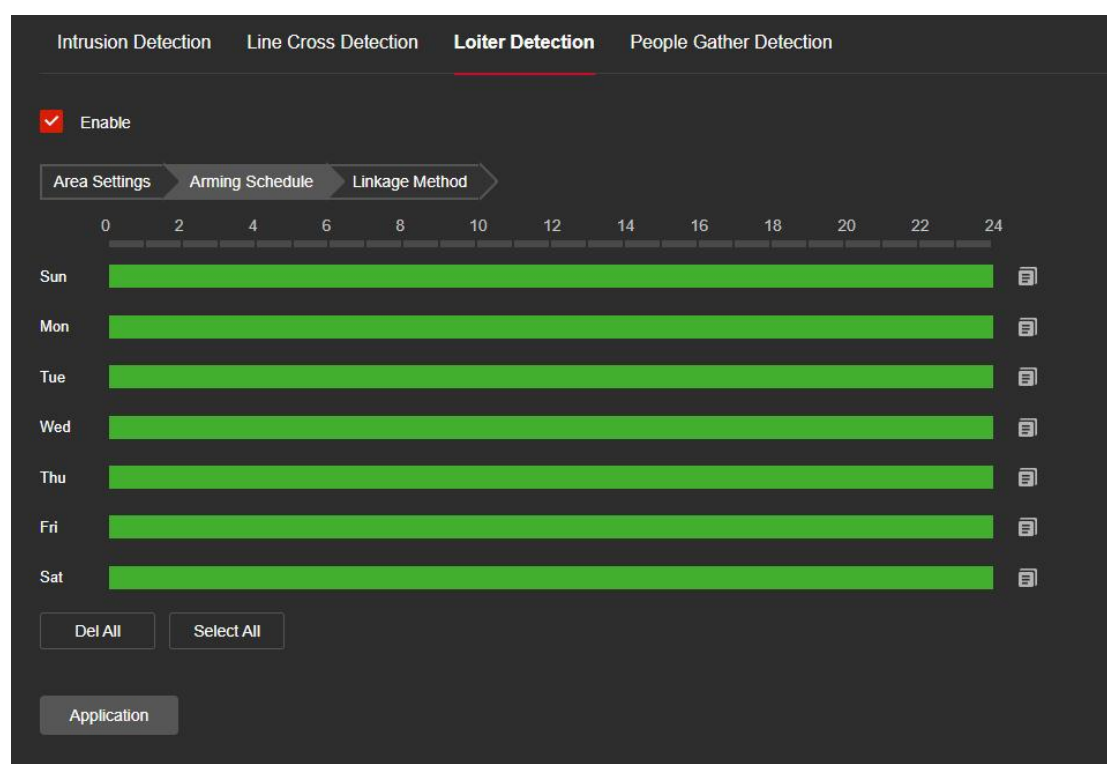- After setting, click "Application" to complete the setting of the arming time.

Figure 8-46

 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(Upload Via SMTP, Upload Via FTP, Upload Via Cloud, Flash Warning,Sound Alarm) and linkage alarm output(IO Output), as shown in Figure 8-47.
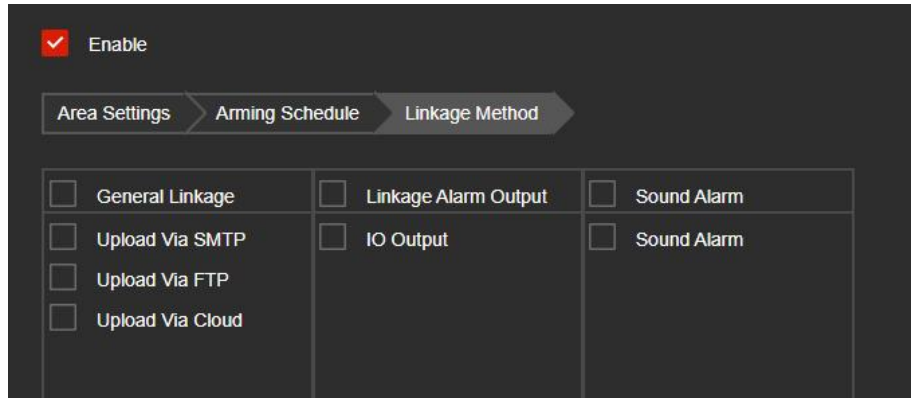
Figure 8-47

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

【Upload Via 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.

