Thermal Bullet Network Camera

User Manual V1.0.0

Table of Contents

1. Camera Login

1.1 Default Account

The factory default super administrator account of the camera: admin.

The factory default super administrator password of the camera: admin.

The factory default IPv4 address of the camera: 192.168.1.123.

1.2 Login to Web Interface

Step 1 Open the IE browser, enter the IP address of the camera in the address bar and press the [Enter] key. For successful login, the web displays an interface as shown in Figure 1.2-1. For the first use, it is required to install the web plug-in. Download and install according to the prompt.

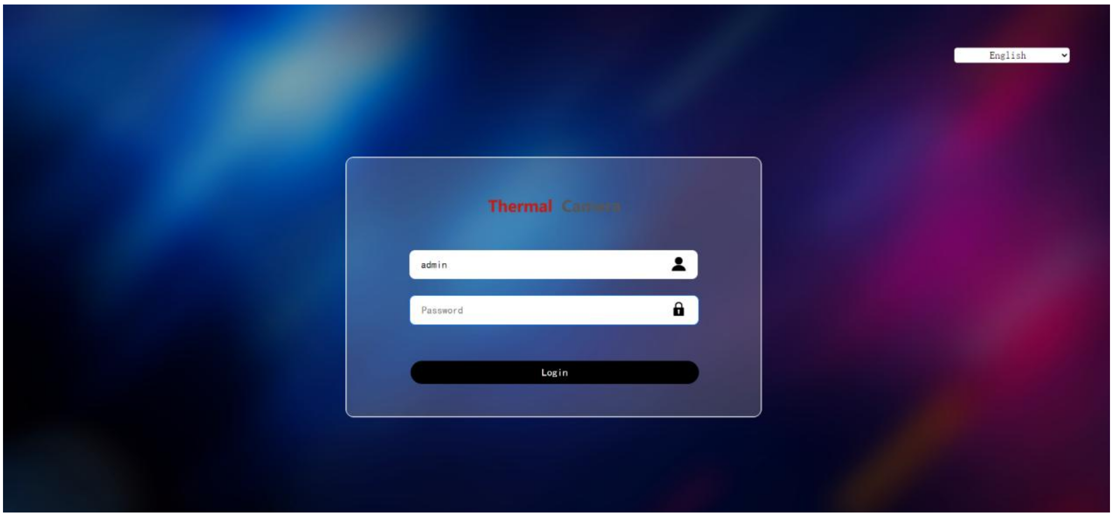
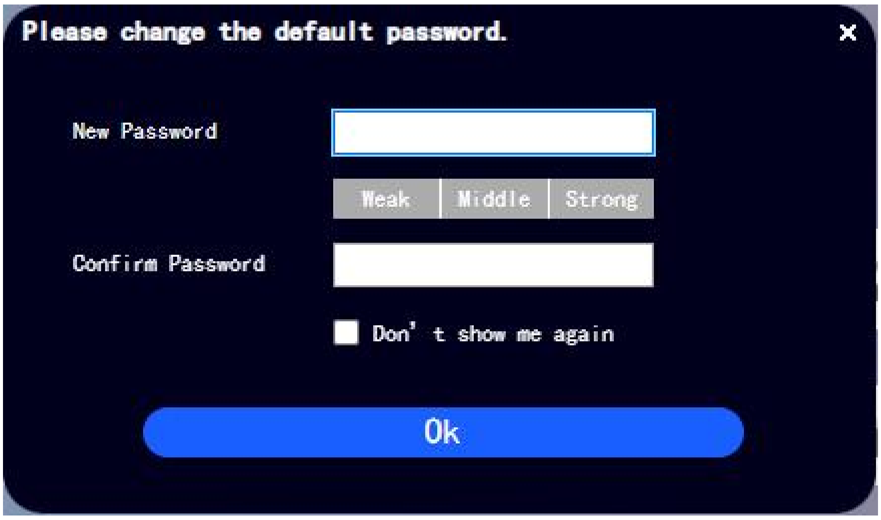


Figure 1.2-1 Web Login Interface

Step 2 Input the user name and passwords to enter the web operation interface (the default administrator user name is admin, and the password is admin) for the first-time login. The system will pop up a prompt box for password modification, as shown in Figure 1.2-2. Please change the administrator password in time and keep it properly.



Please change the default password.

New Password

Confirm Password

□ Don' t show me again

Figure 1.2-2 Passwords Modification

For successful login, the web will display the interface as shown in Figure 1.2-3.

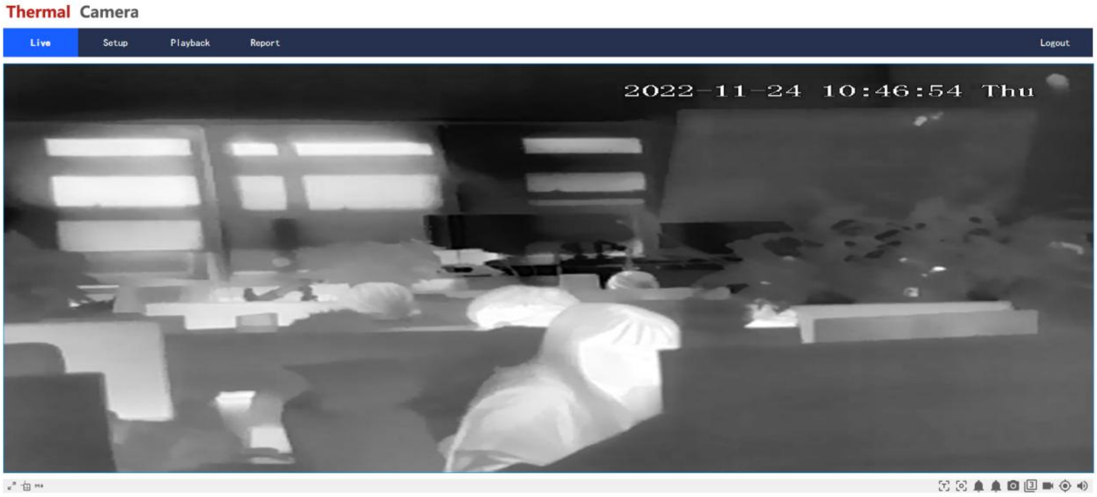


Fig1.2-3 Video Preview Interface

● The interface and settings are only for reference, and the specific interface shall be subject to actual layout.

2. Preview

The preview interface is as shown in Figure 2-1.

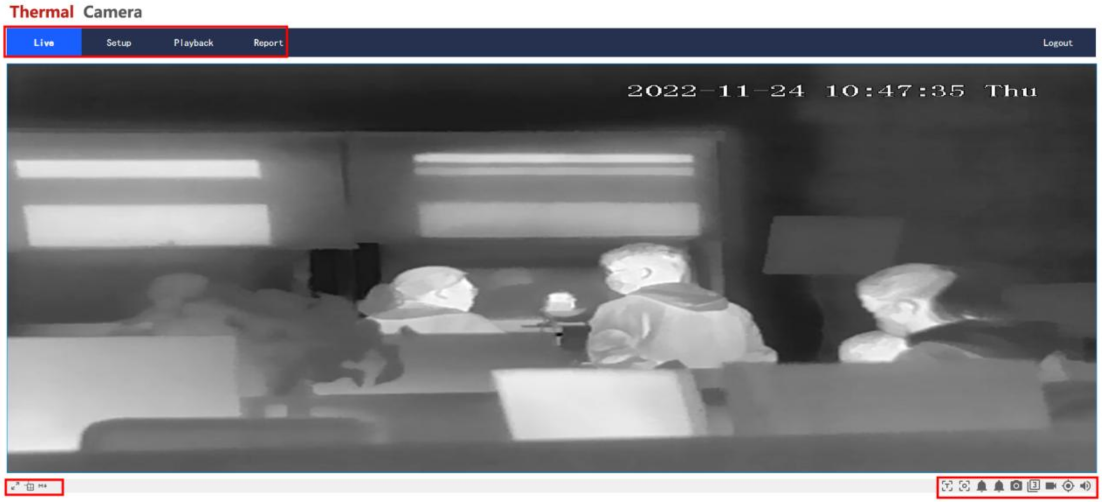


Fig. 2-1 Preview Interface

Refer to Table 2-1 for the description on function bar.

No.	Descriptions
1	System menu bar
2	Video window adjustment bar
3	Video window function-option bar

Table 2-1 Description on Function Bar

2.1 System Menu

Click each function menu tag to enter the corresponding interface, and the system menu is shown in Figure 2.1-1.

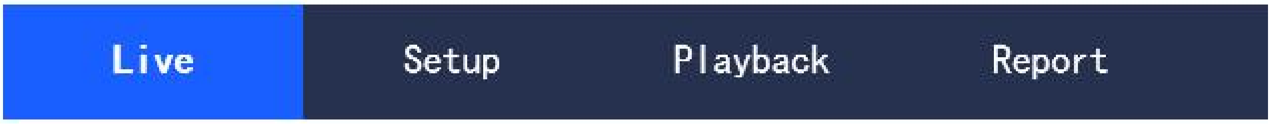


Fig. 2.1-1 System Menu

2.2 Video Window Adjustment

The video adjustment is as shown in Figure 2.2-1, referring to Table 2.2-1 for the parameter descriptions.

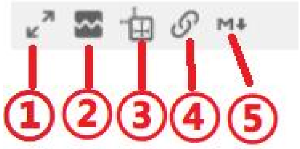


Fig. 2.2-1 Video Window Adjustment

Parameters	Descriptions
1 Window size adjustment	Click this button, three optional image ratios: original ratio, suitable window and original size
2 Fluency adjustment	Click the button to select any of the three fluency levels (real-time, normal, and smooth). The real-time level is set as default.
3 Rules information	Click the button, the intelligent rules will be displayed on the image preview interface. On by default.
4 Type of connection	Click the button to select the video monitoring protocol, supporting TCP, UDP and multicast.
4 Type of streaming	Click the button to select the main stream or the sub stream.

Table 2.2-1 Description on Video Adjustment Parameters

2.3 Video Function Options

The video function options are as shown in Figure 2.3-1, referring to Table 2.3-1 for the parameter descriptions.

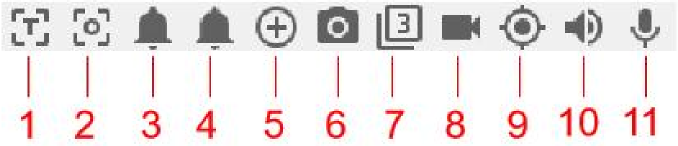


Fig. 2.3-1 Video Function Options

Parameters	Descriptions
1 Temperature measurement	Click the button, and click any position of the thermal imaging video to measure and display the temperature of the point.
2 Region focus	Click this button, select a certain region on the video preview interface, then the camera can perform auto focus targeted by the selected region.
3 Alarm output 1	Display the state of alarm output 1. The alarm output light turns on when the conditions for triggering the alarm reached in the event.
4 Alarm output 2	Display the state of alarm output 2. The alarm output light turns on when the conditions for triggering the alarm reached in the event.
5 Partial magnification	● Click the button, and select any area to magnify when the picture is in the original state. For any picture that is not in the original state, the region can be magnified by dragging within a certain range, the region box will return to the original state by clicking the right mouse button. ● Click the button, you can zoom in and out the picture by scrolling the mouse wheel.
6 Image snapshot	Click the button to conduct image snapshot, and save the images in the set path.
7 Three consecutive snapshot	Click the button to conduct three consecutive snapshot, one image per second, and save the image in the set path.
8 Video recording	Click the button to record a video, and click it again to stop recording; save the video files in the set path.
9 Manual Track	Click the button, select any region by dragging the left mouse within the video window, the camera will perform intelligent track on the objects within the region.
10 Voice	Click the button to turn on /off the audio output of monitoring stream.
11 Intercom	Click the button to turn/off the voice intercom.

Table 2.3-1 Description on Video Function-option Parameters

3. System Settings

3.1 Camera Settings

3.1.1 Conditions

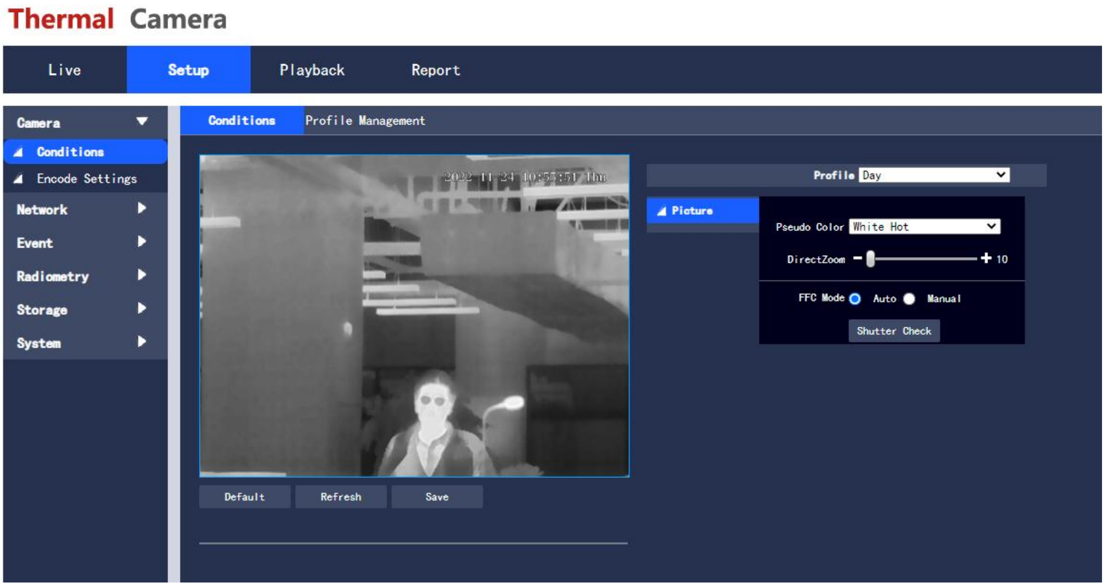
3.1.1.1 Thermal imaging

Image

This function is for thermal properties settings to achieve the best presentation effect. The configuration steps are as follows:

Step 1 Select "Settings > Camera Settings > Conditions"

Step 2 Enter the "Thermal Imaging" interface, as shown in Figure 3.1-1.



Profile Day

Pseudo Color White Hot

DirectZoom 10

FFC Mode ● Auto ○ Manual

Fig.3.1-1 Image

Step 2 Configure each parameter according to actual needs. For the detailed parameters descriptions, please refer to Table 3.1-5.

Parameters	Descriptions
Profile	The normal mode, daytime mode or nighttime mode are available. When a mode is selected, the corresponding configuration and effect can be set and viewed.
Style	It is for setting the picture palette, with such options as white-hot, iron, rainbow 1,

	lava, rainbow 2, sky, medium gray, grayred, purpleorange, special, warning red, icefire, bluered, special 2, gradient red, gradient green, gradient blue, waning green, waning blue. Note: the threshold value can be changed if the waning red, warning blue and waning green is chosen.
Electric Zoom	This function supports magnification configuration of 1~8×.
FFC Mode	It is provided with the automatic and manual options, and the "Automatic" option is set as default.
FFC switch cycle	This can be set when the FFC mode is set as auto, the time interval of auto shutter correction
Shutter Correction	Click *shutter correction* to trigger a shutter correction.

Table 3.1-5 Description of Image Setting Parameters

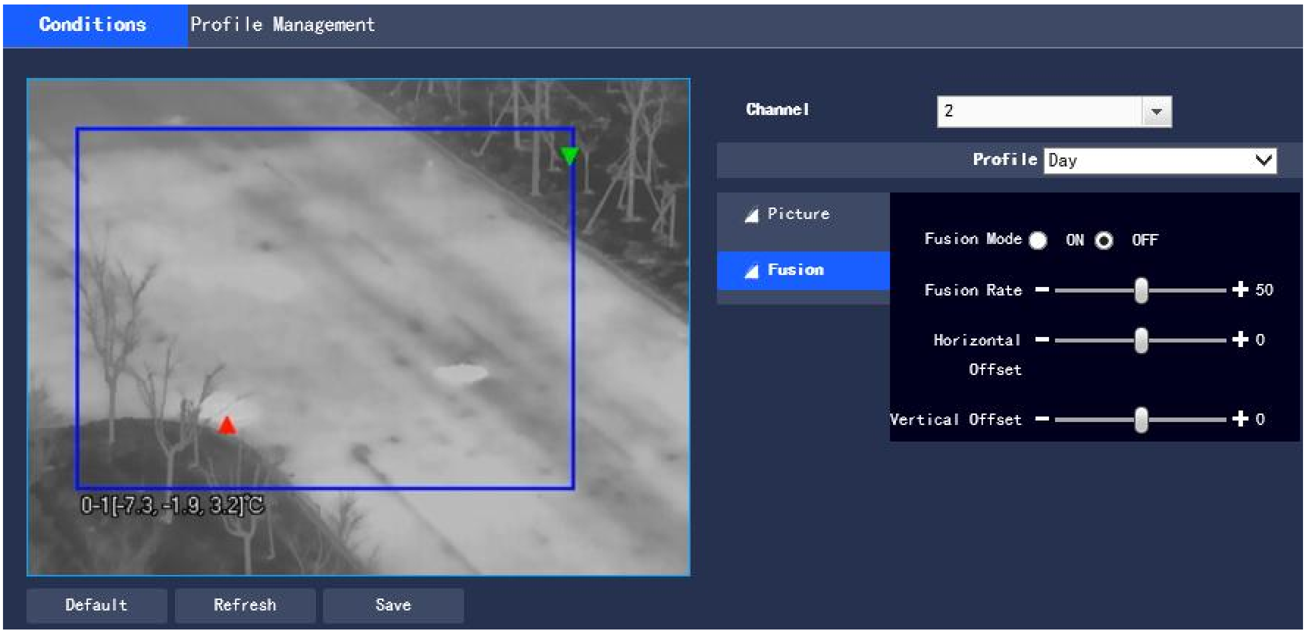
Step 3 Click "Save" to complete the setting.

Fusion

This function is for setting the fusion to achieve the best presentation effect. The configuration steps are as follows:

Step 1 Select "Settings > Camera Settings > Conditions"

Step 2 Select channel "2" to enter the "Thermal Imaging" interface, and select "fusion", as shown in Figure 3.1-13.



Channel: 2

Profile: Day

Fusion Mode ● ON ○ OFF

Fusion Rate: 50

Horizontal Offset: 0

Vertical Offset: 0

Fig. 3.1-13 Fusion

Step 3 Enable the fusion mode, and there are three parameters in the mode: image fusion ratio, horizontal offset and vertical offset.

●Image fusion ratio: affects the surface of the object in the fusion image. The higher the value, the closer to the image effect of visible light, and the range is 0-100.

●Horizontal offset: adjust the fusion deviation of the visible light image and the infrared image in the horizontal direction, the range is -100~100.

●Vertical offset: adjust the fusion deviation of the visible light image and the infrared image in the vertical direction, the range is -100~100.

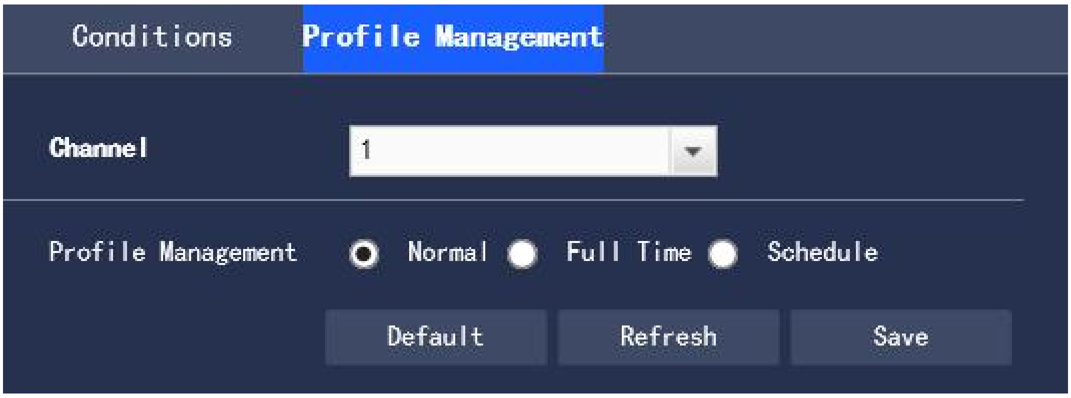
Step 4 Click "Save" to complete the setting.

3.1.1.3 Configuration File Management

There are two channels, with Channel 1 for the visible light configuration file, and Channel 2 for the thermal picture configuration file. Channel 1 is set as default.

The configuration file management can select either of such three types as "Normal", "Full Time" and "Schedule".

● When the "Normal" type is selected, the visible light video conducts surveillance according to the normal configuration of the camera, as shown in Figure 3.1-14.

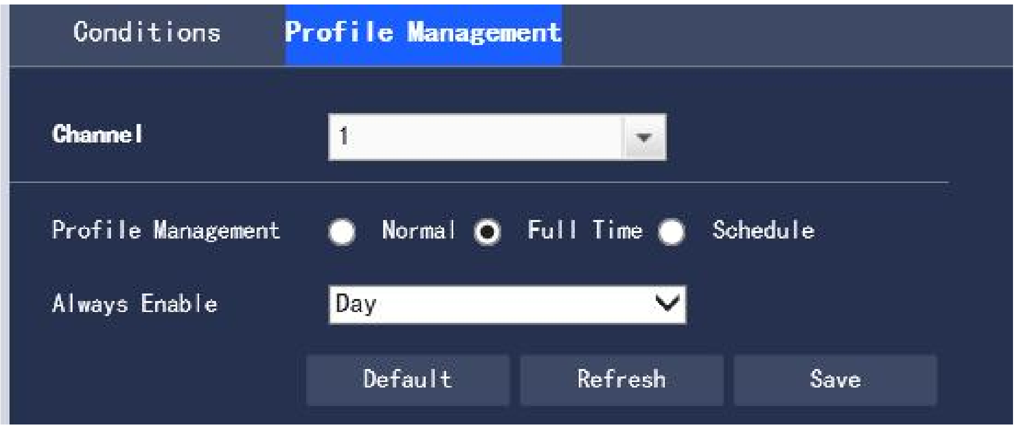


Channel: 1

Profile Management: ◉ Normal ○ Full Time ○ Schedule

Fig. 3.1-14 Configuration File Management - Normal Type

● When the "Full Time" type is selected, there are "Day" or "Night" options, and the corresponding visible light camera property configuration file is day or night, as shown in the Figure 3.1-15.



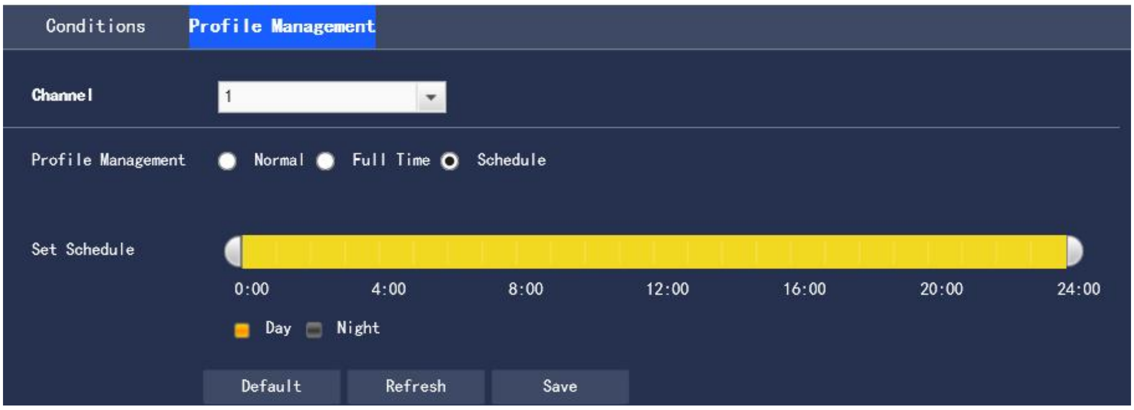
Channel: 1

Profile Management: ○ Normal ◉ Full Time ○ Schedule

Always Enable: Day

Fig. 3.1-15 Configuration File Management - Full Time

● When the "Schedule" type is selected, you can choose a period of time for day configuration and another period of time for night configuration. The configuration interface is as shown in Figure 3.1-16. For example, you can set 7:00～17:00 for day configuration, and 17:00～7:00 for night configuration.



Channel: 1

Profile Management: ○ Normal ○ Full Time ◉ Schedule

Fig. 3.1-16 Configuration File Management - Schedule Type

Click "Save" to complete the configuration.

3.1.2 Encoding Settings

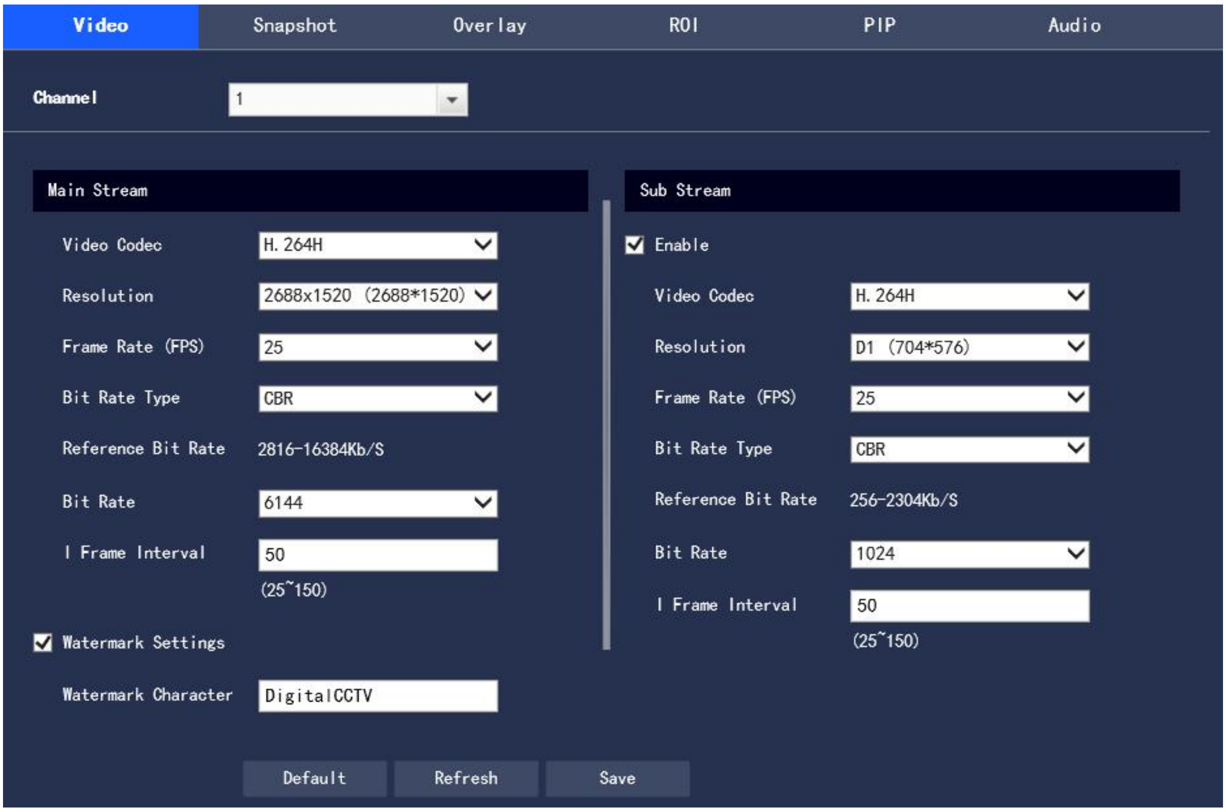
It is for setting the camera in such aspects as the video stream, snapshot stream, video overlay, ROI , PIP, and audio.

● Channel 1 is the visible light setting, and Channel 2 is the thermal picture setting. The following part is described as settings of Channel 1.

3.1.2.1 Video stream

It is for setting the video stream of the surveillance pictures. The configuration steps are as follows:

Step 1 Select "Settings > Camera Settings > Encoding Settings > Video" to enter the "Video stream" interface of the system. Channel 1 is the visible light video stream, and Channel 2 is the thermal video stream, as shown in Figure 3.1-17



Channel: 1

Main Stream

Video Codec: H.264H

Resolution: 2688x1520 (2688*1520)

Frame Rate (FPS): 25

Bit Rate Type: CBR

Reference Bit Rate: 2816-16384Kb/S

Bit Rate: 6144

I Frame Interval: 50 (25~150)

☑ Watermark Settings

Watermark Character: DigitalCCTV

Sub Stream

☑ Enable

Video Codec: H.264H

Resolution: D1 (704*576)

Frame Rate (FPS): 25

Bit Rate Type: CBR

Reference Bit Rate: 256-2304Kb/S

Bit Rate: 1024

I Frame Interval: 50 (25~150)

Fig. 3.1-17 Video Streaming Settings

● The code stream configuration interface of different devices may be different, please refer to the actual interface for details.

● The default value corresponding to different code streams may be different, please refer to the actual interface for details.

Step 2 Configure information of each parameter according to actual needs. For the description of parameters, please refer to Table 3.1-6.

Parameters	Descriptions
Video Codec	There are such options as H.264, H.264H, H.264B, H.265, and MJPEG.
Resolution	There are a variety of resolution types, each of which corresponds to a different stream value recommended.
Frame Rate (FPS)	The number of video frames per second, and the frame rate will vary with different device models and resolutions.
Bit Rate Type	It covers the fixed stream and the variable stream. ● The picture quality can only be set in the variable stream mode, rather than the fixed stream mode. ● In the MJPEG encoding mode, the stream control method can only be the fixed stream.
Reference Bit Rate	It recommends the user a reasonable range of stream value according to the resolution and frame rate configured by the user.
Bit Rate	● In the variable stream mode, this value is the upper limit of stream and in the fixed stream mode, this value is a fixed value. ● Refer to "Reference Bit Rate" for the best reference range.
I Frame Interval	It refers to the number of P frames between two I frames. The range changes with the frame rate, which is up to 150. It is recommended to set it to 2 times the frame rate.
Watermark	By verifying the watermark characters, the user can check whether the video

Settings	has been tampered. This function is enabled after the enable item is selected. The watermark character "Digital CCTV" is set as the default. The watermark characters can only be numbers, letters, underlines, and strikethroughs, which is up to 128 characters.
Sub Stream Enable	Check the enable check box to control sub stream enabling/disabled. Enabling is set as default.

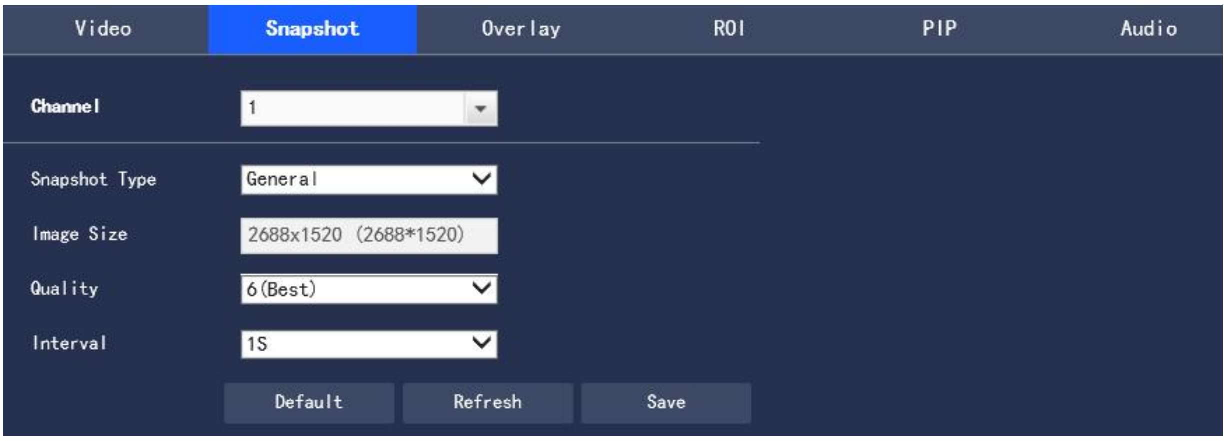
Table 3.1-6 Description of Video Stream Parameter Settings

Step 3 Click "Save" to complete the configuration.

3.1.2.2 Picture Stream

It is for setting the stream information of the image captured by the surveillance, and the configuration steps are as follows:

Step 1 Select "Settings > Camera Settings > Encoding Settings > Snapshot" to enter the "Snapshot" interface of the system, as shown in Figure 3.1-18.



Channel: 1

Snapshot Type: General

Image Size: 2688x1520 (2688*1520)

Quality: 6(Best)

Interval: 1S

Fig. 3.1-18 Picture Stream Setting

Step 2 Configure information of each parameter according to actual needs. For the description of parameters, please refer to Table 3.1-7.

Parameters	Descriptions
Snapshot Type	It covers normal image capture and triggered image capture. ● Normal image capture refers to such operations within the scope set in the timetable. ● Triggered image capture refers to such operations after triggering dynamic detection, video mask, and local alarm.
Image Size	Keep the resolution same to that of the selected image capture stream (main stream or sub stream).
Image Quality	Set the quality of image capture in such six levels as worst, worse, poor, good, better, best.
Capture Interval	Set the frequency of image capture, from 1 second/sheet to 7 second/sheet or customized.

Table 3.1-7 Description of Picture Stream Parameter Settings

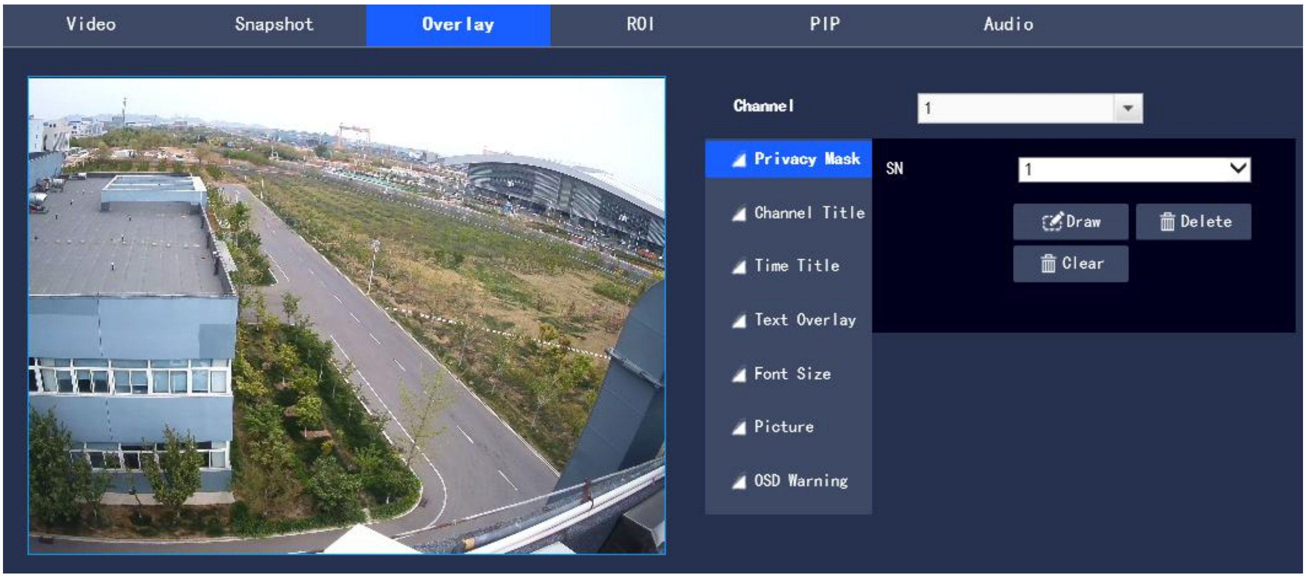
Step 3 Click "Save" to complete the configuration.

