



Network Camera

User Manual

Version: 20.1.27.2

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 network 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 network camera is referred to as IPC for short)

Table of Contents

CHAPTER 1 PRODUCT INTRODUCTION.....	6
1.1 PRODUCT MANUAL.....	6
1.2 PRODUCT FEATURES.....	6
CHAPTER 2 OPERATING INSTRUCTIONS.....	8
2.1 NETWORK CONNECTION.....	8
2.1.1 Wired network connection.....	8
2.1.2 Wireless internet access.....	8
2.2 DETECTING AND CHANGING THE IP ADDRESS.....	9
2.3 SETTING THE NETWORK CAMERA OVER THE WAN.....	10
2.3.1 Static IP Connection.....	10
2.3.2 Dynamic IP Connection.....	10
CHAPTER 3 ACCESS TO THE IPC BY CLIENT SOFTWARE.....	12
CHAPTER 4 ACCESS TO THE IPC BY WEB CLIENT.....	13
4.1 PREPARATION BEFORE INSTALL PLUGIN.....	13
4.2 LOGIN AND EXIT.....	13
4.2.1 Login.....	13
4.2.2 Change password.....	14
4.2.3 Forget password.....	16
4.2.4 Exit System.....	18
4.3 INSTALL THE HSI PCCTL CONTROLS.....	18
4.4 MAIN INTERFACE DESCRIPTION.....	23
CHAPTER 5 LIVE PREVIEW.....	24
5.1 LIVE PREVIEW.....	24
5.2 CAMERA SETTINGS PTZ, ZOOM, CRUISE.....	25
CHAPTER 6 PLAYBACK.....	28
CHAPTER 7 PICTURE.....	31
CHAPTER 8 CONFIGURATION.....	32
8.1 LOCAL CONFIGURATION.....	32
8.2 SYSTEM.....	33
8.2.1 System Configuration.....	33
8.2.2 Scheduled Reboot.....	36
8.2.3 Log Search.....	36
8.2.4 Security.....	37
8.3 STORAGE.....	40
8.3.1 Plan configuration.....	40
8.3.2 Storage management.....	43
8.4 NETWORK.....	47
8.4.1 Basic Setup.....	48
8.4.2 Advance Setup.....	49
8.5 VIDEO.....	60
8.5.1 Video.....	61
8.5.2 Audio.....	62
8.6 IMAGE.....	63
8.6.1 Image.....	63
8.6.2 OSD.....	68

8.7 EVENTS.....	68
8.7.1 Ordinary Event.....	69
8.7.2 Smart Event.....	83
8.8 BODY TEMPERATURE MEASURE.....	94
8.8.1 Body Temperature Measure.....	95
CHAPTER 9 FREQUENTLY ASKED QUESTIONS.....	97

Chapter 1 Product Introduction

1.1 Product Manual

Network 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.

Network 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 network camera, and through the browser to set the network 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 network 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 network camera to support video playback, query and playback card recording.

■ Event detection function

The network camera supports ordinary event and Smart event.

● Ordinary event

Ordinary event include Motion Detection, Privacy Mask, Video Tampering, Exception, Alarm Input/Output, Flash alarm, Audible alarm output and ROI.

● Smart event

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

■ Internet function

Network 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.

● PTZ function

With PTZ function camera support lens zoom, aperture control, PTZ control and cruise settings and other functions.

- **Cloud storage function**

The network 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.

- **Body Temperature Measure**

Some network cameras support the body temperature measurement function. By setting the body temperature measurement parameters, a linkage alarm is given to the target exceeding the temperature threshold.



NOTE

- Network 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 network camera is installed, you can preview and configure related function parameters through the browser.

2.1.1 Wired network connection

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



Figure 2-1

Set network 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 network cameras support wireless network transmission, in the wireless network environment, the network 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 network camera, proceed as follows:

Step 1: Search IPC IP address.

- Using the IP 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:

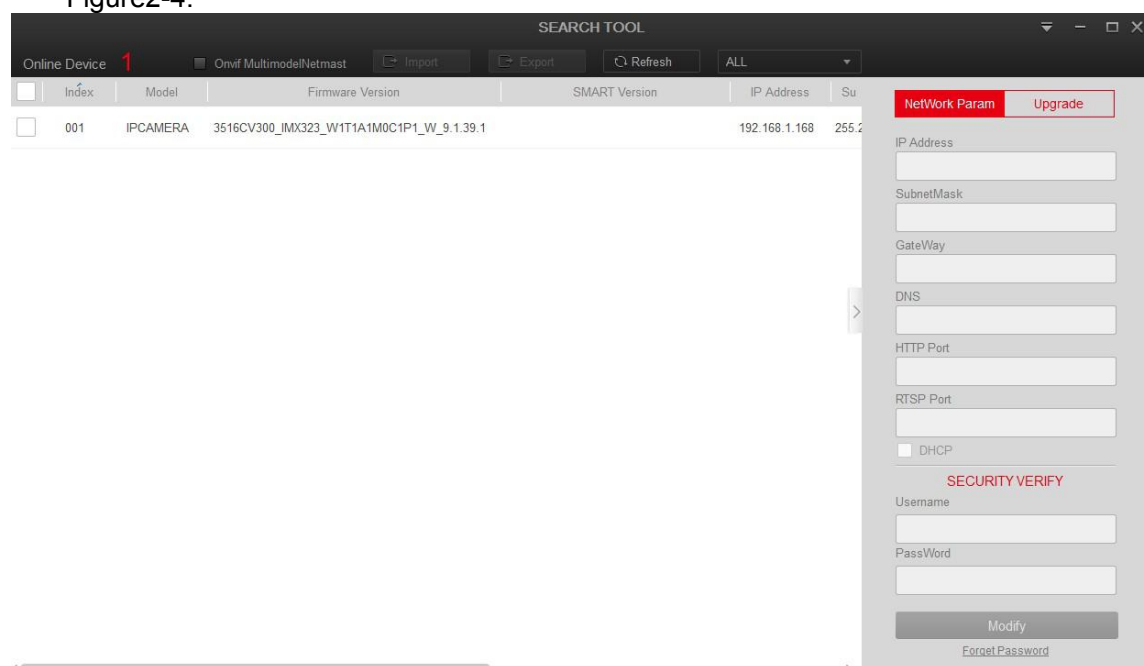


Figure 2-4

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

Step 2: Modify the IP address of the IP camera and connect the computer to the same network segment.

- In the IP 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 network camera after login. For details, see 7.3.1 Configuring TCP/IP.

2.3 Setting the Network Camera over the WAN

This section explains how to connect the network 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 network camera via a router or connect it to the WAN directly.

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

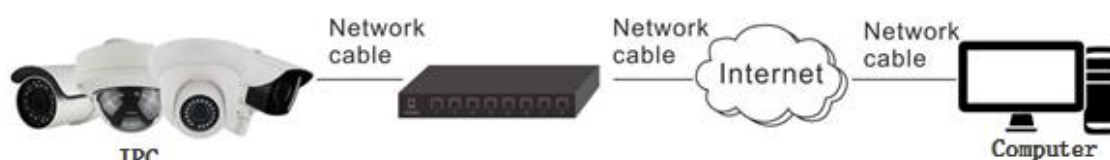


Figure 2-5

Specific steps are as follows:

Step 1: Connect the network camera to the router.

Step 2: Assign a LAN IP address, the sub net mask and the gateway. For details, please refer to 7.3.1.

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 network 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 7.3.1.

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 network camera to a modem or a router.

➤ **The router is connected to the network camera**

Specific steps are as follows:

Step 1: Connect the network camera to the router.

Step 2: Assign a LAN IP address, the sub net mask and the gateway. For details, please refer to 7.3.1.

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:**

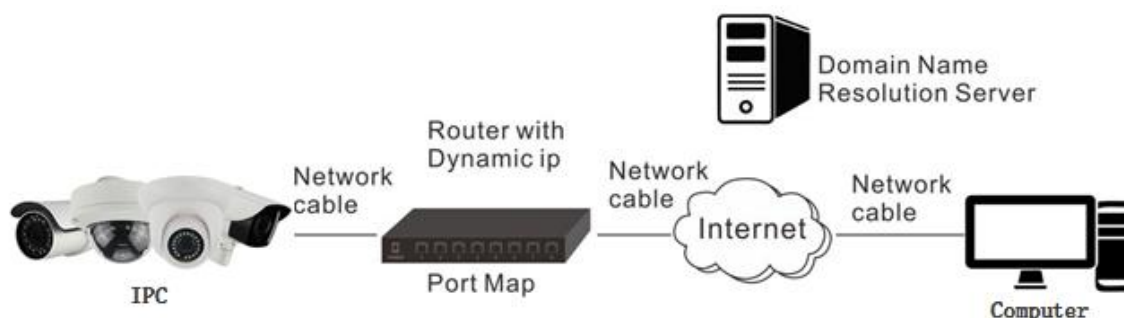


Figure 2-7

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 network camera. For details, please refer to 7.3.2.

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

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

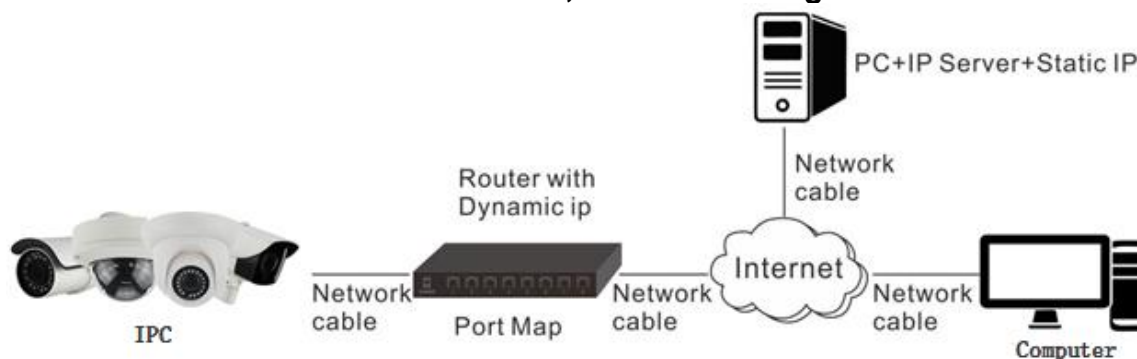


Figure 2-8

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 network 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 7.3.2.

Chapter 3 Access to the IPC by Client Software

The VMS Lite 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 VMS Lite client software are shown in Figure 3-1.

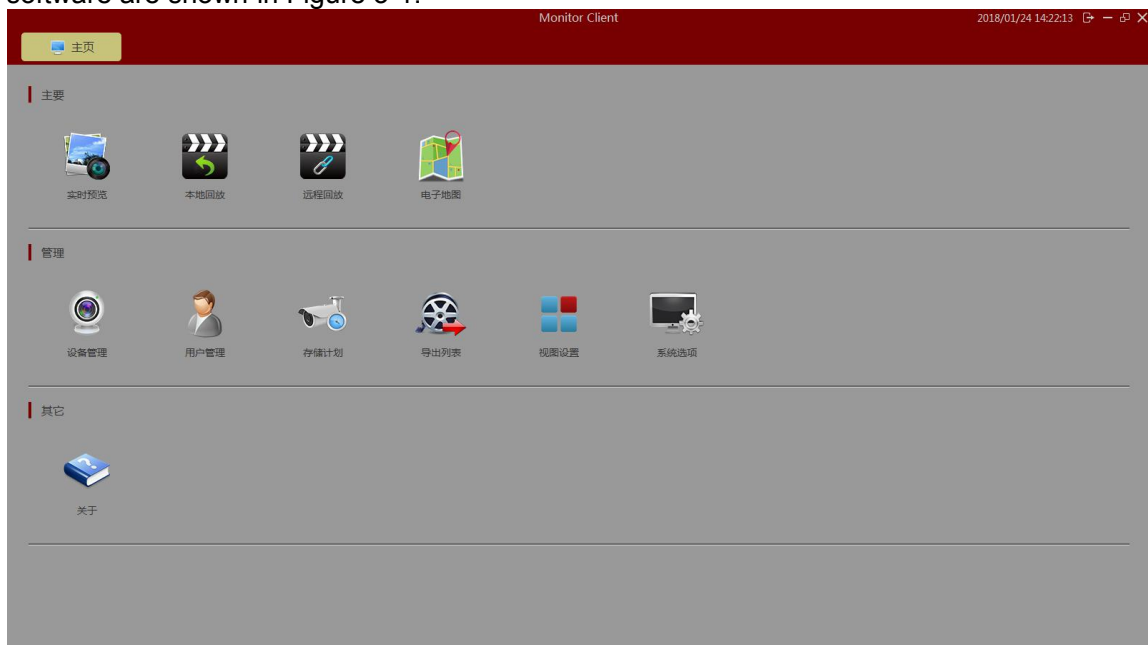


Figure 3-1



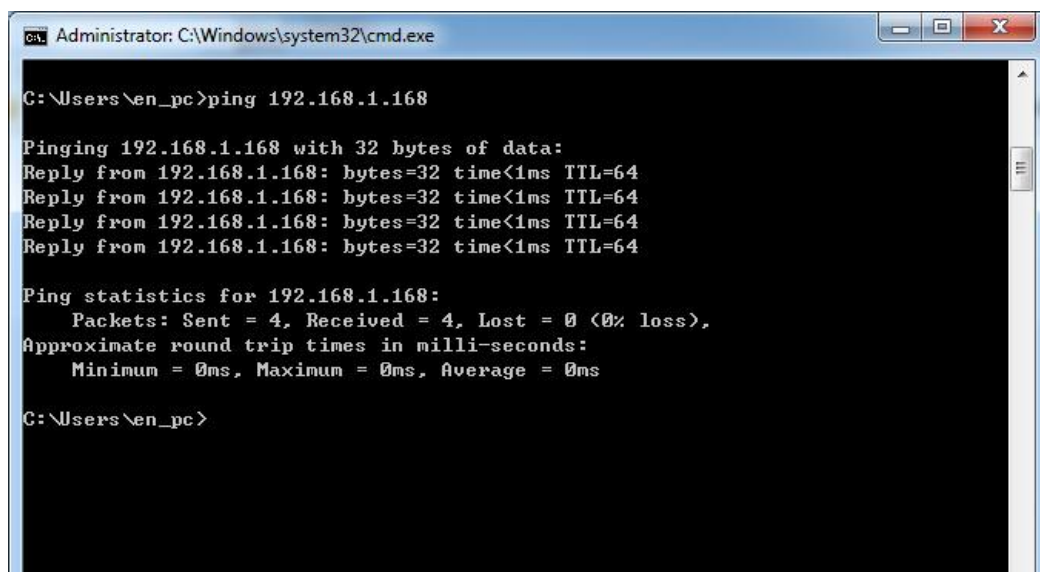
NOTE

- For detailed information about the software, please refer to the user manual of the VMS Lite 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.

A screenshot of a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window shows the command "C:\Users\en_pc>ping 192.168.1.168" and its output. The output indicates a successful ping to 192.168.1.168 with 32 bytes of data, showing four replies with times less than 1ms and TTL=64. Ping statistics show 4 packets sent, 4 received, and 0% loss, with round trip times of 0ms.

```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\en_pc>ping 192.168.1.168

Pinging 192.168.1.168 with 32 bytes of data:
Reply from 192.168.1.168: bytes=32 time<1ms TTL=64
Reply from 192.168.1.168: bytes=32 time<1ms TTL=64
Reply from 192.168.1.168: bytes=32 time<1ms TTL=64
Reply from 192.168.1.168: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.168:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\en_pc>
```

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:

User Management

Users to edit

User Name	admin
User Type	Admin ▼
Old password	
☒ Modify Password	
Password	
Confirm Password	
☒ Do you want to set a new security question	
Security issue1	▼
Answer1	
Security issue2	▼
Answer2	
Security issue3	▼
Answer3	

key export

If you forget the security problem and don't have the key file, you need to return the equipment to the factory.

Save

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"

1 Verify Identity 2 Set New Password 3 Carry Out

Authentication Mode Security question validation

Security issue1 What is the family name of your favourite teacher in p

Answer1

Security issue2 What is the model of your first car?

Answer2

Security issue3 Which street did you grow up on?

Answer3

Next Clear

Figure 4-5 ①

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

1 Verify Identity 2 Set New Password 3 Carry Out

Set New Password

Confirm Password

Next Clear

Figure 4-5 ②

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



Dear user, the password has been reset. Please click on " re-login "to enter the login interface

Re-login

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".