【Flash 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 **People Gather Detection**

The people gather 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 → Events → Smart Event → People Gather Detection" to enter the People Gather Detection settings interface, as shown in Figure 8-48.
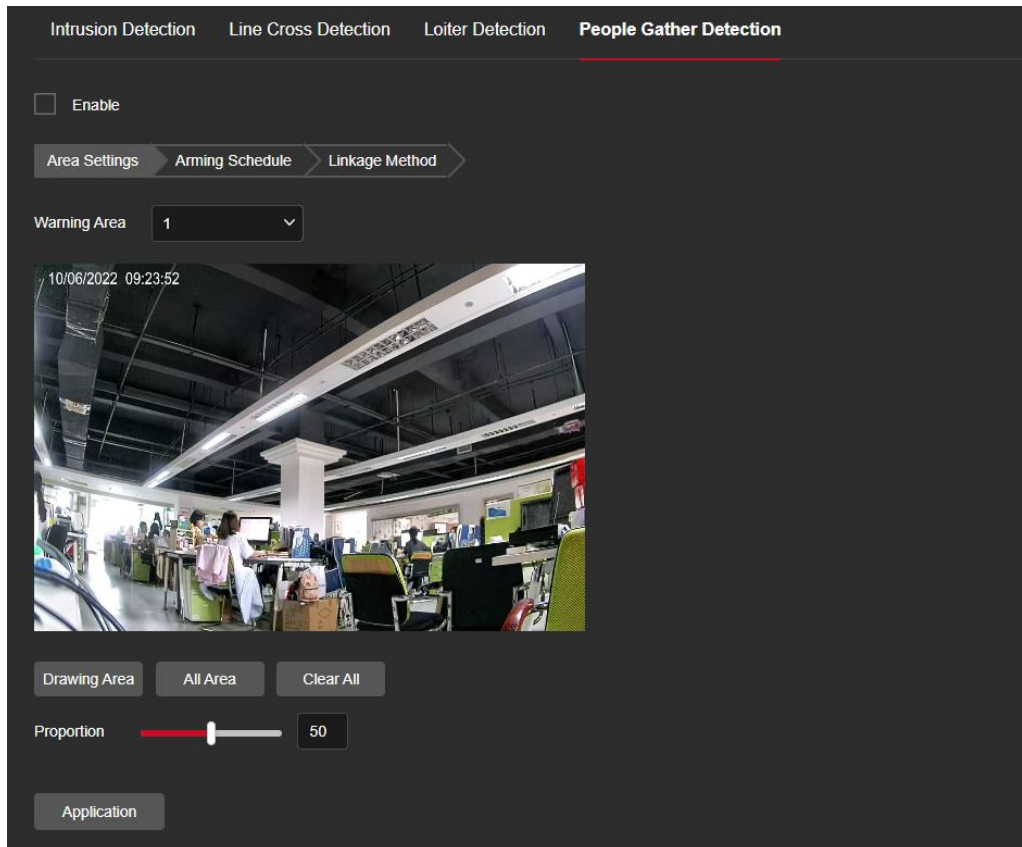
Figure 8-48

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

Step 3: Select "Warn 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.

【Drawing Area】Click "Drawing Area", move the mouse to the preview screen, click the left mouse button and draw the endpoint of the quadrilateral guard area, then click the preview interface to complete the area drawing.

【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.

【Proportion】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 8-49. 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 fill in the start time and end time, set up and click "Application". If you need to delete the time period, click the "Delete" button and then reset the time period.