3.1.2.3 Video Overlay

It is for setting the information overlaid on the surveillance video pictures, and the configuration steps are as follows:

Step 1 Select "Settings > Camera Settings > Encoding Settings > Overlay" to enter the "Video Overlay" interface of the system.

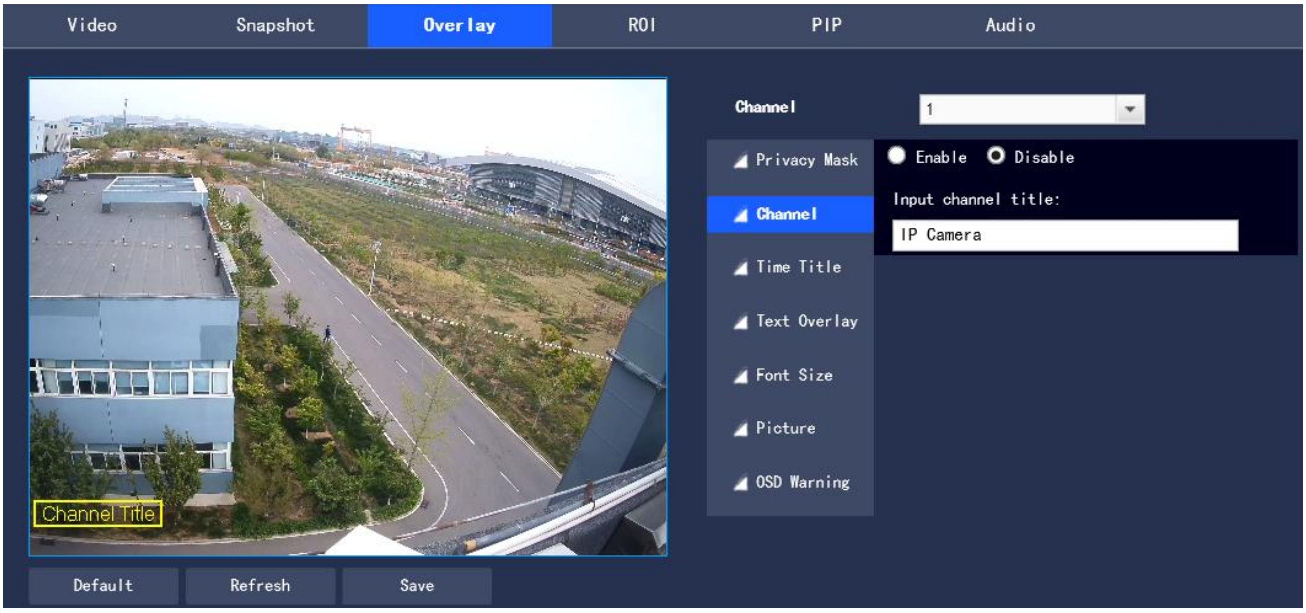
Step 2 Configure the video overlay information according to actual needs. The configuration interface is as shown in Figure 3.1-19 to Figure 3.1-27, referring to Table 3.1-8 for the parameter descriptions.



Channel 1

SN 1

Fig. 3.1-19 Video Overlay - Privacy Mask



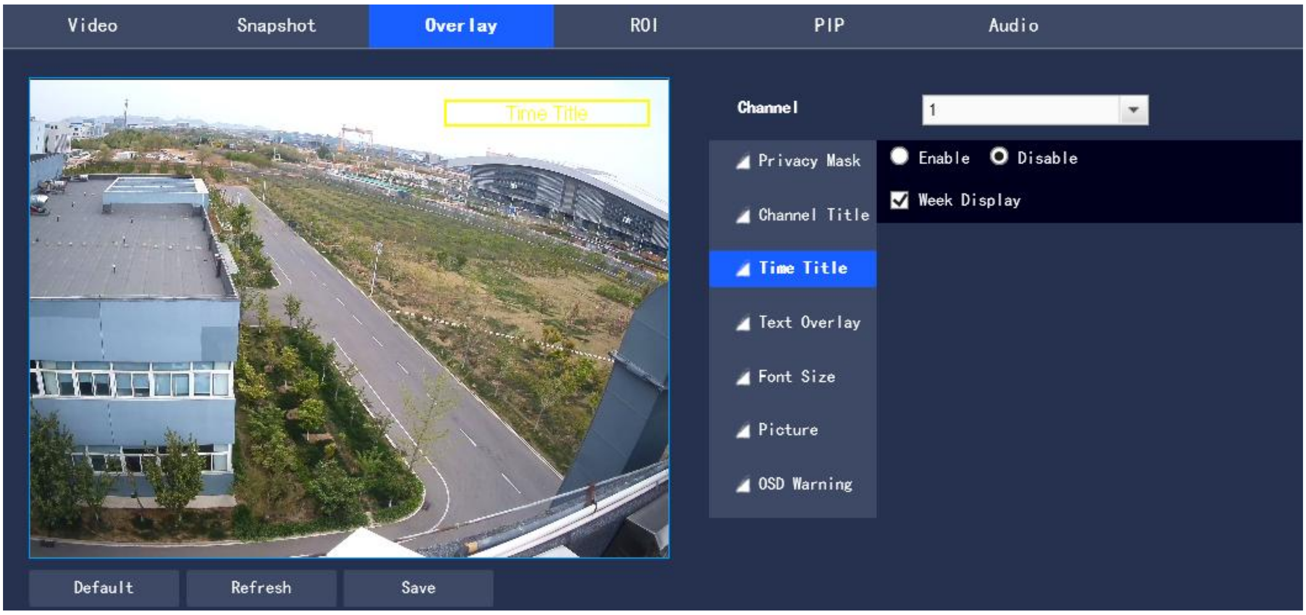
Channel 1

○ Enable ● Disable

Input channel title:

IP Camera

Fig. 3.1-20 Video Overlay - Channel Title

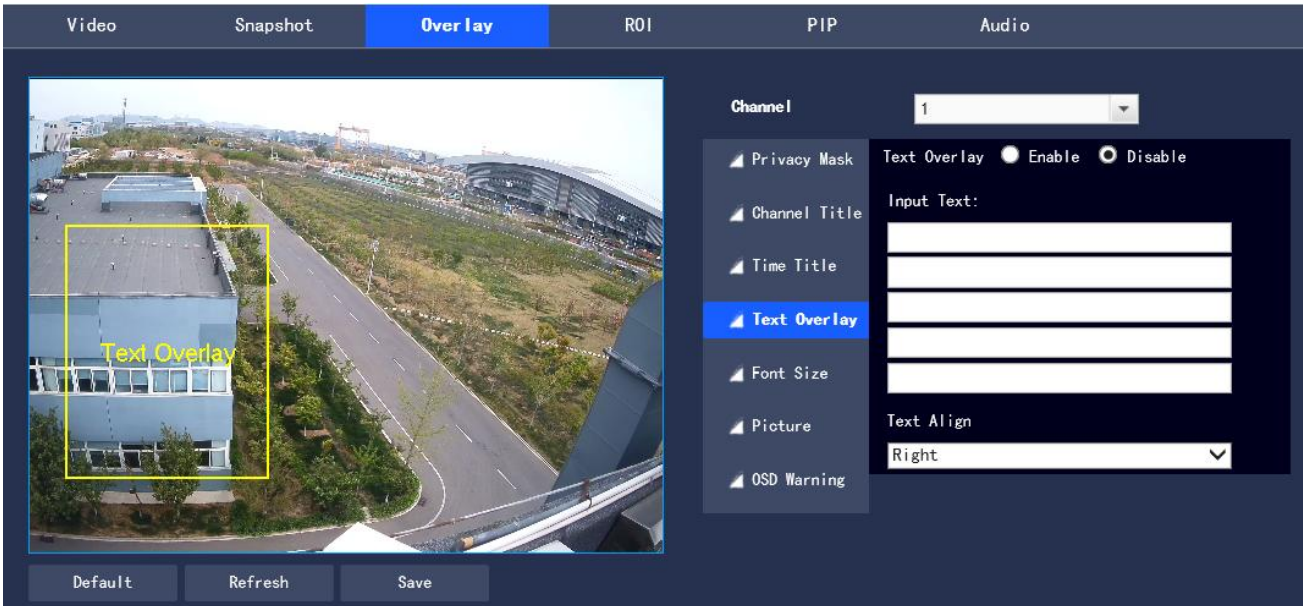


Channel 1

○ Enable ● Disable

☑ Week Display

Fig. 3.1-21 Video Overlay - Time Title



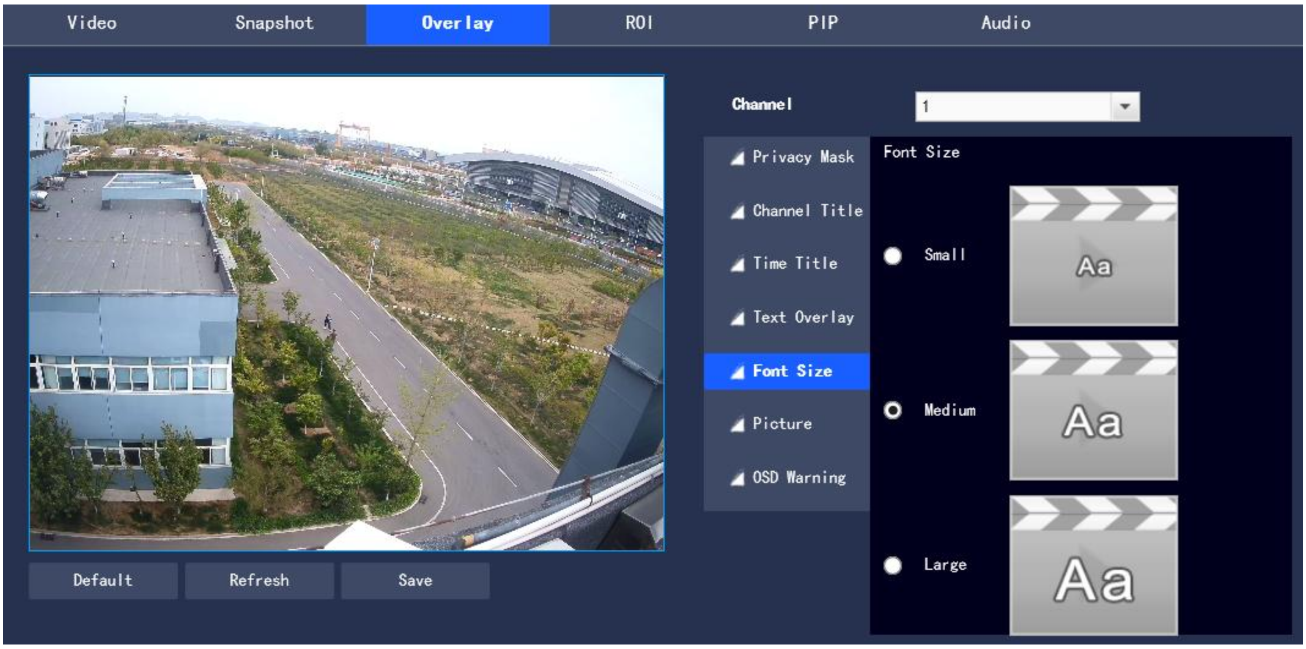
Channel: 1

Text Overlay ● Enable ○ Disable

Input Text:

Text Align: Right

Fig. 3.1-22 Video Overlay – Text Overlay



Channel: 1

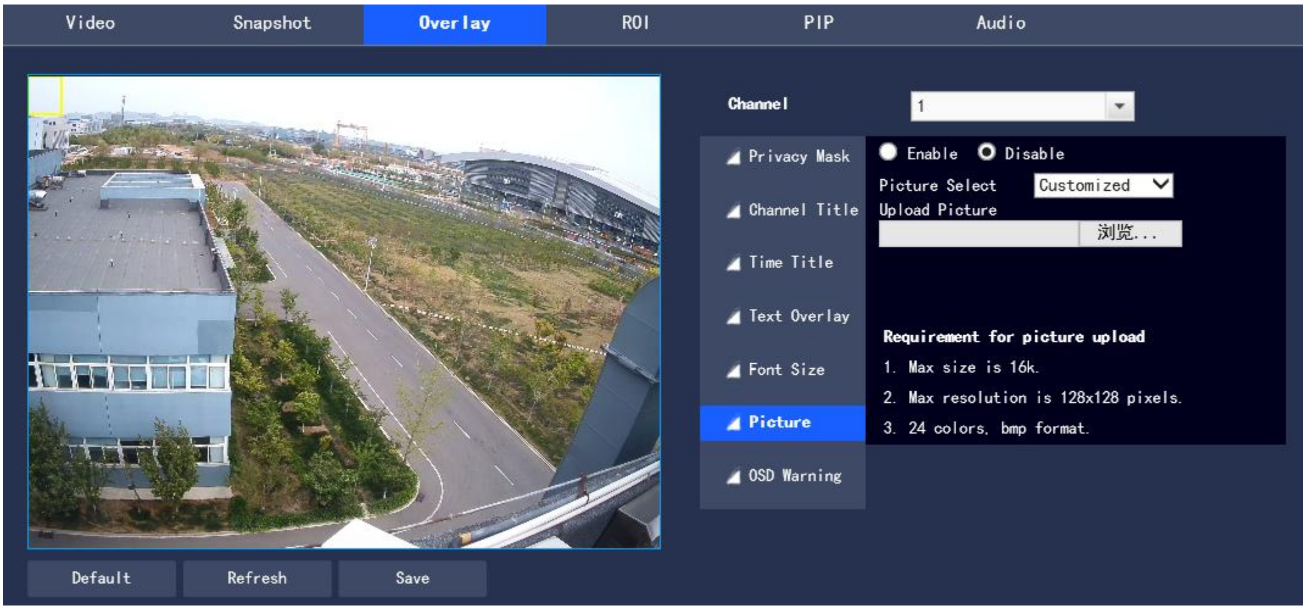
Font Size

● Small

○ Medium

● Large

Fig. 3.1-23 Video Overlay - Font Size



Channel 1

○ Enable ● Disable

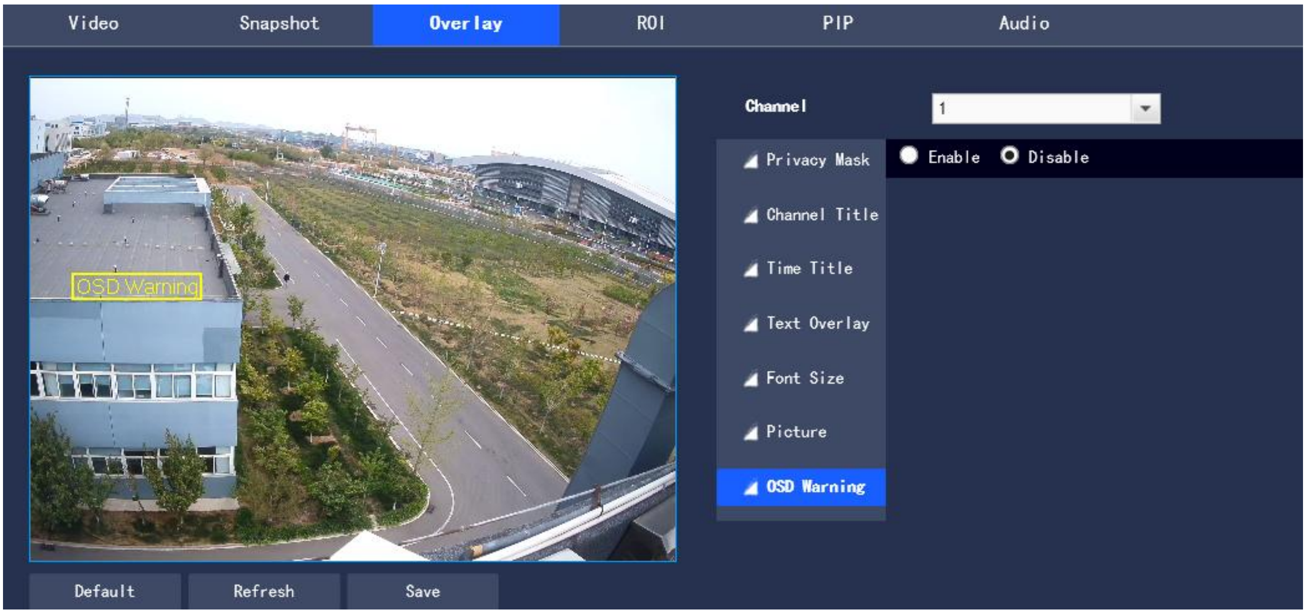
Picture Select: Customized

Upload Picture

Requirement for picture upload

1. Max size is 16k.
2. Max resolution is 128x128 pixels.
3. 24 colors, bmp format.

Fig. 3.1-24 Video Overlay - Picture Overlay



Channel 1

○ Enable ● Disable

Fig. 3.1-25 Video Overlay – OSD Warning

Parameters	Descriptions
Privacy Mask	Privacy Mask refers to setting a certain shielding area within the monitoring screen for privacy protection ● Click "Draw" to draw the privacy mask in the preview picture ● Click "Delete" to delete the corresponding privacy mask4 ● Click "Clear" to remove all privacy masks
Channel Title	Set to enable or disable Channel Title in the monitoring screen, and adjust its position by dragging the "Channel Title" box
Time Title	Set to enable or disable Time Title in the monitoring screen, whether to tick the Week Display box, and adjust the position by dragging the "Time Title" box

Geographic Location	Set whether to display the geographic location on the monitoring screen. You can adjust the position of the time title by dragging the "Geographic Location" box; alignment methods include left-aligned and right-aligned
Font Size	Set the font size in Video Overlay; support the sizes of "Small", "Medium" and "Large", with "Medium" as default
Picture Overlay	Set to enable or disable Overlay Picture in the video screen. Click to upload pictures, and the local picture can be superimposed on the video surveillance window. Adjust the position of the superimposed pictures by dragging the yellow box Note: The geographic/road information of OSD Info and Picture cannot be enabled at the same time
Abnormal Overlay	Set to enable or disable abnormal information in the monitoring screen.

Table 3.1-8 Video Overlay Parameter Setting Description

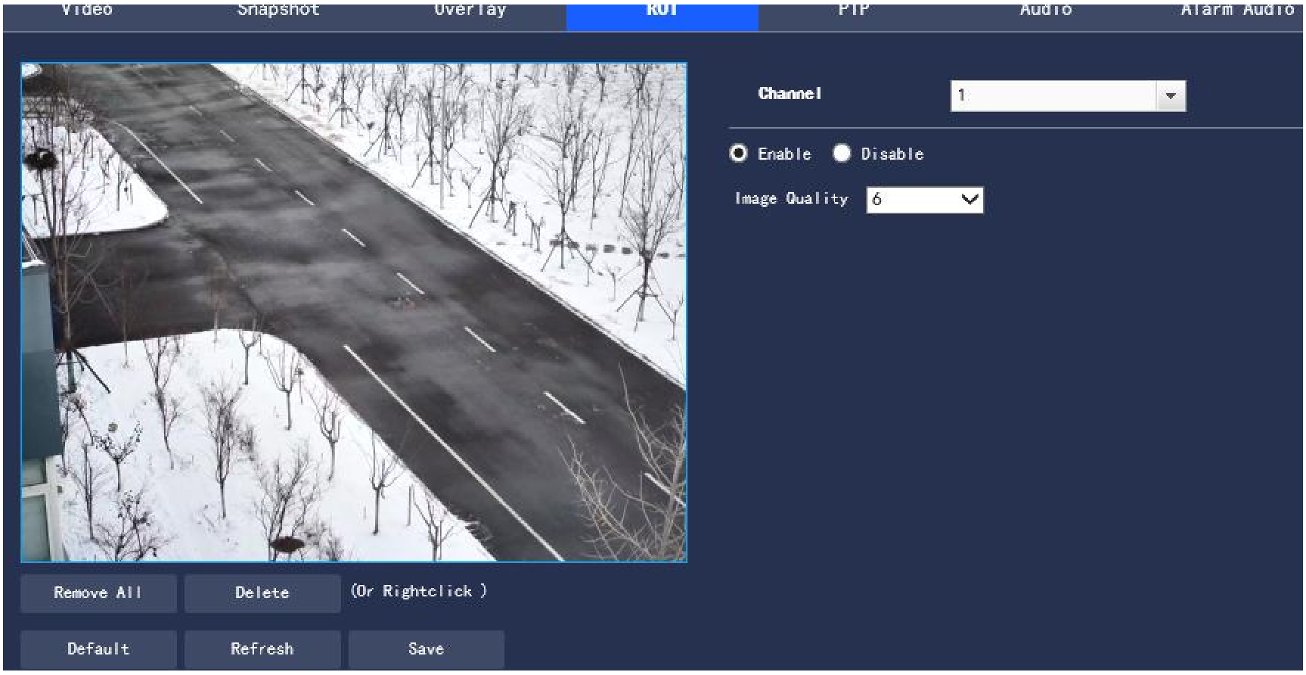
Step 3 Click "Save" to complete the configuration.

3.1.2.4 ROI

To set the key monitoring region as ROI, it can set the image quality of this region. The configuration steps are as follows:

Step 1 Select " Settings > Camera Settings > Encoding Settings > ROI"

The system displays the "ROI" interface as shown in Figure 3.1-26



Channel 1

○ Enable ● Disable

Image Quality 6

Figure 3.1-26 ROI Setting

Step 2 Select "Enable" to turn on the ROI function.

Step 3 Press and hold the left mouse button to select the region in the monitoring screen, up to 4 regions selected at a time.

- Click "Delete" or press the right mouse button to delete the selected region
- Click "Clear" to remove all selected regions

Step 4 Set Image Quality of corresponding ROI

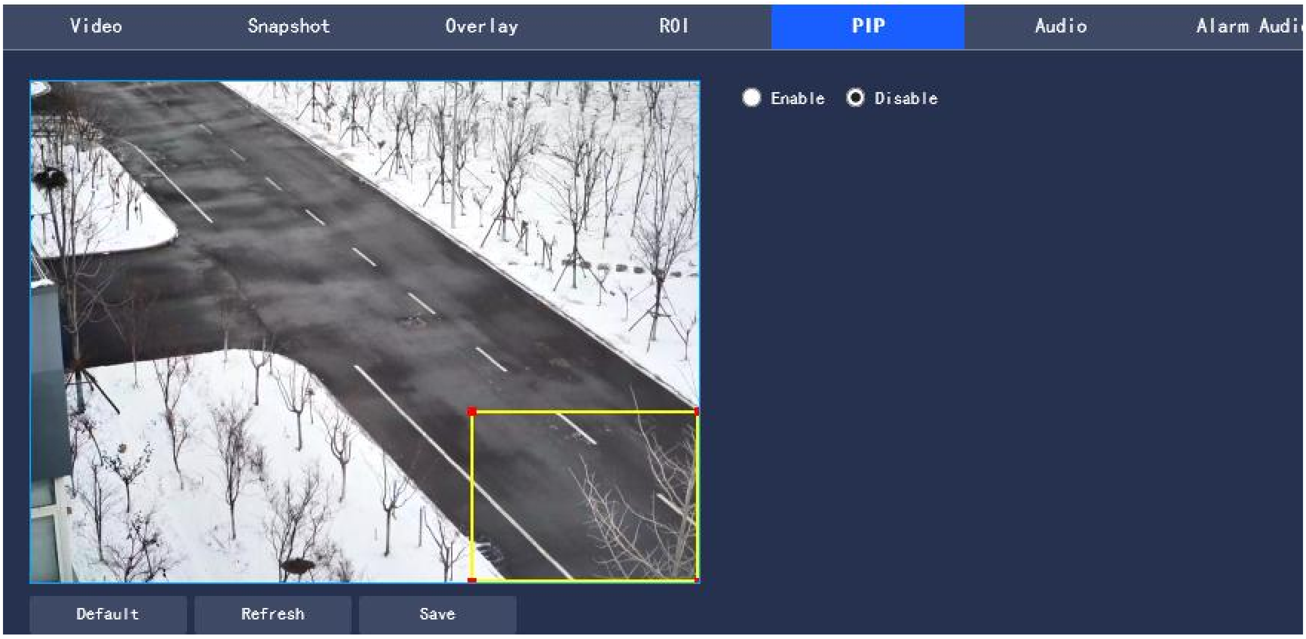
Step 5 Click "Save" to make the configuration effective

3.1.2.5 PIP

To set the PIP mode, the configuration steps are as follows:

Step 1 Select "Settings > Camera Settings > Encoding Settings > PIP"

The system displays the "PIP" interface as shown in Figure 3.1-27



○ Enable ● Disable

Figure 3.1-27 PIP

Step 2 Select "Enable" to turn on the PIP function

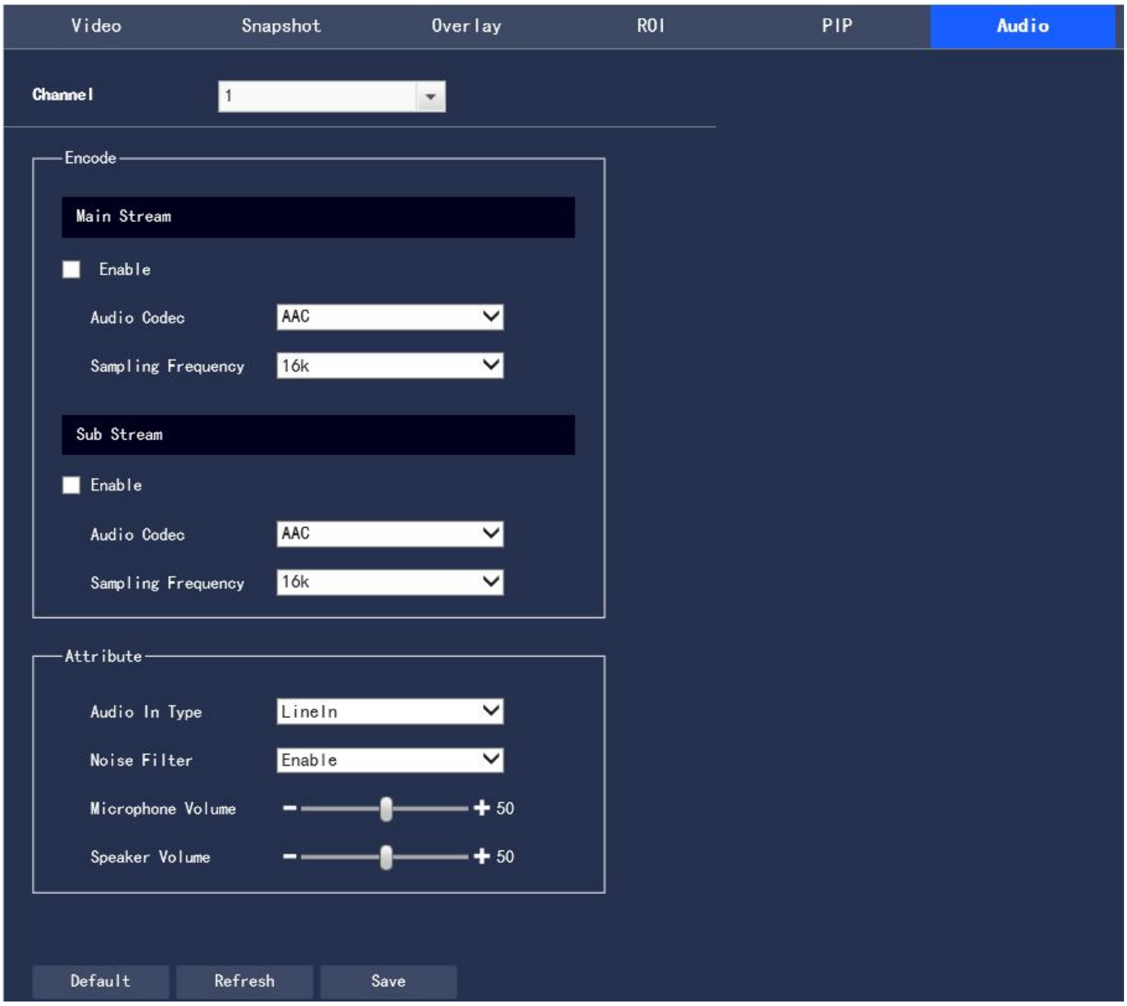
Step 3 Adjust the position and size of the thermal imaging region in the visible light monitoring screen

Step 4 Click "Save" to make the configuration effective

3.1.2.6 Audio

To set the audio parameters of the device, the configuration steps are as follows:

Step 1 Select "Settings > Camera Settings > Encoding Settings > Audio". The system displays the "Audio" interface as shown in Figure 3.1-28



Channel 1

Encode

Main Stream

□ Enable

Audio Codec AAC

Sampling Frequency 16k

Sub Stream

□ Enable

Audio Codec AAC

Sampling Frequency 16k

Attribute

Audio In Type LineIn

Noise Filter Enable

Microphone Volume 50

Speaker Volume 50

Figure 3.1-28 Audio Setting

Step 2 Configure each parameter information according to actual needs, and please refer to Table 3.1-9 for parameter description.

Parameters	Descriptions
Enable Audio	Select the audio channel number to be enabled, and the code stream transmitted by the network is a composite audio and video stream, otherwise only video images are included
Audio Codec	Audio Codec includes ACC and MPEG2-Layer2, with ACC as default
Sampling Frequency	Sampling Frequency supports 8K and 16K, with 16K as default
Audio-In Type	Set the audio in such types as LineIn or Mic, with Mic as default
Noise Filter	Set to enable or disable the Noise Filter function, with Enable as default

Microphone Volume	Adjust the volume of the microphone within the range of 0～100, 100 by default.
Speaker Volume	Adjust the volume of the speaker within the range of 0～100, 100 by default.

Table 3.1-9 Audio Parameter Setting Description

Step 3 Click "Save" to complete the setting.

3.2 Network Settings

3.2.1 General Settings

3.2.1.1TCP/IP

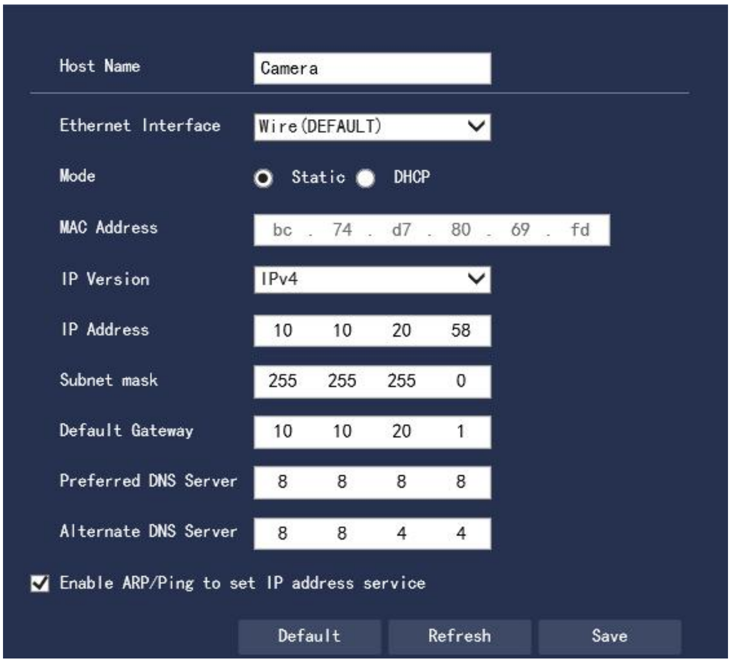
Configure the IP address and DNS server of the camera to ensure its interconnection with other devices in the network.

Note: Please confirm the correct connection of the camera to the network before setting the network parameters.

● If there is not a routing device in the network, please assign an IP address in the same network segment

● If there is a routing device in the network, the corresponding gateway and subnet mask should be set

Step 1 In the system menu, select "Settings > Network Settings > General Settings > TCP/IP". The system displays the "TCP/IP" interface as shown in the Figure 3.2-1



Host Name	Camera
Ethernet Interface	Wire(DEFAULT)
Mode	● Static ○ DHCP
MAC Address	bc . 74 . d7 . 80 . 69 . fd
IP Version	IPv4
IP Address	10 10 20 58
Subnet mask	255 255 255 0
Default Gateway	10 10 20 1
Preferred DNS Server	8 8 8 8
Alternate DNS Server	8 8 4 4

☑ Enable ARP/Ping to set IP address service

Figure 3.2-1 TCP/IP Configuration

Step 2 To configure TCP/IP parameters, please refer to Table 3.2-1 for detailed parameter descriptions.

Parameters	Descriptions
Host Name	Set the name for the current host device within the maximum length of 15 characters
NIC	Select the network interface card (NIC) to be configured, with Wire as default Note: When the device has multiple NICs, the default one can be changed. To reset the default NIC, it should restart the device.
Mode	Static and DHCP modes are available. When the DHCP mode is selected, IP address is automatically filled and the IP/mask/gateway cannot be changed; when the Static mode is selected, the IP/mask/gateway needs to be manually set
MAC Address	Display the address of device MAC
IP Version	Two address formats of IPv4 and IPv6 are available. Currently, both IP addresses are supported and can be accessed
IP Address	Enter the corresponding number to change the IP address
Subnet Mask	Make settings according to the actual situation. The numeric subnet prefix

	supports to enter 1～255, and identifies a specific network link, usually including a hierarchical structure Note: The device will check the validity of all IPv6 addresses, and the IP address and the default gateway must be in the same network segment, that is, to pass the inspection, the length of the subnet prefix must be the same
Default Gateway	Make settings according to the actual situation, and it must be in the same network segment as IP Address
Preferred DNS Server	DNS Server IP address
Alternate DNS Server	Alternate IP address of DNS Server
Enable ARP/Ping to set IP address service	If the MAC address is known, the device IP address can be modified and set through the ARP/Ping command When it is enabled by default, during the device restarting, the device IP can be set through a ping packet of a specific length within 2 minutes. After 2 minutes, the service will be turned off, or turned off immediately after the successful IP setting; if it is disabled, the IP setting through the ping packet is impossible

Table 3.2-1 TCP/IP Parameter Description

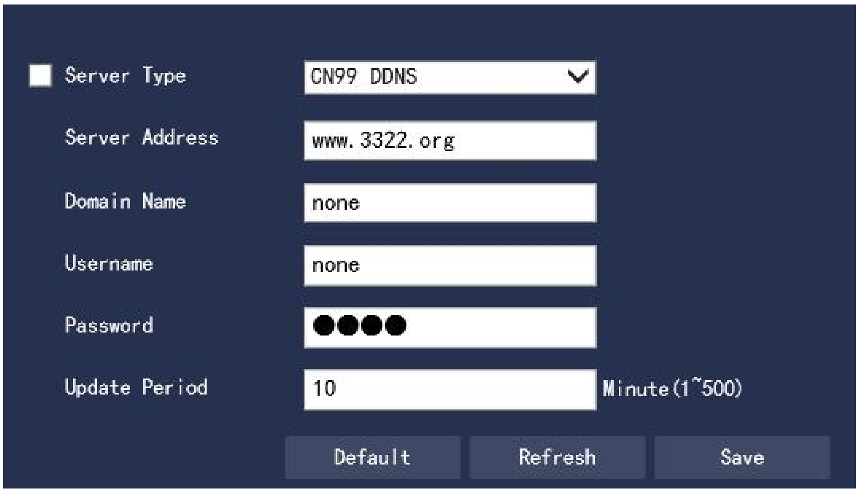
Step 3 Click "Save" to complete the setting.

3.2.1.2 DDNS

DDNS (Dynamic Domain Name Server) is used when the IP address of the device changes frequently, to dynamically update the relationship between the domain name and the IP address on the DNS server to ensure the device access of users through the domain name.