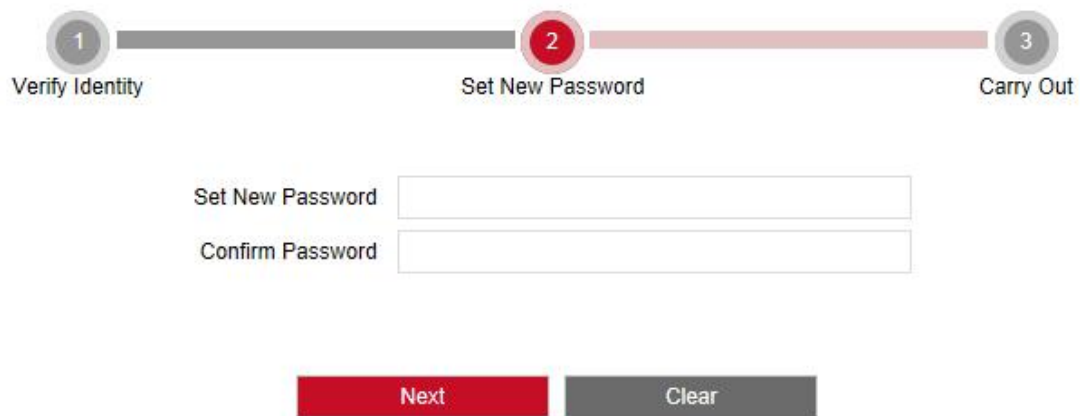


Figure 4-6 ② shows a three-step process for password reset. Step 1, 'Verify Identity', is completed. Step 2, 'Set New Password', is the current step and is highlighted with a red circle and a red bar. It contains two input fields: 'Set New Password' and 'Confirm Password'. Step 3, 'Carry Out', is also highlighted with a red circle. Below the input fields are two buttons: 'Next' (red) and 'Clear' (gray).

Figure 4-6 ②

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

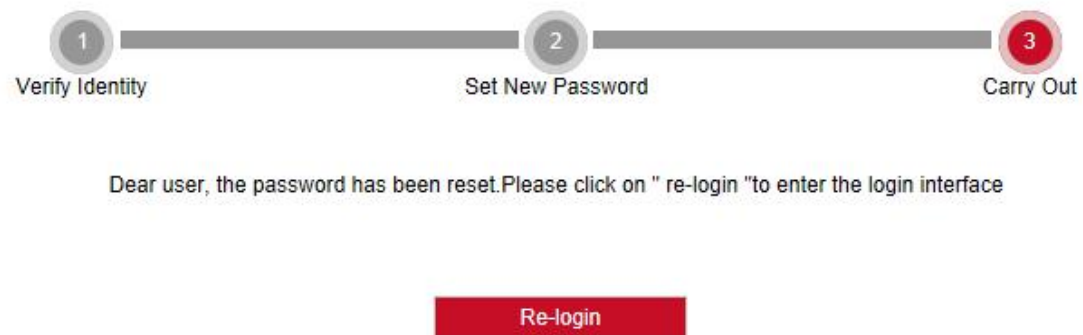


Figure 4-6 ③ shows the completion of the password reset process. The progress bar indicates that Step 3, 'Carry Out', is the current step and is highlighted with a red circle. Below the progress bar, a message reads: 'Dear user, the password has been reset. Please click on " re-login "to enter the login interface'. Below the message is a red button labeled 'Re-login'.

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 network camera main interface, you can click the upper right corner of the "  Logout " safe exit system.

4.3 Install the HsIPCctl Controls



NOTE

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

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

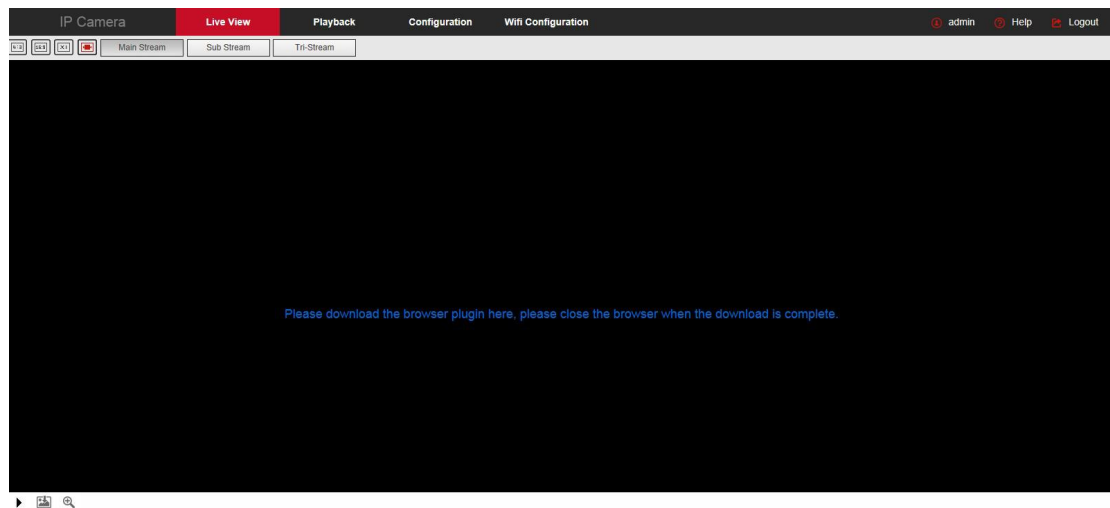


Figure 4-7

Click "Please download the browser plugin here, please close the browser when the download is complete." → "Run" → "Next" → "Next" → "Next" → "Next" → "Finish".

Follow the instructions in Figure 4-8 (①、②、③、④、⑤、⑥) to complete the installation:

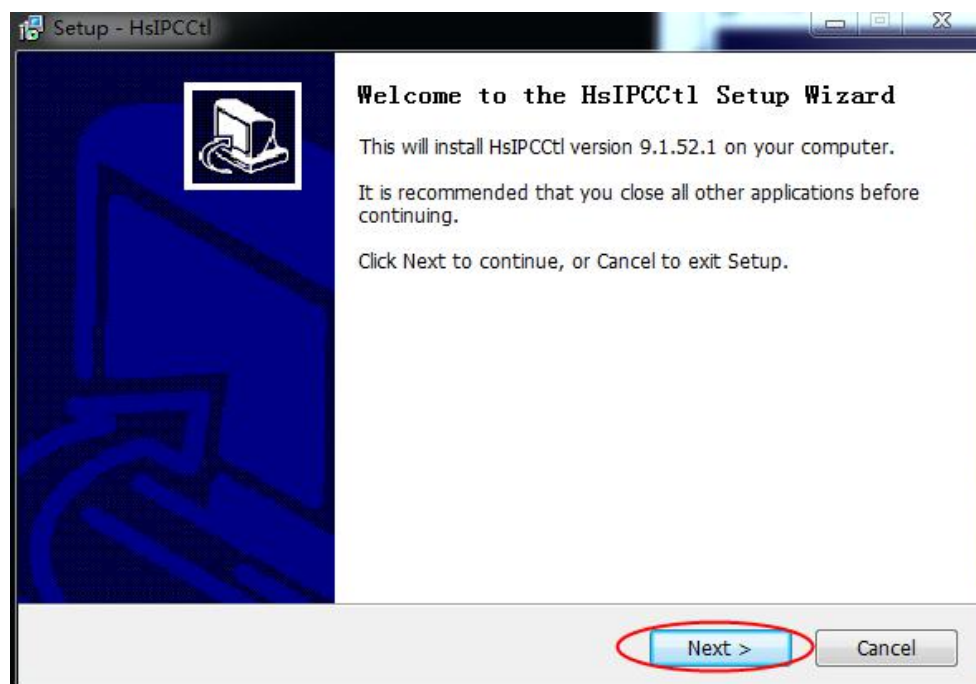


Figure 4-8 ①

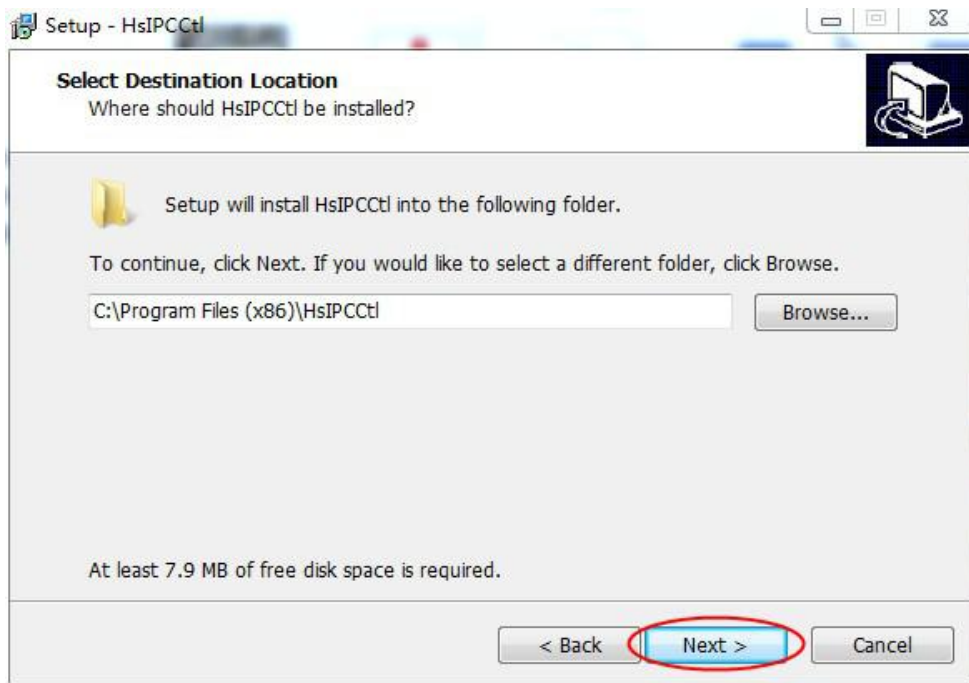


Figure 4-3 ②

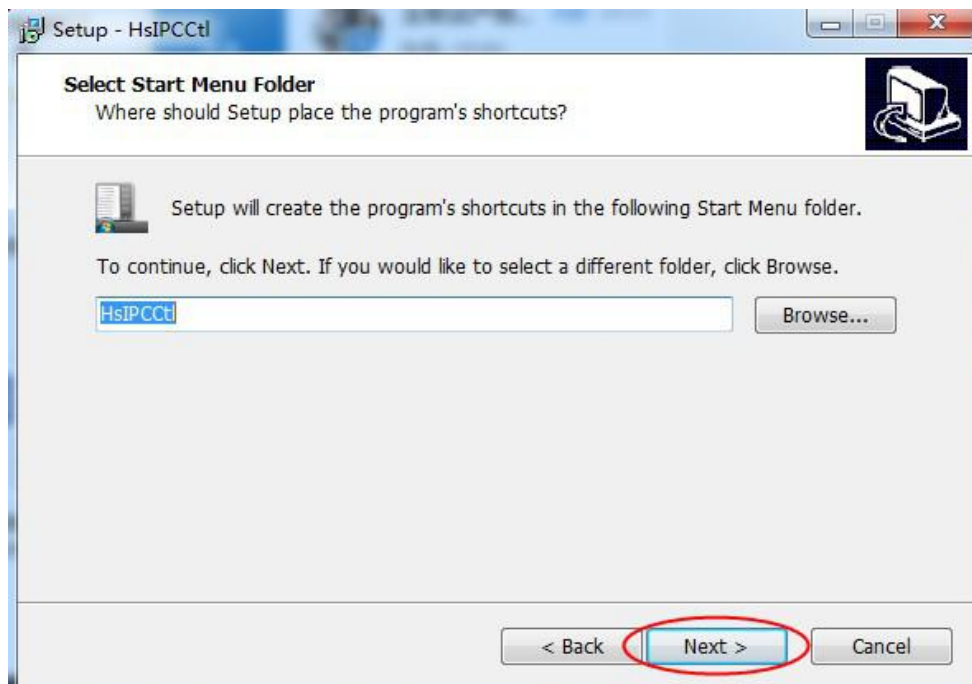


Figure 4-3 ③

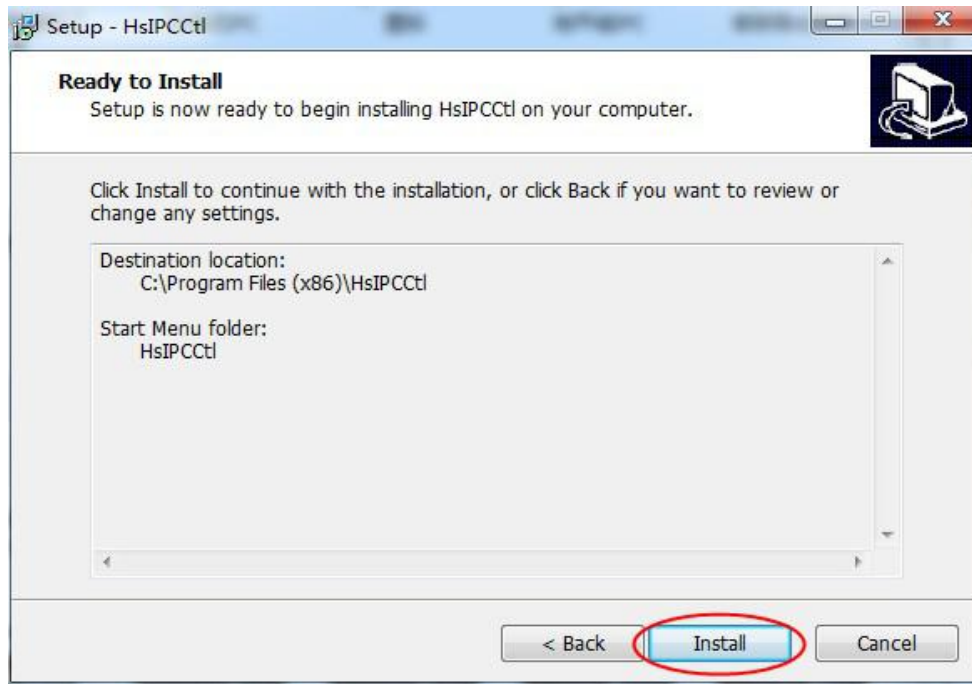


Figure 4-3 ④

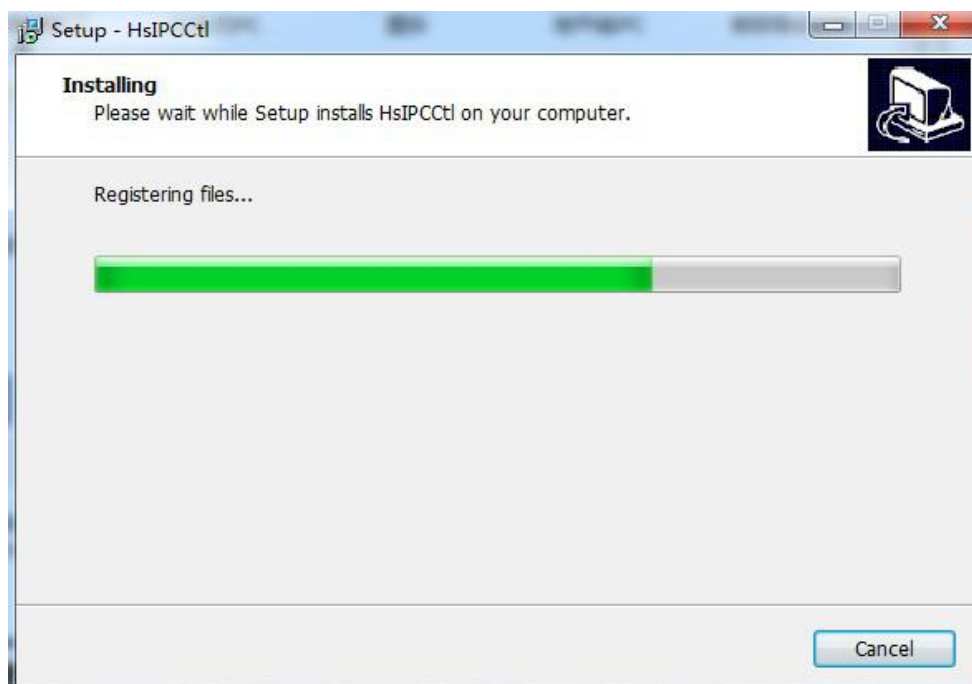


Figure 4-3 ⑤

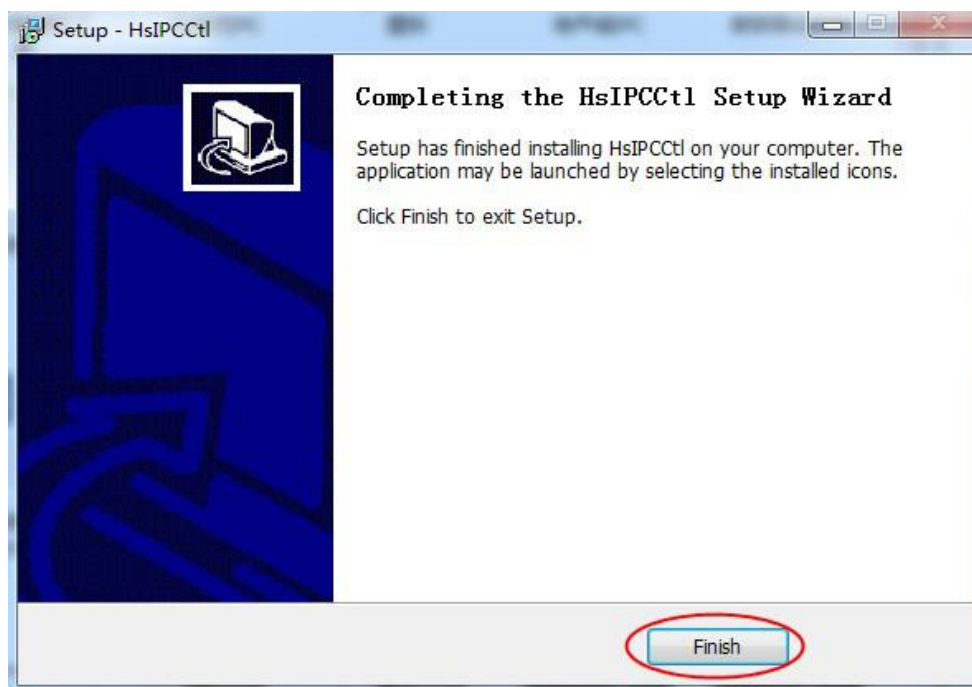


Figure 4-3 ⑥



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 HsIPCCtl after save settings.