- Method 2: Click the time of deployment, the time period will display two circles at both ends, the mouse moves to the circle, will show the left and right direction of the adjustment arrow, and move the adjustment arrow to adjust the arming time.
- You can set up more than one time period for up to 8 time periods.
- After the day of deployment time is set, if the other time also need to set the same arming time, click the right side of the timeline "⊟" copy button, in the "copy to" interface check the "Select All" or a day, then Click "OK".
- After setting, click "Application" to complete the setting of the arming time.
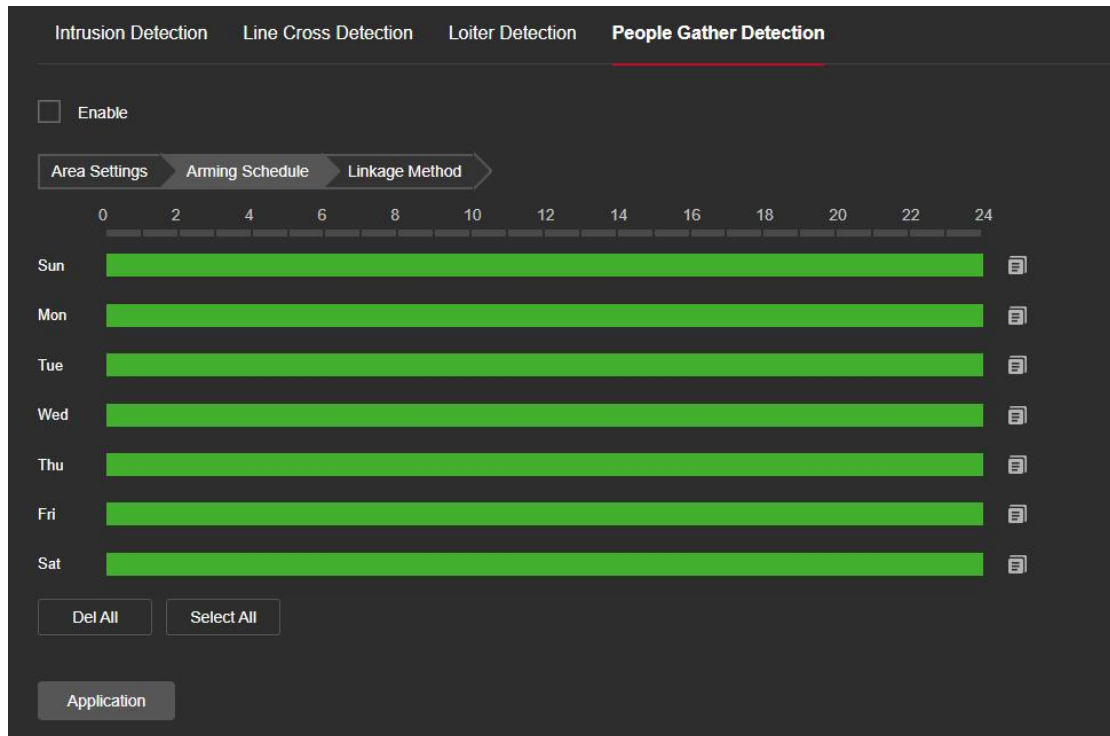

Figure 8-49

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(Upload Via SMTP, Upload Via FTP, Upload Via Cloud,Flash Warning, Sound Alarm) and linkage alarm output(IO Output), as shown in Figure 8-50.
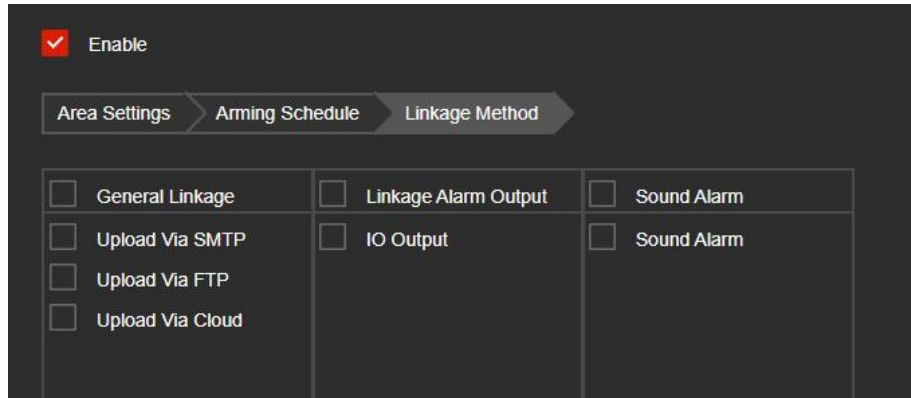
Figure 8-50

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

【Upload Via 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.

【Flash 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 Storage

8.7.1 Schedule Configuration

① **Record Schedule**

The specific operation steps are as follows:

Step 1: In the main interface, click "Configuration → Storage → Schedule Configuration → Record Schedule" to enter the recording setting interface, as shown in Figure 8-10 ①.
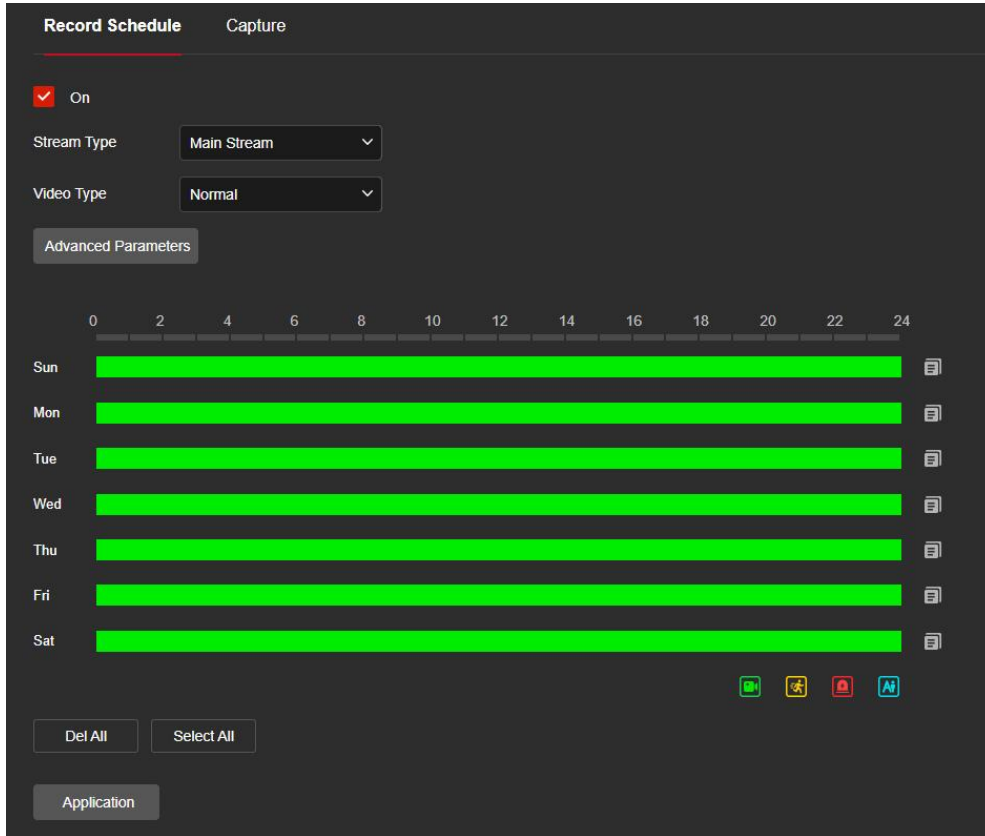
Figure 8-10 ①

Step 2: To enable record, select the stream type (Main Stream, Sub Stream, Tri-Stream）、 video type （Normal Record, Motion Detection, External Alarm, Intelligent).

Step 3: Set the recording schedule time period.

－ Method 1: Click the arming time period, manually fill in the start time and end time, set up and click Save. If you need to delete the time period, click the "Del All" button and then reset the time period.

－ Method 2: Click the arming time period, two arrows will be displayed at both ends of the time period. Move the adjustment arrow left or right to adjust the arming time.

Step 4: Set the Pre-recorded time and Video delay time，click the "Advance parameters",You can set the Pre-recorded time (Unlimited, 10s, 15s, 20s, 25s,30s) and Video delay (5s, 10s, 30s, 1min, 2min, 5min, 10min), as shown in Figure 8-10.
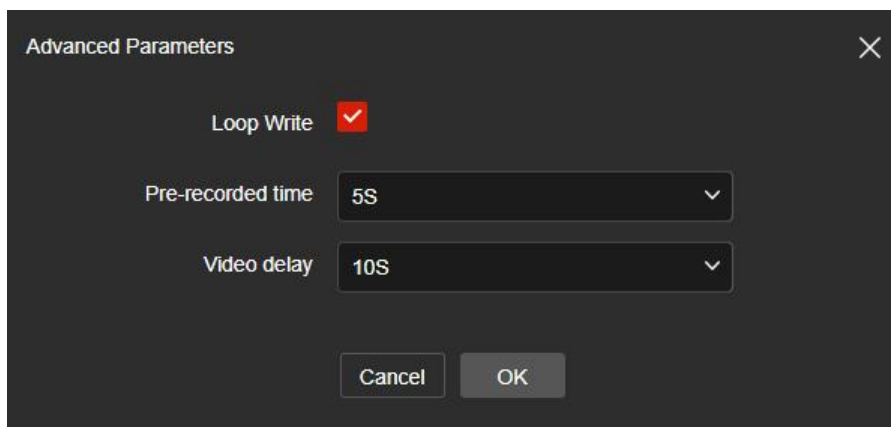
Figure 8-10 ②

Step 5: Click "Application" to complete the setting of the arming time.