Note: Before configuration, please confirm whether the device supports the domain name server type, and log in to the website of the DDNS server provider on the WAN PC to register the domain name and other information

If DDNS type is selected as other types, the interface is shown in Figure 3.2-2. Please set DDNS parameters by referring to Table 3.2-2.



□ Server Type: CN99 DDNS

Server Address: www.3322.org

Domain Name: none

Username: none

Password: ●●●●

Update Period: 10 Minute(1~500)

Figure 3.2-2 DDNS Interface

Parameters	Descriptions
Server Type	The address corresponding to the name of the DDNS server provider is as follows: ● The address of CN99 DDNS is: members.3322.org ● The address of NO-IP DDNS is: dynupdate.no-ip.com ● The address of Dynans DDNS is: members.dyndns.org
Server Address	
Domain Name	The registered domain name of users on the website of the DDNS server provider
Username	Enter the username and password obtained from the DDNS service provider. The user has to get registered (including username and password) on the website of the DDNS server provider
Password	
Update Period	Specify the time interval for regularly initiating update requests after the DDNS update is started, in unit of minutes

Table 3.2-2 DDNS Parameter Description

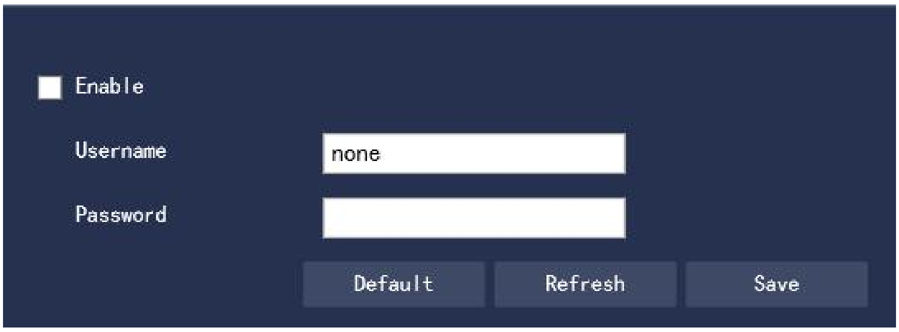
1. After setting, click "Save"

2. Enter the domain name in the PC web browser and press [Enter]; if the device web interface can be displayed, it is successful; if not, the configuration is failed.

3.2.1.3 PPPoE

By enabling the PPPoE (Point-to-Point Protocol over Ethernet) dial-up mode to establish a network connection, the device will obtain a dynamic IP address for the WAN. Before enabling, please obtain the PPPoE username and password provided by the ISP (Internet Service Provider)

Step 1 Select "Settings > Network Settings > General Settings > PPPoE". The system displays the "PPPoE Setup" interface as shown in Figure 3.2-3.



□ Enable

Username: none

Password:

Figure 3.2-3 PPPoE Interface

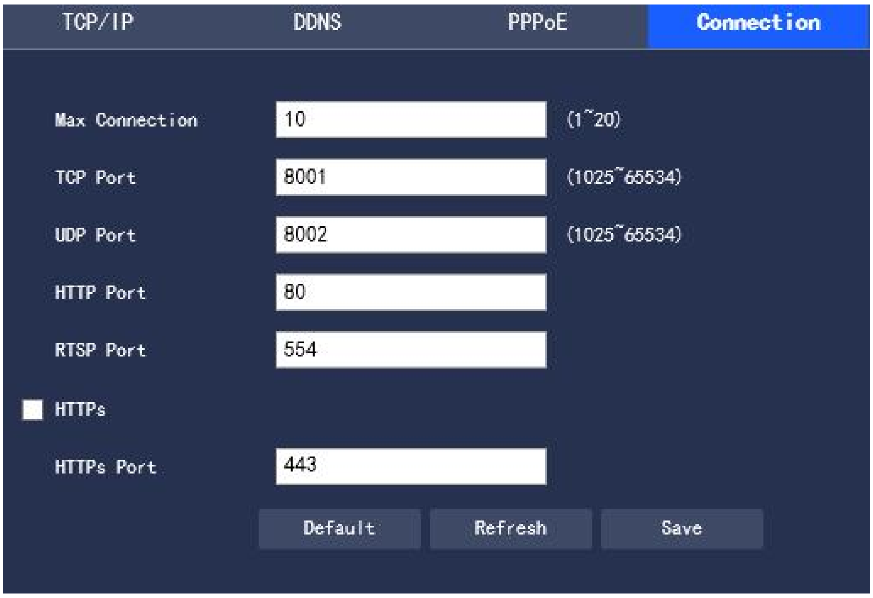
Step 2 Select "Enable" and enter the PPPoE Username and Password.

Step 3 Click "Save" to complete the PPPoE configuration. When the system prompts "Save successfully" and displays the obtained public network IP address in real time, users are allowed to access the device through this IP.

3.2.1.4 Connection

The maximum number of connection ports for the device and the value of each port can be configured on this interface.

Step 1 Select "Settings > Network Settings > General Settings > Connection". The system displays the "Connection" interface as shown in Figure 3.2-4



Max Connection 10 (1~20)

TCP Port 8001 (1025~65534)

UDP Port 8002 (1025~65534)

HTTP Port 80

RTSP Port 554

□ HTTPs

HTTPs Port 443

Figure 3.2-4 Connection

Step 2 To Configure the value of each port for the device, please refer to Table 3.2-3 for detailed parameter description.

Parameters	Descriptions
Max Connection	The maximum number of WEB logins for the user of the same device and the setting range is 1～20 with 20 as default
TCP Port	The setting of the TCP protocol communication service port is subject to users' actual needs, with "8001" as default
UDP Port	The setting of the user data packet protocol port is subject to users' actual needs, with "8002" as default
HTTP Port	The setting of the HTTP communication port is subject to users' actual needs, with "80" as default
RTSP Port	The RTSP default port number is 554, and if it is the default value, leave it blank. The following format is available when users use VLC to play the real-time monitoring. Real-time monitoring stream URL format. To request the real-time monitoring

	stream RTSP streaming media service, the requested channel number and stream type should be specified in the URL. If authentication information is required, the username and password should also be provided. rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0 Username: User name, such as admin. Password: Password, such as admin. IP: Device IP, such as 192.168.1.122. Port: Port number, the default is 554, and if it is the default value, leave it blank. Channel: Channel number, starting with 1. If it is channel 2, then channel=2. Subtype: Stream type, the main stream is 0 (that is, subtype=0), and the sub stream is 1 (that is, subtype=1). For example, to request the channel 2 sub stream of a certain device, the URL is as follows: rtsp://admin:admin@192.168.1.123:554/cam/realmonitor?channel=2&subtype=1 If authentication is not required, it is no need to specify the username and password, just to use the following format: rtsp://ip:port/cam/realmonitor?channel=1&subtype=0
Enable HTTPs	HTTPs communication service control. When it selects to "Enable HTTPs", https://ip:port can be adopted to log in to the device; the https://ip can be used to log in at the default port. Default enable is off
HTTPs Port	The setting of the HTTPs communication port is subject to users' actual needs, with as "443" by default

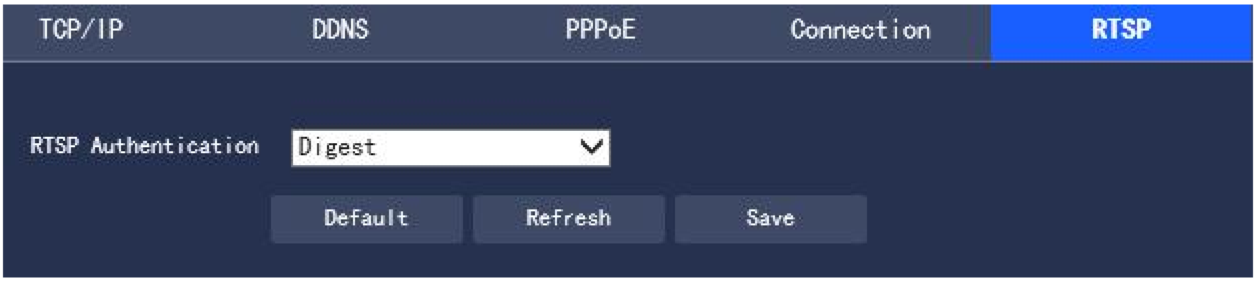
Table 3.2-3 Connection Parameter Description

Step 3 Click "Save" to complete the setting.

3.2.1.5 RTSP

You can configure the RTSP authentication method of the camera on this interface.

Step 1 Select "Settings> Network Settings> General Settings> RTSP", the system displays the "Connect" interface, as shown in Figure 3.2-5:



RTSP Authentication: Digest

Figure 3.2-5 RTSP Setting

Step 2 Select the authentication method to be set: None/Basic/Digest, the default is Digest;

Step 3 Click "Save" to complete the setting.

3.2.1.6 UPnP

Users on the external network can access the internal network device by visiting the external IP address through the UPnP protocol to establish a mapping relationship between the private network and the external network. The internal port is a network camera port, while the external port is a router port. The user can access the network camera when accessing the external port. When the router is not used for UPnP, please turn off the UPnP function to avoid affecting the use of other functions

When the UPnP is enabled, the network camera supports the UPnP protocol. In the Windows XP or Windows Vista operating system, if the system UPnP is enabled, the network camera is automatically detected in Windows Network Neighborhood

Refer to the following steps to install the UPnP network service in Windows operating systems:

Step 1 Open Control Panel and select "Add or Remove Programs"

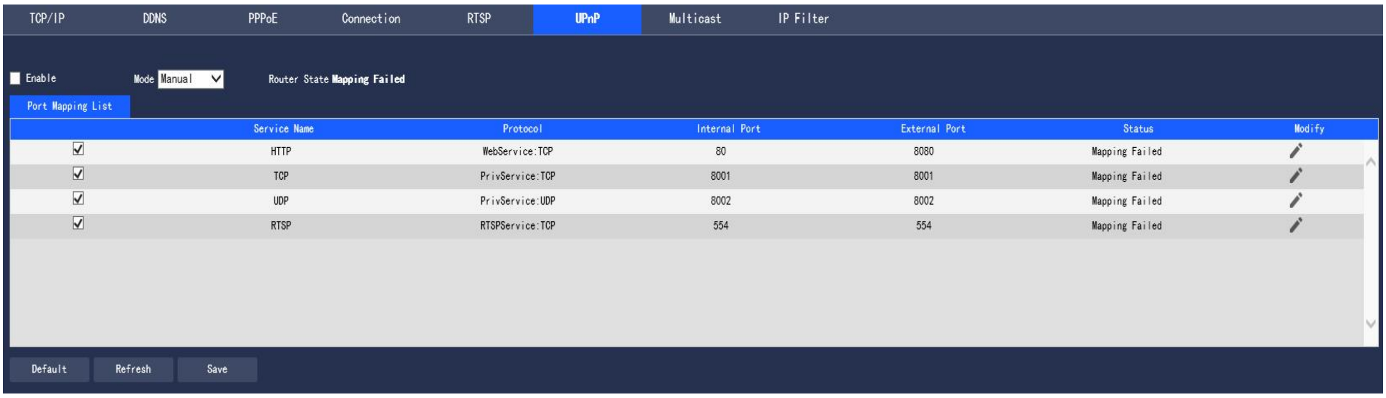
Step 2 Click "Add/Remove Windows Components".

Step 3 Select "Network Service" in the wizard and click "Details"

Step 4 Select "Internet Gateway Device Discovery and Control Client" and "UPnP User Interface", confirm and install.

The UPnP configuration steps are as follows:

Step 1 Select "Settings > Network Settings > General Settings > UPnP". The system displays the "UPnP" interface as shown in Figure 3.2-5



□ Enable Mode Manual Router State Mapping Failed

	Service Name	Protocol	Internal Port	External Port	Status	Modify
☑	HTTP	WebService:TCP	80	8080	Mapping Failed	✎
☑	TCP	PrivService:TCP	8001	8001	Mapping Failed	✎
☑	UDP	PrivService:UDP	8002	8002	Mapping Failed	✎
☑	RTSP	RTSPService:TCP	554	554	Mapping Failed	✎

Figure 3.2-6 UPnP

Step 2 Select the check box to enable the UPnP function.

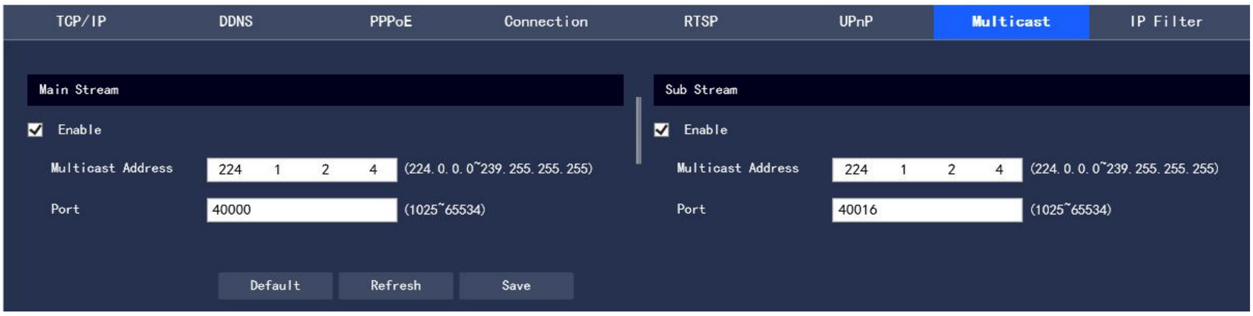
Step 3 Select Mode.UPnP supports two mapping modes: automatic and manual modes. The manual mapping mode allows users to modify external ports, while as the automatic mapping mode selects unoccupied ports to automatically complete port mapping, there is no need for users to change the mapping

Step 4 Click "Save" to make the configuration effective

3.2.1.7 Multicast

To preview the video screen through the network access device, if it exceeds the device access limit, the video screen cannot be previewed. At this time, it can be solved by setting the multicast IP to the device and using the multicast protocol access.

Step 1 Select "Settings > Network Settings > General Settings > Multicast". The system displays the "Multicast" interface as shown in Figure 3.2-7



Main Stream

☑ Enable

Multicast Address 224 1 2 4 (224.0.0.0~239.255.255.255)

Port 40000 (1025~65534)

Sub Stream

☑ Enable

Multicast Address 224 1 2 4 (224.0.0.0~239.255.255.255)

Port 40016 (1025~65534)

Figure 3.2-7 Multicast

Step 2 Select "Enable" to enable the multicast function.

Step 3 Enter the multicast address and port.

Step 4 Click "Save" to complete the configuration.

3.2.1.7 IP Filter

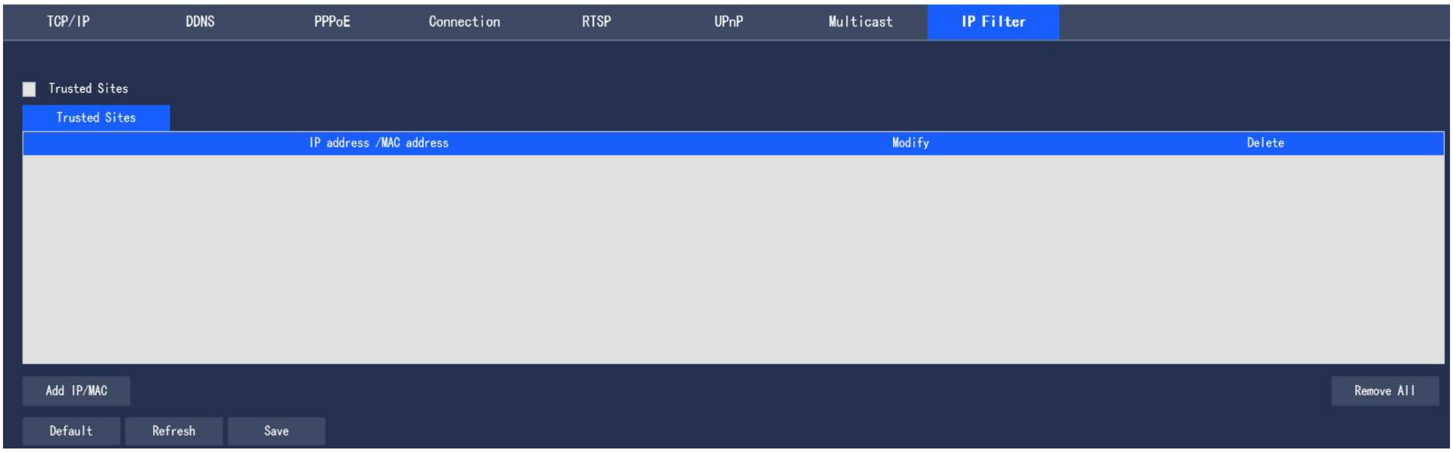
The user can set the users allowed to access the camera through IP Filter

● Trusted Sites: add IP/MAC of users allowed to log in to the camera. If Trusted Sites is enabled, only the users whose IP/MAC is in the list are allowed to log in to this camera; if not, there is no restriction on users to access this camera.

● Users are not allowed to add the device IP/MAC to Trusted Sites

The MAC verification will take effect when the IP of the device and the PC are in the same LAN

Step 1 Select "Settings > Network Settings > General Settings > IP Filter". The system displays the "IP Filter" interface as shown in Figure 3.2-8



☐ Trusted Sites

IP address /MAC address	Modify	Delete

Figure 3.2-8 IP Filter Interface

Step 2 Select the corresponding check box to enable the Trusted Sites

Step 3 Click "Add IP/MAC", and configure the IP address information in the pop-up dialog box, by reference to Table 3.2-4

Parameter	Description
IP Address	Enter the host IP address to be added
IP Network Segment	Enter the start address and end address of the network segment to be added
MAC	Enter the host MAC address to be added

Table 3.2-4 IP Filter Parameter Description

Step 4 Click "Save" to make the configuration effective; Use the IP host in Trusted Sites to log in to the device web interface, and it can log in to the device successfully

3.2.2 Advanced Settings

3.2.2.1 SNMP

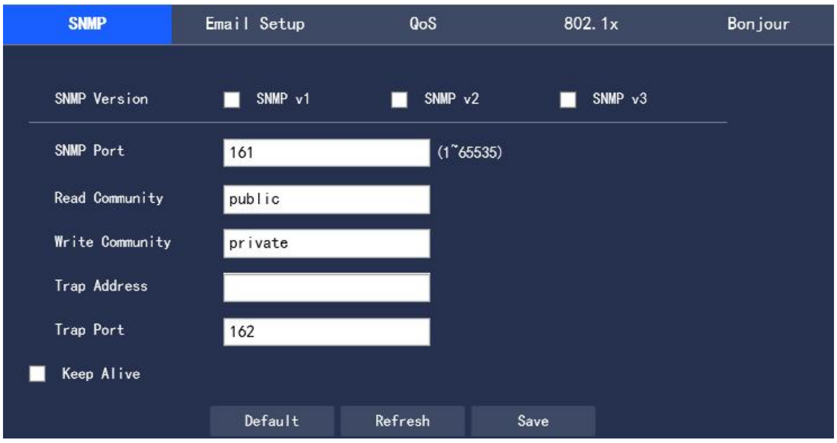
SNMP (Simple Network Management Protocol) provides the network management system with a framework for the underlying network management; SNMP functions can be controlled in the network service settings; through the relevant software tools, after successful connection to the device, the relevant device configuration information can be obtained

The following conditions must be met to enable the SNMP function:

● Install SNMP equipment monitoring and management tools, such as MIB Builder and MG-SOFT MIB Browser

● Obtain two MIB files corresponding to the current version from technical support

Step 1 Select "Settings > Network Settings > Advanced Settings > SNMP". The system displays the "SNMP" interface as shown in Figure 3.2-9 and 3.2-10



SNMP Version □ SNMP v1 □ SNMP v2 □ SNMP v3

SNMP Port 161 (1~65535)

Read Community public

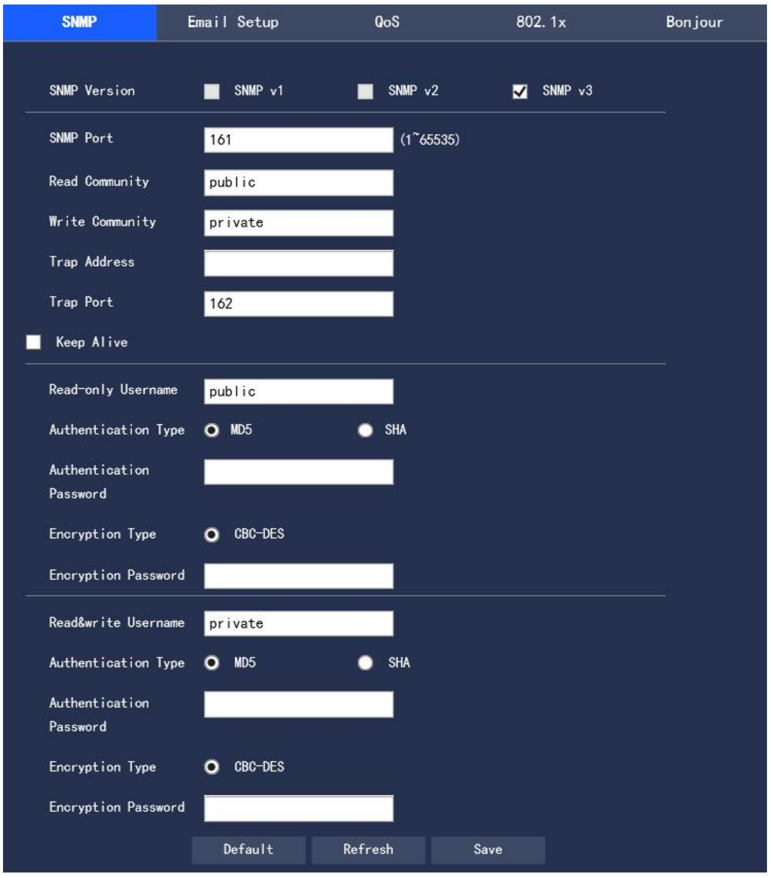
Write Community private

Trap Address

Trap Port 162

□ Keep Alive

Figure 3.2-9 SNMP (1)



SNMP Version □ SNMP v1 □ SNMP v2 ☑ SNMP v3

SNMP Port 161 (1~65535)

Read Community public

Write Community private

Trap Address

Trap Port 162

□ Keep Alive

Read-only Username public

Authentication Type ● MD5 ○ SHA

Authentication Password

Encryption Type ● CBC-DES

Encryption Password

Read&write Username private

Authentication Type ● MD5 ○ SHA

Authentication Password

Encryption Type ● CBC-DES

Encryption Password

Figure 3.2-10 SNMP (2)

Step 2 To configure each parameter information according to actual needs, refer to Table 3.2-5 for parameter description

Parameters	Descriptions
SNMP Version	● For SNMP v1, the device can only process the information in v1 version ● For SNMP v2, the device can only process information in v2 version ● for SNMP v3, it supports the settings of the account, password and

	authentication type. When the server is going to access the device, the corresponding account, password and authentication type must be set for security verification, and the v1 and v2 versions are not subject to selection.
SNMP Port	The agent listening port on the device. The range is 1～65535 with 161 as default
Community	It is a string, as a clear text password between the management process and the agent process, and defines the authentication, access control, and escrow relationship between an agent and a group of managers. It should ensure consistency between the device and the agent
Read Community	With the specified name, read-only access to all SNMP-supported objects. The default configuration is: public
Write Community	With the specified name, read/write access to all SNMP-supported objects. The default configuration is: private
Trap	SNMP Trap refers to an SNMP agent sending information to the administrator, and an agent notifying important events or status changes of the management station.
Trap Address	The destination address for the agent on the device to send the Trap message
Trap Port	The destination port for the agent on the device to send the Trap message. The range is 1～65535 with 162 as default
Read-only Username	The default is public ● The name consists of numbers, letters, and underscores only
Read&write Username	The default is private ● The name consists of numbers, letters, and underscores only
Authentication Type	The MD5 or SHA type is available with MD5 as default
Authentication Password	The password length is no less than 8 digits
Encryption	The default is CBC-DES

Type	
Encryption Password	The password length is no less than 8 digits

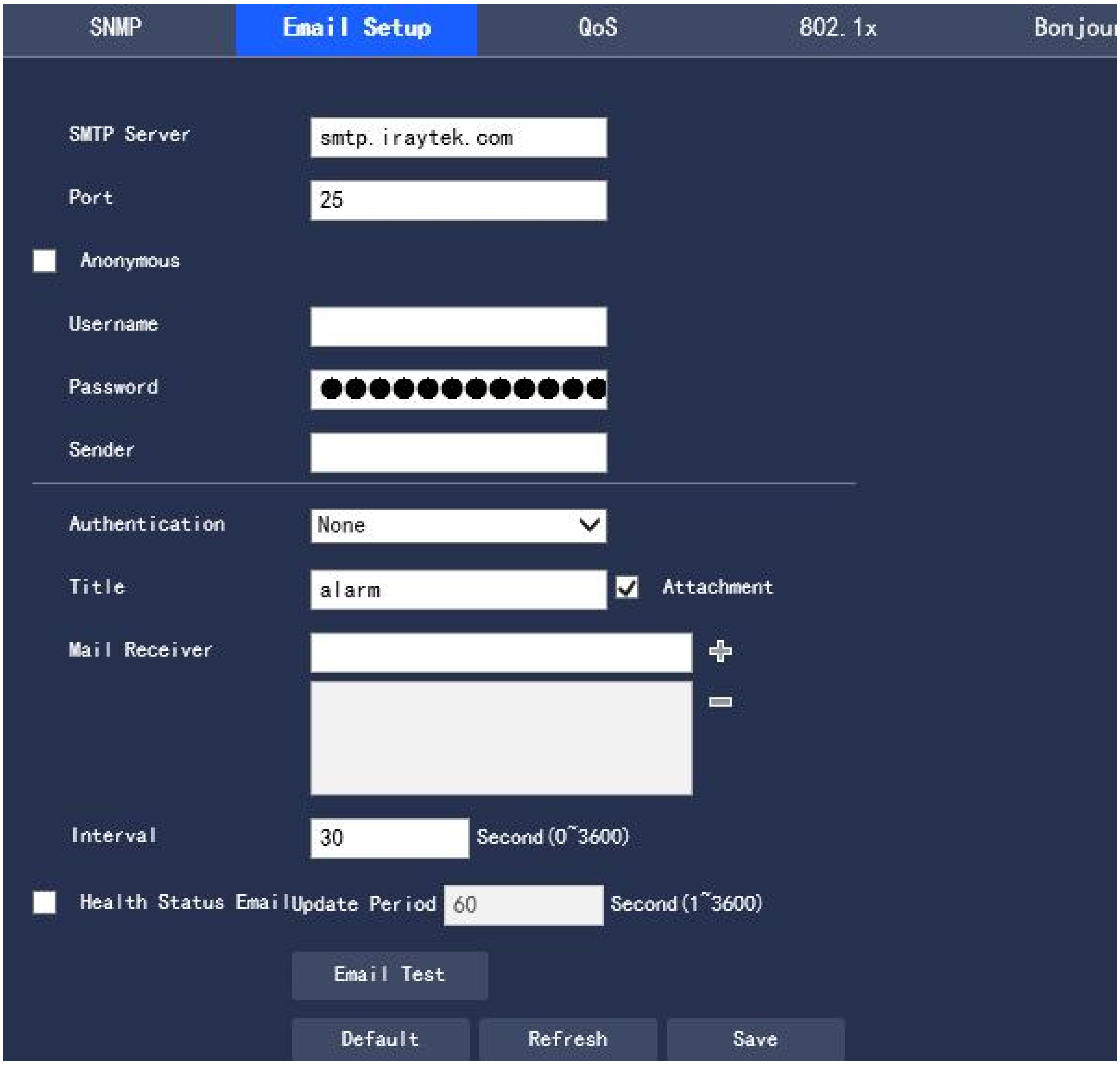
Table 3.2-5 SNMP Parameter Setting Description

Step 3 Click "Save" to make the configuration effective.

3.2.2.2 Email Setup

By setting Email Setup, when alarms, video detections, or abnormal events occur, an e-mail will be sent immediately. When alarms, video detection, and abnormal events are triggered, an email will be sent to the recipient's server through SMTP Server. The recipient logs in to the receiving server to receive the email.

Step 1 Select "Settings > Network Settings > Advanced Settings > Email Setup". The system displays the "SMTP (Mail)" interface as shown in Figure 3.2-11



SMTP Server smtp. iraytek. com

Port 25

□ Anonymous

Username

Password ●●●●●●●●●●●●●

Sender

Authentication None

Title alarm ☑ Attachment

Mail Receiver

Interval 30 Second(0~3600)

□ Health Status EmailUpdate Period 60 Second(1~3600)

Figure 3.2-11 Email Setup

Step 2 To configure each parameter information according to actual needs, refer to Table 3.2-6 for parameter description.

Parameters	Descriptions
SMTP Server	The IP address of the outgoing SMTP mail server
Port	The port number of the outgoing SMTP mail server, with 25 as default
Anonymous	For servers that support the anonymous mail, it supports the anonymous login automatically without entering the username, password and sender information

Username	Username of the email-sending mailbox
Password	Password of the email-sending mailbox
Sender	Address of the email-sending mailbox
Authentication	It supports SSL, TLS or none
Attachment	If attachment is selected, an email with a Image capture picture can be sent
Title	The email title is subject to customization
Mail Receiver	Enter the recipient address of the outgoing mail, and up to three mail receivers are allowed
Interval	The value range of interval for email sending is 0 ～ 3600 seconds, and "0" means sending email without intervals; If Interval is enabled, when the email is triggered by alarms, video detections, and abnormal events, the mail will be sent according not to the immediate alarm signal trigger, but to the interval of the previous mails for the same type of events. It is mainly applied in the phenomenon of over pressure on the mail server for a large number of emails generated from frequent abnormal events.
Health Status Email	Health Status Email can use the test information sent by the system to determine whether the email link is successful. If Health Status Email is enabled with the setting of Interval for sending emails, then the system will send the email test information according to the set interval
Email Test	Test whether the email sending and receiving functions is normal. If the configuration is correct, the mailbox will receive the test email; before the test, the mail configuration information should be saved

Table 3.2-6 Email Setup Parameter Description

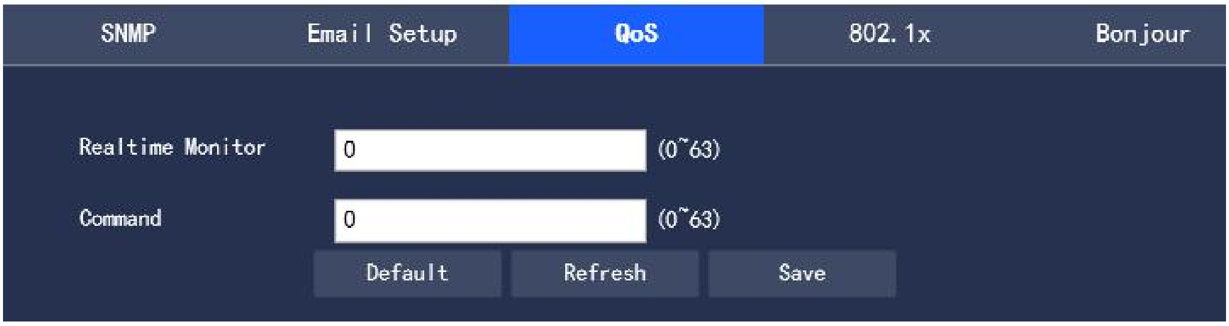
Step 3 Click "Save" to complete the setting.

3.2.2.3 Qos

QoS (Quality of Service) is a security mechanism for the network, which is a kind of technology used to solve such problems as network delay and congestion. For network services, QoS includes transmission bandwidth, transmission delay, data packet loss rate; in the network, the QoS can be improved through such measures as the guarantee of the transmission bandwidth, the reduction in the transmission delay and the data packet loss rate as well as the delay jitter.

For DSCP (Differentiated Services Code Point), there are 64 priority levels (0～63), identifying the different priorities of the packet. 0 is the lowest priority and 63 is the highest priority. Different outgoing queues are selected according to the packet priority, and the bandwidth resources occupied by different outgoing queues have different discard ratios when congested, so as to achieve the service quality goal.

Step 1 Select "Settings > Network Settings > Advanced Settings > QoS". The system displays the "QoS" interface as shown in Figure 3.2-12



Realtime Monitor 0 (0~63)

Command 0 (0~63)

Figure 3.2-12 QoS Interface

Step 2 To set Real-time Monitor and Command, please refer to Table 3.2-7 for parameter description

Parameters	Descriptions
Real-time Monitor	The value range of the data packet for network video surveillance is 0～63
Command	The value range of the non-monitoring data packets such as device configuration and query is 0～63

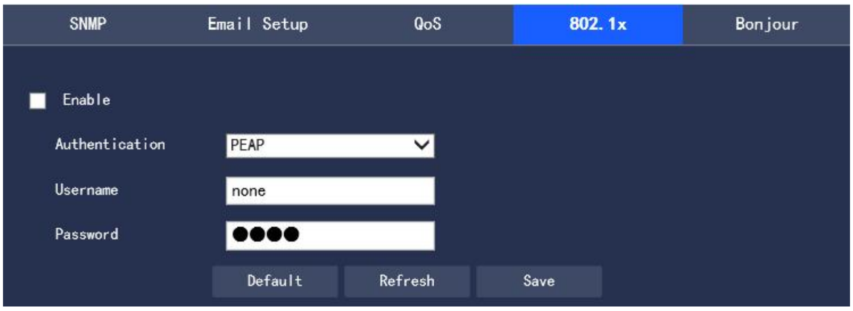
Table 3.2-7 QoS Parameter Setup Description

Step 3 Click "Save" to complete the configuration.

3.2.2.4 802.1x

802.1x is called port based network access control protocol. It supports users to manually select the authentication type to control whether the device connected to the LAN can access the LAN, and can well support the network authentication, billing, security and management requirements.

Step 1 Select "Settings > Network Settings > Advanced Settings > 802.1x". The system displays the "802.1x" interface as shown in Figure 3.2-13



□ Enable

Authentication: PEAP

Username: none

Password: ●●●●

Figure 3.2-13 802.1x

Step 2 Select "Enable" to turn on the 802.1x function

Step 3 Select the Authentication type, and set Username and Password. Please refer to Table 3.2-8 for the parameter description

Parameters	Descriptions
Authentication	PEAP(protected EAP protocol)
Username	The user name for authentication needs to be a name that is recognized and authorized on the server side
Password	The set Password should be corresponding to Username

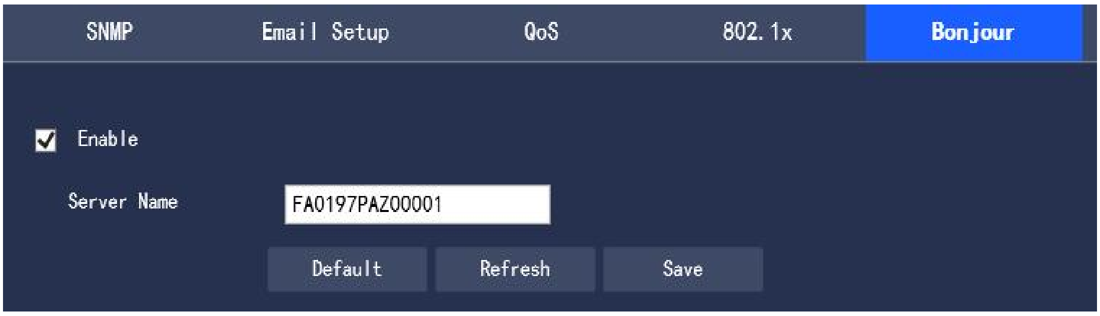
Table 3.2-8 802.1x Parameter Setup Description

3.2.2.5 Bonjour

Bonjour, also known as zero-configuration networking, can automatically discover computers, devices, and services on an IP network. Bonjour uses industry standard IP protocol to allow devices to automatically discover each other without the need to enter IP addresses or configure DNS servers

After the Bonjour function is enabled, the network camera will be automatically detected in Bonjour-supported operating systems and clients. When the network camera is automatically detected by Bonjour, the "Server Name" configured by the user will be displayed.