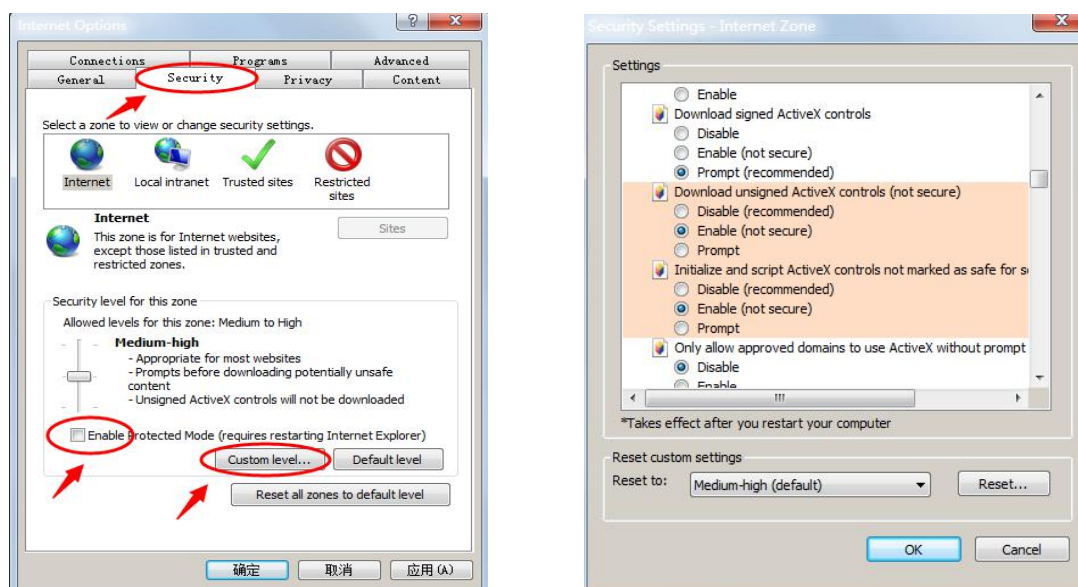


Figure 4-9

4.4 Main interface description

In the IPC main interface, you can preview real-time video, playback, configuration and PTZ control and other functions, the interface shown in Figure 4-10:

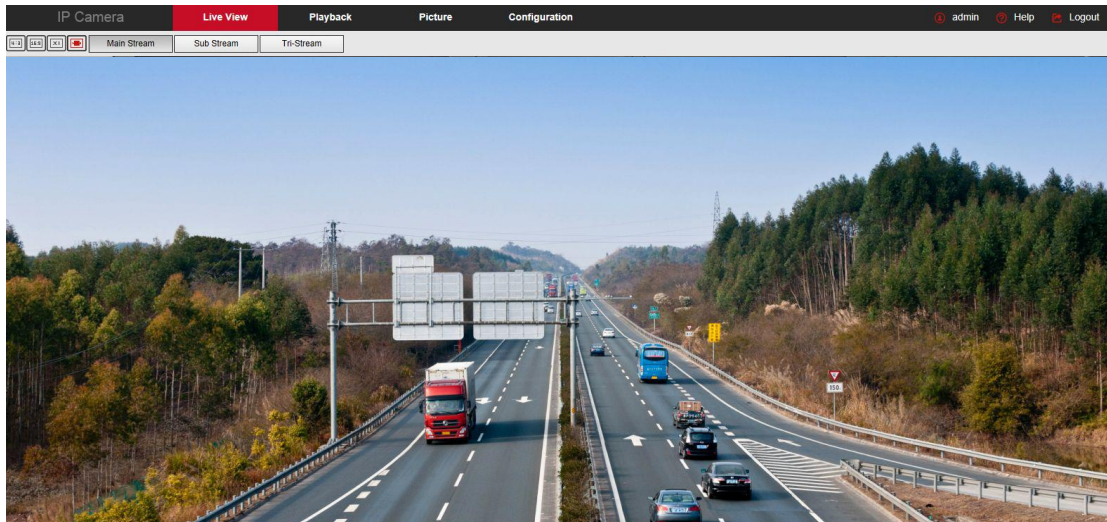


Figure 4-10

【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 network camera SD card.

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

【PTZ Control】 Used to set the PTZ preset point, cruise line and PTZ rotation direction preview real-time video and so on.



NOTE

- Network 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:

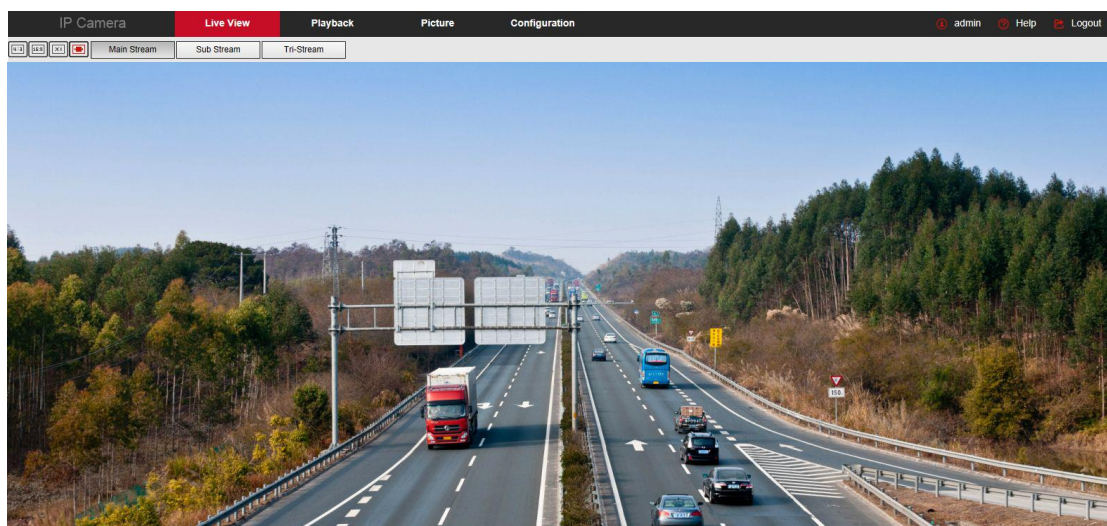


Figure 5-1

【switching window size】 In the real-time preview interface on the top left of the preview ratio option, click "4: 3", "16: 9", "X1", "full screen" to switch the video preview scale.

【switching option】 In the upper left of the real-time preview interface, there is a stream switching option. Click "Main Stream", "Sub Stream" and "Triple Stream" to switch preview video stream.

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

Icon	Description
	The window size is 4:3.
	The preview screen is displayed in its original size.
	The window size is 16:9.
	Self-adaptive window size.
Main Stream/Sub Stream/Tri-stream	To switch the real-time preview stream (the main stream is a high-definition stream, and the sub-stream is a standard definition stream) , take the actual function of the device.
	Start/Stop live view.
	Manually start/stop recording.

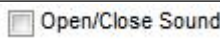
	Manually capture the picture.
	Turn on / off the electronic zoom function, turn on the electronic zoom function, in the preview image, hold down the left mouse button to select the electronic zoom area, the interface shows the region to enlarge the image
 Open/Close Sound	Turn on/off Sound.
	Open / Close talk back

Table 5-1

5.2 Camera settings PTZ, zoom, cruise

Click "<" on the right side of the window to display the PTZ control interface. Click ">" to hide the PTZ control interface, where you can set the direction of the PTZ rotation of the camera, Zoom in / out, focus - / focus +, one-key focus, lens initialization, cruise, as shown in Figure 5-2:

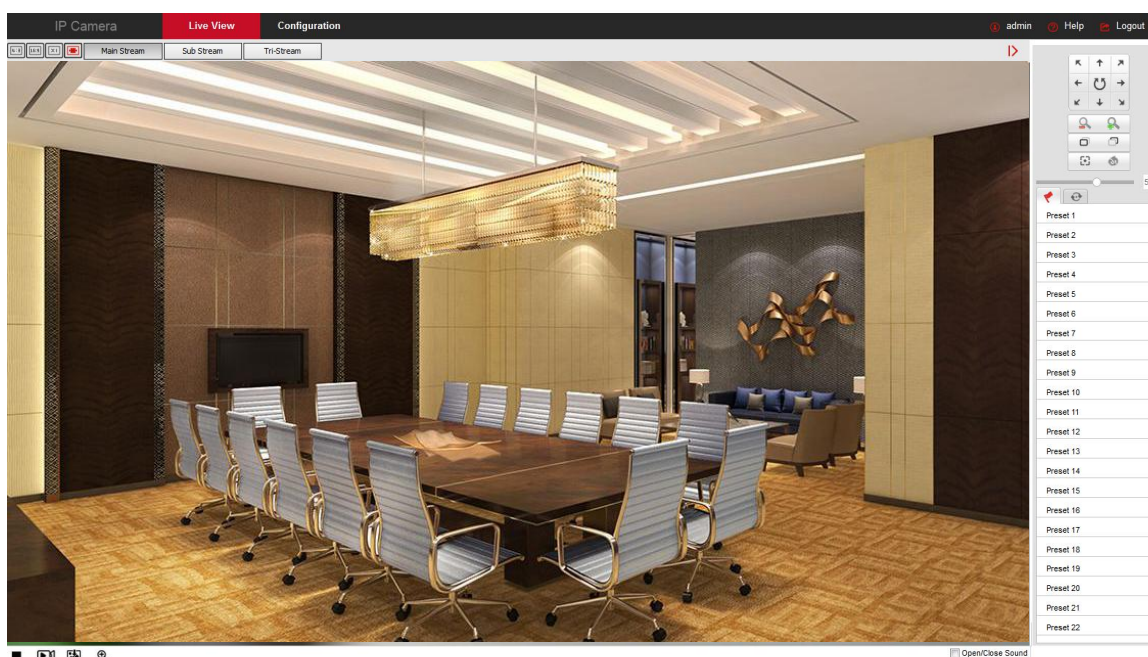


Figure 5-2

The PTZ control menu is shown in Figure 5-3 below:

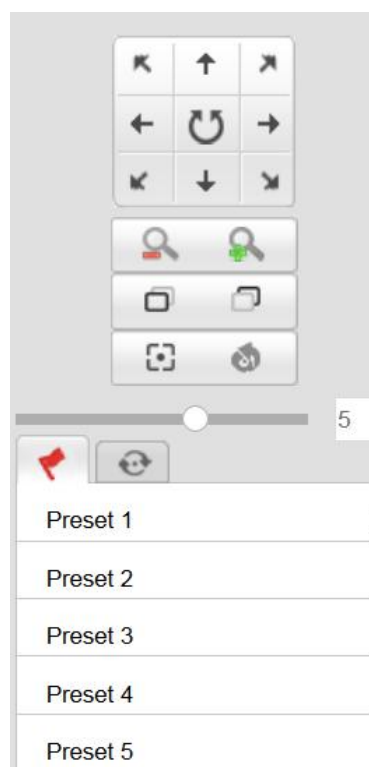


Figure 5-3

The PTZ control interface operation buttons are shown in Table 5-2 below.

按 钮	说 明
	Long press the arrow keys to control the horizontal and vertical direction, such as vertical rotation. (NOTE one of the bolt can only rotate horizontally, does not support vertical rotation). Click " ", the network camera will continue to rotate horizontally, then the button will turn red; then click once, then stop turning.
	"Zoom-" and "Zoom +". When you hold down the " ", the lens closer, the scene zoom; hold down the " ", the lens away, the scene becomes smaller.
	"Focus-" and "Focus +". In manual focus mode, adjust the " " and " " keys to make the objects within the scene clear.
	One Key Focus.
	Init Camera.
	Adjust the speed of rotation of the pan / tilt.

	Preset Click Preset to enter the Preset Settings menu and click the Presets icon to edit and recall the preset points. Select the preset number, click the "" button after the number, turn the preview channel image, make the image stay in a certain position; click "" button to call the preset point rotation; click "" button Clear the preset point.
	Cruise Click "Cruise" to enter the cruise settings menu, click the cruise icon area can be cruise editing and call. Select a cruise path, click the cruise path "" to enter the cruise path interface, select the preset point number, set the speed and time, click "OK", according to this method to add multiple preset points, and finally click "" Button to save, you can call the cruise line.

Table 5-2



NOTE

- Some cameras that support PTZ, Zoom, Preset, Cruise, etc. have a PTZ control button related interface. Please refer to the specific device.
- Zoom camera without cruise function; PTZ can only rotate horizontally, does not support vertical rotation.
- PTZ control function only supports the camera with PTZ function or PTZ camera, please refer to the actual function of the specific equipment.
- Up to 128 preset points are configured.
- A cruise line must set at least 2 preset points.
- "One Touch" and "Lens Initialization" are available for cameras equipped with an electric lens. Due to the limitation of the scene, the effect of the one-button focus function may not be as expected. In this case, it is recommended that you manually click the focus button to complete the focus operation. In the models with the electric lens can be PTZ speed adjustment to change the focus and zoom speed.
- Click the "one-click focus" to automatically complete the focus action, when the "one-click focus" appears difficult to focus clear case, click the "lens initialization", the lens parameters back to the initial position, click " You can focus clear.

Chapter 6 Playback

In the main interface, click “**Playback**” into the video playback interface. Playback interface can be stored in the camera SD card / 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 SD / 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 "normal video" or "alarm video", click "🔍" to find, meet the conditions of the video file will be on the right side of the calendar interface to select the red date (red date on behalf of the day of video), select the start time, Displayed on the timeline.

【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.

【Video cut】Video playback, click " ", start the current playback video to start recording, click " " again, will stop the video, the interface pops up the clip folder, which shows just the clip video.