👉 **NOTE**

- You can set up more than one time period for up to 8 time periods.
- After the day of deployment time is set, if the other time also need to set the same arming time, click the right side of the timeline "▤" copy button, in the "copy to" interface check the "Select All" or a day, then Click "OK".
- 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.
- When the video type selects motion detection, alarm, the device will also perform scheduled recording while recording the selected recording type.
- The pre-recording time and recording delay can be used for motion detection recording, alarm recording, motion detection and alarm recording.

② **Screenshot**

The snapshot is used to set the camera capture plan and capture parameters. After setting, the IP camera will automatically capture images. In the snapshot parameters interface, when the Enable timed capture is selected, the camera can set the snapshot schedule as needed.

The specific operation steps are as follows:
Step 1: In the main interface, click "Configuration → Storage → Schedule Configuration → Capture" to enter the capture parameter setting interface, as shown in Figure 8-11 ①.

Figure 8-11 ①

Step 2: Set the capture plan.

- Method 1: Click the capture plan, manually fill in the start time and end time, set up and click Save. If you need to delete the time period, click the "Del All" button and then reset the time period.
- Method 2: Click the capture plan, two arrows will be displayed at both ends of the time period. Move the adjustment arrow left or right to adjust the arming time.

Step 3: Repeat **step 2** to set up a complete recording plan.

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

Step 5: Click "Capture Parameters" to enter the capture parameters interface, as shown in Figure 8-11 ②.
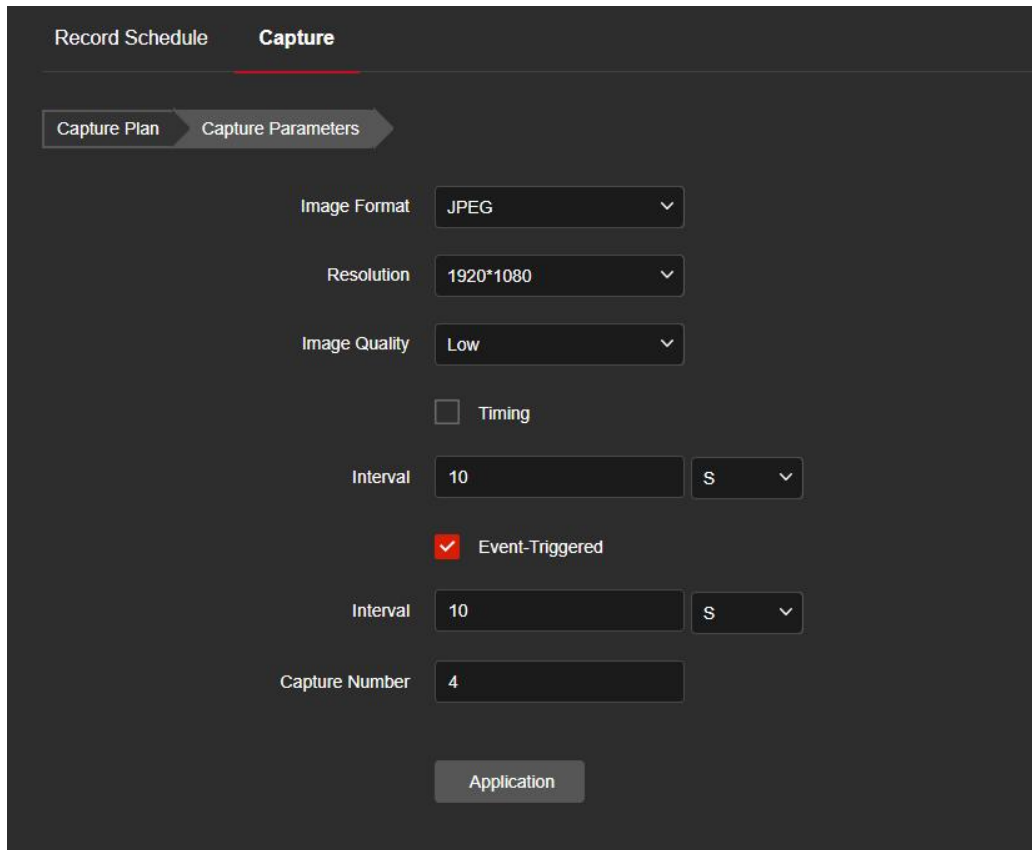
Figure 8-11 ②

Step 6: Select options such as image format (JPEG), resolution, and picture quality as required, and set up timed snapshots and event snapshots.