Step 1 Select "Settings > Network Settings > Advanced Settings > Bonjour". The system displays the "Bonjour" interface as shown in Figure 3.2-14



☑ Enable

Server Name FA0197PAZ00001

Figure 3.2-14 Bonjour

Step 2 Select "Enable" and set Server Name.

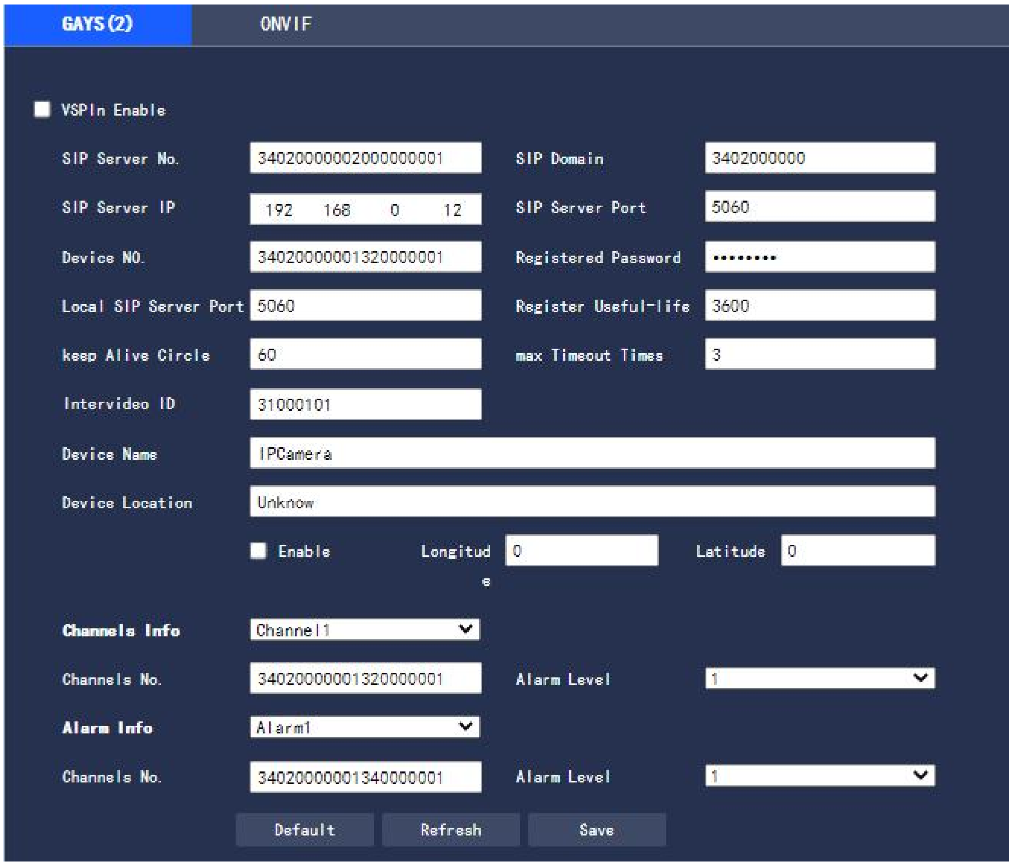
Step 3 Click "Save" to make the configuration effective.

3.2.3 Platform Settings

3.2.3.1 GB 28181(1)

GB28181 refers to the "Security and protection video monitoring network system technical specification for information transport, switch and control" (GB/T 28181-2011), industry abbreviation: SIP national standard. This specification specifies in the security and protection video monitoring network system (hereinafter referred to as the "network system") the information transmission, exchange and control interconnection structure and communication protocol structure, basic requirements and security requirements for transmission, exchange and control, as well as control, transmission process, protocol interfaces and other technical requirements.

Step 1 Select "Settings > Network Settings > Platform Setup > GB 28181(1)". The system displays the "GB 28181" interface as shown in Figure 3.2-15



□ VSPIn Enable

SIP Server No. 34020000002000000001
SIP Domain 3402000000
SIP Server IP 192 168 0 12
SIP Server Port 5060
Device NO. 34020000001320000001
Registered Password ••••••••
Local SIP Server Port 5060
Register Useful-life 3600
keep Alive Circle 60
max Timeout Times 3
Intervideo ID 31000101
Device Name IPCamera
Device Location Unknow
□ Enable Longitude 0 Latitude 0
Channels Info Channel1
Channels No. 34020000001320000001
Alarm Level 1
Alarm Info Alarm1
Channels No. 34020000001340000001
Alarm Level 1

Figure 3.2-15 Platform Access-GB 28181

Step 2 To configure each parameter information according to actual needs, please refer to Table 3.2-9 for parameter description.

Parameters	Descriptions
SIP Server No.	28181 Server platform number
SIP domain	28181 Server platform domain number
SIP Server IP	28181 Server IP
SIP Server Port	28181 Server Port
Keep Alive Circle	Keep-alive time between the device and 28181 Server
Timeout Times	Count the number of timeouts between the device and 28181 Server. Once this number is exceeded, the device actively disconnects the communication with 28181 Server
Intervideo ID	It indicates how the device communicates with 28181 Server, generally with

	the value agreed between the device side and the server side

Table 3.2-9 Platform Access-GB 28181 Parameter Setup Description

Step 3 Click "Save" to complete the configuration.

3.2.3.2 ONVIF

The ONVIF (Open Network Video Interface Forum) standard aims to implement a network video framework protocol, making network video products (including the camera front end and the video taking equipment) produced by different vendors fully interoperable.

Step 1 Select "Settings > Network Settings > Platform Settings > ONVIF". The system displays the "ONVIF" interface as shown in Figure 3.2-16

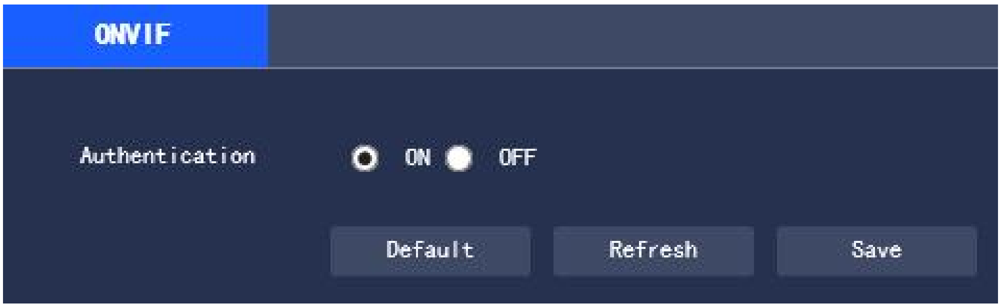


Figure 3.2-16 ONVIF

Step 2 Set "Authentication" to "On"

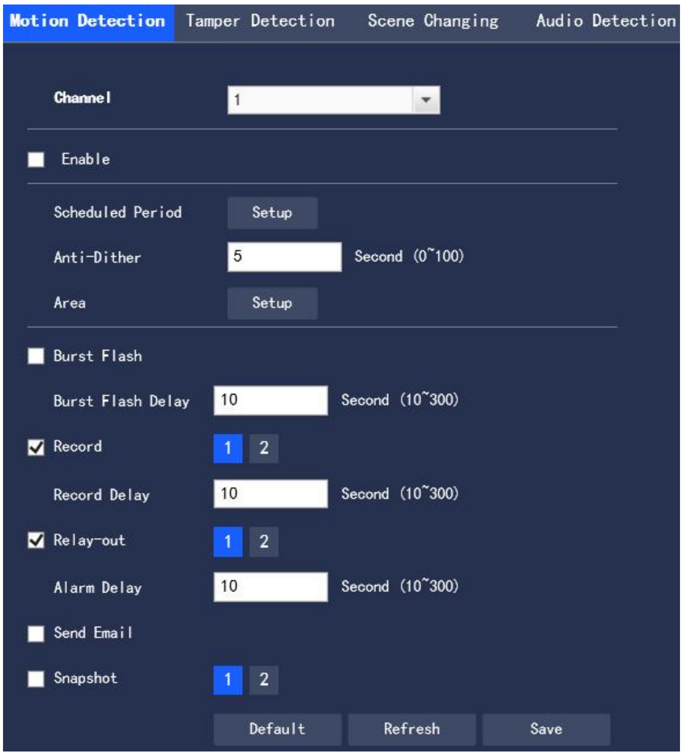
Step 3 Click "Save" to complete the setting

3.3 Event Management

3.3.1 General Events

3.3.1.1 Motion Detection

Step 1 Select "Settings > Event Management > General Events > Motion Detection". The system displays the "Motion Detection" interface as shown in Figure 3.3-1



Channel 1

□ Enable

Scheduled Period

Anti-Dither 5 Second (0~100)

Area

□ Burst Flash

Burst Flash Delay 10 Second (10~300)

☑ Record 1 2

Record Delay 10 Second (10~300)

☑ Relay-out 1 2

Alarm Delay 10 Second (10~300)

□ Send Email

□ Snapshot 1 2

Figure 3.3-1 Video Detection-Motion Detection Setting

Step 2 Select "Enable" and to configure each parameter information according to actual needs, refer to Table 3.3-1 for parameter description

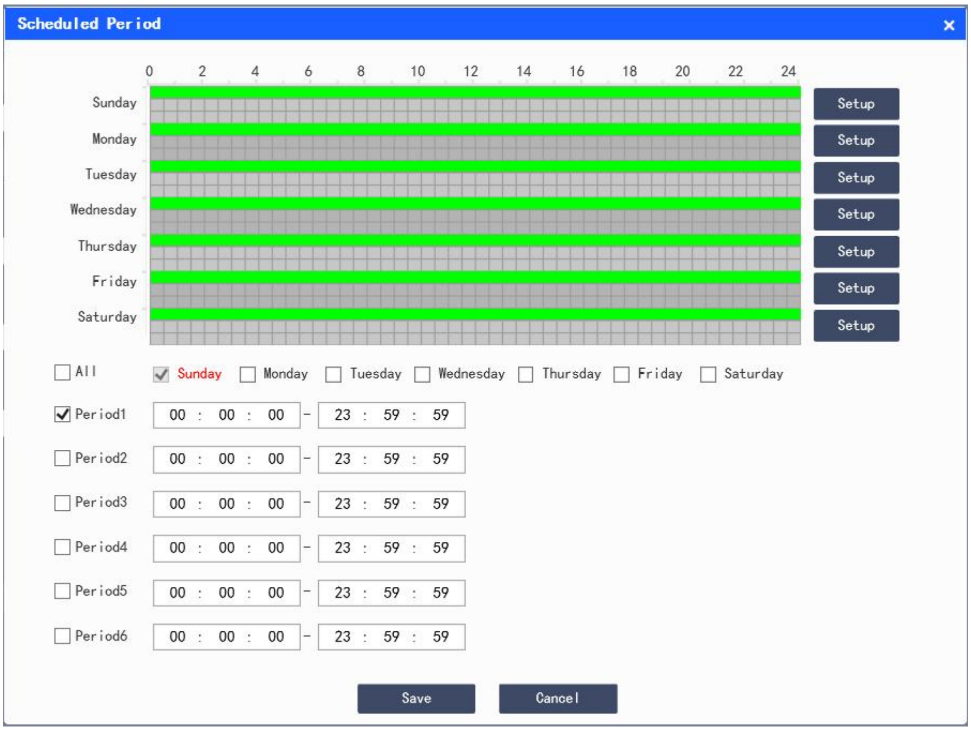
Parameter	Description
Anti-Dither	It means that the Motion detection time is recorded only once in this anti-dither period, in unit of second with the value range of 0 ～100
Burst Flash	When an alarm occurs, the system is linked the burst flash. Please refer to "3.3.5.2 Burst Flash" for the burst flash configuration
Burst Flash Delay	When the alarm is over, the burst flash will be extended for a period of time before stopping.
Record	After being selected, when a local alarm occurs, the system will automatically record the alarm (it must set the alarm video taking period in "Storage Management > Schedule", while selecting automatic video taking in the recording control interface)

Record Delay	It indicates that when the alarm is over, the alarm video taking will continue for a period of time before stopping, in unit of second with the value range of 10～300
Relay-out	Connect the alarm device (such as lights, sirens) to the Alarm Output, select the check box and set the Alarm Output device, and start the alarm linkage output port. When an alarm occurs, the system can link the corresponding Alarm Output device.
Alarm Delay	When the alarm is over, the alarm output will be extended for a period of time before stopping.
Send Email	When an alarm occurs, an email will be sent to notify the user who can set his own email address in "3.2.2.2 Email Setup"
Snapshot	When an alarm occurs, the system will automatically take an Image capture of the alarm

Table 3.3-1 Video Detection Parameter Setup Description

● Scheduled Period

Click "Setup" to set Scheduled Period in the interface as shown in Figure 3.3-2



☐ All ☑ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday

☑ Period1 00 : 00 : 00 – 23 : 59 : 59

☐ Period2 00 : 00 : 00 – 23 : 59 : 59

☐ Period3 00 : 00 : 00 – 23 : 59 : 59

☐ Period4 00 : 00 : 00 – 23 : 59 : 59

☐ Period5 00 : 00 : 00 – 23 : 59 : 59

☐ Period6 00 : 00 : 00 – 23 : 59 : 59

Figure 3.3-2 Scheduled Period Setup

Set the alarm time period, and the alarm event will be activated only within the set time period

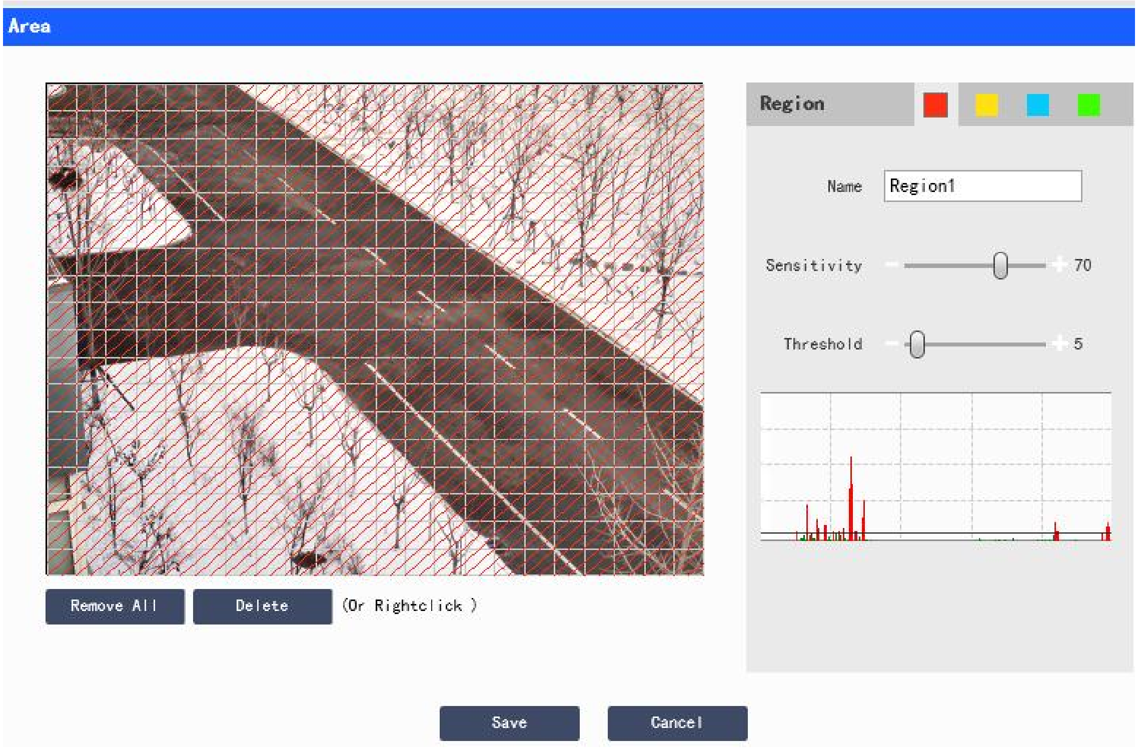
There are 6 time periods available for setting every day. Select the check box in front of the time period, and the set time will be valid

Select the day of the week (the default is Sunday; if "All" is ticked, it means that the setting will be applied to the entire week; or it supports to tick the box in front of the days to make separate settings for certain days)

After setting, click "Save" to return to the "Motion Detection" interface

● Setup Area

Click "Setup" to set the Area in the interface as shown in Figure 3.3-3. Please refer to Table 3.3-2 for parameter description.



Name Region1

Sensitivity 70

Threshold 5

Figure 3.3-3 Area Setup

Parameters	Descriptions
Name	The default names are Region1, Region2, Region3, Region4, which can be customized
Sensitivity	Sensitivity to brightness changes; for the same brightness change, the higher the

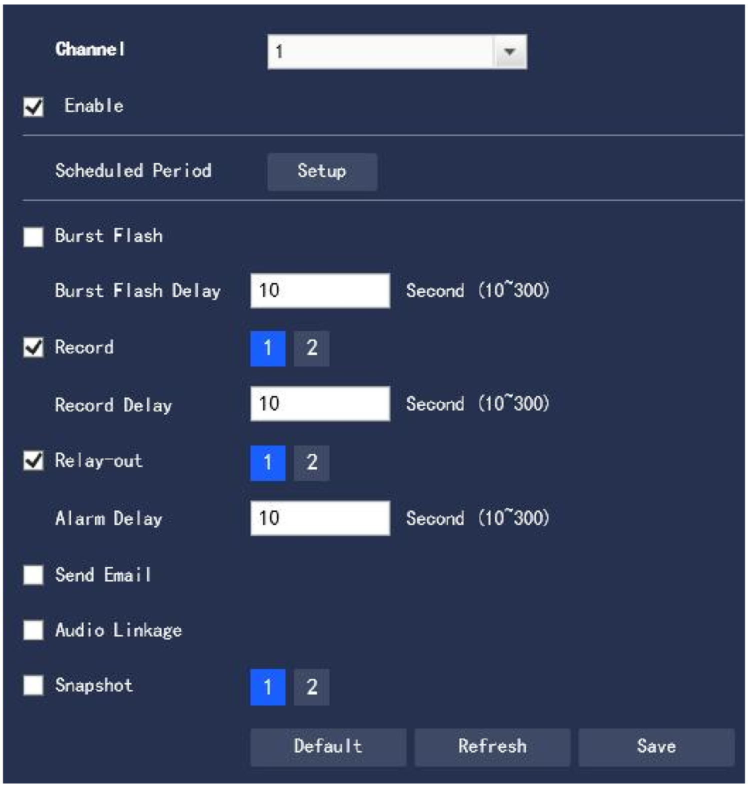
	sensitivity, the easier it is to generate motion detection events The settings of sensitivity can vary for each area, with the value range of 0～100, and the recommended value is 30～70
Threshold	The relationship between the detection object and the area, the smaller the threshold value is, the easier it is to trigger the motion detection The settings of mutation thresholds can vary for each area, with the value range of 0～100, and the recommended value is 1～10
Waveform Graph	The red line indicates that the motion detection is triggered, while the green line indicates that the motion check is not triggered
Remove All	Empty all detection areas
Delete	Delete the detection area of the selected color block

Table 3.3-2 Area Setup Parameter Description

Step 3 Click "Save" to complete the configuration.

3.3.1.2 Video Block

Step 1 Select "Settings > Event Management > General Events > Video Block". The system displays the "Video Block" interface as shown in Figure 3.3-4.



Channel 1

☑ Enable

Scheduled Period Setup

□ Burst Flash

Burst Flash Delay 10 Second (10~300)

☑ Record 1 2

Record Delay 10 Second (10~300)

☑ Relay-out 1 2

Alarm Delay 10 Second (10~300)

□ Send Email

□ Audio Linkage

□ Snapshot 1 2

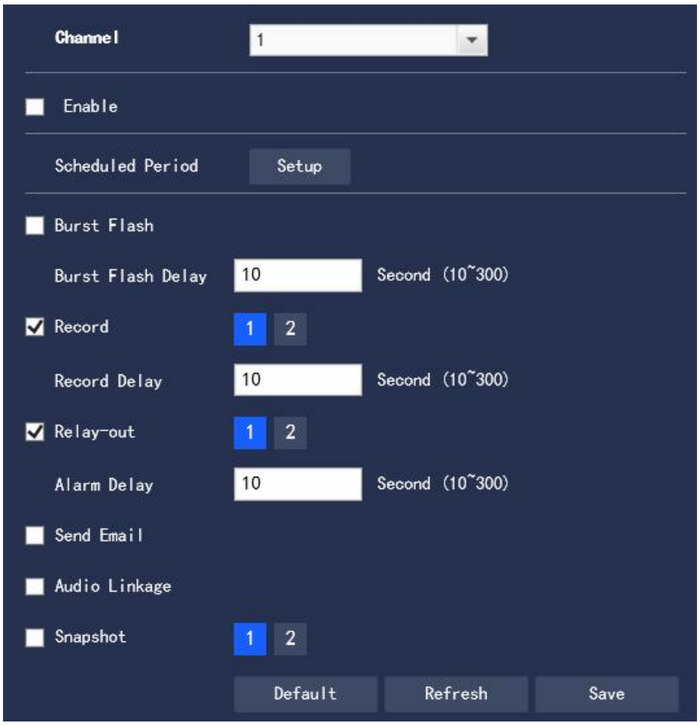
Figure 3.3-4 Video Detection-Video Block Settings

Step 2 Select "Enable", and configure each parameter information according to actual needs (please refer to "3.4.1.1 Motion Detection" for parameter configuration)

Step 3 Click "Save" to complete the configuration.

3.3.1.3 Scene Change

Step 1 Select "Settings > Event Management > General Events > Scene Change". The system displays the "Scene Change" interface as shown in Figure 3.3-5.



Channel 1

□ Enable

Scheduled Period Setup

□ Burst Flash

Burst Flash Delay 10 Second (10~300)

☑ Record 1 2

Record Delay 10 Second (10~300)

☑ Relay-out 1 2

Alarm Delay 10 Second (10~300)

□ Send Email

□ Audio Linkage

□ Snapshot 1 2

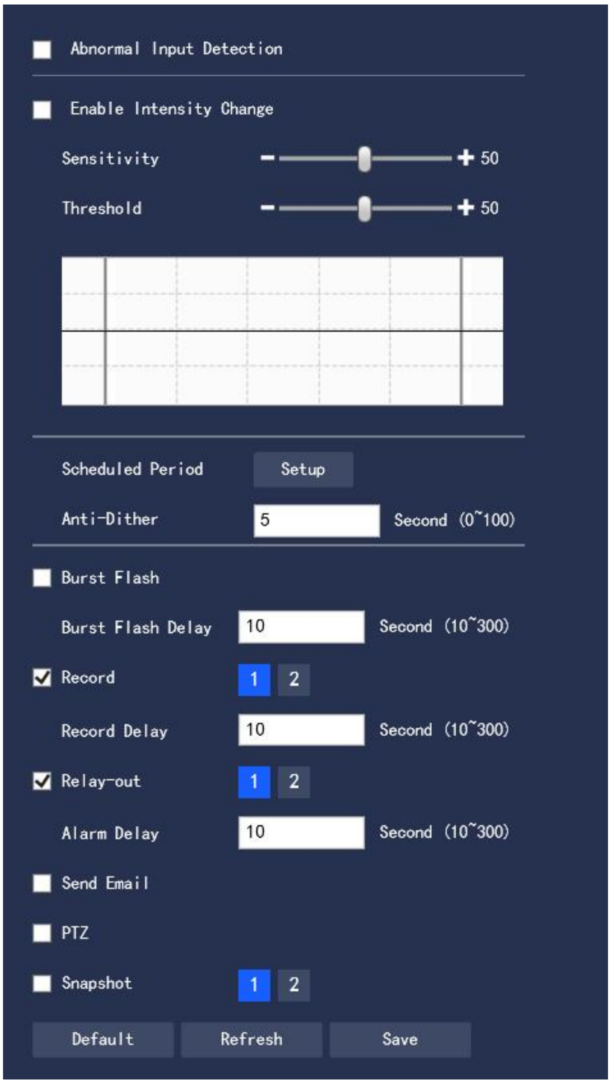
Figure 3.3-5 Video Detection-Scene Change Settings

Step 2 Select "Enable", and configure each parameter information according to actual needs (please refer to "3.3.1.1 Motion Detection" for parameter configuration)

Step 3 Click "Save" to complete the configuration.

3.3.1.4 Audio Detection

Step 1 Select "Settings > Event Management > General Events > Audio Detection". The system displays the "Audio Detection" interface as shown in Figure 3.3-6



□ Abnormal Input Detection

□ Enable Intensity Change

Sensitivity 50

Threshold 50

Scheduled Period Setup

Anti-Dither 5 Second (0~100)

□ Burst Flash

Burst Flash Delay 10 Second (10~300)

☑ Record 1 2

Record Delay 10 Second (10~300)

☑ Relay-out 1 2

Alarm Delay 10 Second (10~300)

□ Send Email

□ PTZ

□ Snapshot 1 2

Default Refresh Save

Figure 3.3-6 Audio Detection

Step 2 To configure each parameter information according to actual needs, please refer to Table 3.3-3 for parameter description.

Parameters	Descriptions
Abnormal Input Detection	Select "Abnormal Input Detection" and an alarm will be generated when an abnormal audio input is detected
Enable Intensity Change	Select to "Enable Intensity Change" and an alarm will be generated when it detects that the audio sound intensity has a sudden change and exceeds the threshold
Sensitivity	The value range is 1～100. The smaller the value, the more the input sound

	volume changes over the continuous environment volume before it can be judged as the audio abnormality; the user needs to make tests and adjustments according to the actual environment
Threshold	The value range is 1～100. It is used to set the intensity of the filtered environment sound. The larger the environment noise, the higher the value, and the user needs to make tests and adjustments according to the actual environment

Table 3.3-3 Audio Detection Parameter Setup Description

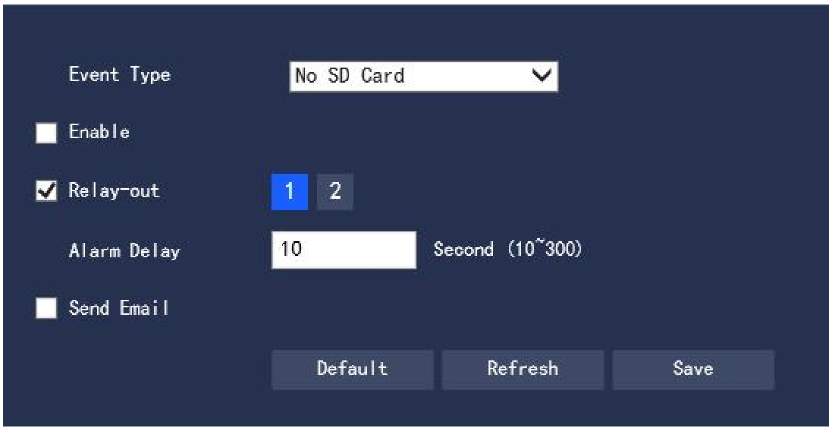
Note: Refer to "3.3.1.1 Motion Detection" for other parameter description.

Step 3 Click "Save" to complete the configuration.

3.3.1.5 SD Card Abnormality

When the SD card is abnormal, an alarm event will be generated. The configuration steps are as follows:

Step 1 Select "Settings > Event Management > General Events > SD Card Abnormality". The system displays the "SD Card Abnormality" interface as shown in Figure 3.3-7, Figure 3.3-8 and Figure 3.3-9.



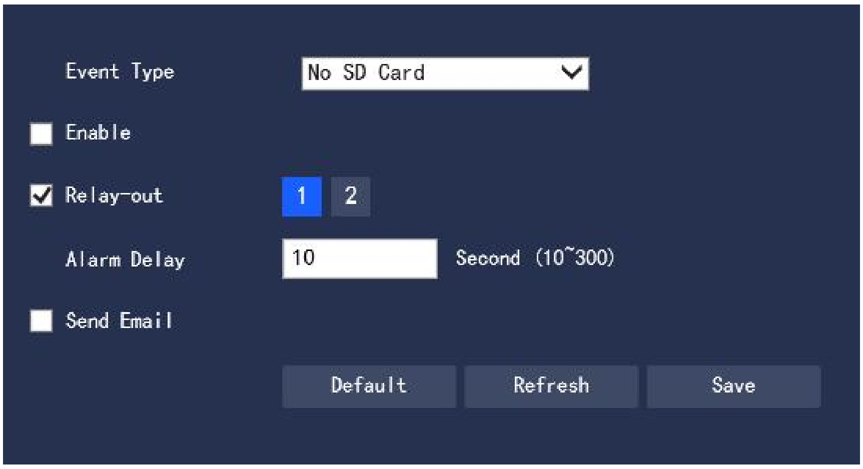
Event Type: No SD Card

□ Enable

☑ Relay-out: 1 2

Alarm Delay: 10 Second (10~300)

□ Send Email



Event Type No SD Card

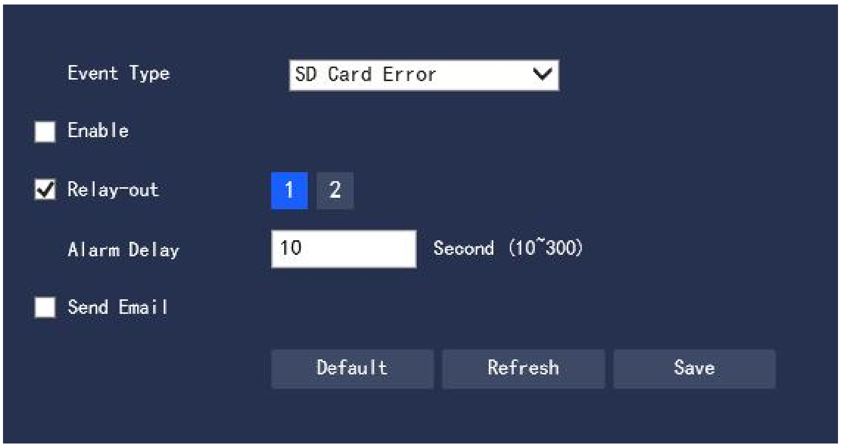
□ Enable

☑ Relay-out 1 2

Alarm Delay 10 Second (10˜300)

□ Send Email

Figure 3.3-7 No SD Card



Event Type SD Card Error

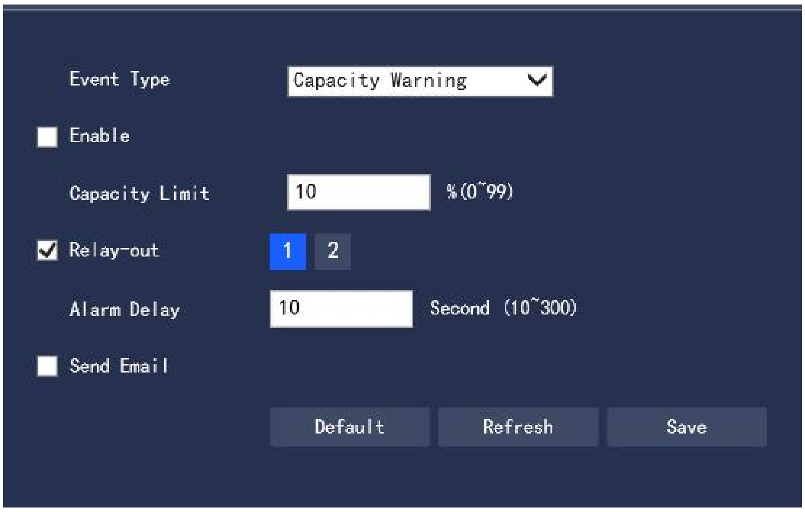
□ Enable

☑ Relay-out 1 2

Alarm Delay 10 Second (10˜300)

□ Send Email

Figure 3.3-8 SD Card Error



Event Type Capacity Warning

□ Enable

Capacity Limit 10 %(0˜99)

☑ Relay-out 1 2

Alarm Delay 10 Second (10˜300)

□ Send Email

Figure 3.3-9 Capacity Warning

Step 2 To configure each parameter information according to actual needs, please refer to Table 3.3-4 for parameter description.

Parameters	Descriptions
Enable	Select to enable the SD card abnormality alarm function
Space capacity of SD Card	It can set Capacity Limit and when the remaining capacity is below this limit, it will trigger an alarm

Table 3.3-4 SD Card Abnormality Settings Parameter Description

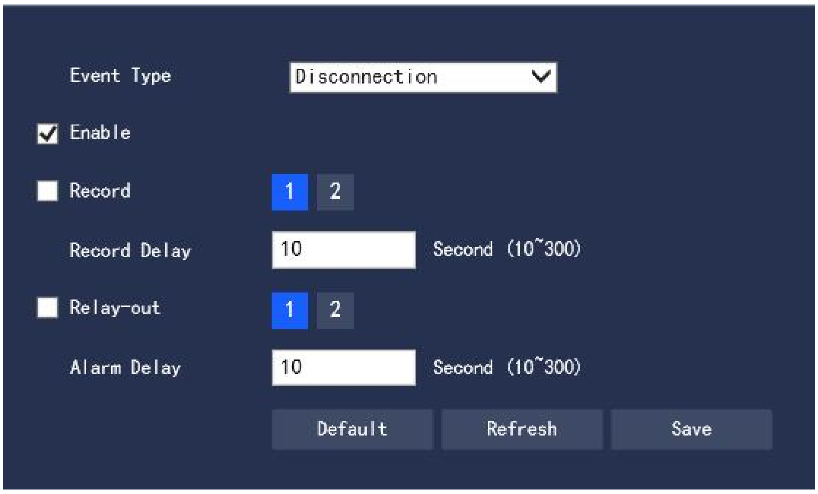
Please refer to "3.3.1.1 Motion Detection" for other parameter descriptions

Step 3 Click "Save" to complete the configuration.