【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:

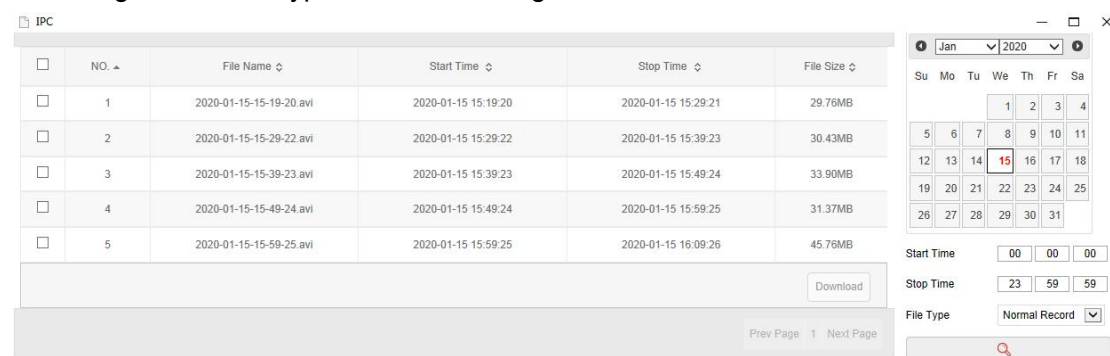


Figure 6-2

【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 SD card storage video camera and no video playback settings interface, please take the camera physical specific functions shall prevail.
- Before querying the video, please make sure that the SD card status in the device is "in use" and the 8.2.5 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**” in the main interface to enter the Picture interface. The picture interface can query and download the picture files stored in the camera SD card, as shown in Figure 7-1.

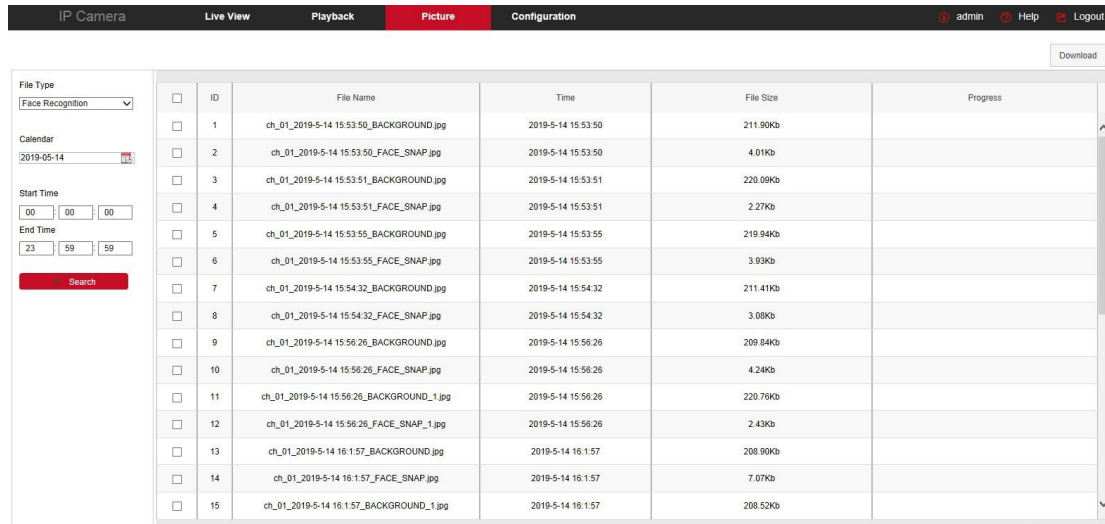


Figure 7-1

【Query】 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.

【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.



NOTE

- The picture is stored in the TF card of the device.

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", "Picture and Clip", "Log Export", "Online Upgrade", "Import / Export Param" storage path. Change the path by selecting Browse, as shown in Figure 8-1.

Local Configuration

Record File Settings		
Save record files to	C:\IPC\Record	Browse
Save downloaded files to	C:\IPC\DownloadFiles	Browse
Picture and Clip Settings		
Save capture files in live view to	C:\IPC\Capture	Browse
Save capture files when playback to	C:\IPC\PlaybackPics	Browse
Save clips to	C:\IPC\PlaybackFiles	Browse
Log export		
Log export save path	C:\IPC\LogSavaPath	Browse
Online Upgrade		
Upgrade package save path	C:\	Browse
Export param		
Export parameter path	C:\	Browse Export file
Import param		
Import parameter path		Browse Import file

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.

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

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

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

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

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

【Save clips to】Set the saving path of the clipped video files in playback mode.

【Log export】Set the storage path of the device log in the local computer to save the device log file.

- 【Log export save path】 Set the storage path for IPC export logs.
- 【Online Upgrade】Set the storage path of the device upgrade file on the local computer to save the file of the device online upgrade package.
- 【Upgrade package save path】 Set the storage path of the IPC online upgrade package.
- 【Export param】 Set device parameters in the computer's storage path, used to save the web-side device parameters of the file.
- 【Export parameter path】 Set the storage path for IPC export parameters.
- 【Import param】 Set device parameters in the computer's storage path, the file used to save the parameters of the web page egg device.
- 【Import parameter path】 Set the storage path for the IPC import parameters.

8.2 System

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

8.2.1 System Configuration

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

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 8-2:

Device Information

Time Settings

Dst

Maintenance

Basic Information

Device Name

IPC

Firmware Version

3516DV300_IMX335_AR_EM_THERMAL_BD_W_olute

Software Version

20.1.26.2

WEB Version

20.1.25.200623

Number of Channels

1

Figure 8-2

- 【Device Name】 The name of the current IPC.
- 【Firmware Version】 The current version of the IPC.
- 【Software Version】 The current HsIPCctl control version of the IPC.
- 【WEB Version】 The current page version of the IPC.
- 【Number of Channels】 The current channels of the IPC, the default is 1.

② 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 8-3.

Figure 8-3

【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 "Save" 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".

【NTP auto-time】 After it is enabled, IPC performs time synchronization with the SNTP server at the time interval.

【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 "Save" 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 "Save" 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.

③ 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 8-4.

The screenshot shows the 'DST' configuration page under the 'Time Settings' tab. It includes a 'Device Information' tab, a 'Time Settings' tab (active), a 'DST' tab (highlighted in red), and a 'Maintenance' tab. The 'DST' section contains a checkbox for 'Enable DST', which is currently unchecked. Below this are three rows of settings: 'Start Time' (Apr, First, Sun, 2), 'End Time' (Oct, The End, Sun, 2), and 'DST Bias' (30 minutes). A red 'Save' button is located at the bottom left.

Figure 8-4

④ Maintenance

In the System Configuration interface, click "Maintenance" to enter the system maintenance settings interface, where you can restart the device, restore factory settings, manual upgrade, online upgrade, as shown in Figure 8-5.

The screenshot shows the 'Maintenance' configuration page under the 'Time Settings' tab. It includes a 'Device Information' tab, a 'Time Settings' tab, a 'Dst' tab, and a 'Maintenance' tab (highlighted in red). The 'Maintenance' section contains several options: 'Reboot System' (with a 'Reboot' button), 'Default' (with 'Simple recovery' and 'Full recovery' buttons), 'Upgrade' (with a 'Firmware' input field, 'Browse' button, and 'Upgrade' button), and 'Online Upgrade' (with a 'Current Version' input field, 'Check' button, and 'Progress' bar). A note at the bottom states: 'The upgrade process will take about 1-8 minutes, please do not turn off the power, The device reboots automatically after upgrading.'

Figure 8-5

【Reboot System】 The IPC will restart again automatically after clicking "Reboot System".

【Default】 Divided into Simple recovery and Full recovery.

After clicking “Simple recovery”, IPC will automatically restore the parameters to the factory parameters except the network parameters.

After clicking "Full recovery", all parameter settings of IPC will be automatically restored to the factory parameter settings (please operate this function carefully).

【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.

8.2.2 Scheduled Reboot

In the main interface, click "Configuration → System → Schedule Reboot" 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 "Save", IPC will be at 3 o'clock on the 3rd 3 times a reboot. As shown in Figure 8-6.

Scheduled Reboot

Monthly Day Hour Minute

Save

Figure 8-6

8.2.3 Log Search

In the main interface click on the "Configuration → System → Log Search" into the log search interface, where you can query the device login, account number, alarm and all other relevant information. As shown in Figure 8-7.

Log Search

ID ▲	Time ↕	Detail ↕
1	2020-06-18 20:32:36	Private : index 0: 2 index 1: 2 index 2: 2 Rtsp : index 0: 0 index 1: 0 index 2: 0
2	2020-06-18 20:17:45	Set Time
3	2020-06-18 19:44:34	Set Time
4	2020-06-18 19:44:32	Set Time
5	2020-06-18 19:02:43	Set Time
6	2020-06-18 18:13:13	Set Time
7	2020-06-18 18:13:03	Set Time
8	2020-06-18 18:12:55	Set Time
9	2020-06-18 18:12:45	Set Time
10	2020-06-18 18:12:30	Set Time
11	2020-06-18 18:12:21	Set Time
12	2020-06-18 18:12:09	Set Time
13	2020-06-18 18:12:00	Set Time
14	2020-06-18 18:11:51	Set Time
15	2020-06-18 18:11:33	Set Time
16	2020-06-18 18:11:18	Set Time
17	2020-06-18 18:11:09	Set Time
18	2020-06-18 18:11:00	Set Time

Start Time :

2020-06-18 00:00:00

End Time:

2020-06-18 23:59:59

Search

Clear

Log export

Figure 8-7

【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.

【Log export】 Save the contents of the current log to the location you specified in txt format.

8.2.4 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 8-8.

User Management

User Name	Competence	Edit	Delete
admin	Admin	Edit	

Add User

Figure 8-8

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 8-9.

Users to edit ×

User Name

Alen

User Type

Operator

▼

Password

••••••••

Confirm Password

••••••••

OK

Cancel

Figure 8-9



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 network camera is used in a high security risk environment, it is recommended to update once a month or every week.
 - It is recommended that the system administrator manage the user effectively, remove the unrelated user and shut down the unnecessary network port.
-



NOTE

- The admin user cannot be deleted and you can only change the *admin* password.
- User permission description:
 - Administrator** -- all permissions.
 - Operator** -- All permissions (cannot make system security parameter settings).
 - Viewer** -- only preview permission.
- When setting the network 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 "Save" 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, check "Modify Password", and enter a new password in the Password and Confirm Password fields;

Step 3: Click "Save" 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 Storage

8.3.1 Plan configuration

① Rec Setup

The specific operation steps are as follows:

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

Rec Setup

Screenshot

☐ Enable Record

StreamType

Main Stream

Video Type

Normal Record

Advanced parameters

Del All

Select All

Sun	00	02	04	06	08	10	12	14	16	18	20	22	24
Mon	00	02	04	06	08	10	12	14	16	18	20	22	24
Tue	00	02	04	06	08	10	12	14	16	18	20	22	24
Wed	00	02	04	06	08	10	12	14	16	18	20	22	24
Thu	00	02	04	06	08	10	12	14	16	18	20	22	24
Fri	00	02	04	06	08	10	12	14	16	18	20	22	24
Sat	00	02	04	06	08	10	12	14	16	18	20	22	24

Normal Record
Motion Detection
alarm
Motion detection and alarm

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, Alarm, Motion detection and alarm).etc.

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 "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.

Step 4: Repeat **step 3** to set up a complete recording plan.

Step 5: Click "Save" 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.
- Tick "Select all" to enable 24 hours of daily video recording throughout the week. .
- No SD card video recording function of the camera No SD card management

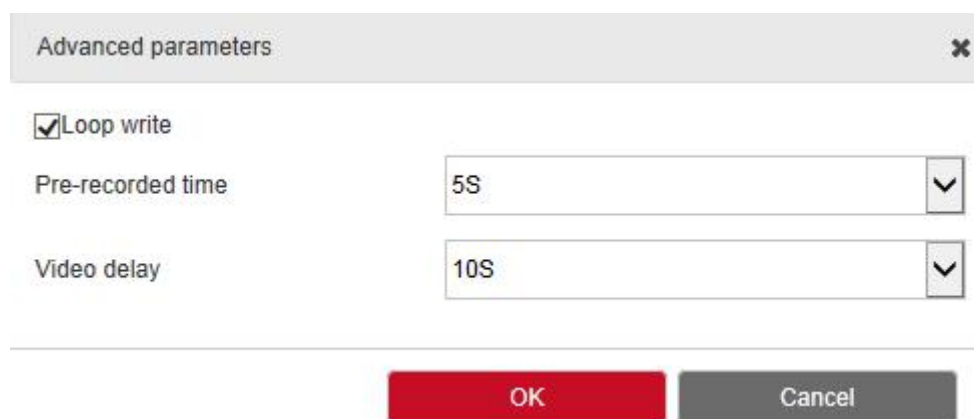
interface, please take the camera physical specific functions shall prevail.

- When the video type selects motion detection, alarm, motion detection and alarm, the device will also perform scheduled recording while recording the selected recording type.

【Stream Type】 Select to set the stream type of recording, including Main Stream, Sub Stream, Tri-Stream.

【Video Type】 Including Normal Record, Motion Detection, Alarm, Motion detection and alarm.

【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.



Advanced parameters

☒ Loop write

Pre-recorded time 5S

Video delay 10S

OK Cancel

Figure 8-10 ②



NOTE

- 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 relevant parameters such as the image format, resolution, capture interval, number and other parameters when the camera takes a picture.

The specific operation steps are as follows:

Step 1: In the main interface, click "Configuration → Storage → Plan configuration → Screenshot" to enter the screenshot parameter setting interface, as shown in Figure 8-11.

Rec Setup

Screenshot

Snapshot parameters

Event trigger

☒ Enable event snapshot

Image Format

JPEG

Resolution

1920*1080

Capture interval

10S

Number of screenshots

1

Save

Figure 8-11

Step 2: To enable event snapshot, select the image format, resolution, snapshot interval, and number of snapshots through the drop-down box.

Step 3: Click "Save" to complete the configuration.

8.3.2 Storage management

① Storage

In the main interface, click "Configuration → Storage → Storage management → Storage" to enter the SD Card management settings interface, here you can view the SD card related information and format the SD card as shown in Figure 8-12:

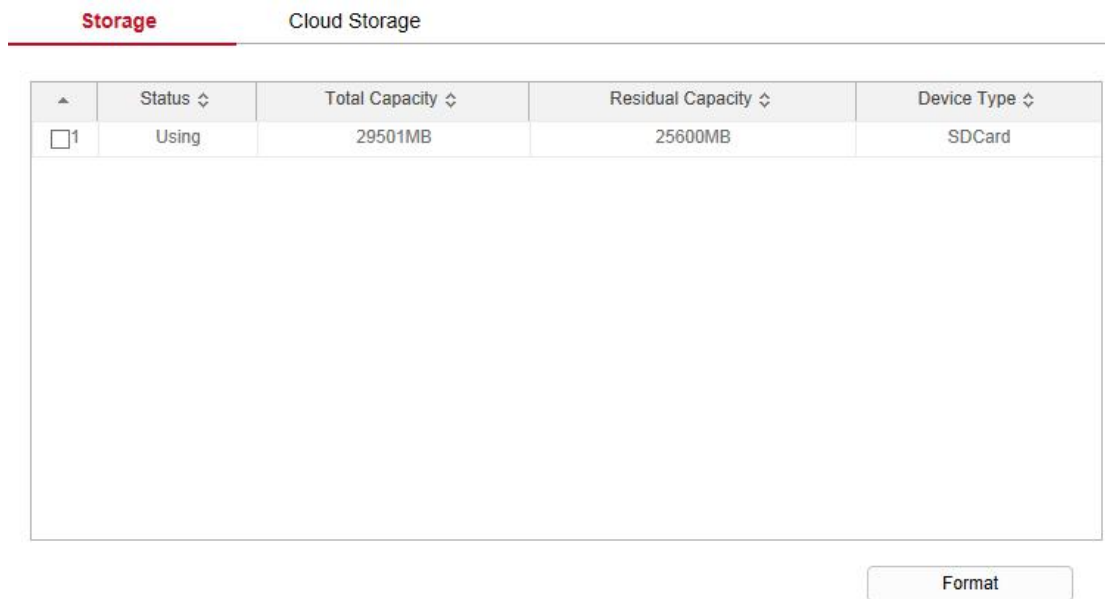


Figure 8-12

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.

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 or Dropbox 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.

Storage

Cloud Storage

Cloud

Cloud Storage Type

None

▼

Unbound

Web

Auth Code

User Name

Total Capacity

Used Capacity

Bind

IPEYE

☐ IPEYE enable

Save

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".

【Cloud Storage Type】 Select the cloud storage type, Dropbox or Google in the drop-down menu.

【Web】 Depending on the type of cloud storage selection play a cloud url, login web site registered account according to clew clouds.

【Auth Code】 Login cloud web, the verification code will display on the cloud storage interface, than copy it in the space.

Fill in the verification code, click on the "Bind" after the success. "User name", "Total Capacity" and "Used Capacity" that information will be automatically displayed.