【Image Format】Support JPEG format.

【Resolution】The captured image resolution.

【Image Quality】Three levels of "Low", "Midd" and "High" can be selected.

【Timed capture】During the set time period, grab a picture according to the set time interval.

【Interval time】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 7: Click "Application" to complete the settings.

  NOTE

- You can set up more than one time period for up to 8 time periods.
- After the day of deployment time is set, if the other time also need to set the same arming time, click the right side of the timeline "" copy button, in the "copy to" interface check the "Select All" or a day, then Click "OK".
- 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.

8.7.2 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 8-12 below :
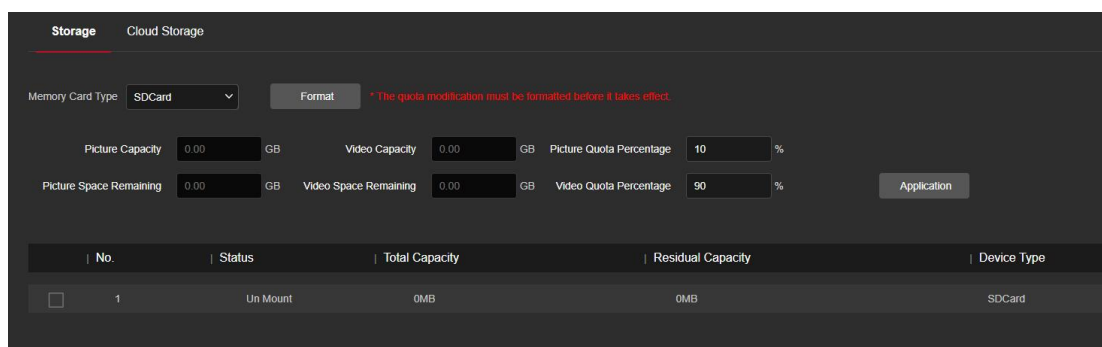

Figure 8-12

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, Total Capacity = Residual Capacity, 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 does not support time recording
● EMMC storage requires the camera to support EMMC hardware,please refer to the actual product.

② **Cloud Storage**
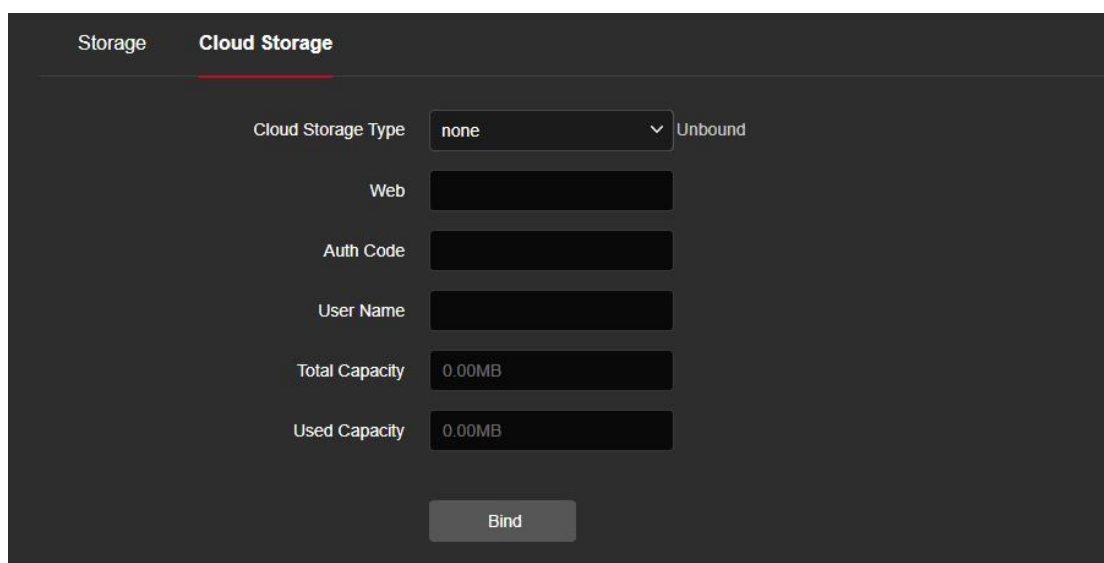
■ **Cloud Storage**

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 8-13.

Figure 8-13

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 "Auth code" field of the cloud storage interface.

Step 5: Click "Bind".