3.3.1.6 Network Abnormality

When the network abnormality occurs, an alarm event will be generated. The configuration steps are as follows:

Step 1 Select "Settings > Event Management > General Events > Network Abnormality". The system displays the "Network Abnormality" interface as shown in Figure 3.3-10 and Figure 3.3-11



Event Type: Disconnection

☑ Enable

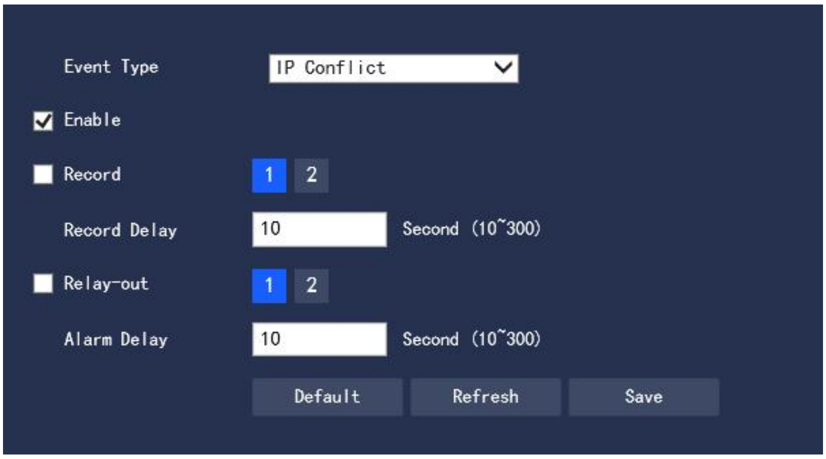
□ Record 1 2

Record Delay 10 Second (10~300)

□ Relay-out 1 2

Alarm Delay 10 Second (10~300)

Figure 3.3-10 Network Disconnection



Event Type: IP Conflict

☑ Enable

□ Record 1 2

Record Delay 10 Second (10~300)

□ Relay-out 1 2

Alarm Delay 10 Second (10~300)

Figure 3.3-11 IP Conflict

Step 2 To configure each parameter information according to actual needs. Please refer to Table 3.3-5 for parameter description

Parameters	Descriptions
Enable	Select to enable the network abnormality alarm function

Table 3.3-5 Network Abnormality Setting Parameter Description

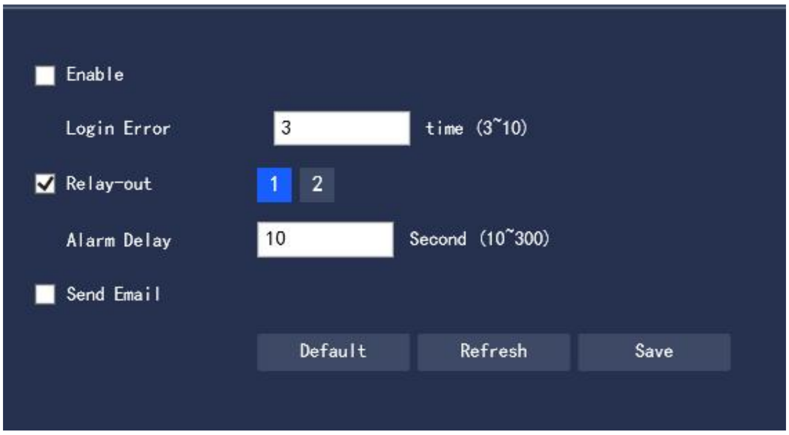
Please refer to "3.3.1.1 Motion Detection" for other parameter descriptions

Step 3 Click "Save" to complete the configuration.

3.3.1.7 Unauthorized Access

When the occurrence of the login password error reaches a certain number of times, it will generate an alarm event of unauthorized access. The configuration steps are as follows:

Step 1 Select "Settings > Event Management > General Events > Unauthorized Access". The system displays the "Unauthorized Access" interface as shown in Figure 3.3-12



□ Enable

Login Error 3 time (3~10)

☑ Relay-out 1 2

Alarm Delay 10 Second (10~300)

□ Send Email

Figure 3.3-12 Unauthorized Access

Step 2 To configure each parameter information according to actual needs. Refer to Table 3.3-6 for parameter description

Parameter	Description
Enable	Select to make settings of the unauthorized access alarm
Login error	Entering the wrong password this time is when the unauthorized access alarm is triggered and the account is locked

Table 3.3-6 Unauthorized Access Setup Parameter Description

Please refer to "3.3.1.1 Motion Detection" for other parameter descriptions

Step 3 Click "Save" to complete the configuration.

3.3.2 Smart Plan

Step 1 Select "Settings > Event Management > General Events > Smart Plan". The system displays the "Smart Plan" interface as shown in Figure 3.3-13

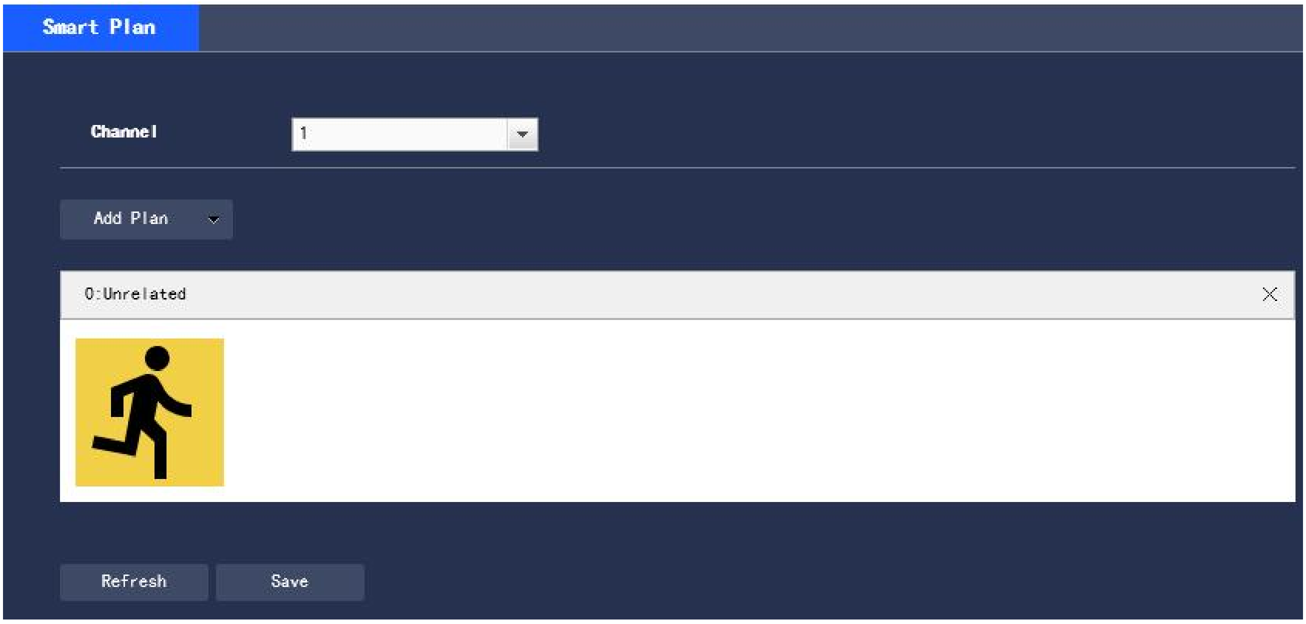


Figure 3.3-13 Smart Plan

Step 2 Turn on the corresponding smart functions according to actual needs

● Enable the general behavior analysis, face detection or license plate recognition functions

1. Select the preset point in "Add Plan", and the system will display the plan corresponding to the preset point

2. Click General behavior analysis to turn on the corresponding intelligent function

Step 3 The selected intelligent function will be highlighted, and can be canceled by clicking it

3.3.3 General Behavior Analysis

Basic requirements for scene selection

● The target size is no more than 10% of the screen

● The target size ≥ 10 pixels × 10 pixels; the remaining object size ≥ 15 pixels × 15 pixels (CIF image); the height and width of the target is no more than 1/3 of the image height and width; the recommended target height is about 1/10 of the image height.

● It ensures at least that the target appears within the sight for more than 2 consecutive seconds, and the movement distance is wider the width of the target itself, and is not less than 15 pixels (CIF image)

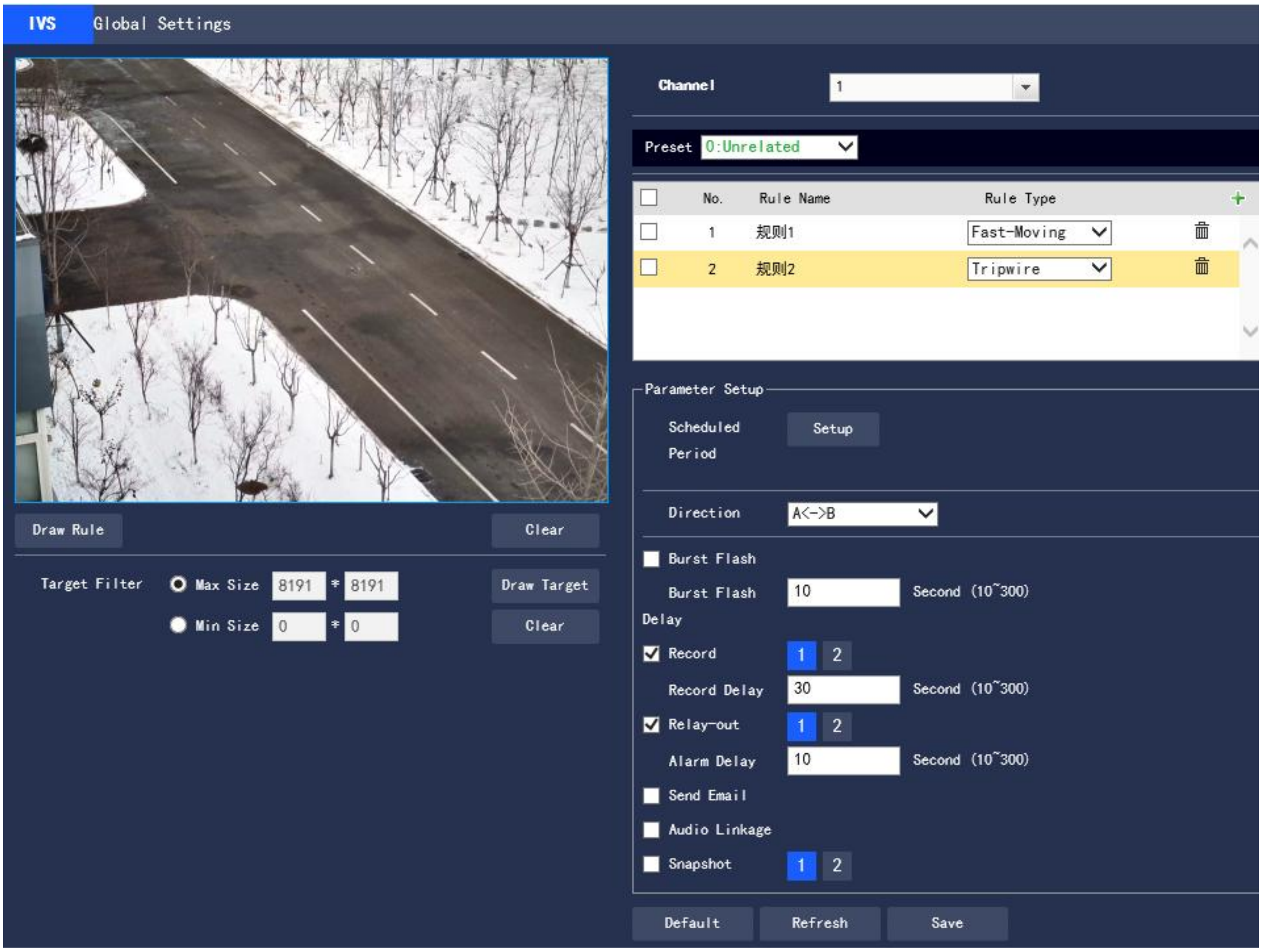
● Where conditions permit, the complexity of monitoring and analyzing scenes should be reduced to the minimum; for scenes with dense targets and frequent light changes, it is not recommended to turn on the General Behavior Analysis function

● Great efforts should be made to avoid such areas as glass, ground reflections and water surface; branches, shadows, and mosquito interference areas; backlit scenes and direct light

3.3.3.1 IP Rule

Set up smart rules. The configuration steps are as follows:

Step 1 Select ""Settings > Event Management > General Behavior Analysis > IVS". The system displays the "IVS" interface as shown in Figure 3.3-14



Channel 1

Preset 0:Unrelated

□	No.	Rule Name	Rule Type
□	1	规则1	Fast-Moving
□	2	规则2	Tripwire

Target Filter ● Max Size 8191 * 8191

○ Min Size 0 * 0

Parameter Setup

Scheduled Period

Direction A<->B

□ Burst Flash

Burst Flash Delay 10 Second (10~300)

☑ Record 1 2

Record Delay 30 Second (10~300)

☑ Relay-out 1 2

Alarm Delay 10 Second (10~300)

□ Send Email

□ Audio Linkage

□ Snapshot 1 2

Figure 3.3-14 Add Smart Rule

Step 2 Select the preset point that needs to be configured with smart rules

Step 3 Click ➕ to add smart rules

- Double click "Rule Type" to modify the type of the rule
- On entering the IP Rule interface, the lock function will be automatically turned on, and the lock time is 180s. Within the 180s, except for unlocking manually, no other methods can control the camera. Click "Unlock" to remove the control

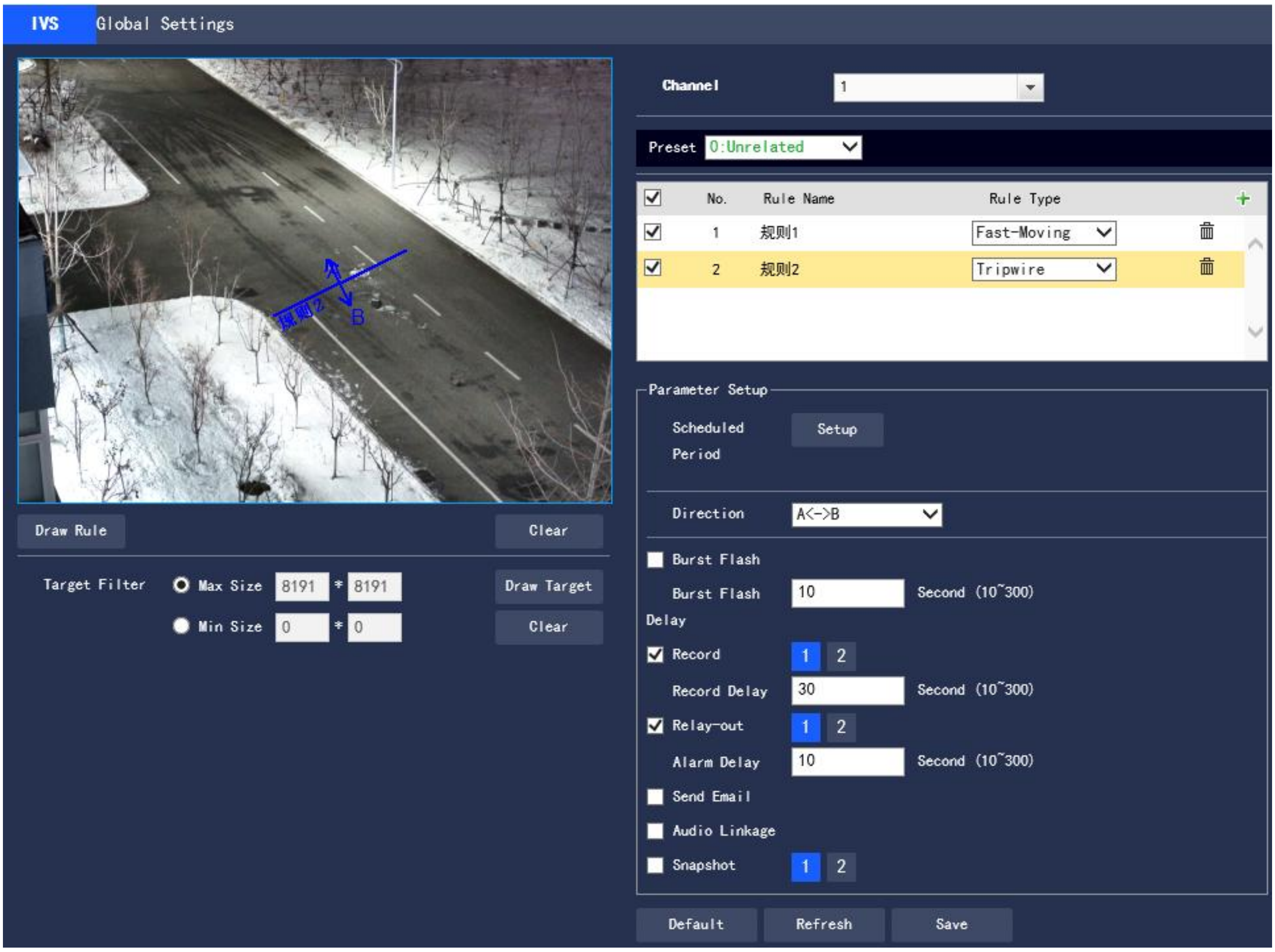
Step 4 Click "Save" to complete the configuration

3.3.3.1.1 Tripwire Intrusion

An alarm will be triggered when the target crosses the warning line following the set direction of movement. As it takes some time and space from the appearance of the target to the confirmation, it must leave certain space on both sides of the warning line, and do not set it near obstructions, while setting the warning line.

Application Scenarios: suitable only for scenarios with sparse targets and without mutual obstruction between the targets, such as the perimeter protection in unattended areas

Step 1 If the rule type is selected as "Tripwire Intrusion", the configuration interface is as shown in Figure 3.3-15



Channel: 1

Preset: 0:Unrelated

☑	No.	Rule Name	Rule Type
☑	1	规则1	Fast-Moving
☑	2	规则2	Tripwire

Target Filter: ● Max Size 8191 * 8191; ○ Min Size 0 * 0

Parameter Setup

Scheduled Period: Setup

Direction: A<->B

□ Burst Flash

Burst Flash Delay: 10 Second (10~300)

☑ Record: 1 2

Record Delay: 30 Second (10~300)

☑ Relay-out: 1 2

Alarm Delay: 10 Second (10~300)

□ Send Email

□ Audio Linkage

□ Snapshot: 1 2

Figure 3.3-15 Tripwire Intrusion Settings

Step 2 Click "Draw Rule" to draw rules in the monitoring screen

Step 3 Configure the parameter information according to actual needs. Please refer to Table 3.3-7 for parameter description.

Parameters	Descriptions
Scheduled Period	Click "Settings" and the "Scheduled Period" setup interface will pop up. Settings can be made through entering the time value or pressing and holding the left mouse button while dragging the progress bar directly on the setup interface There are 6 time periods available for setting every day. Select the check box in front of the time period, and the set time period is valid Select the day of the week (the default is Sunday; if "All" is ticked, it means that

	the setting will be applied to the entire week; or it supports to tick the check box in front of the days to make separate settings for certain days) After completing the settings, click "Save" to return to the IVS setup page, and click "Save" to complete the time period setting for Tripwire
Direction	Set the direction of Tripwire Intrusion, with A→B, B→A, and A↔B available
Burst Flash	When an alarm occurs, the system is linked the burst flash. Please refer to "3.3.5.2 Burst Flash" for the burst flash configuration
Burst Flash Delay	When the alarm is over, the burst flash will continue for a period of time before stopping, in unit of seconds, and the value range is 10～300
Record	After being selected, when a local alarm occurs, the system will automatically record the alarm. Meanwhile, it should set the time period for alarm video taking in "Settings > Storage Management> Schedule", while selecting automatic video taking in the recording control interface.
Record Delay	When the alarm is over, the alarm video taking will continue for a period of time before stopping
Relay-out	Connect the alarm device (such as lights, sirens) to the Alarm Output, select the check box and set the Alarm Output device, and start the alarm linkage output port. When an alarm occurs, the system can link the corresponding Alarm Output device.
Alarm Delay	When the alarm is over, the Alarm Output will be extended for a period of time before stopping.
Send Email	After being selected, an email will be sent to notify the user when an alarm occurs, and the user can set the email address in "Settings > Network Settings > Email Setup"
Audio Linkage	The audio linkage will inform the users when the alarm is triggered.
Snapshot	After being selected, when an alarm occurs, the system will automatically take an

	alarm Image capture, while the alarm Image capture time period should be set in "Setup > Storage Management> Schedule"

Table 3.3-7 Tripwire Intrusion Parameter Description

Step 4 Click "Save" to complete the configuration

3.3.3.1.2 Virtual Fence

The Virtual Fence alarm is equivalent to multiple targets triggering two warning lines one after another. The fence setting requirements are as follows:

● Not support transparent fences, such as iron fences

● Not support too short walls (the height is lower than that of a normal person)

Virtual Fence is divided into Upstairs Line or Downstairs Line

● The criteria for Upwards Line are: The target rectangle intersects with the warning line at the bottom -> The bottom of the target rectangle separates from the warning line at the bottom

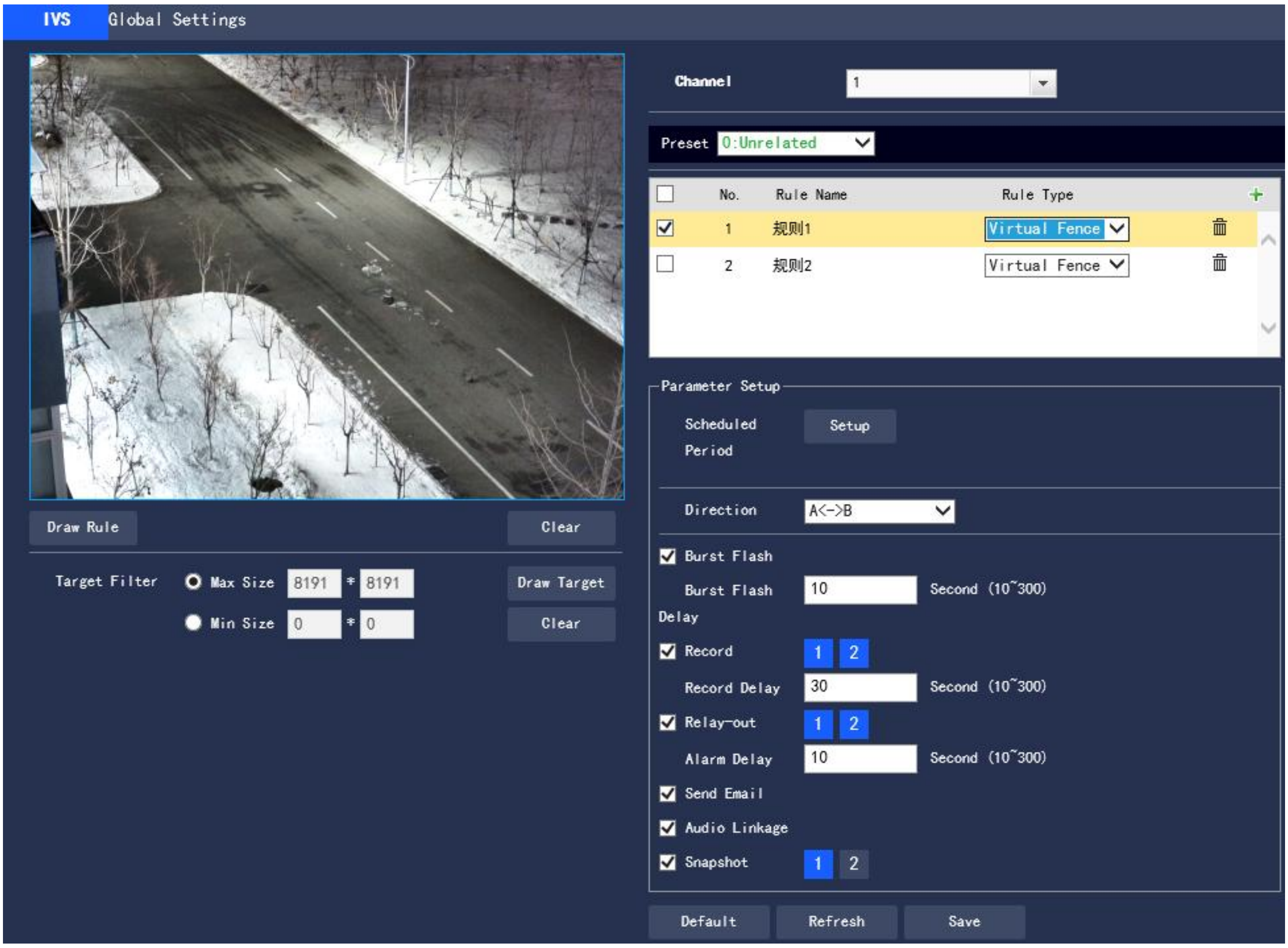
-> The center of the target rectangle crosses the top warning line -> Alarm

● The criteria for Downwards Line are: The center of the target rectangle crosses the top warning line -> The bottom of the target rectangle leaves the bottom warning line

-> The target rectangle intersects with the warning line at the bottom -> Alarm

The configuration steps are as follows:

Step 1 If the rule type is selected as "Virtual Fence", the configuration interface is as shown in Figure 3.3-16



Channel 1

Preset 0:Unrelated

☐	No.	Rule Name	Rule Type
☑	1	规则1	Virtual Fence
☐	2	规则2	Virtual Fence

Target Filter ● Max Size 8191 * 8191

○ Min Size 0 * 0

Parameter Setup

Scheduled Period

Direction A<->B

☑ Burst Flash

Burst Flash Delay 10 Second (10~300)

☑ Record 1 2

Record Delay 30 Second (10~300)

☑ Relay-out 1 2

Alarm Delay 10 Second (10~300)

☑ Send Email

☑ Audio Linkage

☑ Snapshot 1 2

Figure 3.3-16 Virtual Fence Setting

Step 2 Click "Draw Rule" to draw rules in the monitoring screen

Step 3 Configure the parameter information according to actual needs. Refer to Table 3.3-8 for parameter description

Parameters	Descriptions
Direction	Set Direction for Virtual Fence, with A→B, B→A, and A↔B available

Table 3.3-8 Virtual Fence Parameter Description

Please refer to "3.3.3.1.1 Tripwire" for other parameter descriptions.

Step 4 Click "Save" to complete the configuration.

3.3.3.1.3 Regional Intrusion

Regional intrusion includes the Cross and Appear functions.

- The Cross function means that the target will alarm when entering or leaving the area.

● The “appear” function means that in the set alarm area, at a given time, when a specified number of targets appear, an alarm will be issued. This function is simply to count the number of targets in the detection area, regardless of whether they are the same target

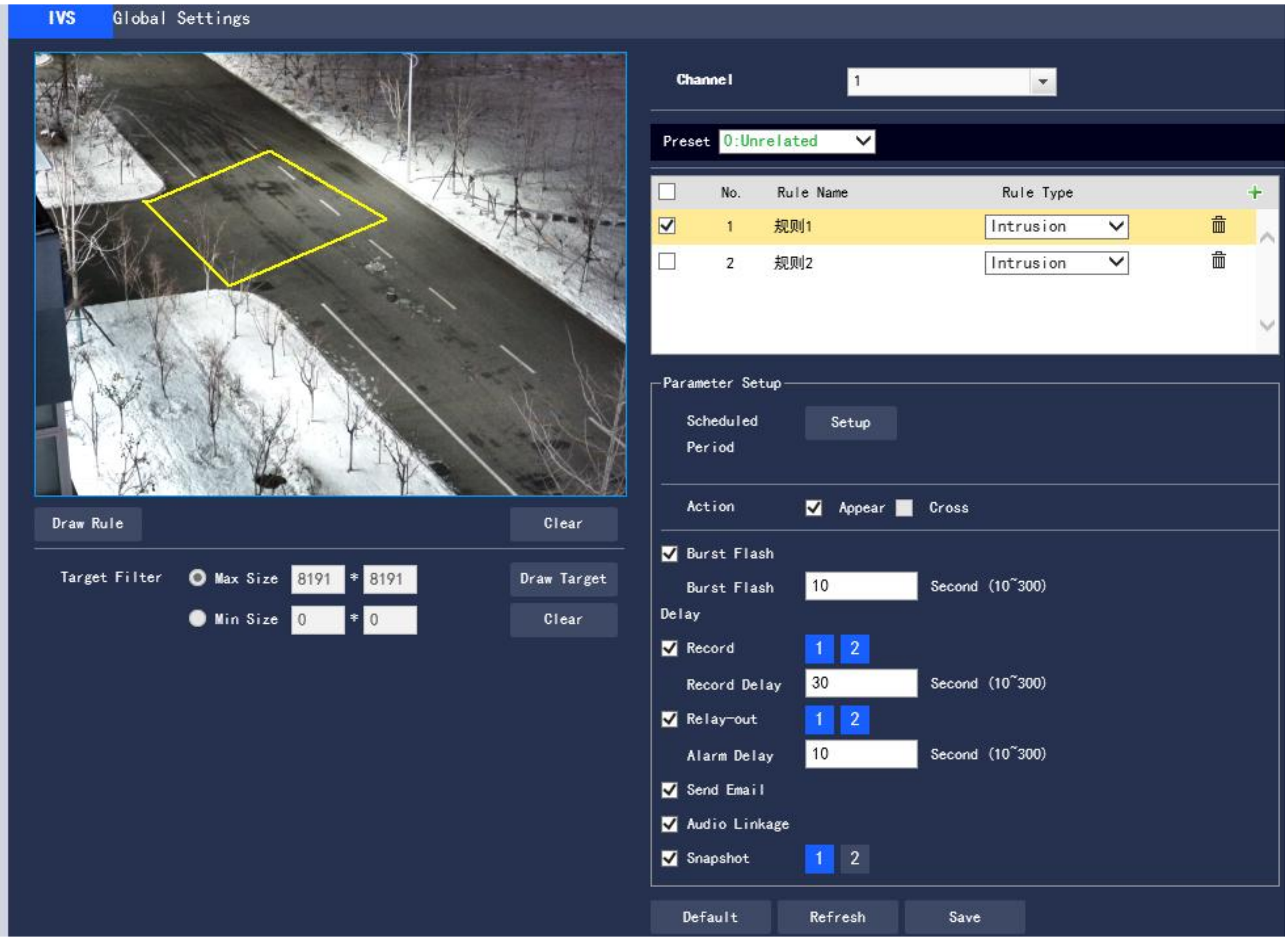
● For the reporting interval of the Appear function, the system will detect whether there is occurrence of the same things within the interval after triggering the first alarm. If the same event does not occur within this period of time, the alarm counter will be cleared

Similar to the warning line, to detect entry/exit events, it must leave certain space around the area line for the target movement

Application Scenarios: suitable only for scenarios with sparse targets and without mutual obstruction between the targets, such as the perimeter protection in unattended areas

The configuration steps are as follows:

Step 1 If the rule type is selected as "Intrusion", the configuration interface is as shown in Figure 3.3-17



IVS | Global Settings

Channel: 1

Preset: 0:Unrelated

☐	No.	Rule Name	Rule Type
☑	1	规则1	Intrusion
☐	2	规则2	Intrusion

Draw Rule | Clear

Target Filter: ○ Max Size 8191 * 8191; ● Min Size 0 * 0 | Draw Target | Clear

Parameter Setup

Scheduled Period: Setup

Action: ☑ Appear ■ Cross

☑ Burst Flash

Burst Flash Delay: 10 Second (10~300)

☑ Record: 1 2

Record Delay: 30 Second (10~300)

☑ Relay-out: 1 2

Alarm Delay: 10 Second (10~300)

☑ Send Email

☑ Audio Linkage

☑ Snapshot: 1 2

Default | Refresh | Save

Figure 3.3-17 Regional Intrusion Setting

Step 2 Click "Draw Rule" to draw rules in the monitoring screen

Step 3 Configure the parameter information according to actual needs. Please refer to Table 3.3-9 for parameter description

Parameter	Description
Action	Set Action for regional intrusion, with Appear or Cross available
Direction	Set the direction of Cross from entry and exit

Table 3.3-9 Regional Intrusion Parameter Description

Please refer to "3.3.3.1.1 Tripwire" for other parameter descriptions.

Step 4 Click "Save" to complete the configuration.

3.3.3.1.4 Abandoned Object

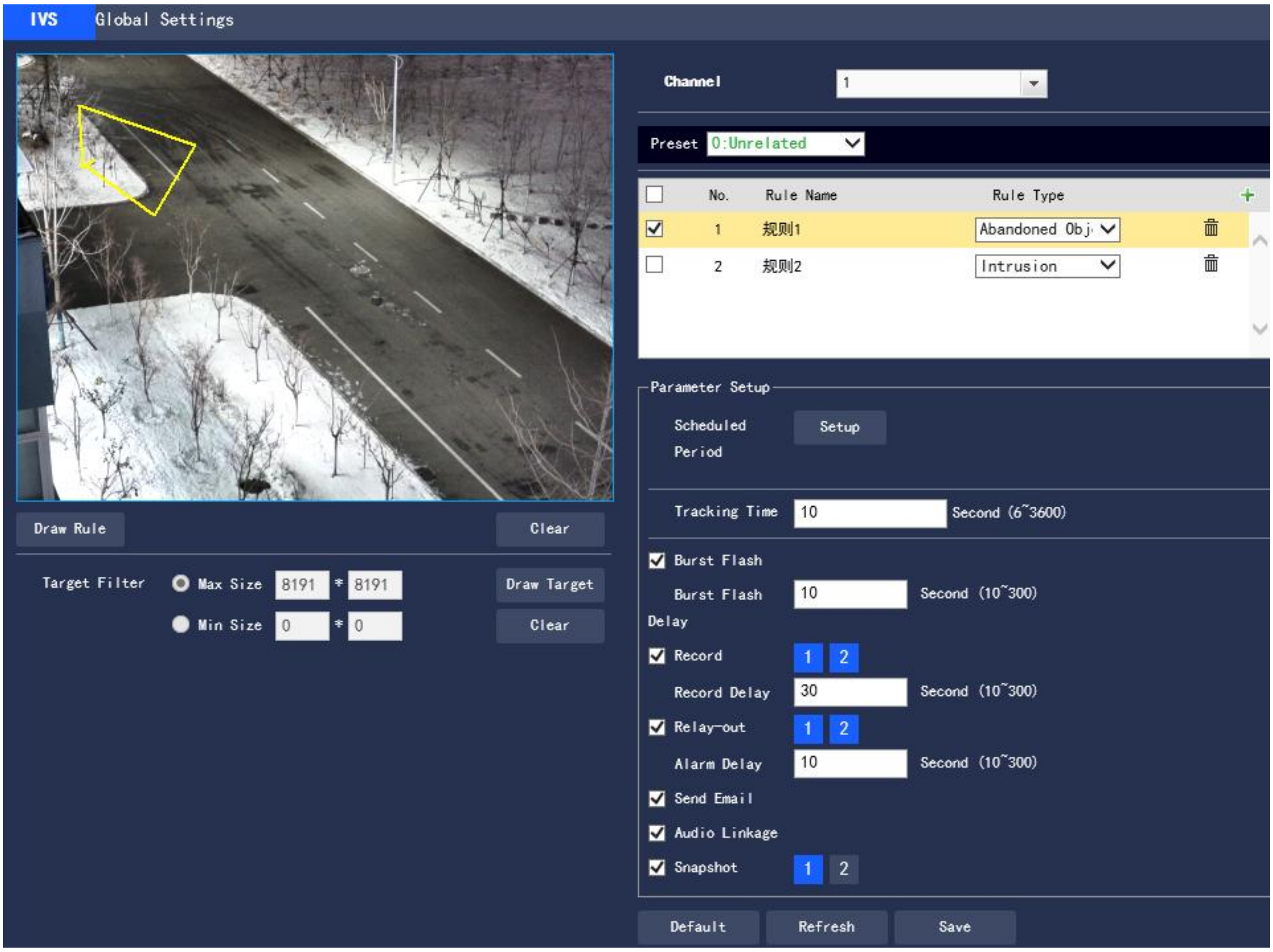
Abandoned Object means that when the selected target in the monitoring screen stays in the screen for more than the set time, an alarm will be triggered.

Pedestrians or vehicles staying for too long will also be judged as an abandoned object and trigger the alarm. In order to filter such alarms, generally the abandoned object is smaller in size than people and vehicles. Therefore, people and vehicles can be filtered by the setting in Target Filter; in addition, the alarm time can be appropriately extended to avoid legacy time false positive caused by short stays of people.

Application Scenarios: suitable for scenarios with sparse targets, no obvious and frequent light changes; for scenarios with a high target density and frequent occlusion, underreporting will increase; for scenarios with a lot of people staying, false positives will increase; the detection area is required to have a texture as simple as possible, and it is not suitable for areas with too complex textures.