■ IPEYE

In the main interface, click "Configuration → Storage → Storage management → Cloud" 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 8-14 ①.



IPEYE

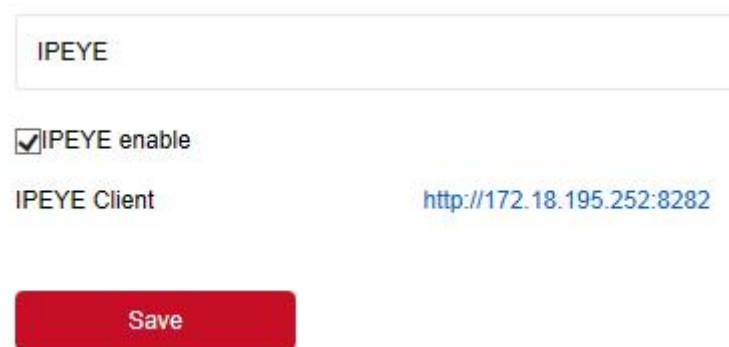
☐ IPEYE enable

Save

Figure 8-14 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 8-14 ②.



IPEYE

☒ IPEYE enable

IPEYE Client <http://172.18.195.252:8282>

Save

Figure 8-14 ②

Step 2: Log in to IPEYE Client "<http://182.18.195.252:8282>", enter IPEYE login account & password, IPC user name & password, click "Confirm" to add the device, as shown in

Figure 8-14 ③.

Добавление камеры в облако

Логин от облака

Для регистрации в облаке перейдите по ссылке <https://ipeye.ru>.

Пароль от облака

Логин от камеры

Пароль от камеры

Добавить в Облако

© IPEYE Company, Inc.

Figure 8-14 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 8-14 ④.

Name	Group	Tariff	Bitrate	Viewers	Options	Action
198.205	No group	Бесплатный	0 kbit/s	0		
cloud_108950	No group	Бесплатный	0 kbit/s	0		
cloud_188.205	No group	Бесплатный	0 kbit/s	0		
cloud_91056	No group	Бесплатный	0 kbit/s	0		

Figure 8-14 ④



NOTE:

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

8.4 Network

8.4.1 Basic Setup

① TCP/IP

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

Enable DHCP:

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

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

Step 1: In the main interface, click "Configuration → Network → Basic Setup → TCP / IP" to enter the TCP / IP interface, as shown in Figure 8-15.

TCP/IP Port

NIC Settings

☐ DHCP

IPv4 Address 172.18.195.252 ✓ Test

IPv4 Subnet Mask 255.255.248.0 ✓

IPv4 Default Gateway 172.18.192.1 ✓

DNS Server

Preferred DNS Server 172.18.192.1 ✓

Save

Figure 8-15

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 "Save" to save the configuration.

② Port

In the main interface, click "Configuration → Network → Basic Setup → Port" to enter the port setting 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 8-16.

TCP/IP
Port

Port

HTTP Port	80
RTSP Port	554
HTTPS Port	443
BITVISION Port	6000

Protocol Port

ONVIF Port	8999	☒ ONVIF Protocol Enable
------------	------	---

Save

Figure 8-16

【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.

8.4.2 Advance Setup

In the main interface click on the "configuration → Network → Advance Setup" to enter the advanced configuration interface, where you can set the device DDNS, FTP, SMTP, P2P, PPPOE and other functions.

① 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 → Advance Setup → DDNS" to enter the DDNS function settings interface, as shown in Figure 8-17:

DDNS

FTP

SMTP

DDNS

☐ DDNS

DDNS Type

Oray

Site Name

DDNS User

DDNS Password

Confirm Password

Status

Login failed

Service Type

Ordinary User

Links to service providers

Oray DDNS to apply

Oray DDNS to help

Save

Figure 8-17

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

Steps 3: Click "Save" 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 and Dyn three 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.

② 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 → Advance Setup → FTP" to enter the FTP server settings interface, as shown in Figure 8-18.

DDNS **FTP** SMTP P2P

FTP

FTP Server 192.168.1.1 Test

Port 21

User Name admin ☐ Anonymous

Password •••••

Confirm Password •••••

FileUpload Default_Folder

☐ AutoCover

Upload Via FTP JPEG

Save

Figure 8-18

Step 2: Enter the server address, port, user name, password, password, file upload path, check "Auto Cover", and select to upload the FTP server file format AVI or JPEG.

Step 3: Click "Save" 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.

【File Upload】 Automatically creates a folder that you named in the FTP storage path.

【Auto Cover】 When enabled, the oldest FTP server will be overwritten automatically when the FTP server is full.

【Upload Via FTP】 In the drop-down menu, select FTP file format, JPEG image format and AVI video for selection. Click on the "Save" after completing the settings.

③ SMTP

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 → Advance Setup → SMTP" to enter the mail settings interface, as shown in Figure 8-19.

DDNS	FTP	SMTP	P2P									
Sender Sender User@domain.com SMTP Server SMTP.domain.com Port 25 Upload Via SMTP MESSAGE ▼ ☐ My Server Requires Authentication User Name User@domain.com Password •••••••• Confirm Password ••••••••												
Receiver <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Email1</td> <td style="width: 40%; border: 1px solid #ccc; padding: 2px;">User@domain.com</td> <td style="width: 30%; border: 1px solid #ccc; text-align: center; padding: 2px;">Test</td> </tr> <tr> <td>Email2</td> <td style="border: 1px solid #ccc; padding: 2px;"></td> <td style="border: 1px solid #ccc; text-align: center; padding: 2px;">Test</td> </tr> <tr> <td>Email3</td> <td style="border: 1px solid #ccc; padding: 2px;"></td> <td style="border: 1px solid #ccc; text-align: center; padding: 2px;">Test</td> </tr> </table> Save				Email1	User@domain.com	Test	Email2		Test	Email3		Test
Email1	User@domain.com	Test										
Email2		Test										
Email3		Test										

Figure 8-19

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 "Save" to save the configuration.

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.

【Alarm Duration】 Set the sending interval.

【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.

④ 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.



Instruction

- 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 → Advance Setup → P2P" to enter the P2P settings interface, as shown in Figure 8-20.

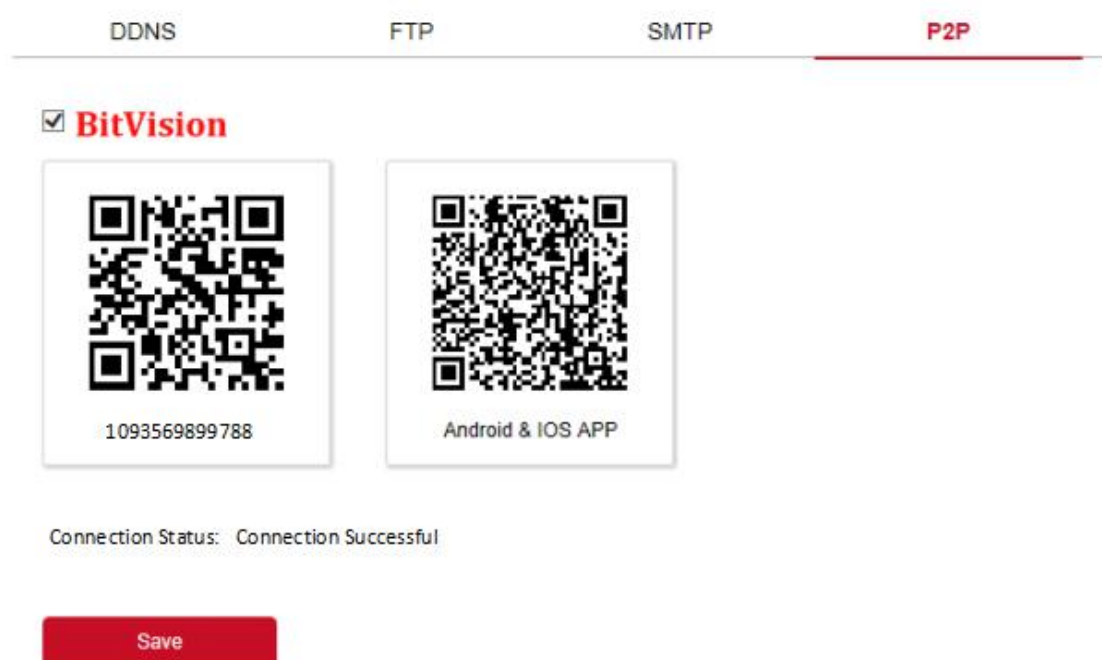


Figure 8-20

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

Step 3: Click "Save" 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.

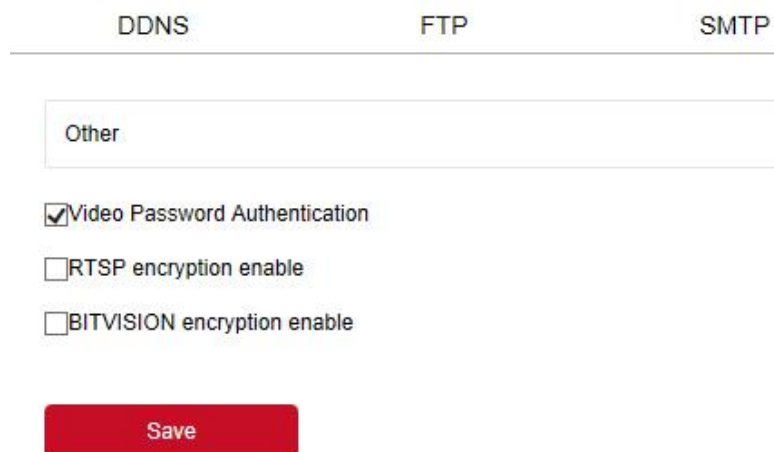
After login, click "Device manage",  and  "Add device", select "SN Add", enter the device user name, password and verification code after scan the QR code (the verification code printed on the label), click "Add" to set device NOTE and group, click "Send" after add successfully.

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".

⑤ Other

In the main interface, click "Configuration → Network → Advance Setup → Other" to enter the Video Password Authentication interface, as shown in Figure 8-21.



DDNS	FTP	SMTP
Other		
☒ Video Password Authentication		
☐ RTSP encryption enable		
☐ BITVISION encryption enable		
Save		

Figure 8-21

【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.

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

【BITVISION encryption enable】 When enabled, encrypts the stream between the camera and the BitVision App.

⑥ 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 → Advance Setup → PPPOE" to enter PPPOE to set the interface, as shown in Figure 8-22.

The screenshot shows a web-based configuration interface. At the top, there are three tabs: 'DDNS', 'FTP', and 'SMTP'. Below these tabs is a section titled 'PPPOE'. Inside this section, there is a checkbox labeled 'PPPOE'. Below the checkbox, there are four input fields: 'Device Dynamic IP' (containing '0.0.0.0'), 'User Name', 'Password', and 'Confirm Password' (all containing masked text represented by asterisks). At the bottom of the section is a red button labeled 'Save'.

Figure 8-22

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.

⑦ Wifi

In the main interface, click "Configuration → Network → Advance Setup → Wifi" to enter the Wifi configuration interface. Here you can configure the camera to connect the Wifi to the camera, as shown in Figure 8-23.

Wifi

Scan

	SSID ▲	Encryption ◆	Signal Strength ◆	channel ◆
☐	04wifi	WPA-PSK	94	1
☐	111111	WPA-PSK	83	6
☐	360免费WiFi-6K	WPA-PSK	99	6
☐	360免费WiFi-7Z	WPA-PSK	78	8
☐	666	WPA-PSK	89	11
☐	@PHICOMM_E9	WPA-PSK	94	9
☐	Aoty	WPA-PSK	57	11
☐	APC-201909031050	WPA-PSK	57	11
☐	CMCC-g3xF	WPA-PSK	78	11
☐	CMCC-Rk7d	WPA-PSK	68	9

Wireless Wifi Management

Wireless Wifi Management

SSID ▲	Encryption	Connect	Delete ◆
PM1	WPA-PSK	☒	☒
VPN_TEST	WPA-PSK	☒	☒

Status	Connection succeeded
SSID	VPN_TEST
Key	••••••••
Encryption	WPA-PSK 
☒ DHCP	
IP Address	192.168.199.178
Netmask	255.255.255.0
Default Gateway	192.168.199.1
Preferred DNS Server	8.8.8.8



Figure 8-23

【Wireless Wifi Management】Wifi IPC can remember the accounts that have been connected to Wifi, and make the device connect or delete the Wifi account through wireless Wifi management.

IPC Wifi configuration steps are as follows:

Step 1: Click the "Scan" button to search for nearby WiFi hotspots;

Step 2: Select to connect to WiFi, enter the WiFi password in the Key field;

Step 3: Turn on "Enable DHCP" and click "Save".



NOTE

- Only cameras that support the wifi function have a wifi interface. Please refer to the specific function of the camera.
- Also can not open the DHCP, manual input and choose the same WiFi network segment of the preferred DNS server IP address, default gateway, set the camera Wifi network information.
- Wifi IPC can remember up to 3 connected Wifi accounts.

⑧ WIFI Access Point

In the main interface, click "Configuration → Network → Advance Setup → WIFI Access Point" to enter the WIFI Access Point interface. The WiFi hotspot of the camera can be turned on and set. After setting, the device such as the mobile phone can connect to the hotspot to access the IPC. The WIFI Access Point interface is shown in Figure 8-24.

DDNS	FTP	SMTP	P2P	Cloud	Other	Wifi	WIFI AccessPoint
WIFI AccessPoint							
Wireless Mode	accessPoint						
ApEssid							
ApPsk							
ApMode	802.11n						
80211nChannel	auto						
EssId Enabled	☐ Open ☒ Shut Down						
WpaMode	WPA2						
Wlan0 StaticIP	192.168.0.1						
Wlan0 StaticNetmask	255.255.255.0						
Wlan0 StaticGateway	192.168.0.1						
DHCP	☐ Open ☒ Shut Down						
DHCP First IP	192.168.0.2						
DHCP IP Range	20						
DNS	192.168.0.1						
DHCP Gateway	192.168.0.1						
Save							

Figure 8-24

The steps to turn on and set the camera wifi hotspot are as follows:

Step 1: Select "access Point" in the Wireless Mode field;

Step 2: Set the AP ESSID, AP Psk, 80211nChannel, EssId Enabled switch, WpaMode, wireless IP, subnet mask, and wireless gateway address.

Step 3: Click "Save" to complete the setup.



NOTE

- Only cameras that support the wifi hotspot function have a WIFI hotspot interface. Please refer to the specific function of the camera.
- When configuring the camera WIFI hotspot, you can also enable DHCP and manually enter the starting address, assigned number, DNS address and gateway information.

⑨ PTZ

In the main interface, click "Configure → Network → Advance Setup → PTZ" to enter the PTZ configuration interface, as shown in Figure 8-25.

DDNS	FTP	SMTP	P2P	Cloud
PTZ				
Protocol	peleo D			
Address	1			
Baud Rate	2400			
Data bits	8			
Stop bits	1			
Check	NO			
Save				

Figure 8-25



NOTE

- Only PTZ-enabled cameras have a PTZ interface. Please refer to the actual camera function.

⑩ RS485

In the main interface, click "Configure → Network → Advance Setup → RS485" to enter the RS485 configuration interface, as shown in Figure 8-26. By configuring the parameters of the RS485 serial port for interface configuration, please set the baud rate, data bit and other information of the interface according to the actual environment.

DDNS	FTP	SMTP	P2P	Cloud
Communication baud rate	2400			
Verification method	No			
Data bits	8			
Stop bits	1			
Save				

Figure 8-26



NOTE

- RS485 depends on the model, please refer to the actual equipment.

8.5 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.

8.5.1 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 8-27.

The screenshot shows a web-based configuration interface for video settings. At the top, there is a red header with the word "Video" in white. Below the header, there is a list of configuration items, each with a label on the left and a corresponding input field on the right. The input fields are mostly dropdown menus, except for "Bit Rate" and "Watermark name" which are text boxes. At the bottom left, there is a red "Save" button.

Parameter	Value
StreamType	Main Stream
Profile	Main Profile
Video Encoding	H.264
Resolution	1920x1080
Framerate	25 fps
Bit Rate	3072
Rate Control	VBR
I-Frame Interval	75
H264+	Off
Watermark	Off
Watermark name	

Save

Figure 8-27

【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.
- When the frame rate is set too low, it will cause video carton, please be careful.
- The higher the bit rate, the greater the current network bandwidth and the greater the transmission pressure.
- Only cameras that support the H264+/H265+ function display H264+/H265+ on/off items on the video interface.
- When the camera turns the H265+/H264+ on or off, it takes 30-60 seconds. Please be patient.