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 System Configuration 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:
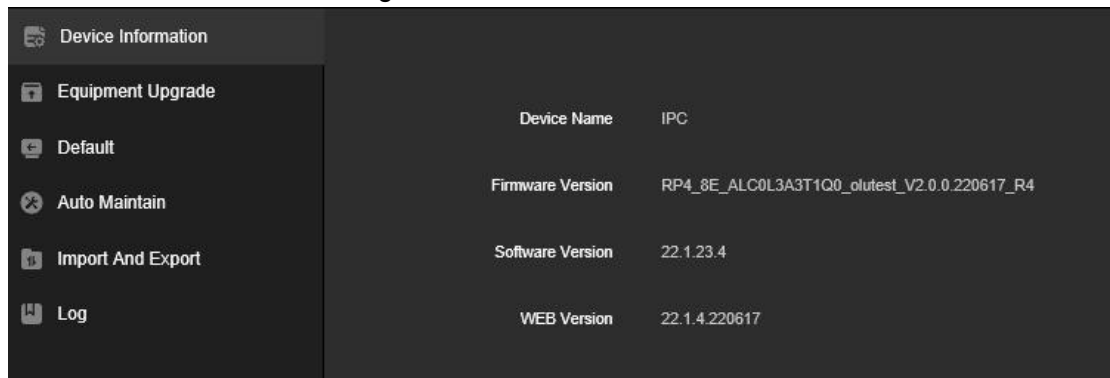

Figure 9-1

【Device Name】The name of the current IPC.

【Firmware Version】The current version of the IPC.

【Software Version】The LsIPCPlugin version of the IPC.

【WEB Version】The current page version of the IPC.

9.2 Equipment Upgrade

In the Maintain interface, click "Equipment Upgrade" to enter the device upgrade interface, where you can manual upgrade, online upgrade, as shown in Figure 9-2.
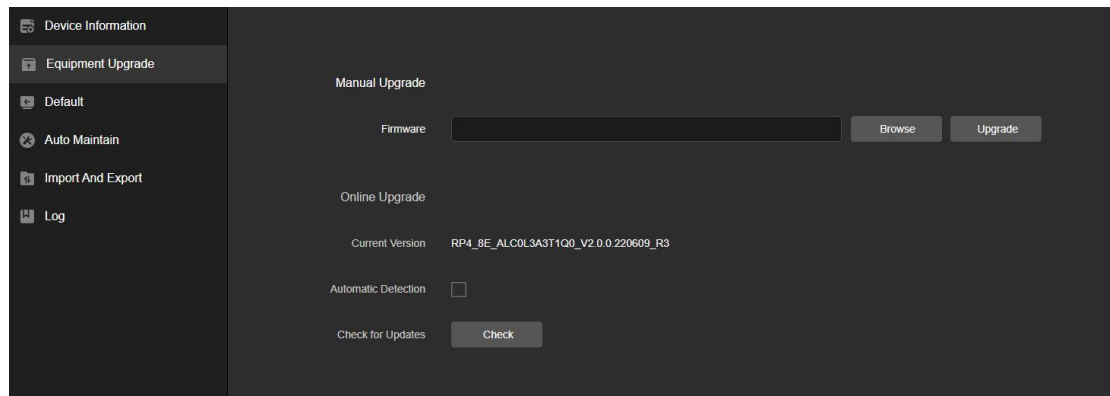

Figure 9-2

【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】To determine the device connected to the network, check the current version number, click on the "Check", such as the pop-up prompts the latest upgrade version, whether to download, click "OK", the device began to download the upgrade

version to complete the automatic upgrade. Click "Cancel" to cancel the upgrade.

【Automatic Detection】To determine the device connected to the network, the device will automatically detect whether there is the latest upgrade version, such as the pop-up prompts the latest upgrade version, whether to download, click "OK", the device began to download the upgrade version to complete the automatic upgrade. Click "Cancel" to cancel the upgrade.