The configuration steps are as follows:

Step 1 If the rule type is selected as "Abandoned Object", the configuration interface is as shown in Figure 3.3-18



Channel 1

Preset 0:Unrelated

	No.	Rule Name	Rule Type
☑	1	规则1	Abandoned Obj
□	2	规则2	Intrusion

Target Filter ◉ Max Size 8191 * 8191
○ Min Size 0 * 0

Parameter Setup

Scheduled Period

Tracking Time 10 Second (6~3600)

☑ Burst Flash

Burst Flash Delay 10 Second (10~300)

☑ Record 1 2

Record Delay 30 Second (10~300)

☑ Relay-out 1 2

Alarm Delay 10 Second (10~300)

☑ Send Email

☑ Audio Linkage

☑ Snapshot 1 2

Figure 3.3-18 Abandoned Object Setting

Step 2 Click "Draw Rule" to draw rules in the monitoring screen

Step 3 Configure the parameter information according to actual needs. Please refer to Table 3.3-10 for parameter description

Parameters	Descriptions
Tracking Time	Set the shortest time from leaving the object to triggering the alarm

Table 3.3-10 Abandoned Object Parameter Description

Please refer to "3.3.3.1.1 Tripwire" for other parameter descriptions

Step 4 Click "Save" to complete the configuration

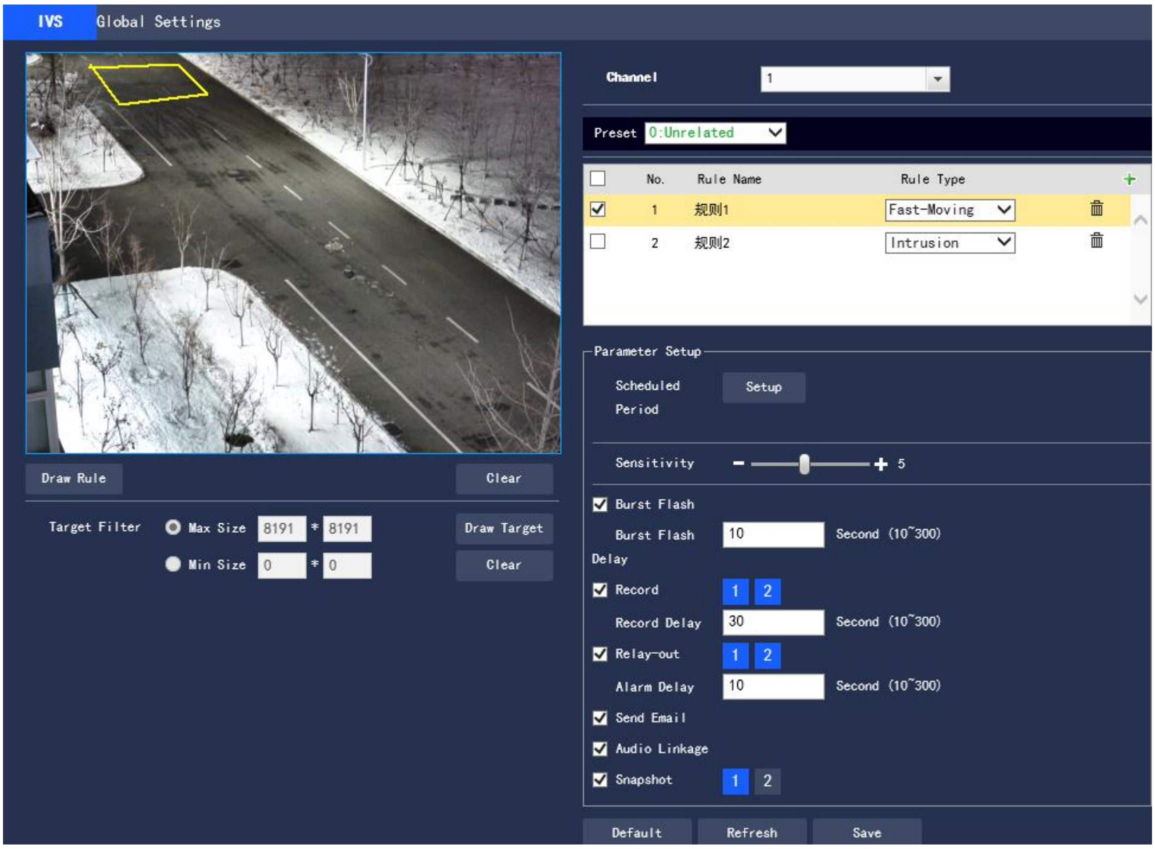
3.3.3.1.5 Fast-Moving

This function must first be configured for depth-of-field calibration, and calculate the actual movement speed of the target according to depth-of-field calibration. If the movement speed exceeds the set alarm speed, an alarm will be triggered (triggering speed is linked to sensitivity, with sensitivity 1～10 corresponding to actual speed 10m/s～1m/s)

Application Scenarios: suitable for scenarios with sparse targets and no obvious occlusion. The camera should be installed above the monitoring area as directly as possible, and the optical axis direction should be as vertical as possible to the movement direction of the target

The configuration steps are as follows:

Step 1 If the rule type is selected as "Fast-Moving", the configuration interface is as shown in Figure 3.3-19



Channel 1

Preset 0:Unrelated

□	No.	Rule Name	Rule Type
☑	1	规则1	Fast-Moving
□	2	规则2	Intrusion

Target Filter ● Max Size 8191 * 8191
○ Min Size 0 * 0

Parameter Setup

Scheduled Period

Sensitivity 5

☑ Burst Flash

Burst Flash Delay 10 Second (10~300)

☑ Record 1 2

Record Delay 30 Second (10~300)

☑ Relay-out 1 2

Alarm Delay 10 Second (10~300)

☑ Send Email

☑ Audio Linkage

☑ Snapshot 1 2

Figure 3.3-19 Fast-Moving Setting

Step 2 Click "Draw Rule" to draw rules in the monitoring screen.

Step 3 Configure the parameter information according to actual needs. Please refer to Table 3.3-11 for parameter description.

Parameters	Descriptions
Sensitivity	Set Sensitivity for alarm triggering, with the value range of 1～10, and the default is 5

Table 3.3-11 Fast-Moving Parameter Description

Please refer to "3.3.3.1.1 Tripwire" for other parameter descriptions

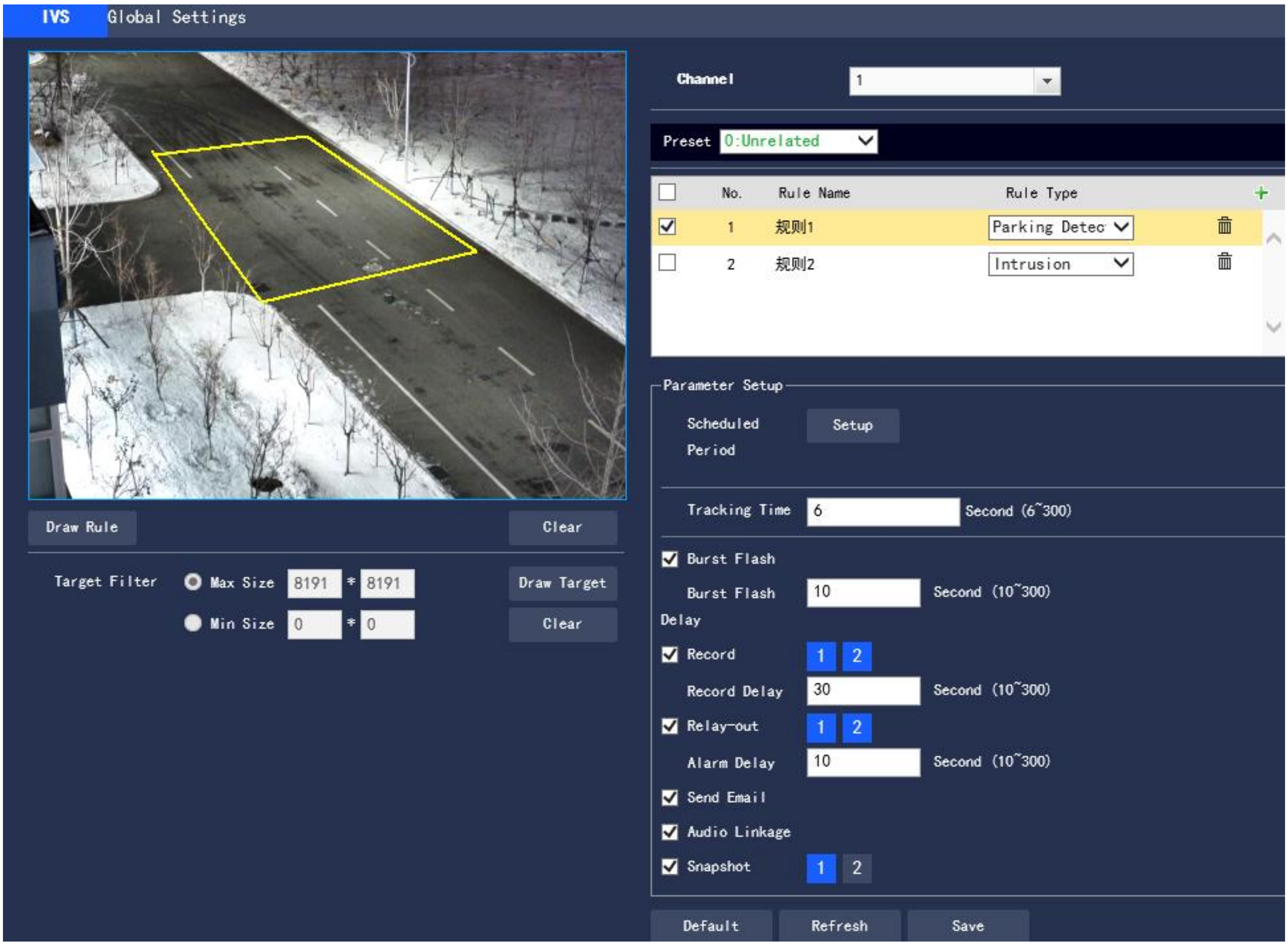
Step 4 Click "Save" to complete the configuration

3.4.3.1.6 Parking Detection

The system will judge whether the target is static based on the track information. When the static time exceeds the set time, an alarm will be triggered

The configuration steps are as follows:

Step 1 If the rule type is selected as "Parking Detection", the configuration interface is as shown in Figure 3.3-20



IVS | Global Settings

Channel: 1

Preset: 0:Unrelated

□	No.	Rule Name	Rule Type
☑	1	规则1	Parking Detec
□	2	规则2	Intrusion

Draw Rule | Clear

Target Filter ● Max Size 8191 * 8191 | Draw Target

○ Min Size 0 * 0 | Clear

Parameter Setup

Scheduled Period: Setup

Tracking Time: 6 Second (6~300)

☑ Burst Flash

Burst Flash Delay: 10 Second (10~300)

☑ Record: 1 2

Record Delay: 30 Second (10~300)

☑ Relay-out: 1 2

Alarm Delay: 10 Second (10~300)

☑ Send Email

☑ Audio Linkage

☑ Snapshot: 1 2

Default | Refresh | Save

Figure 3.3-20 Parking Detection Setting

Step 2 Click "Draw Rule" to draw rules in the monitoring screen.

Step 3 Configure the parameter information according to actual needs. Please refer to Table 3.3-12 for parameter description.

Parameters	Descriptions
Tracking Time	Set the shortest time from leaving the object to triggering the alarm

Table 3.3-12 Parking Detection Parameter Description

Please refer to "3.3.3.1.1 Tripwire" for other parameter descriptions.

Step 4 Click "Save" to complete the configuration.

3.3.3.1.7 Crowd Detection

Crowd Detection is mainly aimed at outdoor squares, government gates, station entrances and other areas. When there is an event of crowd gathering and staying or excessive crowd density, an alarm will be triggered

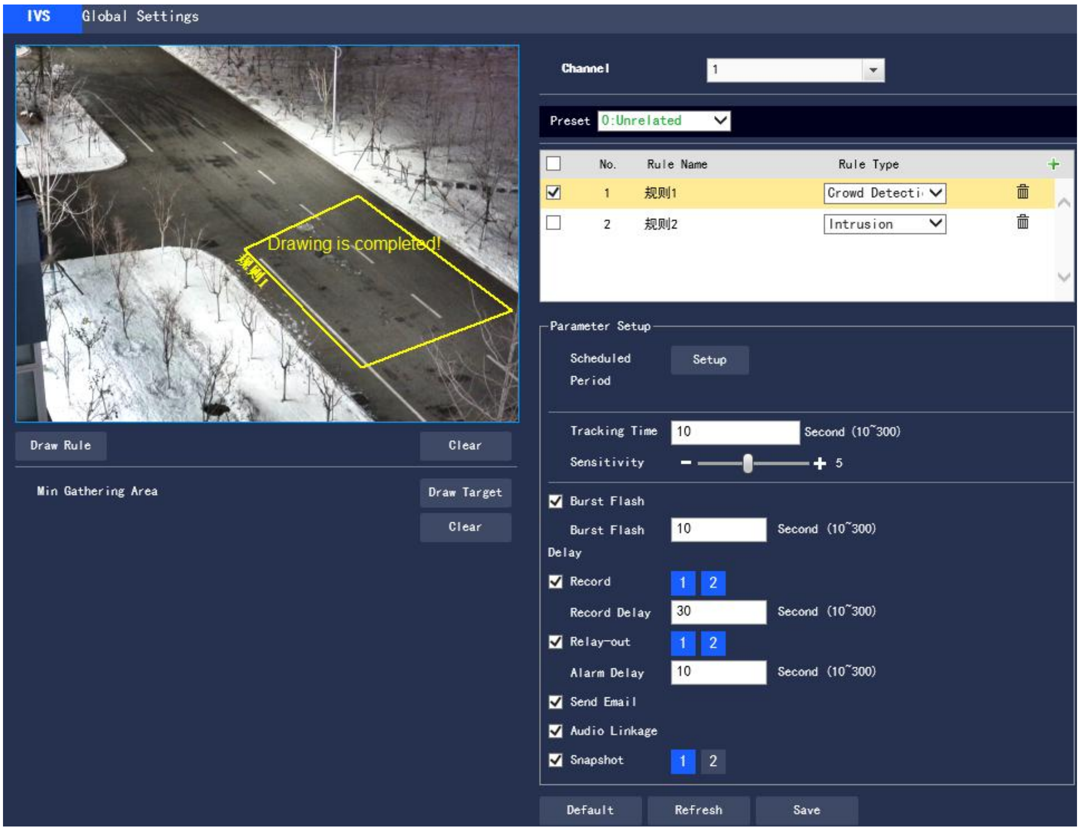
False positives will occur in the continuous shaking of the camera, leaves and shades, the frequent opening and closing of the retractable doors of the park, the dense traffic or the flow of people

Application Scenarios: middle and far scenarios

Unsuitable scenarios: low installation height, a large proportion of the screen occupied by a single person, or serious occlusion of the target

The configuration steps are as follows:

Step 1 If the rule type is selected as "Crowd Detection", the configuration interface is as shown in Figure 3.3-21



Channel: 1

Preset: 0:Unrelated

□	No.	Rule Name	Rule Type
☑	1	规则1	Crowd Detecti
□	2	规则2	Intrusion

Min Gathering Area

Parameter Setup

Scheduled Period: Setup

Tracking Time: 10 Second (10~300)

Sensitivity: 5

☑ Burst Flash

Burst Flash Delay: 10 Second (10~300)

☑ Record: 1 2

Record Delay: 30 Second (10~300)

☑ Relay-out: 1 2

Alarm Delay: 10 Second (10~300)

☑ Send Email

☑ Audio Linkage

☑ Snapshot: 1 2

Figure 3.3-21 Crowd Detection Setting

Step 2 Click "Draw Rule" to draw rules in the monitoring screen

Step 3 Configure the parameter information according to actual needs. Please refer to Table 3.3-13 for parameter description

Parameters	Descriptions
Tracking Time	Set the minimum time between the target appearance in the area and the trigger of the alarm
Sensitivity	Set Sensitivity for alarm triggering, with the value range of 1～10, and the default is 5
Min Gathering Area	Click "Draw Target" to draw the smallest gathering area model in the screen; when the number of people in the designated area is greater than this model scale and their stay exceeds the set Tacking Time, an alarm will be triggered; click "Clear" to delete the drawn smallest gathering area model

Table 3.3-13 Crowd Detection Parameter Description

Please refer to "3.3.3.1.1 Tripwire" for other parameter descriptions.

Step 4 Click "Save" to complete the configuration.

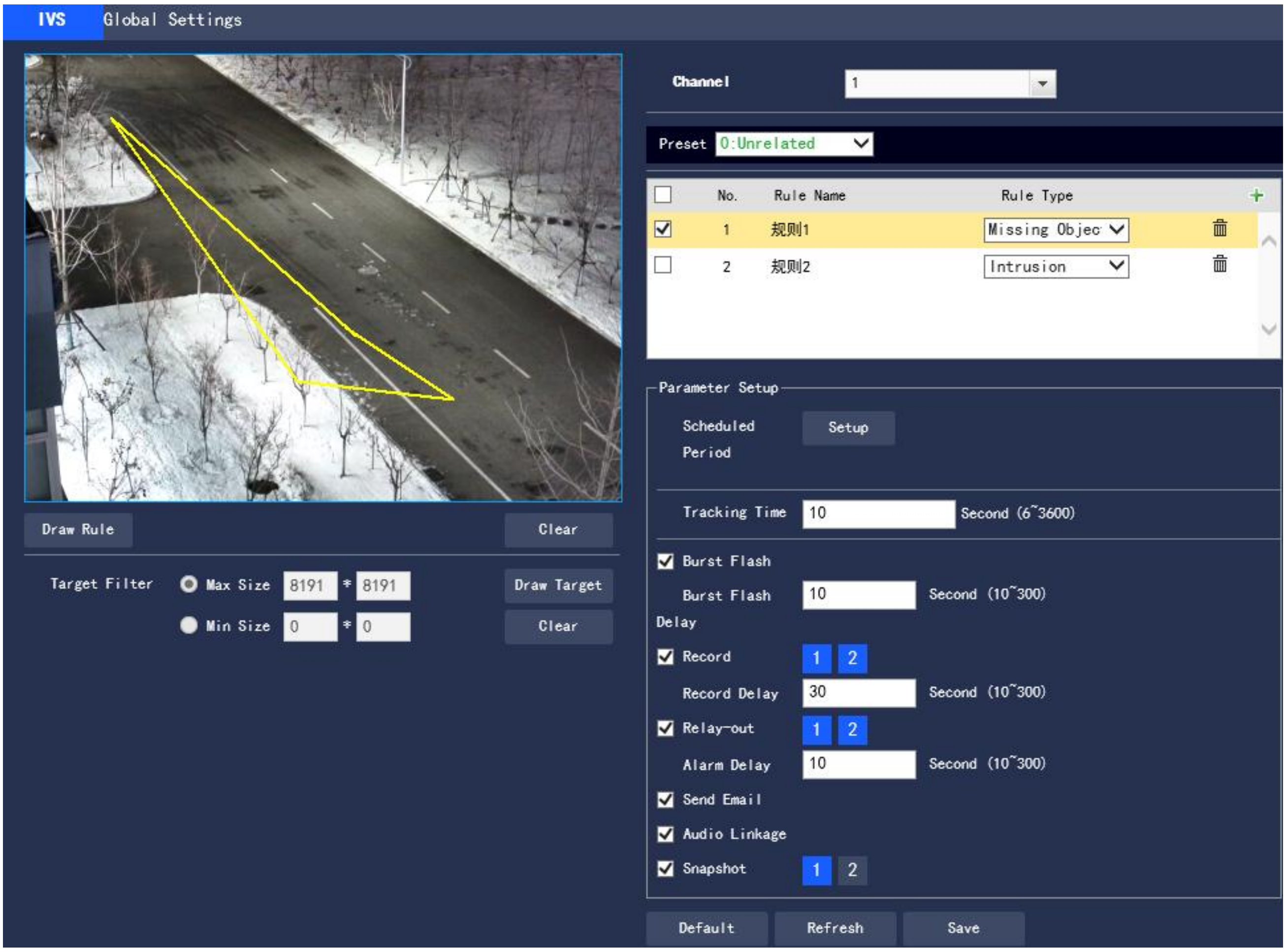
3.4.3.1.8 Missing Object

Missing Object refers to the triggering of an alarm when the selected target in the original scene is taken away for more than a certain period of time. The system will make statistics on the stationary area in the foreground area, and distinguish between Missing Object and Abandoned Object according to the similarity between the foreground and the background. If the time set by the user is exceeded, an alarm will be triggered.

Application Scenarios: suitable for scenarios with sparse targets, no obvious and frequent light changes; for scenarios with a high target density and frequent occlusion, underreporting will increase; for scenarios with a lot of people staying, false positives will increase; the detection area is required to have a texture as simple as possible, and it is not suitable for areas with too complex textures

The configuration steps are as follows:

Step 1 If the rule type is selected as "Missing Object", the configuration interface is as shown in Figure 3.3-22



Channel 1

Preset 0:Unrelated

☐	No.	Rule Name	Rule Type	
☑	1	规则1	Missing Objec	🗑
☐	2	规则2	Intrusion	🗑

Target Filter ● Max Size 8191 * 8191

○ Min Size 0 * 0

Parameter Setup

Scheduled Period Setup

Tracking Time 10 Second (6~3600)

☑ Burst Flash

Burst Flash Delay 10 Second (10~300)

☑ Record 1 2

Record Delay 30 Second (10~300)

☑ Relay-out 1 2

Alarm Delay 10 Second (10~300)

☑ Send Email

☑ Audio Linkage

☑ Snapshot 1 2

Figure 3.3-22 Missing Object Setting

Step 2 Click "Draw Rule" to draw rules in the monitoring screen

Step 3 Configure the parameter information according to actual needs. Please refer to Table 3.3-14 for parameter description

Parameters	Descriptions
Tracking Time	Set the shortest time between the disappearance of the object and the triggering of the alarm

Table 3.3-14 Missing Object Parameter Description

Please refer to "3.3.3.1.1 Tripwire" for other parameter descriptions.

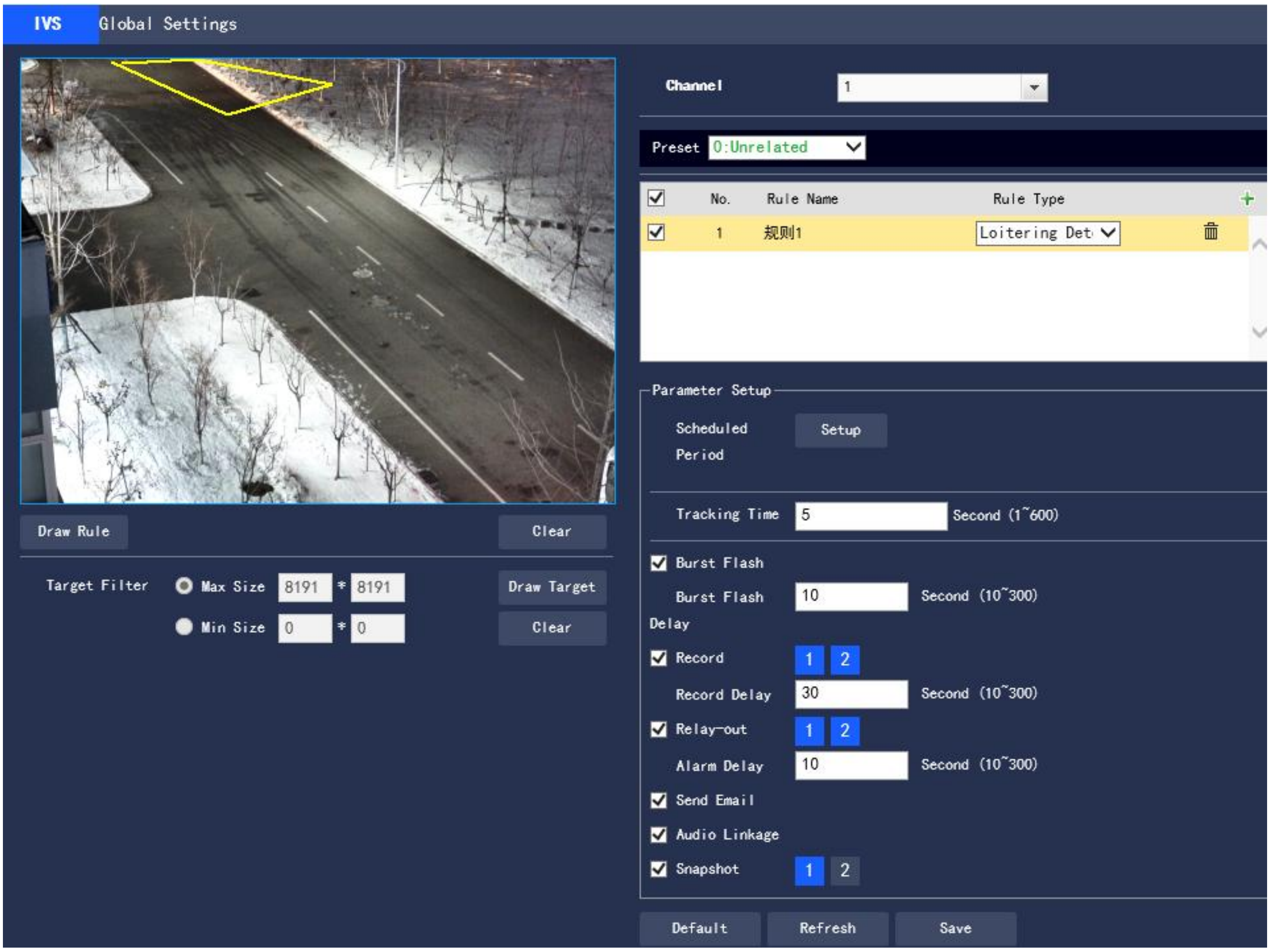
Step 4 Click "Save" to complete the configuration.

3.3.3.1.9 Loitering Detection

When the target has a trajectory in the set area and its stay exceeds the set time, an alarm will be generated; for a stationary target, the wandering is invalid.

The configuration steps are as follows:

Step 1 If the rule type is selected as "Loitering Detection", the configuration interface is as shown in Figure 3.3-23



Channel 1

Preset 0:Unrelated

☑	No.	Rule Name	Rule Type
☑	1	规则1	Loitering Det

Target Filter ● Max Size 8191 * 8191 ○ Min Size 0 * 0

Scheduled Period

Tracking Time 5 Second (1~600)

☑ Burst Flash

Burst Flash Delay 10 Second (10~300)

☑ Record 1 2

Record Delay 30 Second (10~300)

☑ Relay-out 1 2

Alarm Delay 10 Second (10~300)

☑ Send Email

☑ Audio Linkage

☑ Snapshot 1 2

Figure 3.3-23 Wandering Setting

Step 2 Click "Draw Rule" to draw rules in the monitoring screen.

Step 3 Configure the parameter information according to actual needs. Please refer to Table 3.3-15 for parameter description.

Parameters	Descriptions
Tracking Time	Set the shortest time between the disappearance of the object and the triggering of the alarm

Table 3.3-15 Wandering Parameter Description

Please refer to "3.3.3.1.1 Tripwire" for other parameter descriptions

Step 4 Click "Save" to complete the configuration.

3.3.3.2 Global Settings

Purpose and Principle of Depth-of-Field Calibration

According to 1 plane line and 3 height lines calibrated by the user, and the corresponding distance in the actual environment, it can estimate the internal parameters of the camera (including internal geometric characteristics and optical characteristics) and external parameters (the camera's three-dimensional position and direction relative to the actual environment coordinate system), and then determine the correspondence between the two-dimensional image obtained by the camera and the three-dimensional real object.

Methods and Notes for Depth-of-field Calibration Configuration

● Usage scenarios:

It should choose as many mid and far scenarios with a camera installation height of more than 3 meters as possible, while not supporting scenarios where the angle is too flat or ceiling-mounted

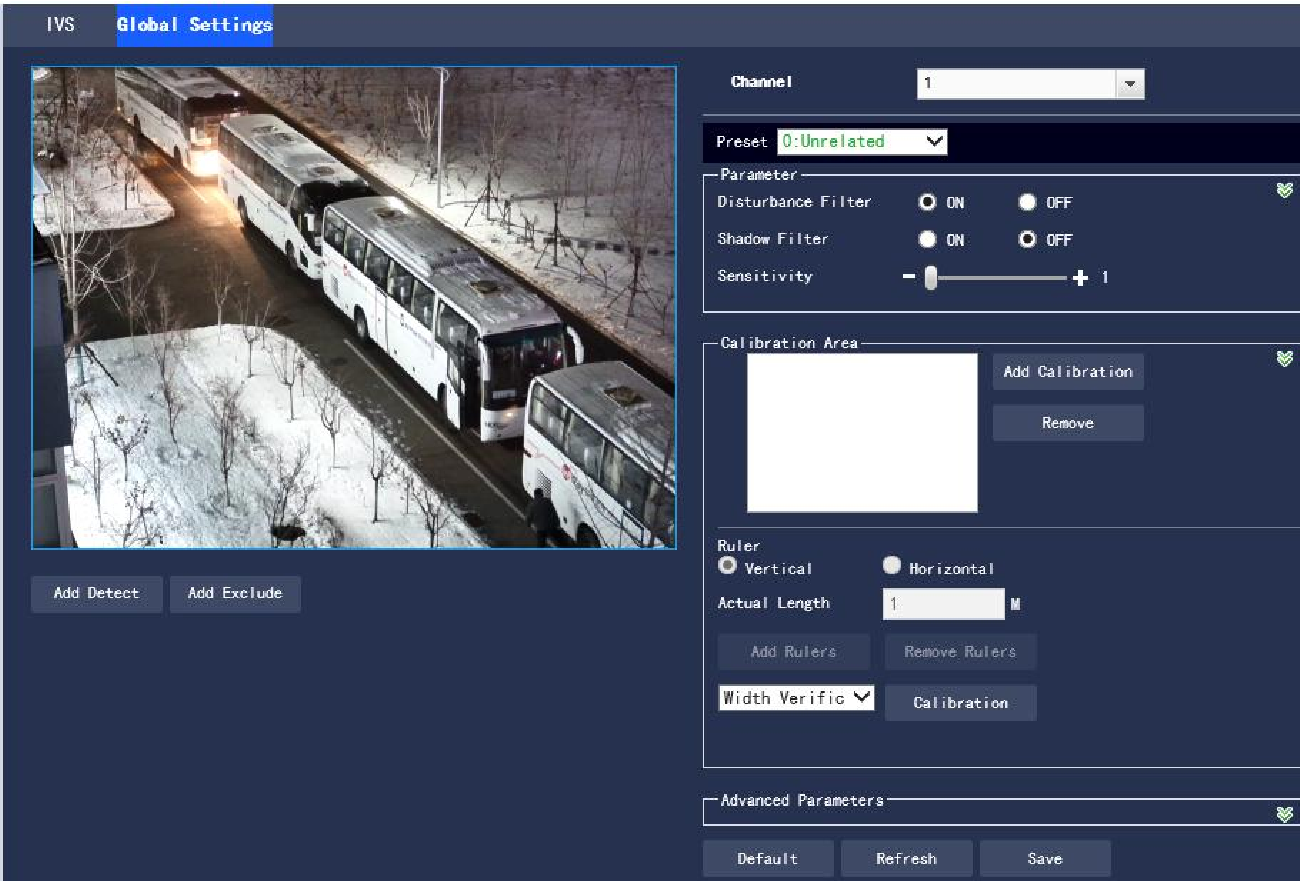
It supports calibration only on the horizontal plane, but not on vertical walls or inclined planes.

It does not support scenarios with distorted images, such as ultra-wide-angle cameras and fish-eye cameras

● Calibration settings. The drawn calibration area should be in the same horizontal plane

The configuration steps are as follows:

Step 1 Select "Settings > Event Management > General Behavior Analysis > Global Settings". The system displays the "Global Settings" interface as shown in Figure 3.3-24.



Channel: 1

Preset: 0:Unrelated

Disturbance Filter: ● ON ○ OFF

Shadow Filter: ○ ON ● OFF

Sensitivity: 1

Ruler: ● Vertical ○ Horizontal

Actual Length: 1 M

Figure 3.3-24 Global Settings

Step 2 Select Preset point for the Global Settings function

● This preset point has been configured with a smart plan. Please refer to "3.3.2 Smart Plan" for details on the smart plan configuration method

Step 3 Click "Add Calibration" and draw the calibration area in the monitoring screen

Step 4 Select to draw "Vertical" or "Horizontal" rulers according to actual needs

● Vertical ruler settings: the bottom of the three vertical rulers should be on the same horizontal plane, and it should select the reference objects with three fixed heights distributed in a triangle as a vertical ruler, such as a vehicle stopped on the roadside, or a street light pole; the best way is to arrange a dedicated person to select three standing positions in the monitoring scene, and then make drawings separately

● Horizontal ruler settings: similarly, it also selects a reference object with a known length on the ground, such as an indicator on the road, or use a tape to measure the actual length

Step 5 Set the length of the ruler to be drawn in the actual environment

Step 6 Click "Add Rulers" and draw a ruler in the monitoring screen

Step 7 Select the calibration type, and click "Calibration" and drawing a line in the monitoring screen can display its corresponding actual length

● After the ruler setting is finished, verification tools should be applied to verify the set parameters. If it is found that the calibration error is significantly different from the actual one the settings need to be fine-tuned or reset until the error requirements are met

Step 8 Configure the parameter information according to actual needs. Please refer to Table 3.3-16 for parameter description

Parameters	Descriptions
Disturbance Filter	On by default, and suppress random disturbance to some extent
Shadow Filter	Off by default. For scenes with shadows, turning on this function can make the target frame only contain the target itself (excluding shadows), and multiple shadow-attached targets can be detected separately, providing a more accurate initial target position for tracking. The negative effect of this function is that a part of the target similar to the shadow will be misjudged as the shadow and then removed
Sensitivity	The value range is 1～10, and the default is 5. The larger the value is, the easier it is to trigger low-contrast targets and small targets, the greater the pseudo detection rate, the higher the false detection rate
Add Detect	Click this button to draw the detection area, and the camera will perform detection in this area
Add Exclude	Click this button to draw an exclusion zone, and the area within this zone will be excluded from the detection range
Set Track Rate	Click this button to set the current rate as the track rate
Save Preset	Click this button to save the settings of this preset point

Effective Target Overlap Rate	The value range is 0～100, and the default value is 0. The larger the value, the easier the detection frame will appear, the lower the missed detection rate, and the higher the false detection rate
Effective Target Movement Distance	The value range is 0～100, and the default value is 10. The smaller the value, the earlier the detection, while the larger the value, the higher the missed detection rate and the lower the false detection rate
Effective Target Movement Time	The value range is 0～100, and the default value is 10. The smaller the value, the earlier the detection, while the larger the value, the higher the missed detection rate and the lower the false detection rate

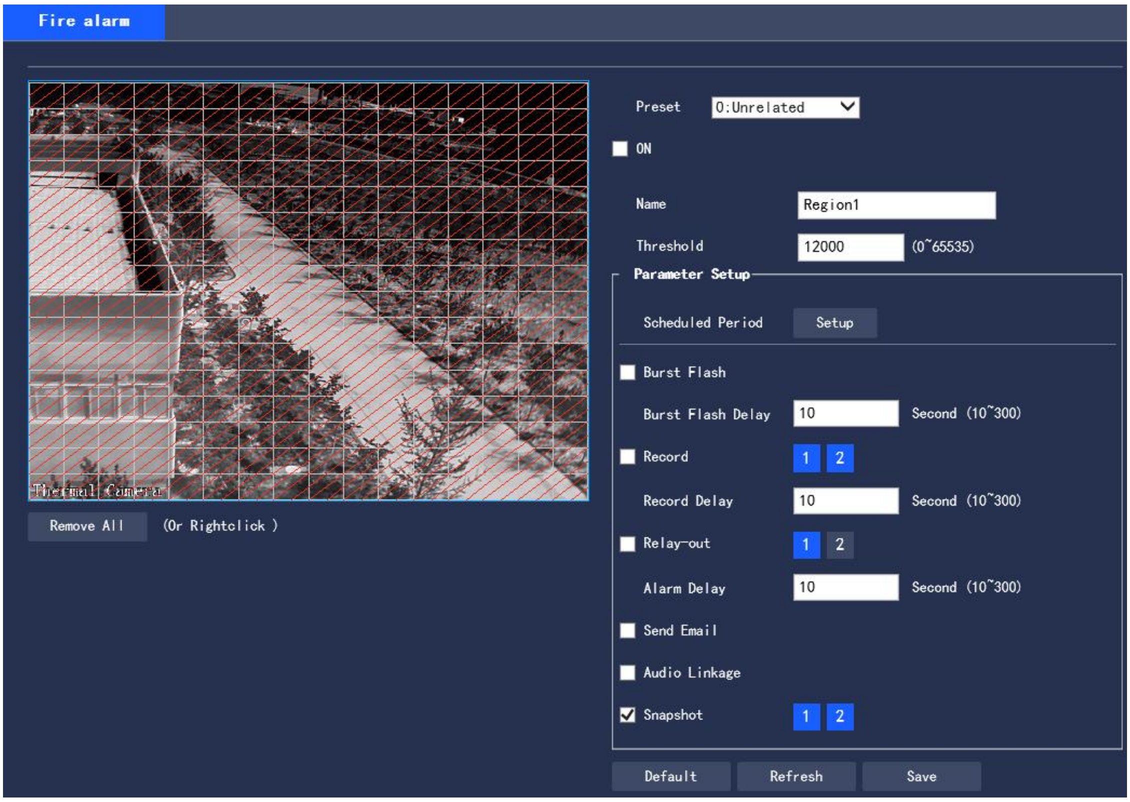
Table 3.3-16 Global Settings Parameter Description

Step 9 Click "Save" to complete the configuration.