8.5.2 Audio

In the main interface, click "Configuration → Video → 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 8-28.

Audio Configuration

☐ Audio enable

Audio input

LINE Input

Audio Output

External

Audio Encode

G711U

Volume

Input volume

50

output volume

50

Save

Figure 8-28

【Audio Enable】 Turn on / off device audio input.

【Audio Input】 Select the audio input method.

- 【Audio Output】 Select the audio output method.
- 【Audio Encode】 Choose audio encoding, G711U/ G711A /AAC.
- 【Input Volume】 Set the device input volume.
- 【Output Volume】 Set the device output volume.

8.6 Image

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

8.6.1 Image

In the main interface, click "Configuration → Image → Image" to enter the image configuration interface, where you can adjust the related image parameters such as Image Adjustment, Exposure Settings, Focus, BackLight Settings, Day and night switch, White Balance, Video Adjustment, Image Enhancement, Defog Mode, Distortion, and Image rotation as shown in Figure 8-29.

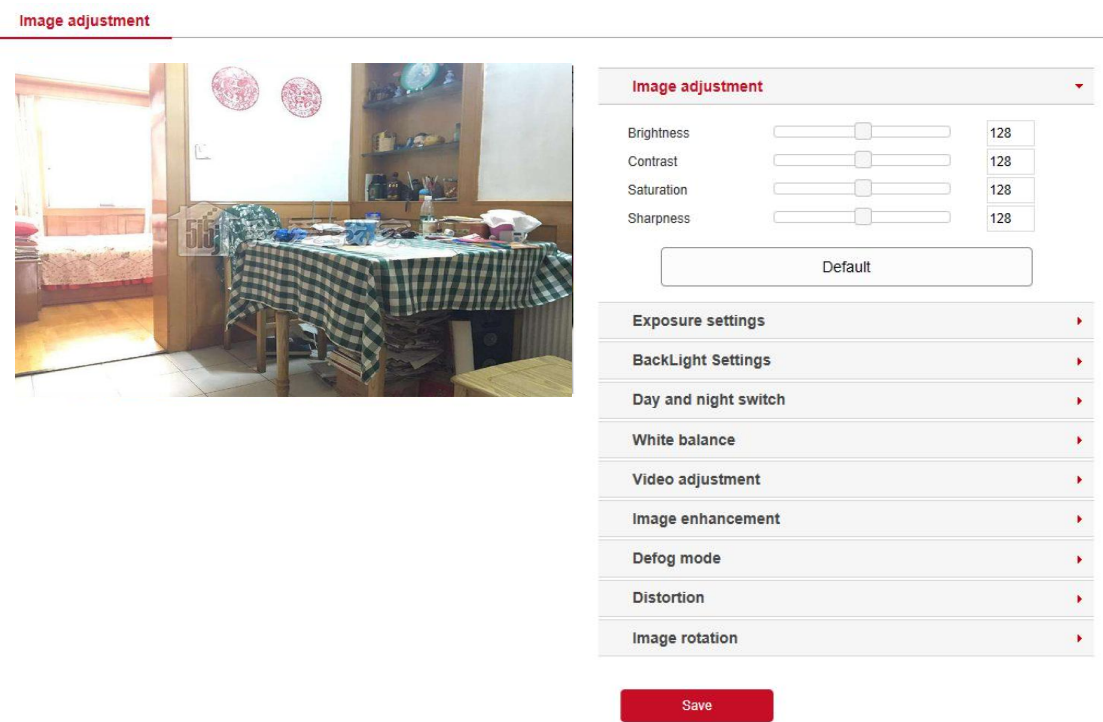


Figure 8-29

【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 8-30.

Image adjustment

Brightness	<input type="range"/>	128
Contrast	<input type="range"/>	128
Saturation	<input type="range"/>	128
Sharpness	<input type="range"/>	128

Default

Figure 8-30

【Exposure settings】 The default is automatic exposure, according to the actual need to switch the manual exposure mode, select "Manual", the Exposure Time and Gain Control is activated, click "Save". As shown in Figure 8-31

Exposure settings

Exposure settings ☒ Auto ☐ Manual

Exposure time

Automatic gain ☒

Gain Control 128

Figure 8-31

【Focus】 It is used to select the focus mode of the zoom camera. The default is "semi-autofocus", and "Automatic" focus and "Manual" focus can also be selected, as shown in Figure 8-32..

Focus

Focus mode

Figure 8-32

【BackLight Settings】 It is used to set backlight compensation and strong light suppression. The default is off, it can be turned on manually, and the backlight, strong light suppression intensity and dark area boost strength can be set, as shown in Figure 8-33.

BackLight Settings

Back light compensation

☒ Off
☐ On

Backlight

min

Strong light suppression

☒ Off
☐ On

Strong light suppression intensity

0

Dark area boost strength

0

Figure8-33

【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 8-34 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.

Day and night switch

Fill light mode

Automatic

Sensitivity

3

Filter time

3

Light mode

☐ Auto
☒ Manual

light brightness

100

Figure 8-34 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 8-34 ②.

Day and night switch

Fill light mode

Time

6

:

30

18

:

0

light brightness

70

Figure 8-34 ②

- When the fill mode is "Daytime", the device monitor video is lighted into a daytime effect.
- When the fill mode is "Night", the device monitor video is added to the night effect.

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, Fluorescent Lamp, Incandescent, Warm Light, Natural Light. As shown in Figure 8-35.

White balance

Auto

Red gain

128

Green gain

128

Blue gain

128

Figure 8-35

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

【Video adjustment】 Here you can turn on and set 2D or 3D digital noise reduction, as shown in Figure 8-36.

Video adjustment

DNR model

Off

2D DNR

32

3D DNR

32

Figure 8-36

【Image enhancement】 Including flicker control, wide dynamic switch, HDR, as shown in Figure 8-37.

Image enhancement

Flicker control: PAL(50HZ)

Sensor linear WDR: Shut Down

Figure 8-37

Flicker control: The flash mode is selected according to the camera installation environment and the flicker standard. The default setting is PAL (50HZ) shipment.

Sensor linear WDR: The default is Shut Down, you can switch in the drop-down menu Automatic, Weak, Moderate, Strong, Super.

【Defog mode】 Used to set the defog mode and strength, as shown in Figure 8-38.

Defog mode

Defog mode: Off

Defog strength: 0

Figure 8-38

Defog Mode: The default is off, you can choose from the drop-down menu to On or Auto.

Defog Strength: The default is 0, when the fog mode is open, you can set the fog strength, can be set to a value range of 0-255.

【Distortion】 Used to set image distortion correction, as shown in Figure 8-39.

Distortion

Distortion mode: Off

Distortion intensity: 128

Figure 8-39

Distortion mode: The default is Off. You can select On from the drop-down menu.

Distortion intensity: The default is 128. When the distortion mode is on, the distortion correction strength can be set, and the value range can be set from 0-255.

【Image rotation】 Used to set image mirroring and corridor pattern, as shown in Figure 8-40.

Image rotation

Mirroring: Off

Corridor Pattern: Off

Figure 8-40

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.



NOTE

- The camera image interface only displays the device support functions. The specific interface is subject to the actual product.

8.6.2 OSD

The OSD is information displayed on the real-time monitoring screen. The name, date, and day of the IPC can be displayed on the monitor screen.

In the main interface, click "Configuration → Image → OSD" to enter the OSD configuration interface, where you can set the preview interface to display menu time, OSD text and other information, as shown in Figure 8-41.

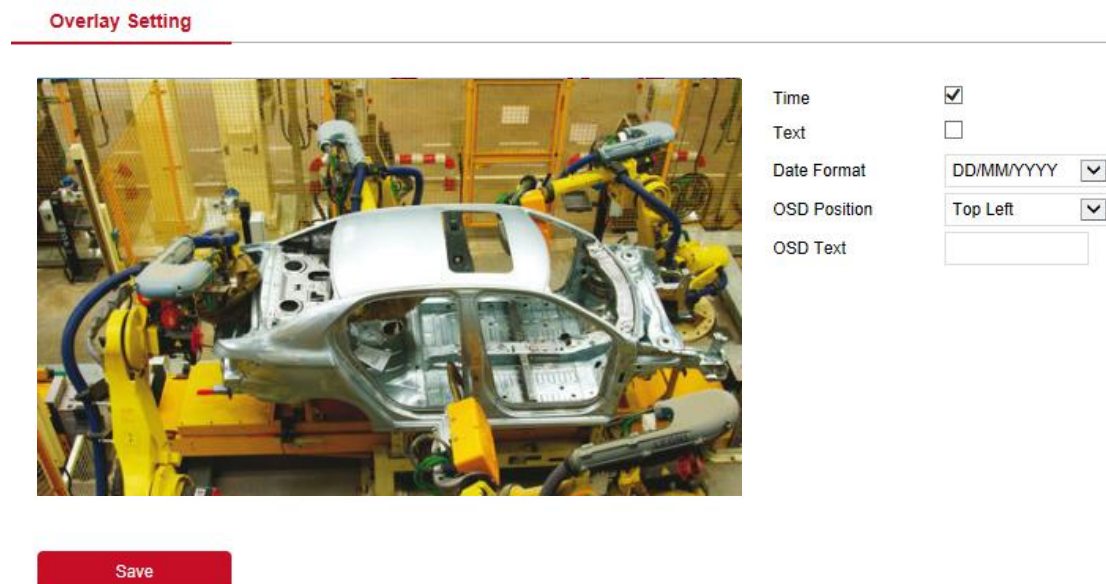


Figure 8-41

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

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

【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.

8.7 Events

In the main interface, click "Configuration → Events" to enter the event configuration

interface,including common events and Smart events.

8.7.1 Ordinary Event

In the Ordinary event interface, you can set the device's Motion Detection, Privacy Mask, Video Tampering, Alarm Input, Alarm Output, Exception, Flash alarm, 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 → Motion Detection" to enter the motion detection settings interface, as shown in Figure 8-42.

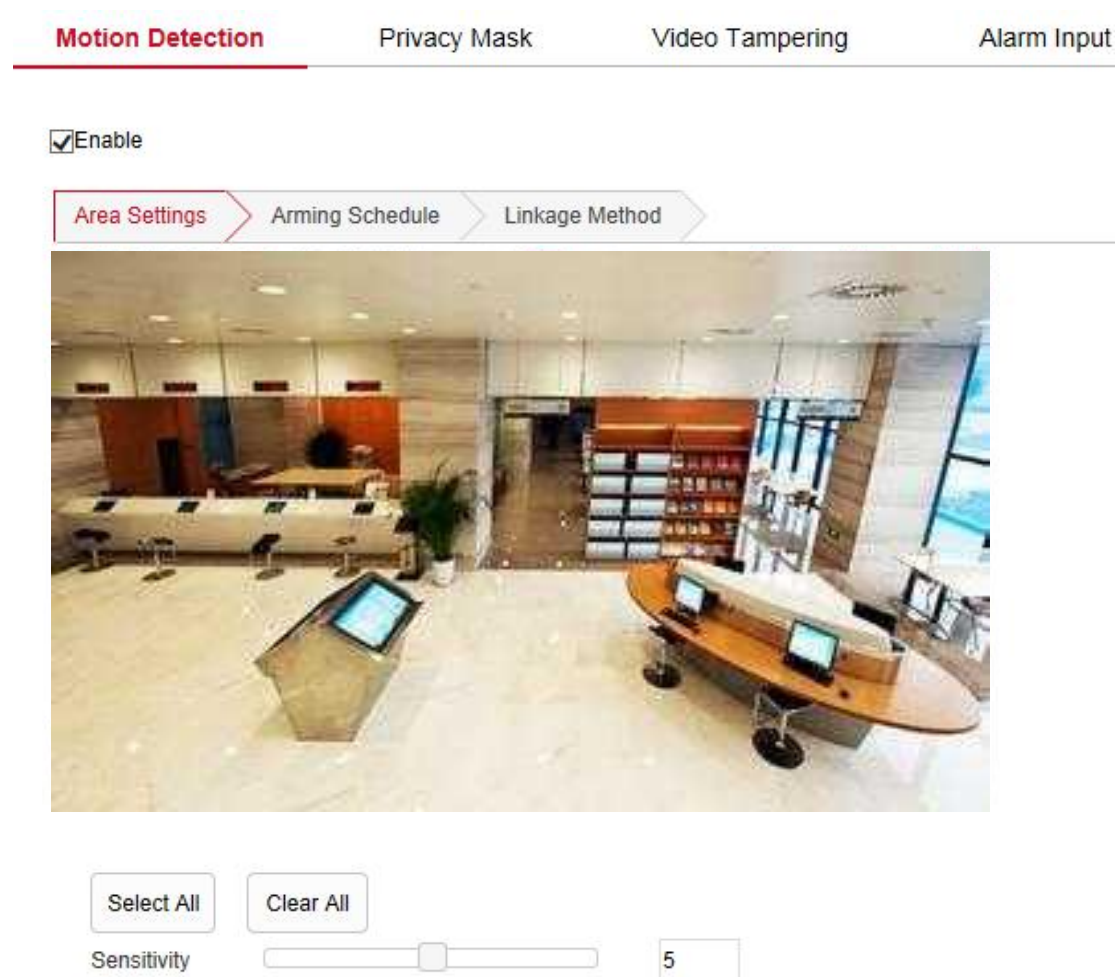


Figure 8-42

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

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

【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 8-43, 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 "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 "Save" to complete the setting of the arming time.

Motion Detection

Privacy Mask

Video Tampering

Alarm Input

Ala

☐ Enable

Area Settings

Arming Schedule

Linkage Method

✕ Del All

☑ Select All

Sun	00	02	04	06	08	10	12	14	16	18	20	22	24	
Mon	00	02	04	06	08	10	12	14	16	18	20	22	24	
Tue	00	02	04	06	08	10	12	14	16	18	20	22	24	
Wed	00	02	04	06	08	10	12	14	16	18	20	22	24	
Thu	00	02	04	06	08	10	12	14	16	18	20	22	24	
Fri	00	02	04	06	08	10	12	14	16	18	20	22	24	
Sat	00	02	04	06	08	10	12	14	16	18	20	22	24	

Figure 8-43



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) and linkage alarm output(IO Output), as shown in 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 when alarming.

【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.

☐ Enable

Area Settings	Arming Schedule	Linkage Method
☐ General Linkage	☐ Linkage Alarm Output	
☐ Upload Via SMTP	☐ IO Output	
☐ Upload Via FTP		
☐ Upload Via Cloud		
☐ Flash Warning		

Figure 8-44

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 → Privacy Mask" to enter the privacy mask settings interface. As shown in Figure 8-45.

Motion Detection	Privacy Mask	Video Tampering	Alarm Input	Alarm Output	Exception																		
																							
<table border="1"> <tbody> <tr> <td>Region1</td> <td>X 0</td> <td>Y 0</td> <td>W 0</td> <td>H 0</td> <td>Delete</td> </tr> <tr> <td>Region2</td> <td>X 0</td> <td>Y 0</td> <td>W 0</td> <td>H 0</td> <td>Delete</td> </tr> <tr> <td>Region3</td> <td>X 0</td> <td>Y 0</td> <td>W 0</td> <td>H 0</td> <td>Delete</td> </tr> </tbody> </table>						Region1	X 0	Y 0	W 0	H 0	Delete	Region2	X 0	Y 0	W 0	H 0	Delete	Region3	X 0	Y 0	W 0	H 0	Delete
Region1	X 0	Y 0	W 0	H 0	Delete																		
Region2	X 0	Y 0	W 0	H 0	Delete																		
Region3	X 0	Y 0	W 0	H 0	Delete																		
Save																							

Figure 8-45

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 "Save" after completing the setting.

③ Video Tampering

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 → Video Tampering" to enter the video tampering settings interface, as shown in Figure 8-46.

Motion Detection
Privacy Mask
Video Tampering
Alar

☐ Enable

Area Settings

Arming Schedule

Linkage Method



Drawing Area
Clear All

Sensitivity

Save

Figure 8-46

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

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

【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 8-47, 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 "Save" to complete the setting of the arming time.

Motion Detection
Privacy Mask
Video Tampering
Alarm Input
Alarr

☐ Enable

Area Settings
Arming Schedule
Linkage Method

	00	02	04	06	08	10	12	14	16	18	20	22	24
Sun													
Mon													
Tue													
Wed													
Thu													
Fri													
Sat													

Figure 8-47



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) and linkage alarm output(IO Output), as shown in Figure 8-48.