9.3 Default

In the maintain 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.
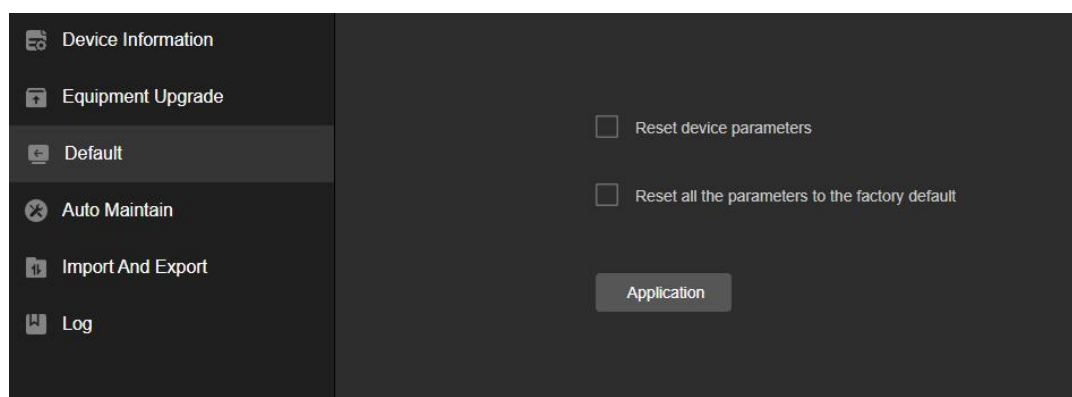

Figure 9-3

【Reset device parameters】IPC will automatically restore the parameters to the factory parameters except the network parameters.

【Reset all the parameters to the factory default】all parameter settings of IPC will be automatically restored to the factory parameter settings (please operate this function carefully).

9.4 Auto Maintain

In the maintain 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 "Application", IPC will be at 3 o'clock on the 3rd 3 times a reboot. As shown in Figure 9-4.
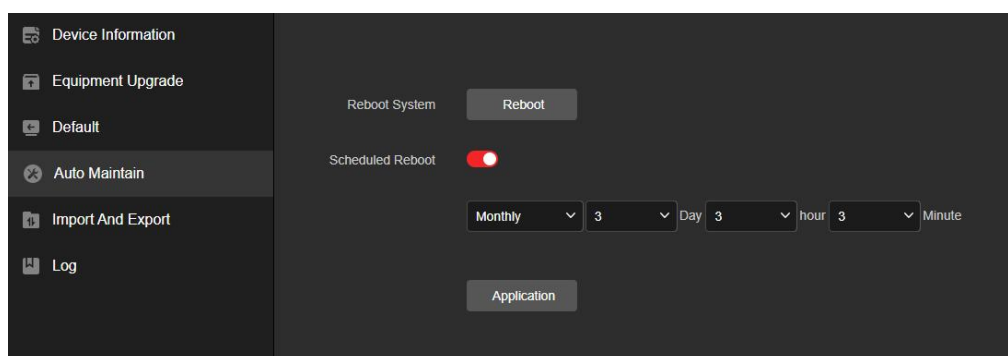
Figure 9-4

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 maintain 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.
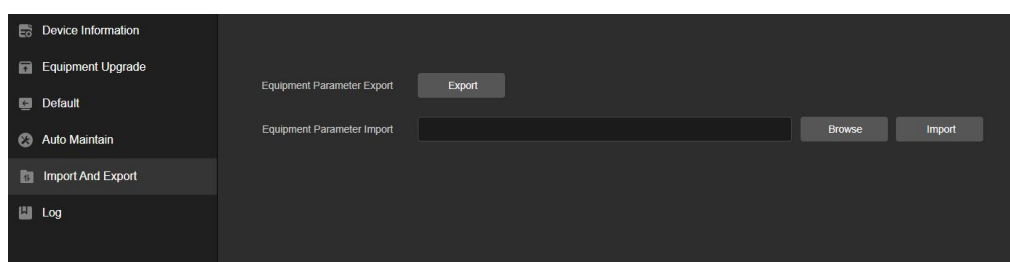

Figure 9-5

9.6 Log

In the maintain 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.
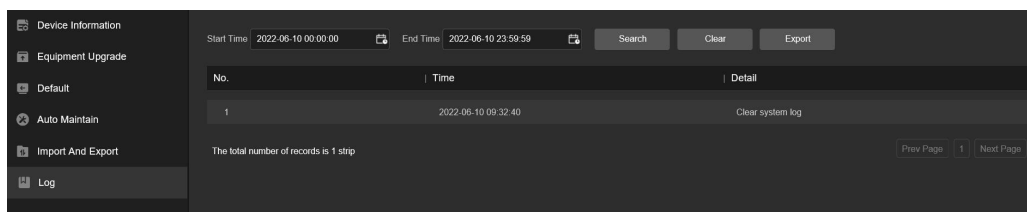

Figure 9-6

【Search】 Set the date 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 IE?
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.