3.3.4 Fire Alarm

After setting the fire alarm rules for the thermal imaging, when the system judges that it is a fire, it will generate an alarm and link the set action.

Step 1 Select "Settings > Event Management> Fire alarm". The system displays the thermal imaging fire alarm interface as shown in Figure 3.3-25.



Preset: 0:Unrelated

□ ON

Name: Region1

Threshold: 12000 (0~65535)

Scheduled Period: Setup

□ Burst Flash

Burst Flash Delay: 10 Second (10~300)

□ Record 1 2

Record Delay: 10 Second (10~300)

□ Relay-out 1 2

Alarm Delay: 10 Second (10~300)

□ Send Email

□ Audio Linkage

☑ Snapshot 1 2

Figure 3.3-25 Fire Alarm

Step 2 Select preset point

The default is Preset 0：Unrelated. All scenarios can use this configuration. If it needs to set the fire alarm of a particular scenario, the settings can be made by the first setting of preset points. The user has to select the fire alarm function associated with the preset points first, and the fire alarm setting can vary for each preset point. Please refer to "3.3.2.1 Preset" for the setting method.

Step 3 Click "On" and set rules.

1. Select "On" to turn on the fire alarm function.
2. Monitor the configuration screen and set the corresponding rules.

Step 4 To set the fire alarm parameters, please refer to Table 3.3-17 for detailed parameter descriptions.

Parameters	Descriptions
Scheduled Period	Set the alarm time period, and the alarm event will be activated only within the set time range. 1. Click "Setup", and the "Scheduled Period" dialog box will pop up. 2. Set the alarm time period. Method 1: Press and hold the left mouse button and drag the progress bar directly

	on the setting interface for setting. Method 2: Click "Setup" corresponding to the day of weeks, tick the box in front of the time period at the bottom of the interface, and enter the time value. There are 6 time periods available for setting each day. 3. Click "Save" to complete the Scheduled Period setting.
Burst Flash	When an alarm occurs, the system is linked the burst flash. Please refer to "3.3.5.2 Burst Flash" for the burst flash configuration
Burst Flash Delay	When the alarm is over, the burst flash will be extended for a period of time before stopping.
Record	Tick the box and set the recording channel number. When an alarm occurs, the corresponding channel will automatically record the alarm. When an alarm occurs, the following two conditions should be met for the system video recording: Motion detection records enabled Automatic video recording enabled
Record Delay	When the alarm is over, the alarm recording will continue for an extended period of time before stopping.
Relay-out	Connect the alarm device (such as lights, sirens) to the Alarm Output, select the check box and set the Alarm Output device, and start the alarm linkage output port. When an alarm occurs, the system can link the corresponding Alarm Output device.
Alarm Delay	When the alarm is over, the alarm output will be extended for a period of time before stopping.
Send Email	Tick the box, and when an alarm occurs, the system will send an email to notify the user. Before enabling this function, the setting of Email is required.
Snapshot	Tick the box and set the snapshot channel number. When an alarm occurs, the

	corresponding channel will automatically take a snapshot of the image.

Table 3.3-17 Fire Alarm Parameter

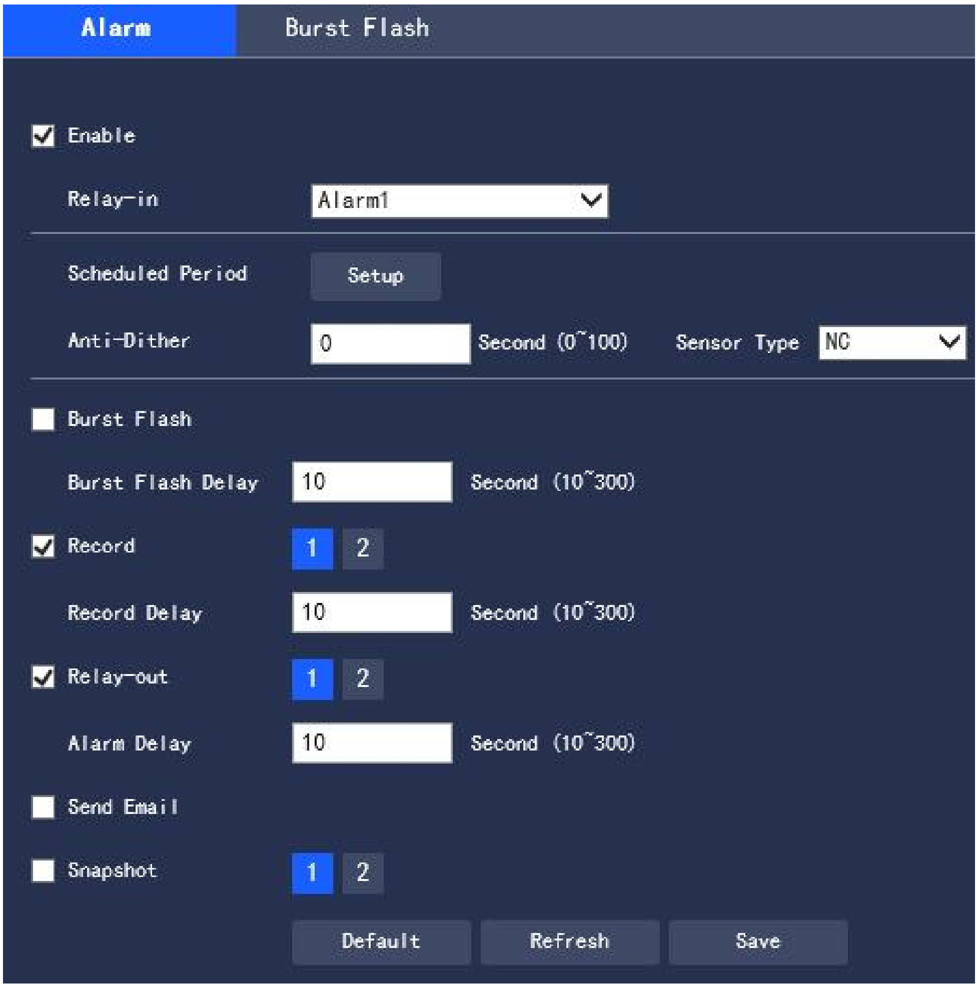
Step 5 Click "Save" to complete the setting.

3.3.5 Alarm Setup

3.3.5.1 Alarm

To set the enabling conditions for the alarm event, the configuration steps are as follows:

Step 1 "Settings > Event Management > Alarm Settings > Alarm ". The system displays the "Alarm Linkage" page as shown in Figure 3.3-26



☑ Enable

Relay-in: Alarm1

Scheduled Period: Setup

Anti-Dither: 0 Second (0~100) Sensor Type: NC

□ Burst Flash

Burst Flash Delay: 10 Second (10~300)

☑ Record: 1 2

Record Delay: 10 Second (10~300)

☑ Relay-out: 1 2

Alarm Delay: 10 Second (10~300)

□ Send Email

□ Snapshot: 1 2

Figure 3.3-26 Alarm Setting

Step 2 Configure each parameter information according to actual needs. Refer to Table 3.3-18 for parameter description

Parameters	Descriptions
Enable	After being selected, the alarm linkage can be enabled
Relay-in	Alarm 1 is corresponding to AlarmIn1 and Alarm GND; Alarm 2 is corresponding to AlarmIn 2 and Alarm GND.
Sensor Type	There are two types: normally open and normally closed; Normally open: the alarm will be triggered when the relay-in terminal is disconnected; Normally closed: the alarm will be triggered when the relay-in terminal is connected with 5VDC and the circuit is switching on.

Table 3.3-18 Alarm Setting Parameter Description

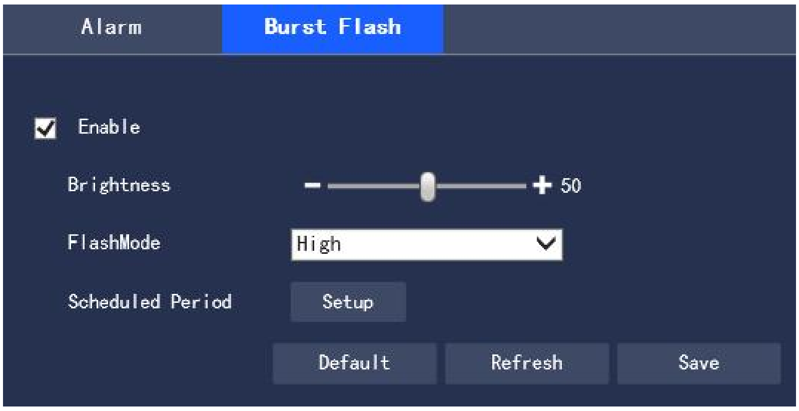
Please refer to "3.3.1.1 Motion Detection" for other parameter descriptions.

Step 3 Click "Save" to complete the configuration.

3.3.5.2 Burst Flash

To set the enabling conditions for the burst flash, the configuration steps are as follows:

Step 1 "Settings > Event Management > Alarm Settings > Burst Flash". The system displays the "Burst Flash" page as shown in Figure 3.3-27



Brightness: 50

FlashMode: High

Figure 3.3-27 Alarm Settings

Step 2 Configure each parameter information according to actual needs. Refer to Table 3.4-19 for parameter description.

Parameter	Description

Enable	After being selected, the Burst Flash function can be enabled
Brightness	Set the brightness of the burst flash. The larger the value, the brighter the burst flash; the value range is 0～100
Flash Mode	The flash mode of the burst flash includes medium, high, low, and on. The default is medium.

Table 3.3-19 Alarm Setting Parameter Description

Please refer to "3.3.1.1 Motion Detection" for other parameter descriptions

Step 3 Click "Save" to complete the configuration.

3.4 Intelligent Temperature Measurement

3.4.1 Global Configuration

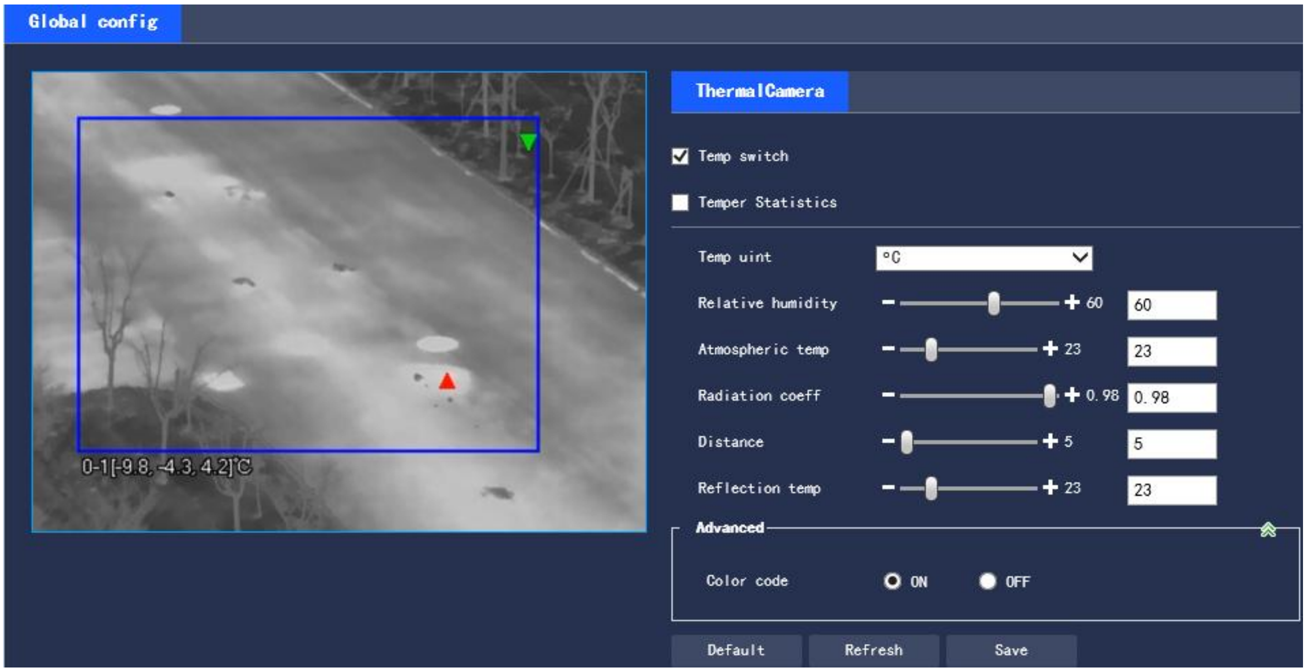
It can turn on Temp switch and Temp Statistics.

After turning on the Temp switch function, the temperature measurement rule takes effect, while the monitoring screen displays the set temperature measurement rules.

After the Temp Statistics function is turned on, the right side of the monitoring interface displays the corresponding color bar, to indicate the color change between the minimum temperature and the maximum temperature.

Step 1 Select "Settings > Intelligent Temperature Measurement > Global Config".

The system displays the "Global Config" interface as shown in Figure 3.4-1.



☑ Temp switch

□ Temper Statistics

Temp uint °C

Relative humidity 60

Atmospheric temp 23

Radiation coeff 0.98

Distance 5

Reflection temp 23

Color code ◉ ON ○ OFF

Figure 3.4-1 Global Config

Step 2 Set global configuration parameters. Please refer to Table 3.4-1 for detailed parameter descriptions.

Parameters	Descriptions
Temp Switch	Tick the box to enable the Temp switch function.
Temp Statistics	Tick the box to turn on the temperature statistics function.
Temp Unit	The units of temperature displayed include ℃ and ℉.
Atmospheric Temp	The temperature of the environment The value range is -50℃～+327.7℃.
Atmospheric Transmissivity	The transmissivity of the environment. The value range is 0～1
Radiation Coefficient	Set the radiation coefficient of the target. The value range is 0～1.
Distance	The distance between the camera and the target. The value range is 0m～10000m.

Reflection Temp	The temperature of the target. The value range is -50℃～+327.7℃.
Temp Range	There are High Gain (-20℃～150℃) and Low Gain(100℃～550℃), High Gain by default.

Table 3.4-1 Global Config Parameter Description

Step 3 Click "Save" to complete the setting.

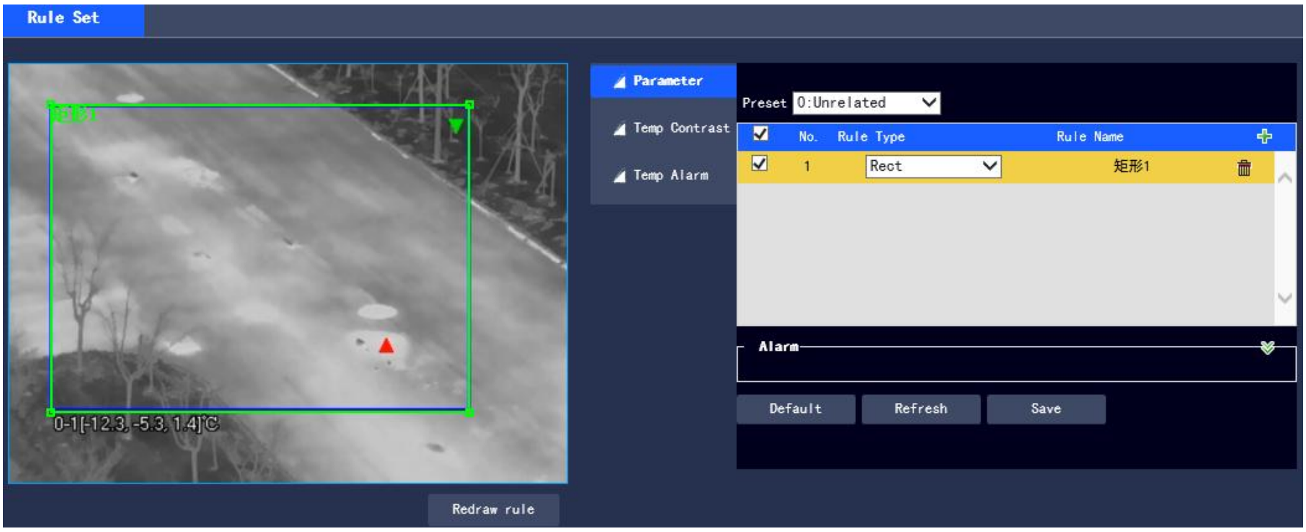
3.4.2 Rule Set

It supports the settings of the temperature measurement rules and temperature comparison. When the temperature meets the set alarm conditions, the alarm output will be linked.

3.4.2.1 Temperature Measurement Rule Set

Step 1 Select "Settings > Intelligent Temperature Measurement > Rule Set > Parameter".

The system displays the "Parameter" interface as shown in Figure 3.4-2.



Preset 0:Unrelated

☑	No.	Rule Type	Rule Name
☑	1	Rect	矩形1

Figure 3.4-2 Parameter Settings

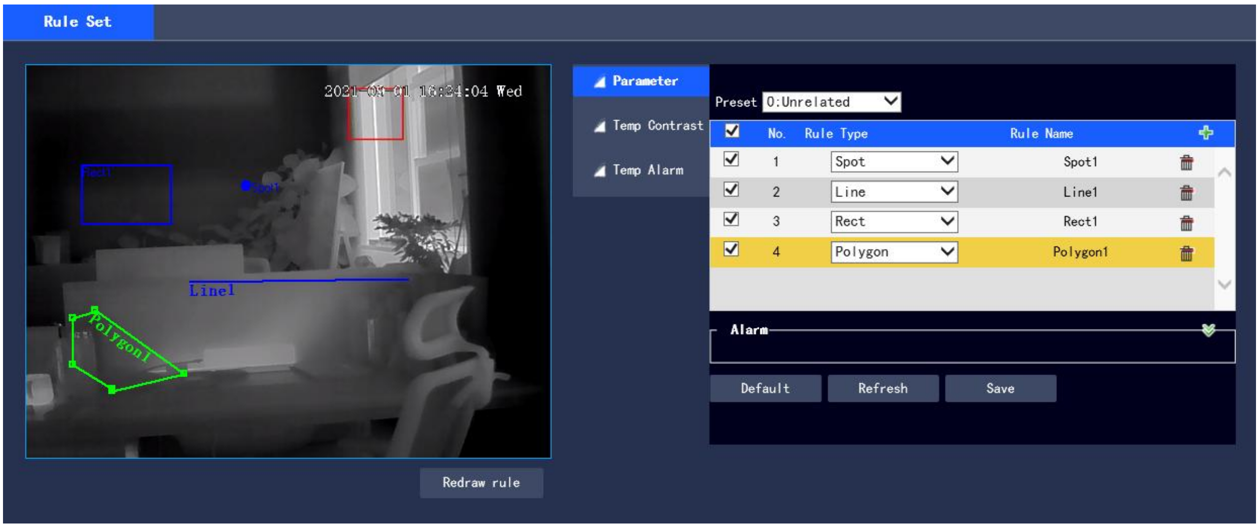
Step 2 Select Preset point

The default is Preset 0, that is, an unrelated preset point. All scenarios can use this configuration.

Note: The settings for the preset points of the temperature measurement and the fire alarm are different. The preset point rule of the temperature measurement rule includes the rules of Preset 0, while the preset point of the fire alarm is set individually or synchronized with the setting of Preset 0.

Step 3 Set temperature measurement rules and parameters.

1. Click + to add new rules. The system displays the new rule interface as shown in Figure 3.4-3.



Preset 0:Unrelated

☑	No.	Rule Type	Rule Name	+
☑	1	Spot	Spot1	🗑
☑	2	Line	Line1	🗑
☑	3	Rect	Rect1	🗑
☑	4	Polygon	Polygon1	🗑

Figure 3.4-3 New Rules

2. Select the desired rule type, double click the rule name to change.

3. Draw Rules.

If the "Rule Type" is selected as "Spot", click the target position in the monitoring screen to draw the rule.

If the "Rule Type" is selected as "Line", "Rect" or "Ellipse", press and hold the mouse left button to draw the rule in the monitoring screen.

If the "Rule Type" is selected as "Polygon", press and hold the left mouse button to draw the rule in the monitoring screen, and click the right button to end the drawing.

Note: Select the drawn rule and click "Redraw Rule" to delete the drawn rule and redraw it.

4. Select "Enable local configuration" and set the local configuration parameters. Refer to Table 3.4-2 for detailed parameter descriptions.

Parameters	Descriptions
Radiation Coefficient	The radiation coefficient of the target. The value range is 0～1.

Distance	The distance between the camera and the target. The value range is 0～10000m.
Reflection Temp	The temperature of the target. The value range is -50℃～+327.7℃.

Table 3.4-2 Local Configuration Parameter Description

5. Select "Alarm Output" and set its parameters. Refer to Table 3.4-3 for detailed parameter descriptions.

Parameters	Descriptions
Alarm Results	The value method of the temperature that triggers the alarm. If the "Rule Type" is selected as "Spot", it includes the average temperature and temperature slope. If the "Rule Type" is selected as "Line", "Rec", "Polygon", or "Ellipse", it includes the highest temperature, lowest temperature, average temperature, temperature slope and temperature difference. **Description** The temperature difference refers to the difference between the highest temperature and the lowest temperature in the current temperature measurement rules, and the temperature slope refers to the temperature change rate in the current temperature measurement rules.
Condition	Set alarm conditions, including Below, Match, and Above.
Threshold Temp	This parameter can be set when the "Results" is set to "highest temperature", "lowest temperature", "average temperature" or "temperature difference". The temperature that triggers the alarm. The value range is -40℃～+550℃.
Temperature Slope	This parameter can be set when the "Results" is set to "temperature slope". The temperature changes per minute. The value range is -600°C per minute～600°C per minute.
Temperature Deviation	The error of the alarm threshold temperature. As long as the alarm threshold temperature or temperature change of the temperature slope is within the error range, it will be treated as reaching the alarm threshold temperature or the temperature slope. The value range is ±0.1℃.

Temperature Duration	The duration of temperature or temperature change. The value range is 0s～1000s.

Table 3.4-3 Alarm Parameter Description

Step 3 Click "Save" to complete the setting.

After the setting, the preview interface on the left displays the temperature of the temperature measurement rule.

3.4.2.2 Temp Contrast Setting

Compare the temperature of the selected point, line or area, and the comparison results are displayed on the preview interface.

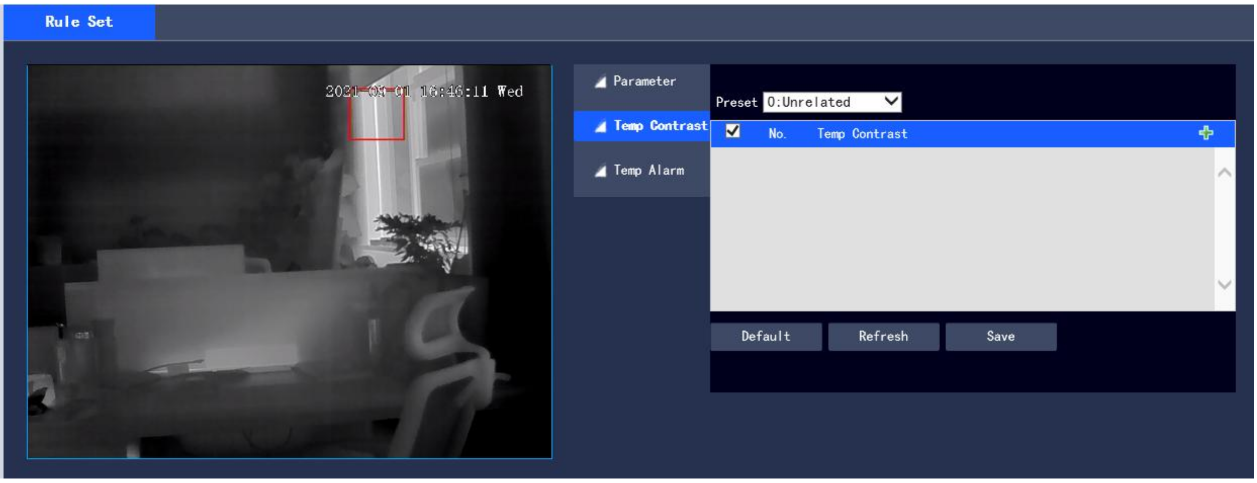
Prerequisites

At least two temperature measurement rules have been set. Please refer to "3.4.2.1 Temperature Measurement Rule Set" for details

Operating Steps

Step 1 Select "Settings > Intelligent Temperature Measurement > Rule Set > Temp Contrast".

The system displays the "Temp Contrast" as shown in Figure 3.4-4.

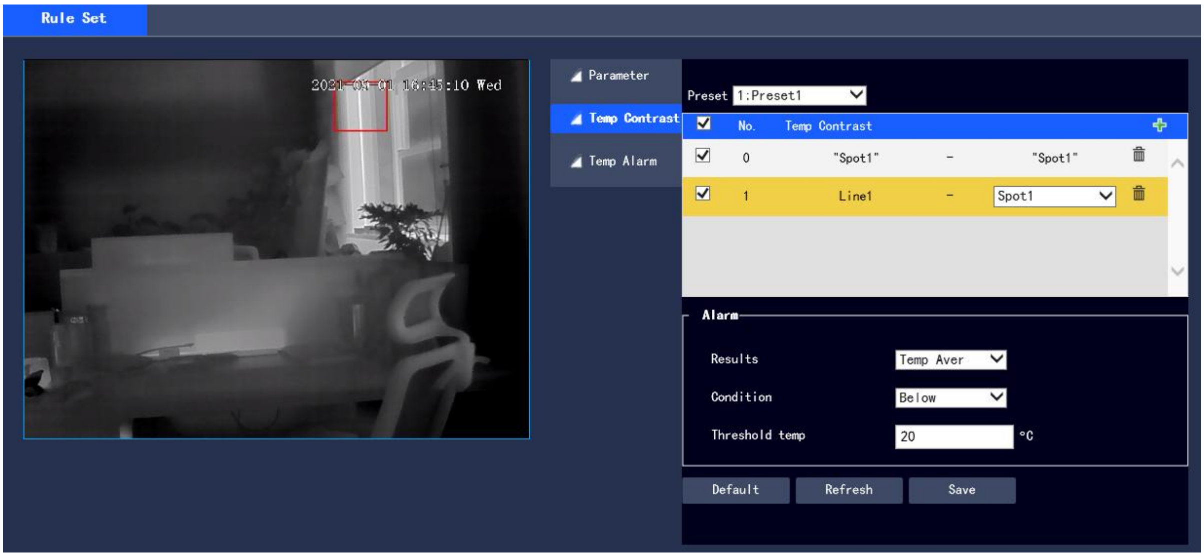


Preset 0:Unrelated

Figure 3.4-4 Temp Contrast

Step 2 Set Temp Contrast rules.

1. Click ✚ to add a temperature contrast rule. The system displays the interface of new temperature contrast rules as shown in Figure 3.4-5.



Preset 1:Preset1

☑ No.	Temp Contrast		
☑ 0	"Spot1"	-	"Spot1"
☑ 1	Line1	-	Spot1

Alarm

Results: Temp Aver

Condition: Below

Threshold temp: 20 °C

Figure 3.4-5 New Temperature Contrast Rules

2. Double click the new temperature contrast rule to select the contrast object.

3. To set the alarm parameters, refer to Table 3.4-4 for detailed parameter descriptions.

Parameters	Descriptions
Results	The value method of the contrast temperature that triggers the alarm. Temp Aver: The average temperature of the two rules. Temp Max: The maximum temperature of the two rules. Temp Min: The lowest temperature of the two rules. **Description** When one of the compare objects is "Spot", the highest temperature and the lowest temperature are both the average temperature.
Condition	The conditions that trigger the alarm include Below, Match, and Over.
Threshold Temp	The temperature that triggers the alarm. The value range is 0°C～550°C.

Table 3.4-4 Temperature Contrast Parameter Description

Step 3 Click "Save" to complete the setting.

After the setting is completed, the preview interface on the left will display the temperature contrast results of the selected object.

3.4.2.3 Temp Alarm Set

When the temperature meets the alarm conditions of the temperature measurement rules, the system will generate an alarm and link the set action.

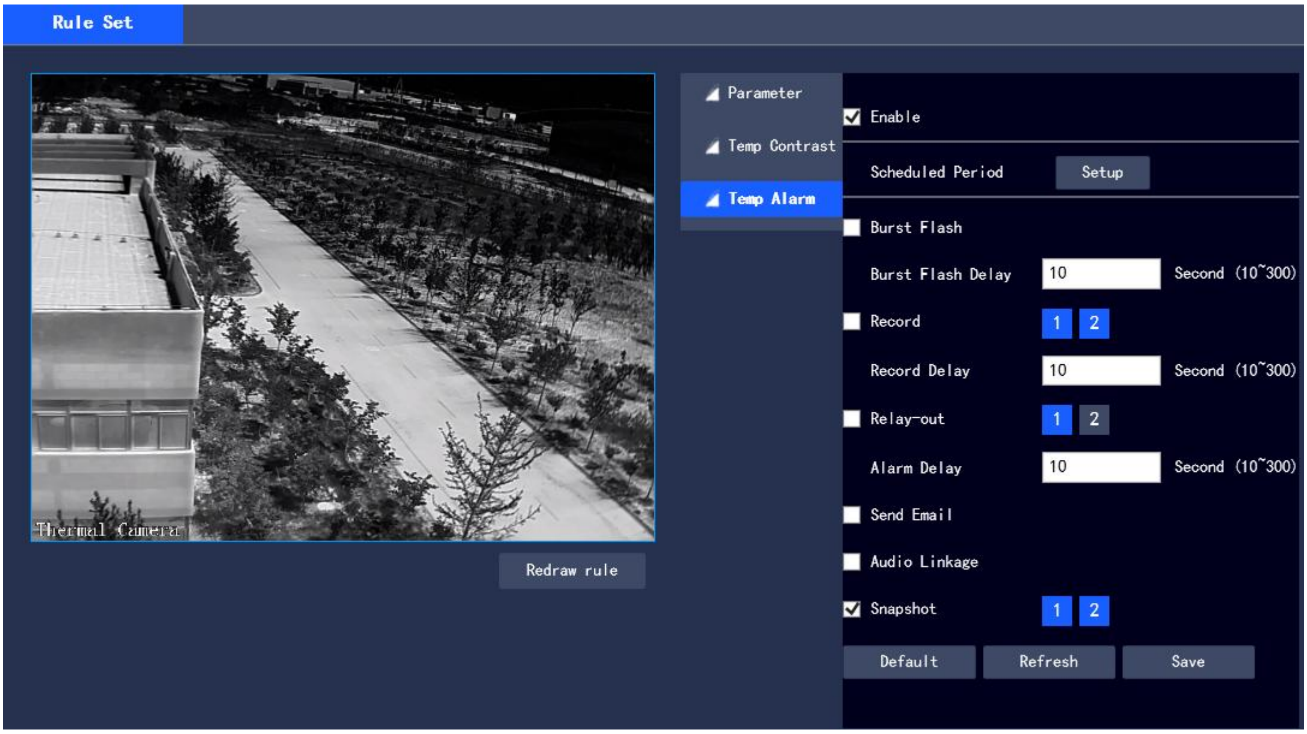
Prerequisites

The temperature measurement rules have been set, and please refer to "3.4.2.1 Temperature Measurement Rule Set" for detailed operations.

Operating Steps

Step 1 Select "Settings> Intelligent Temperature Measurement > Rule Set > Temp Alarm".

The system displays the "Temp Alarm" interface as shown in Figure 3.4-6.



☑ Enable

Scheduled Period

□ Burst Flash

Burst Flash Delay 10 Second (10~300)

□ Record 1 2

Record Delay 10 Second (10~300)

□ Relay-out 1 2

Alarm Delay 10 Second (10~300)

□ Send Email

□ Audio Linkage

☑ Snapshot 1 2

Figure 3.4-6 Temperature Alarm Setting

Step 2 Select "Enable" to turn on the temperature alarm.

Step 3 Set the temperature alarm parameters. Please refer to Table 3.4-5 for detailed parameter descriptions.

Parameter	Description
Enable	Enable temperature alarm

Table 3.4-5 Temperature Alarm Parameter

Please refer to "3.3.1.1 Motion Detection" for other parameter descriptions

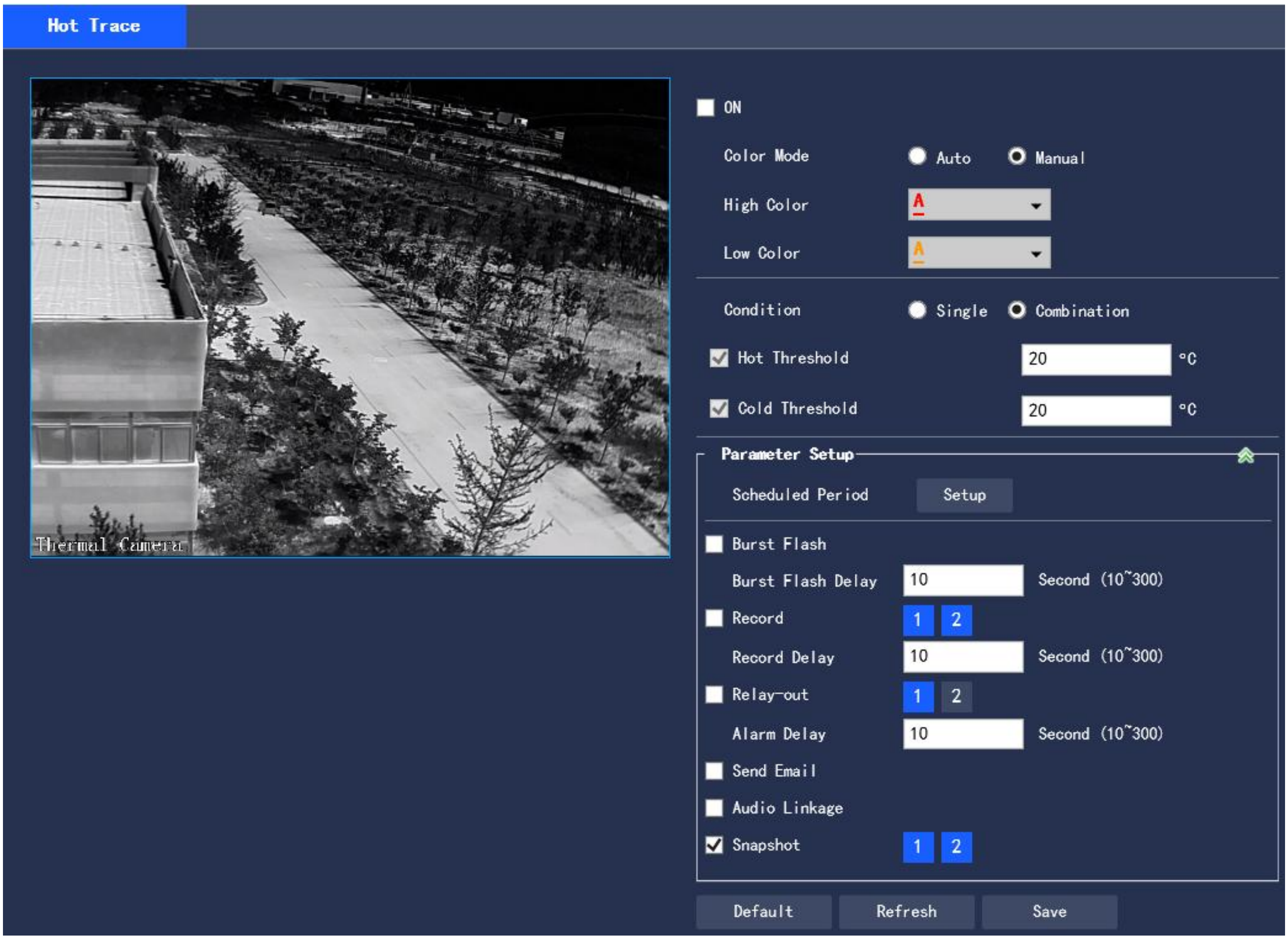
Step 4 Click "Save" to complete the setting.