Motion Detection
Privacy Mask
Video Tampering

☐ Enable

Area Settings
Arming Schedule
Linkage Method

☐ General Linkage	☐ Linkage Alarm Output
☐ Upload Via SMTP	☐ IO Output
☐ Upload Via FTP	
☐ Upload Via Cloud	
☐ Flash Warning	

Figure 8-48

【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 when alarming.

【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.

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 → 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 8-49, 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 "Save" to complete the setting of the arming time.

Motion Detection
Privacy Mask
Video Tampering
Alarm Input
Alarm Output

☒ Alarm Input

Alarm type
Normally open

Arming Schedule
Linkage Method

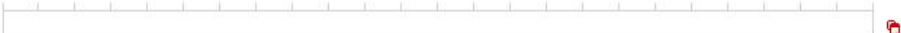
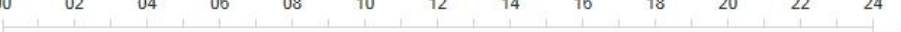
	00	02	04	06	08	10	12	14	16	18	20	22	24
Sun													
Mon													
Tue													
Wed													
Thu													
Fri													
Sat													

Figure 8-49

Step 4: Set the linkage method.

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

Motion Detection

Privacy Mask

Video Tampering

Alarm Input

☒ Alarm Input

Alarm type

Normally open

▼

Arming Schedule

Linkage Method

☐ General Linkage	☐ Linkage Alarm Output
☐ Upload Via SMTP	☐ IO Output
☐ Upload Via FTP	
☐ Upload Via Cloud	
☐ Flash Warning	

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 when alarming.

【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.

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 → 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 8-51, 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 "Save" to complete the setting of the arming time.

The screenshot shows the 'Alarm Output' configuration page. At the top, there are tabs for 'Motion Detection', 'Privacy Mask', 'Video Tampering', 'Alarm Input', and 'Alarm Output' (which is selected). Below the tabs, there is a 'Delay' dropdown menu set to '10S'. A red-bordered box highlights the 'Arming Schedule' section. Inside this section, there are two buttons: 'Del All' (with a red 'x' icon) and 'Select All' (with a checkmark icon). Below these buttons is a 7-day timeline from Sunday to Saturday. Each day has a horizontal timeline from 00 to 24 hours with 2-hour increments. To the right of each day's timeline is a red document icon (copy button). At the bottom of the 'Arming Schedule' section, there are two buttons: 'Manual alarm' and a red 'Save' button.

Figure 8-51

【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 → Exception" to enter the exception settings interface, as shown in Figure 8-52.

Motion Detection	Privacy Mask	Video Tampering
Exception Type Network Disconn ▼		
☐ General Linkage	☐ Linkage Alarm Output	
☐ Flash Warning	☐ IO Output	

Figure 8-52

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

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

【Flash Warning】 After selection, the device will link the alarm light to flash when alarming.

【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.

⑦ Flash alarm

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

The specific operation steps are as follows:

Step 1: In the main interface, click "Configuration → Events → Flash alarm" to enter the Flash alarm setting interface, as shown in Figure 8-53.

Motion Detection	Privacy Mask	Video Tampering	Alarm Input	Exception	Flash alarm	Audible alarm output							
Lighting mode		flicker ▼											
Light color		red ▼											
Flashing time		5 S											
Arming Schedule													
✕ Delete ✕ Del All ☑ Select All													
Mon	0	2	4	6	8	10	12	14	16	18	20	22	24
Tue	0	2	4	6	8	10	12	14	16	18	20	22	24
Wed	0	2	4	6	8	10	12	14	16	18	20	22	24
Thu	0	2	4	6	8	10	12	14	16	18	20	22	24
Fri	0	2	4	6	8	10	12	14	16	18	20	22	24
Sat	0	2	4	6	8	10	12	14	16	18	20	22	24
Sun	0	2	4	6	8	10	12	14	16	18	20	22	24

Figure 8-53

Step 2: Set the lighting mode(Light always on, flicker), color(red, green, blue, cyan-blue, yellow, purple, white), and flashing time(The default is 5s, and the setting range is 1-60s).

Step 3: Set the arming schedule.

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

- Method 1: Click the arming time period, manually 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, 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".

Step 4: Click on the "Save" after completing the settings.



NOTE

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

⑧ Audible alarm output

After configuring the audible alarm output, 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 → Audible alarm output" to enter the Audible alarm output setting interface, as shown in Figure 8-54.

Motion Detection
Privacy Mask
Video Tampering
Alarm Input
Exception
Flash alarm
Audible alarm output

Alert tone
Abnormal body temperature

Alarm times
1

Volume
60

Arming Schedule

☒ Delete
☒ Del All
☒ Select All

Mon	0	2	4	6	8	10	12	14	16	18	20	22	24
Tue	0	2	4	6	8	10	12	14	16	18	20	22	24
Wed	0	2	4	6	8	10	12	14	16	18	20	22	24
Thu	0	2	4	6	8	10	12	14	16	18	20	22	24
Fri	0	2	4	6	8	10	12	14	16	18	20	22	24
Sat	0	2	4	6	8	10	12	14	16	18	20	22	24
Sun	0	2	4	6	8	10	12	14	16	18	20	22	24

Figure 8-54

Step 2: Set the alert tone, alarm times(default 1 time, the adjustable range is 1-5 times) and volume (default 60, the adjustable range is 0-100).

Step 3: Set the arming schedule.

As shown in Figure 8-54. You can view, edit, and delete the arming time of the face recognition. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

- Method 1: Click the arming time period, manually 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, 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".

Step 4: Click on the "Save" after completing the settings.



NOTE

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

⑨ 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 → ROI" to enter the ROI setting interface, as shown in Figure 8-55.

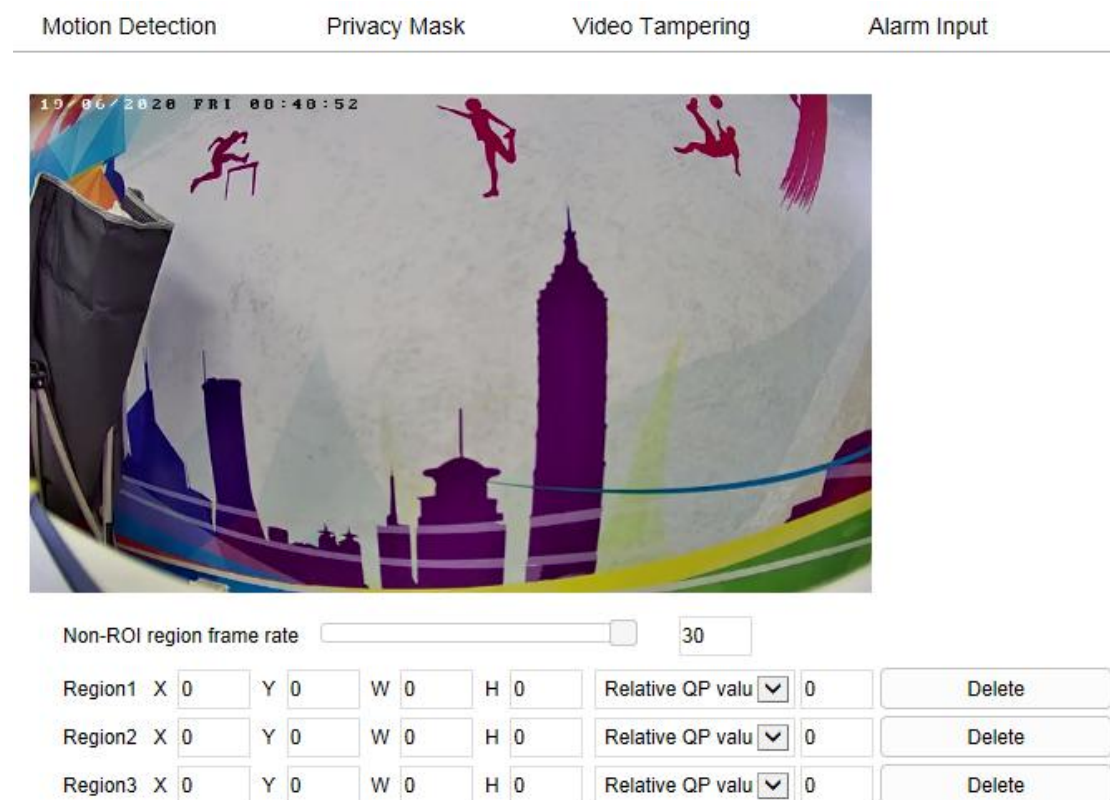


Figure 8-55

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 "Save" 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.

8.7.2 Smart Event

Smart event interface, which can set face recognition, intrusion detection, line cross detection, loiter detection and people gather detection.

① Face Recognition

The face recognition function is used to detect the face appearing in the face database in the monitoring screen, and to perform frame selection tracking on the monitoring interface.

The specific operation steps are as follows:

Step 1: In the main interface click on the "Configuration → Events → Smart Event" to enter the Face Recognition settings interface, as shown in Figure 8-56.

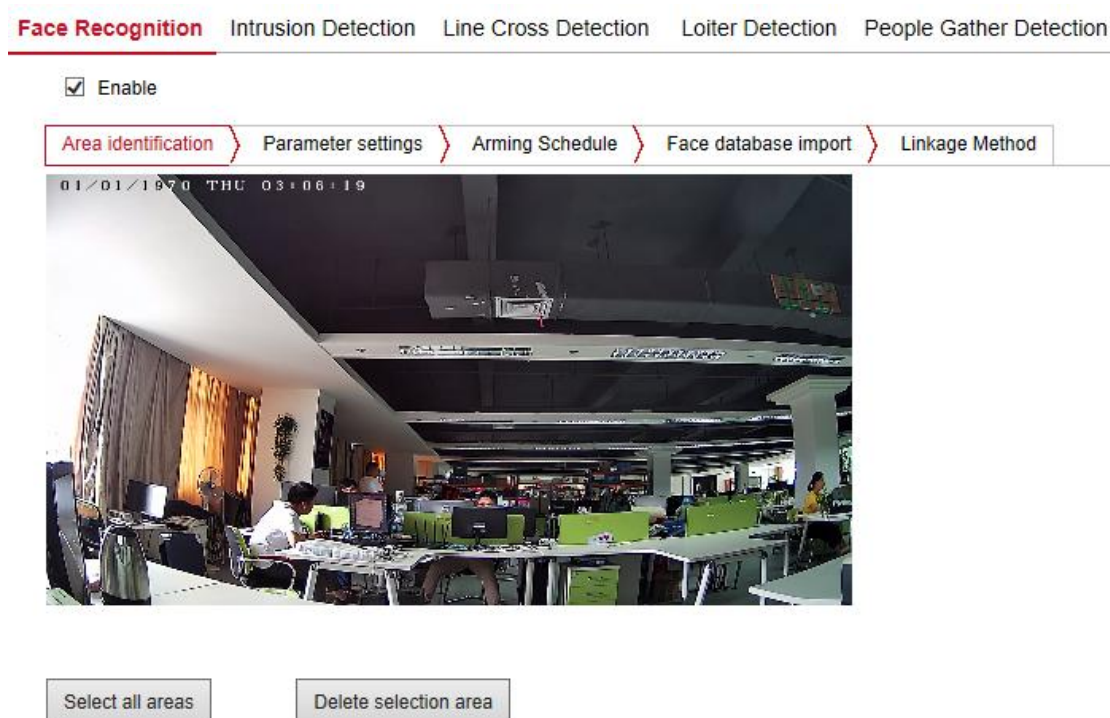


Figure 8-56

Step 2: Check "Enable" to enable face recognition.

Step 3: Set the arming area, move the mouse to the preview screen, hold down the left mouse button to select the area of the face recognition, and release the left mouse button to complete the area drawing.

【Select all areas】 is used to set all areas under the monitor screen as the guard area.

【Delete Selection Area】 is used to delete the selected alert area.

Step 4: Set related parameters(Face recognition minimum pixels, Face tracking frame, Face alarm, Capture blur threshold, Snap mode, Face contrast recognition threshold.etc).

Face Recognition Intrusion Detection Line Cross Detection Loiter Detection People Gather Detection

☒ Enable

Recognition area **Parameter settings** Arming Schedule Face database import Linkage Method

Face recognition minimum pixels	30
Face tracking frame	Open
Face alarm	Off
Capture blur threshold	5
Snap mode	Ordinary capture
Face contrast recognition threshold	60
Model Version	Lg10_HCR99_V1.0.1

Figure 8-57

【Face recognition minimum pixels】 It means that a face larger than the pixel in the monitor screen will be recognized.

【Face tracking frame】 After being turned on, the monitor screen recognizes that the face will be selected by the red frame, and the frame will move as the face moves to realize face tracking.

【Face alarm】 After being turned on, the device will alarm when it detects a face according to the capture mode, and the relevant information can be found in the log.

【Capture blur threshold】 Sets the capture face sharpness value. When the device recognizes that the face reaches the resolution, the device performs a snap action.

【Snap mode】 It consists of Ordinary capture, Face library capture, and Non-face library capture. The device captures according to the capture mode.

【Face contrast recognition threshold】 The smaller the threshold is set, the lower the comparison between the face and the face database is. If the threshold is 20, there are several similarities between tracking the face and the face database. Otherwise, the setting threshold is larger. The higher the requirement is to track the face and face database. If the threshold is set to 100, the tracking face must be 100% similar to a picture in the face database to be recognized.

Step 5: Set the arming schedule.

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

- Method 1: Click the arming time period, manually 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, 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 "Save" to complete the setting of the arming time.

Face Recognition Intrusion Detection Line Cross Detection Loiter Detection People Gather Detection

☒ Enable

Recognition area > Parameter settings > **Arming Schedule** > Face database import > Linkage Method

☒ Delete ☒ Del All ☒ Select All

	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon	[Blue bar from 0 to 24]												
Tue	[Blue bar from 0 to 24]												
Wed	[Blue bar from 0 to 24]												
Thu	[Blue bar from 0 to 24]												
Fri	[Blue bar from 0 to 24]												
Sat	[Blue bar from 0 to 24]												
Sun	[Blue bar from 0 to 24]												

Figure 8-58



NOTE

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

Step 6: Face database import, as shown in Figure 8-59. Click "Face database import" → select the import method "Append" or "Overwrite" according to needs → click "Browse" to select the face library folder → click "Import" → "OK", waiting for the import to successfully import the file, it is recommended to keep power during the import process.

Face Recognition Intrusion Detection Line Cross Detection Loiter Detection People Gather Detection

☒ Enable

Recognition area > Parameter settings > Arming Schedule > **Face database import** > Linkage Method

Overwrite

Figure 8-59



NOTE

- Face database adapts JPG files only, PNG.
- Image must not exceed the limit of 100K.

- The image name is preferably the person name.
- A maximum of 5000 pictures can be imported at a time. The number of pictures depends on the camera model.

Step 7: Set the linkage method as needed.

【Linkage Method】 refers to the response made by the device when an alarm event occurs. The linkage includes "General Linkage", "Capture link".

② Intrusion Detection

The area intrusion detection is used to detect whether an object 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 8-60.

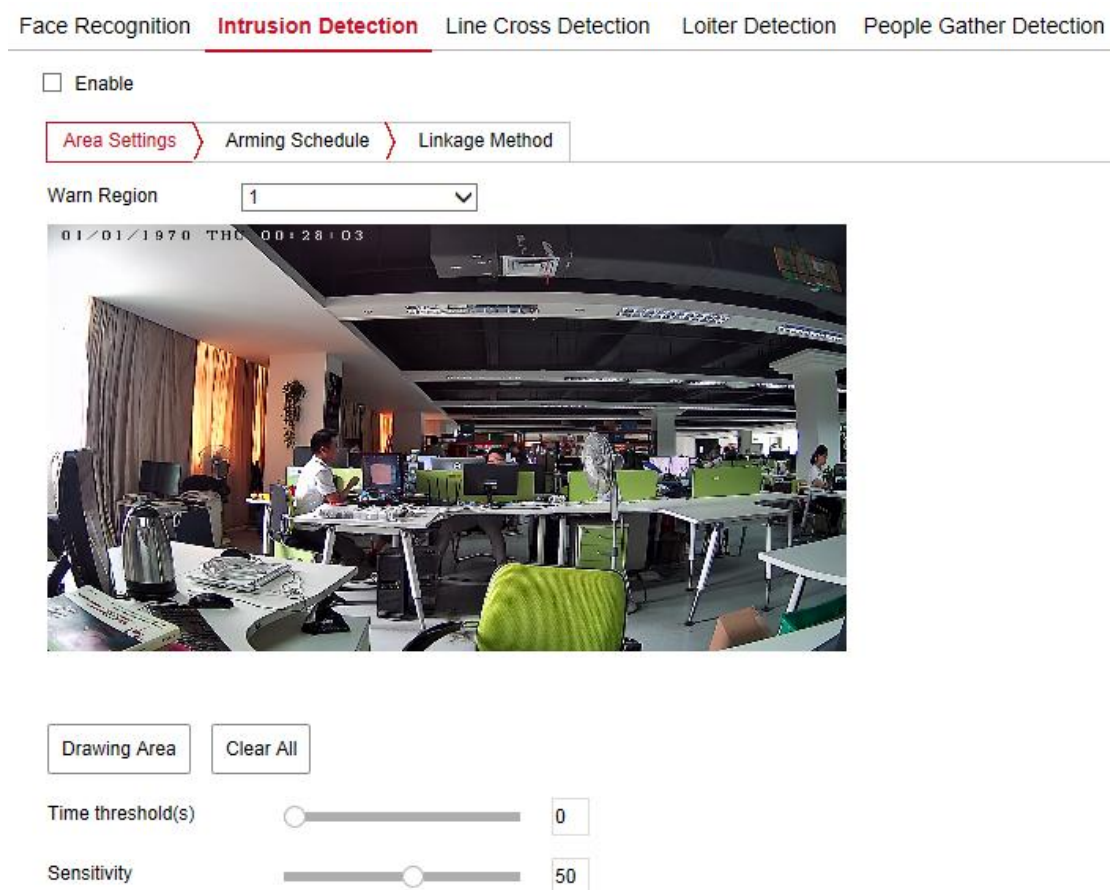


Figure 8-60

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.

【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 8-61. 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 "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, 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 "Save" to complete the setting of the arming time.

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

☐ Enable

Area Settings **Arming Schedule** Linkage Method

☒ Delete ☒ Del All ☒ Select All

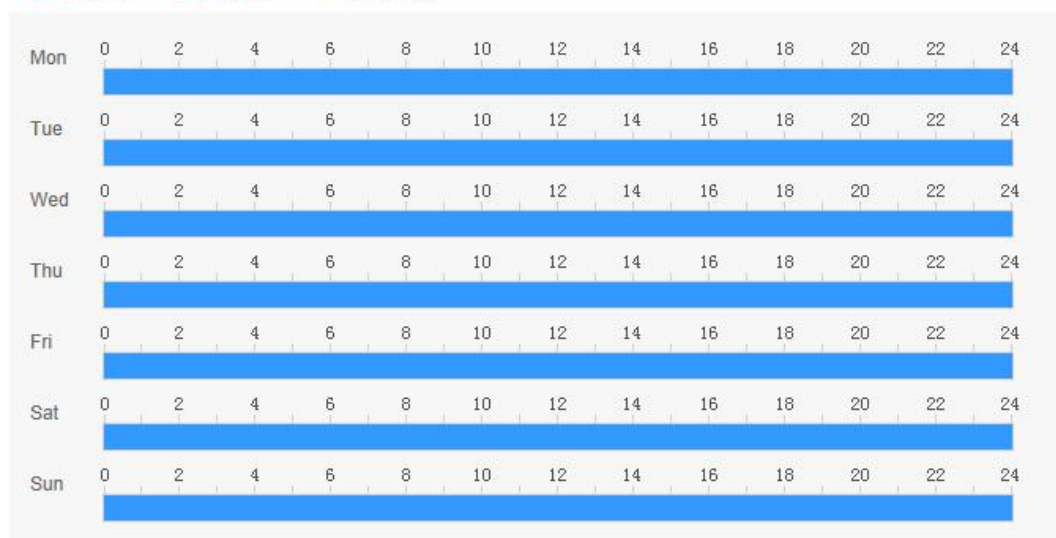


Figure 8-61



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.

【Linkage Method】 refers to the response made by the device when an alarm event occurs. The linkage includes "General Linkage", "Upload Via SMTP" and "Upload Via FTP".

③ 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 8-62.

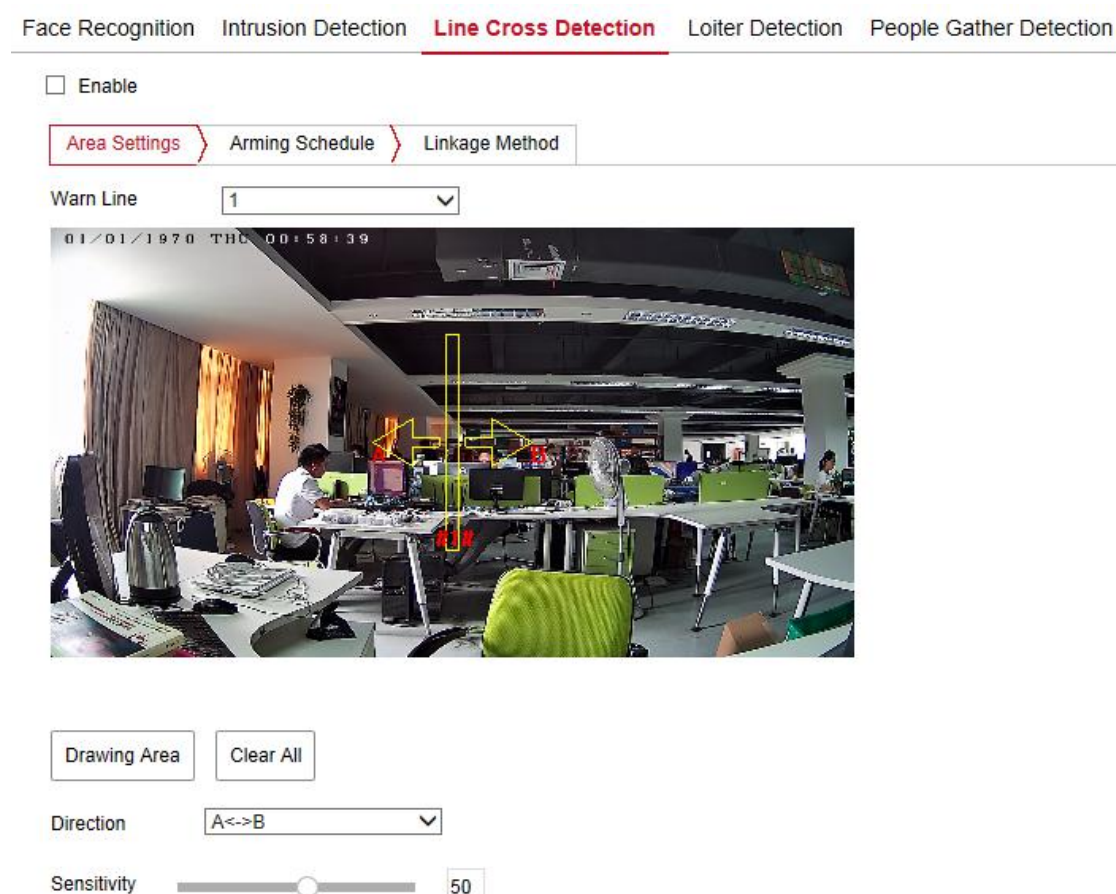


Figure 8-62

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 8-63. 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, 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 "Save" to complete the setting of the arming time.

☐ Enable

Area Settings **Arming Schedule** Linkage Method

☒ Delete ☒ Del All ☒ Select All

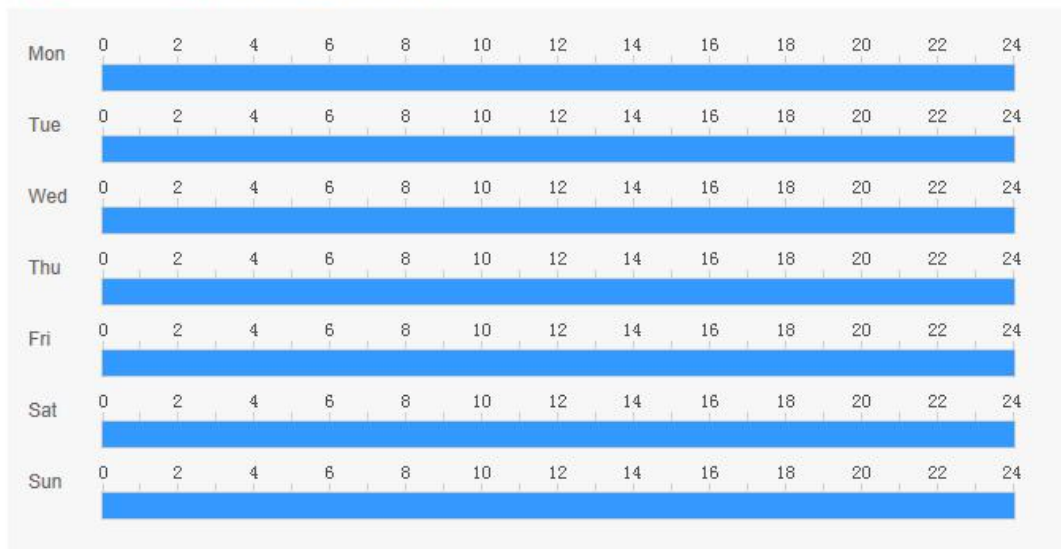


Figure 8-63



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.

【Linkage Method】 refers to the response made by the device when an alarm event occurs. The linkage includes "General Linkage", "Upload Via SMTP" and "Upload Via FTP".

④ 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 8-64.

☐ Enable

Area Settings

Arming Schedule

Linkage Method

Warn Region

1



Drawing Area

Clear All

Time threshold(min)



0

Sensitivity



50

Figure 8-64

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.

【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 8-65. 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 "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, 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 "Save" to complete the setting of the arming time.

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

☐ Enable

Area Settings **Arming Schedule** Linkage Method

☒ Delete ☒ Del All ☒ Select All

	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon													
Tue													
Wed													
Thu													
Fri													
Sat													
Sun													

Figure 8-65



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.

【Linkage Method】 refers to the response made by the device when an alarm event occurs. The linkage includes "General Linkage", "Upload Via SMTP" and "Upload Via FTP".

⑤ 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 8-66.

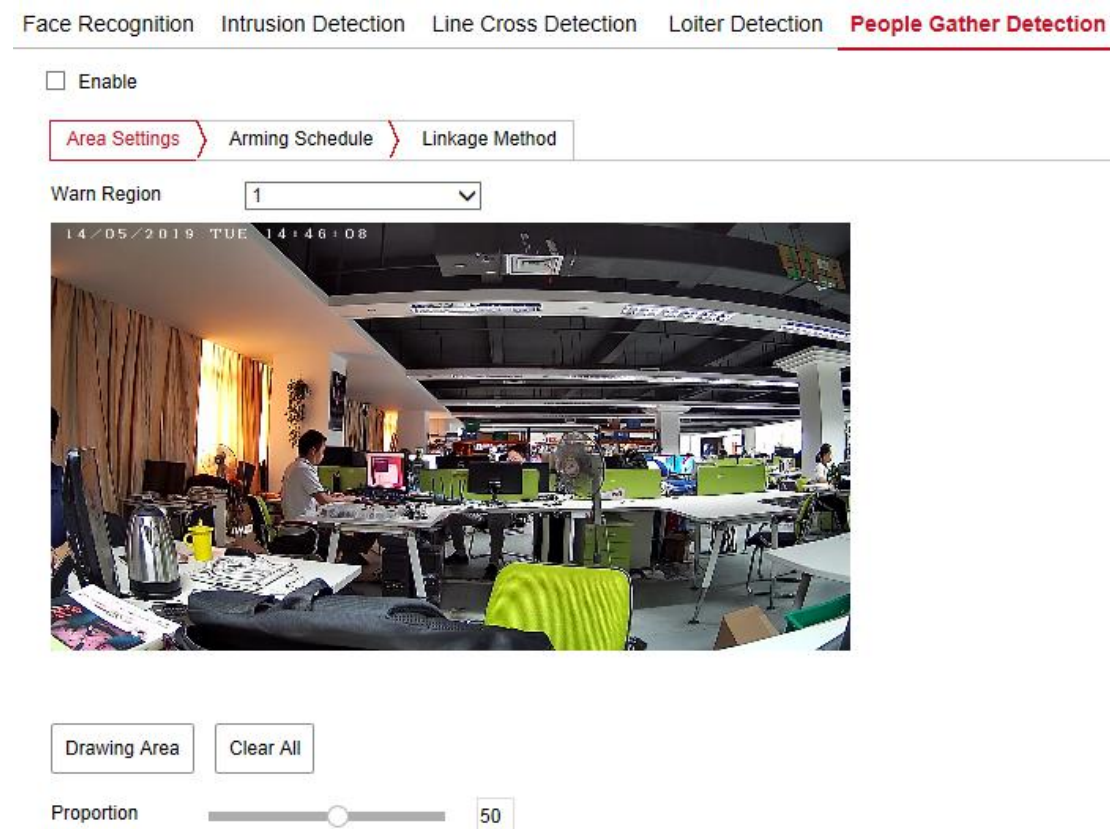


Figure 8-66

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.

【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 8-67. 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 "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, 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 "Save" to complete the setting of the arming time.

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

☐ Enable

Area Settings **Arming Schedule** Linkage Method

☒ Delete ☒ Del All ☒ Select All

	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon													
Tue													
Wed													
Thu													
Fri													
Sat													
Sun													

Figure 8-67



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.

【Linkage Method】refers to the response made by the device when an alarm event occurs. The linkage includes "General Linkage", "Upload Via SMTP" and "Upload Via FTP".

8.8 Body Temperature Measure

8.8.1 Body Temperature Measure

After setting the temperature measurement parameters and test rules, when a target meets the temperature measurement parameters or triggers the temperature measurement rules, it will automatically perform temperature measurement and alarm.

The specific operation steps are as follows:

Step 1: In the main interface click on the "Configuration → Body Temperature Measure → Body Temperature Measure" to enter the Body temperature measurement settings interface, as shown in Figure 8-68.

Body temperature measurement config Linkage Method

☒ Temperature measurement function switch

☒ Temperature information display switch

☒ Heat map display switch

Temperature compensation

Temperature measurement alarm threshold

Temperature measurement information display position

Heat map display position

Temperature measurement trigger

Temperature measurement interval

Temperature measurement unit

Temperature measurement range

0

°C (Compensation range -5~5)

37.3

°C (Temperature measurement alarm threshold range is 36~42)

Upper right corner

Lower right corner

Real-time temperature measurement

3 S

Celsius temperature(°C)

35-42

°C

Save

Figure 8-68

Step 2: Turn on the temperature measurement function switch, temperature information display switch and heat map display switch, configure the related temperature measurement parameters, and click "Save".

【Temperature measurement function switch】 Turn on/off the device temperature measurement function.

【Temperature information display switch】 Turn on/off the display of temperature information on the device screen.

【Heat map display switch】 Turn on/off the screen to display the thermal map.

【Temperature compensation】 Set the equipment temperature compensation according to the equipment usage environment.

【Temperature measurement alarm threshold】 The device triggers an alarm temperature value. When the temperature recognized by the device exceeds this value, the device alarms.

【Temperature measurement information display position】 The position of temperature-related information displayed on the device screen (Upper left corner, Lower left corner, Upper right corner, Lower right corner).

【Heat map display position】 Set the position of the device heat map (Upper left corner, Lower left corner, Upper right corner, Lower right corner).

【Temperature measurement trigger】 Set the temperature measurement trigger method (Real-time temperature measurement, Detect face).

【Temperature measurement interval】 Set the temperature measurement interval 2 times.

【Temperature measurement unit】 Set the temperature unit.

【Temperature measurement range】 Set the temperature measurement range.

Step 3: Click "Linkage Method → Arming Schedule", set the arming schedule.

As shown in Figure 8-69. 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 "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, 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 "Save" to complete the setting of the arming time.

Body temperature measurement config **Linkage Method**



Figure 8-69



NOTE

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

Step 4: Click "Linkage Method", set the linkage method as needed.

【Linkage Method】 Refers to the response of the device when the temperature measurement is triggered. The linkage includes "General Linkage"(Upload Via SMTP,

Upload Via FTP, Flash alarm, and Sound alarm) and "Linkage Alarm Output(IO Output)".

Step 5: Click "Save" to complete the body temperature measurement configuration.

Chapter 9 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".