3.4.3 Hot Trace

After the Hot Trace function is turned on, the highest temperature and lowest temperature will be displayed in different colors on the monitoring screen. (The observation equipment does not display the temperature of hot spot and cold spot, while only the temperature measuring equipment supports this function.)

Step 1 Select "Settings > Intelligent Temperature Measurement > Hot Trace".

The system displays the "Hot Trace" interface as shown in Figure 3.4-7



Hot Trace

□ ON

Color Mode ○ Auto ◉ Manual

High Color A

Low Color A

Condition ○ Single ◉ Combination

☑ Hot Threshold 20 °C

☑ Cold Threshold 20 °C

Parameter Setup

Scheduled Period Setup

□ Burst Flash

Burst Flash Delay 10 Second (10~300)

□ Record 1 2

Record Delay 10 Second (10~300)

□ Relay-out 1 2

Alarm Delay 10 Second (10~300)

□ Send Email

□ Audio Linkage

☑ Snapshot 1 2

Default Refresh Save

Figure 3.47 Hot Trace

Step 2 Select "On" to enable the Hot Spot and Cold Spot Tracing function.

Step 3 Set parameters for Hot Trace. Please refer to Table 3.4-6 for detailed parameter descriptions.

Parameter	Description
Color Mode	The high and low temperature points are displayed in colors. Auto: Select the colors of the high-temperature point and the low-temperature point according to the current screen. Manual: Customize high temperature and low temperature colors.
Condition	The conditions to trigger the alarm. Single: Tick "Hot Threshold", when the maximum temperature is higher than this user-set temperature, the system will generate an alarm. Tick "Cold Threshold", when the lowest temperature is lower than this user-set temperature, the system will generate an alarm. When both are ticked at the same time, it means that as long as one of them is satisfied, the system will generate an alarm. Combination: When the highest temperature is higher than the user-set temperature, and the lowest temperature is lower than the user-set temperature, the system will generate an alarm.

Table 3.4-6 Hot Trace Parameter Description

Please refer to "3.3.1.1 Motion Detection" for other parameter descriptions

Step 4 Click "Save" to complete the setting.

3.4.4 Heat Map

Capture the temperature value of each pixel point on the thermal imaging.

Step 1 Select "Settings > Intelligent Temperature Measurement > Heat Map". The system displays the "Heat Map" interface as shown in Figure 3.4-8.

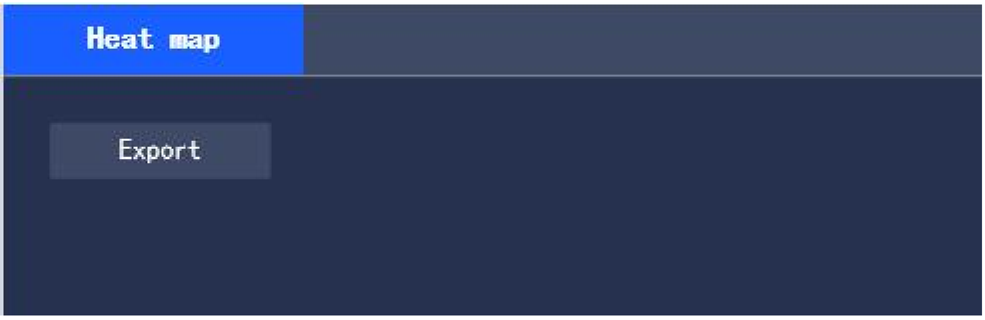


Figure 3.4-8 Heat Map Settings

Step 2 Click "Export" to export the heat map file

3.5 Storage Management

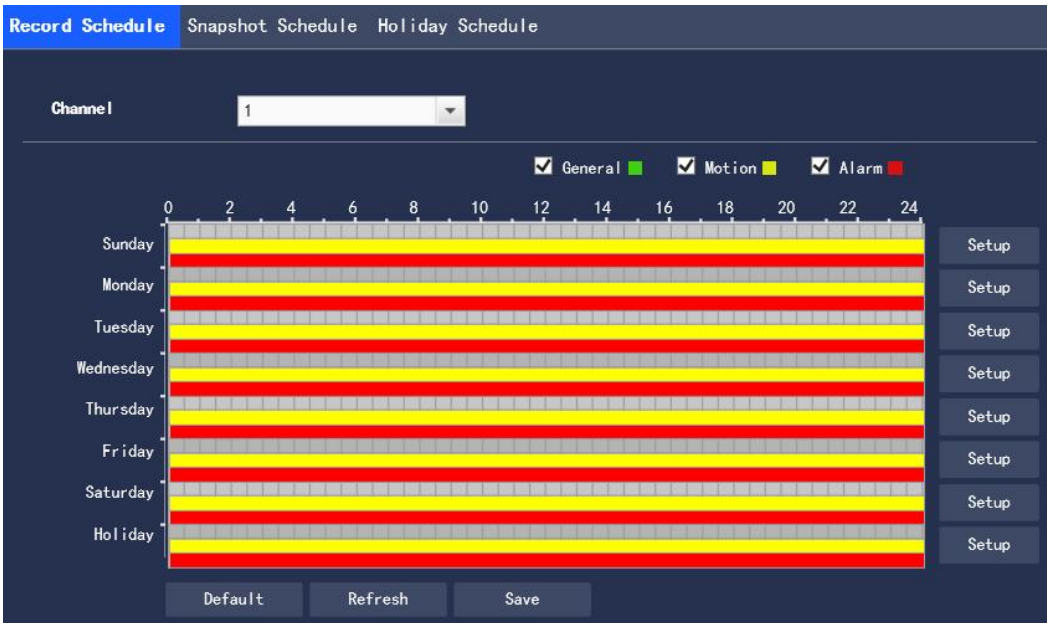
3.5.1 Schedule

Before the setup of Schedule, it should make sure that the Record Mode is Auto in Record Control

Note: If Record Mode in Record Control is "Off", the device will not record or capture pictures as set in Schedule

3.5.1.1 Record Schedule

Step 1 Select "Settings > Storage Management > Schedule > Record Schedule". The system displays the "Record Schedule" interface as shown in Figure 3.5-1



Channel 1

☑ General 🟩 ☑ Motion 🟨 ☑ Alarm 🟥

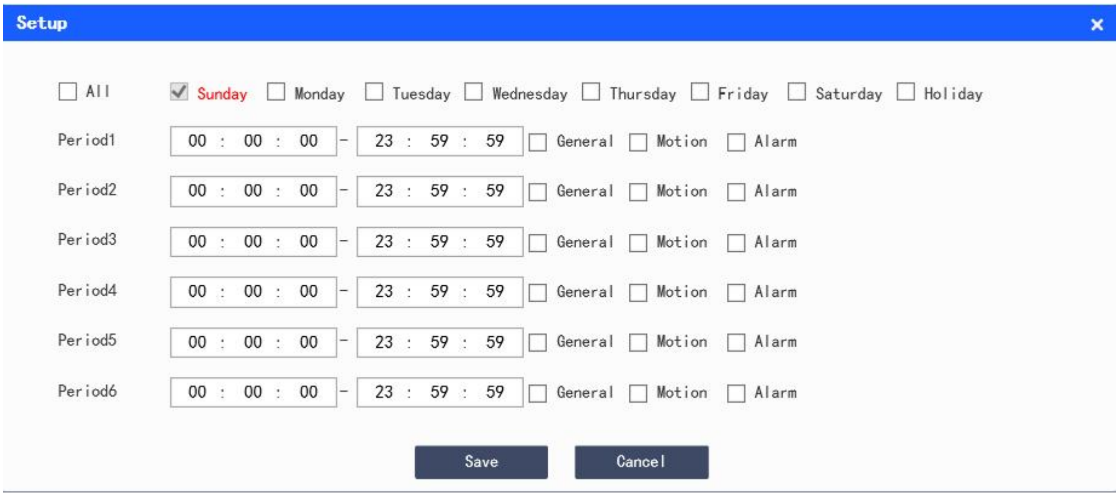
Figure 3.5-1 Record Schedule

Step 2 Select the record time from "Monday to Sunday", click "Setup" on the right and it will display the interface as shown in Figure 3.6-2

● Set the record time period according to your needs, with 6 time periods available every day

● By selecting or canceling, three types of the record schedule can be added or deleted: General, Motion, and Alarm

Note: The time period can also be set by pressing and holding the left mouse button and dragging the progress bar directly on the "Record Schedule" interface.



☐ All ☑ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday ☐ Holiday

Period1	00 : 00 : 00	– 23 : 59 : 59	☐ General	☐ Motion	☐ Alarm
Period2	00 : 00 : 00	– 23 : 59 : 59	☐ General	☐ Motion	☐ Alarm
Period3	00 : 00 : 00	– 23 : 59 : 59	☐ General	☐ Motion	☐ Alarm
Period4	00 : 00 : 00	– 23 : 59 : 59	☐ General	☐ Motion	☐ Alarm
Period5	00 : 00 : 00	– 23 : 59 : 59	☐ General	☐ Motion	☐ Alarm
Period6	00 : 00 : 00	– 23 : 59 : 59	☐ General	☐ Motion	☐ Alarm

Figure 3.5-2 Record Schedule-Schedule Setting

Step 3 Click "Save" to return to the "Record Schedule" interface as shown in Figure 3.5-3

At this time, the color bar graph intuitively represents the set time zone, where:

🟩Green: General

🟨Yellow: Motion

🟥Red: Alarm

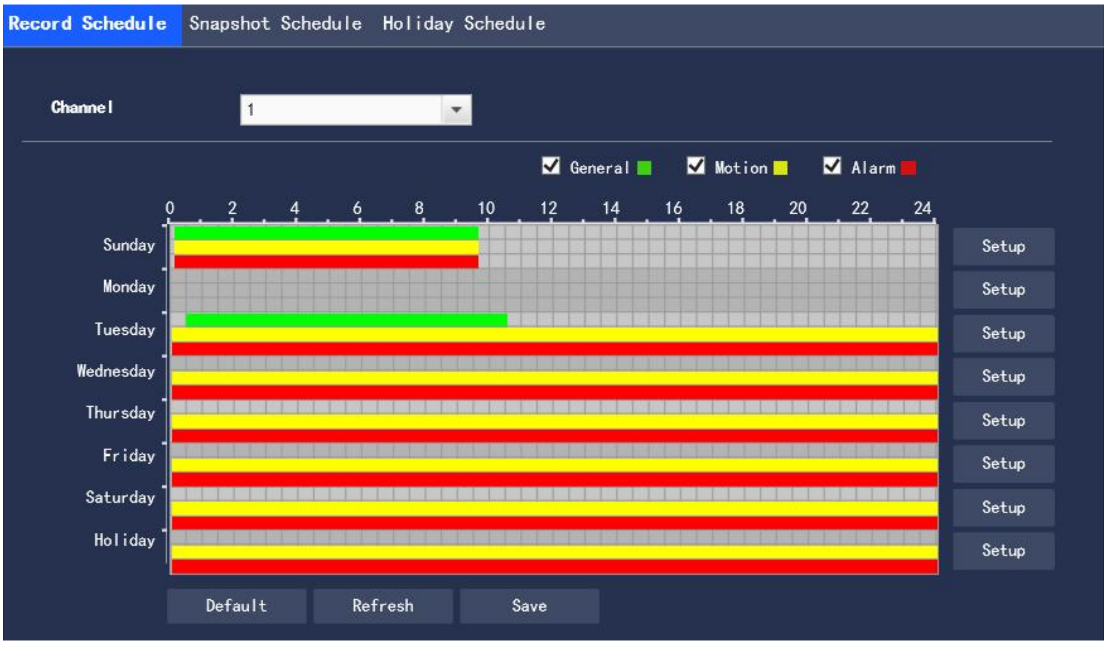
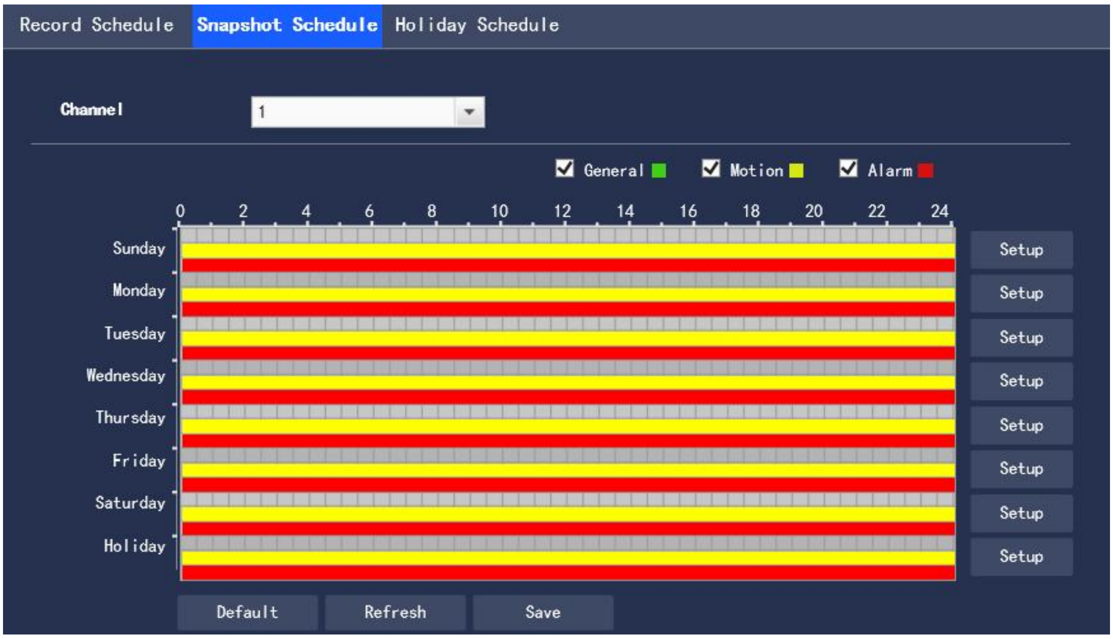


Figure 3.5-3 Record Schedule-Schedule Setting Completed

Step 4 Click "Save" on the "Record Schedule" interface, the system prompts "Save successfully" and the schedule setting is completed

3.5.1.2 Snapshot Schedule

Step 1 Select "Settings > Storage Management > Schedule > Snapshot Schedule". The system displays the "Snapshot Schedule" interface as shown in Figure 3.5-4



Channel 1

☑ General 🟩 ☑ Motion 🟨 ☑ Alarm 🟥

Figure 3.5-4 Snapshot Schedule

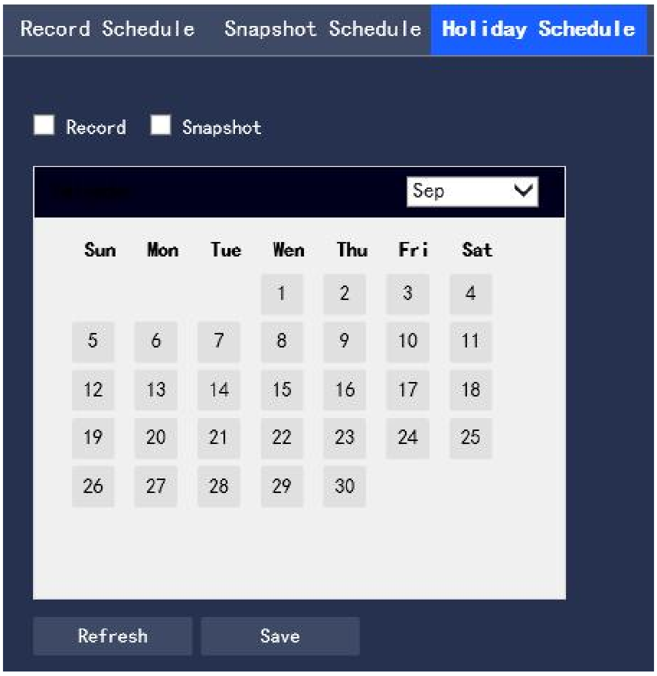
Step 2 Refer to steps 2 to 3 of "3.5.1.1 Recording Schedule" to set the time period for snapshot

Step 3 Click "Save", the system prompts "Save successfully", and the schedule setting is completed

3.5.1.3 Holiday Schedule

Holiday schedule can set specific dates as holidays

Step 1 Select “Settings > Storage Management > Schedule > Holiday Schedule”, and the system displays the “Holiday Schedule” interface, as shown in Figure 3.5-5



Sun	Mon	Tue	Wen	Thu	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

Figure 3.5-5 Holiday Schedule

Step 2 Select the date that you want to set as a holiday, and the selected date is displayed in blue

Step 3 Select “Record/Snapshot”, click “Save”, and system notes “Saved successfully”

Step 4 In the “Record Schedule/Snapshot Schedule” interface, click “Setup” on the right side of “Holiday”. The setting method is the same as “Monday to Sunday”.

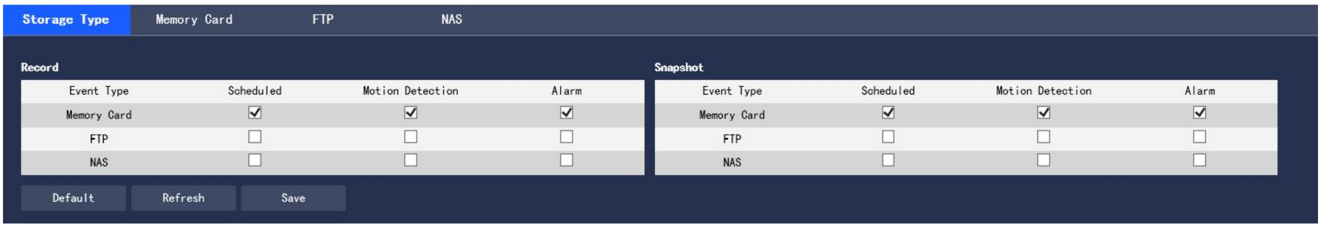
Step 5 After setting the period of a day of “Holiday”, you can video taking or Image capture for the holiday period in the date set in the holiday schedule.

3.5.2 Storage

3.5.2.1 Storage Type

You can configure the storage mode of video taking and Image capture of device in the “Storage Type” interface, and store the records and screenshots in a local SD card, FTP and NAS. You can store the records and screenshots according to the event type, corresponding to “General”, “Motion” and “Alarm” in the schedule. You will store corresponding type of video taking and Image capture after checking “General”, “Motion” or “Alarm”.

Step 1 Select “Settings > Storage Management > Storage > Storage Type”, and the system displays the “Storage Type” interface, as shown in Figure 3.5-6



Record

Event Type	Scheduled	Motion Detection	Alarm
Memory Card	☑	☑	☑
FTP	□	□	□
NAS	□	□	□

Snapshot

Event Type	Scheduled	Motion Detection	Alarm
Memory Card	☑	☑	☑
FTP	□	□	□
NAS	□	□	□

Figure 3.5-6 Storage Type

Step 2 Select the corresponding event type and storage mode according to the actual needs. For the description of parameters, please refer to Table 3.5-1

Parameters	Descriptions
Event Type	Including “Scheduled”, “Motion Detection” and “Alarm”
Memory Card	To store in the SD card
FTP	To store on the FTP server
NAS	To store on the NAS server

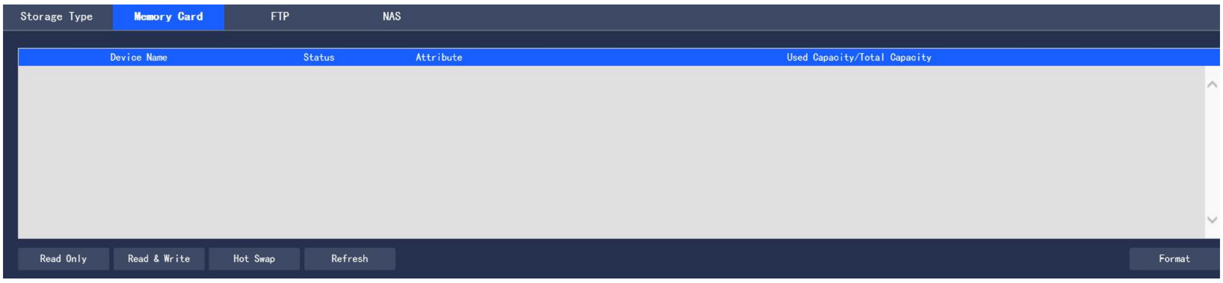
Table 3.5-1 Description of Parameters of “Storage Type”

Step 3 Click “Save” to complete the configuration

3.5.2.2 Memory Card

Various information of local SD card is displayed in the “Memory Card” list. You can click “Read Only”, “Read & Write”, “Hot Swap” and “Format” for operations.

Select “Settings > Storage Management > Storage (Table) > Memory Card”, and the system display is shown in Figure 3.5-7



Device Name	Status	Attribute	Used Capacity/Total Capacity

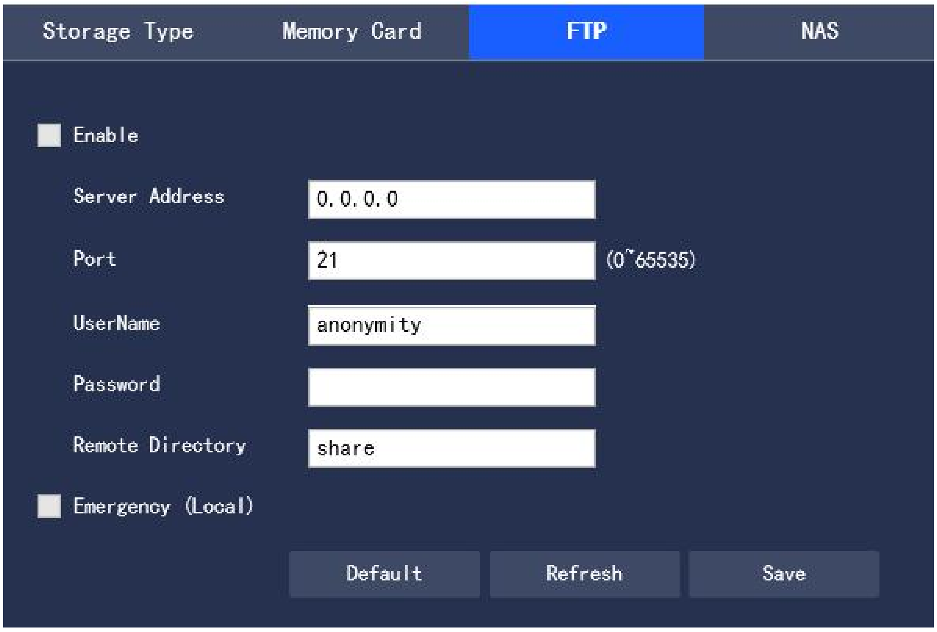
Figure 3.5-7 Memory Card

- Click “Read Only” to set the SD card to read only
- Click “Read & Write” to set the SD card to read/write
- Click “Hot Swap” to hot swap the SD card
- Click “Format” to format the SD card

3.5.2.3 FTP

The FTP function can only be enabled after the FTP storage mode is selected in “Storage Type”. When the network is disconnected or failed, you can store the video taking and Image capture to the local SD card by checking “Emergency (Local)”.

Step 1 Select “Settings > Storage Management > Storage (Table) > FTP”, and the system displays the “FTP” interface, as shown in Figure 3.5-8



□ Enable

Server Address 0.0.0.0

Port 21 (0~65535)

UserName anonymity

Password

Remote Directory share

□ Emergency (Local)

Figure 3.5-8 FTP Interface

Step 2 Configure information of each parameter according to actual needs. For the description of parameters, please refer to Table 3.5-2

Parameter	Description
Enable FTP	Enable the FTP function after you check it
Server Address	Address of FTP server

Port	Port of FTP server
User Name	User name to log in to the FTP server
Password	User name to log in to the FTP server
Remote directory	Directory stored on the FTP server
Emergency storage (Local)	After you check it, the records and snapshots will be stored to the local SD card when an exception occurs in FTP storage.

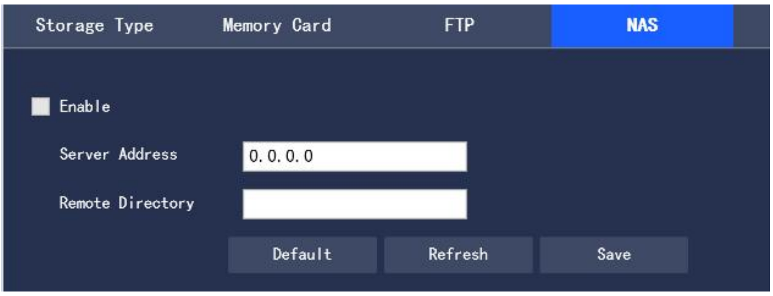
Table 3.5-2 Description of Parameters of "FTP"

Step 3 Click "Save" to complete the configuration.

3.5.2.4 NAS

The NAS function can only be enabled after the NAS storage mode is selected in "Storage Type". You can store files on the NAS server after checking "Enable".

Step 1 Select "Settings > Storage Management > Storage > NAS", and the system displays the "NAS" interface, as shown in Figure 3.5-9.



□ Enable

Server Address 0.0.0.0

Remote Directory

Figure 3.5-9 Settings of "NAS"

Step 2 Configure information of each parameter according to actual needs. For the description of parameters, please refer to Table 3.5-3

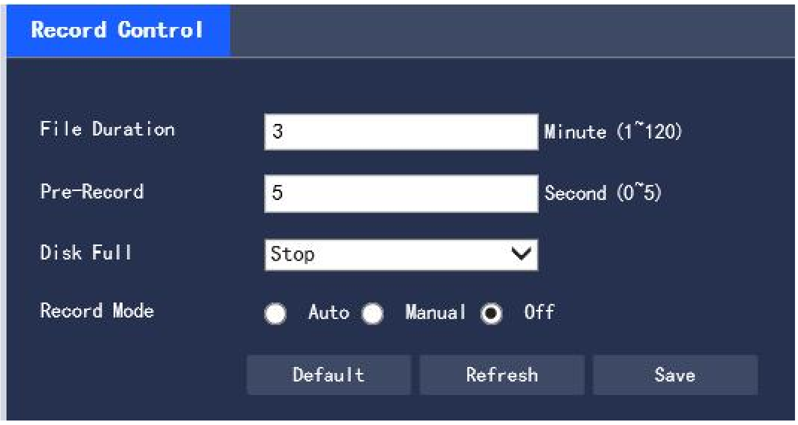
Parameter	Description
Enable NAS	Enable the NAS function after you select it
Server Address	Address of NAS server
Remote Directory	Directory stored on the NAS server

Table 3.5-3 Description of Parameters of "NAS"

Step 3 Click "Save" to complete the configuration.

3.5.3 Record Control

Step 1 Select “Settings > Storage Management > Record Control”, and the system displays the “Record Control” interface, as shown in Figure 3.5-10



Record Control

File Duration: 3 Minute (1~120)

Pre-Record: 5 Second (0~5)

Disk Full: Stop

Record Mode: Auto Manual [✓ Off]

Figure 3.5-10 Record Control

Step 2 Configure information of each parameter according to actual needs. For the description of parameters, please refer to Table 3.5-4

Parameters	Descriptions
File Duration	Set the packaging duration of each Video Taking file, 3 minutes by default
Pre-Record	Set the pre-recording time. For example, when you input “5”, after an alarm occurs, the system will read the video taking of the first 5 seconds in the memory and record it in the file Note: When you configure the pre-recording time, when the system is taking the alarm video or dynamic detection, it will also record the video data within n seconds before the recording is started into the record file if no recording is taken before.
Disk Full	You can select “Stop” or “Overwrite” Stop: stop video taking when the working disk is full. Overwrite: overwrite the earliest video taking file when the working disk is full.
Record Mode	You can select “Auto”, “Manual” and “Off” modes. When you select the “Manual” mode, the system will start recording; when you select the “Auto”, the system

	will record within the scope of the schedule.

Table 3.5-4 Description of Parameters of "Video Taking Control"

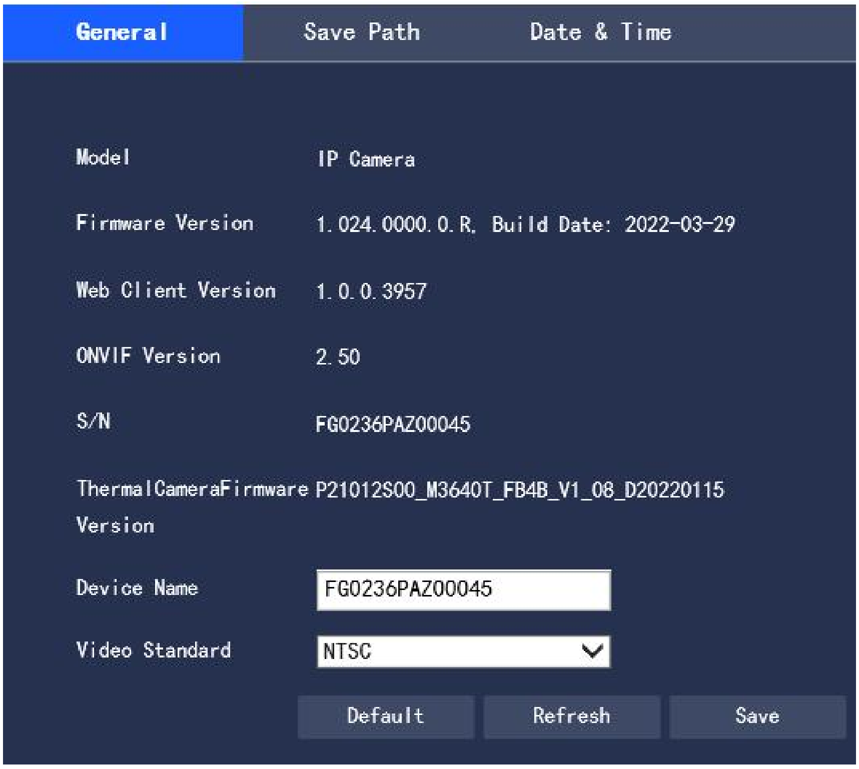
Step 3 Click "Save" to complete the configuration.

3.6 System Management

3.6.1 General

3.6.1.1 General

Step 1 Select "Settings > System Management > General > General", and the system displays the "General" interface, as shown in Figure 3.6-1.



Model IP Camera

Firmware Version 1.024.0000.0.R, Build Date: 2022-03-29

Web Client Version 1.0.0.3957

ONVIF Version 2.50

S/N FG0236PAZ00045

ThermalCameraFirmware Version P21012S00_M3640T_FB4B_V1_08_D20220115

Device Name FG0236PAZ00045

Video Standard NTSC

Figure 3.6-1 Settings of "General"

Step 2 Configure information of each parameter according to actual needs. For the description of parameters, please refer to Table 3.6-1.

Parameters	Descriptions
Device Name	Set the name of the device, the serial number of devices by default

Video Standard	The video standard of the display device, 50 Hz and 60 Hz are optional, and 50 Hz by default

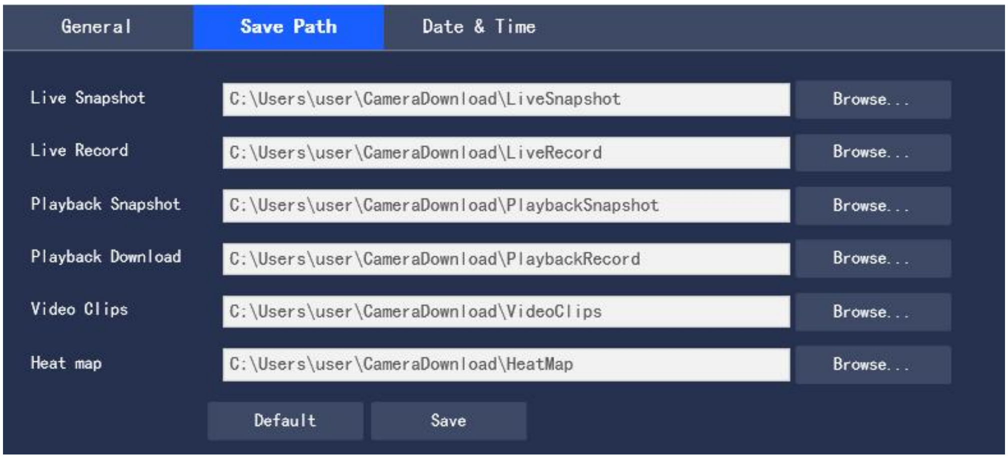
Table 3.6-1 Description of Parameters of "General"

Step 3 Click "Save" to complete the configuration.

3.6.1.2 Save Path

In the "Save Path" interface, you can set the storage paths of "Live Snapshot", "Live Record", "Playback Snapshot", "Playback Download", "Video Clips" and "Heat map" respectively. The configuration steps are as follows:

Step 1 Select "Settings > System Management > General > Save Path", and the system displays the "Save Path" interface, as shown in Figure 3.6-2



Live Snapshot: C:\Users\user\CameraDownload\LiveSnapshot

Live Record: C:\Users\user\CameraDownload\LiveRecord

Playback Snapshot: C:\Users\user\CameraDownload\PlaybackSnapshot

Playback Download: C:\Users\user\CameraDownload\PlaybackRecord

Video Clips: C:\Users\user\CameraDownload\VideoClips

Heat map: C:\Users\user\CameraDownload\HeatMap

Figure 3.6-2 Settings of "Save Path"

Step 2 Set the storage path of each storage item respectively

- Default path of monitoring "Live Snapshot": C:\Users\Administrator\CameraDownload\LiveSnapshot
- Default path of "Live Record": C:\Users\Administrator\CameraDownload\LiveRecord
- Default path of "Playback Snapshot": C:\Users\Administrator\CameraDownload\PlaybackSnapshot
- Default path of "Playback Download": C:\Users\Administrator\CameraDownload\PlaybackRecord
- Default path of "Video Clips": C:\Users\Administrator\CameraDownload\VideoClips
- Default path of "Heat map": C:\Users\Administrator\CameraDownload\HeatMap

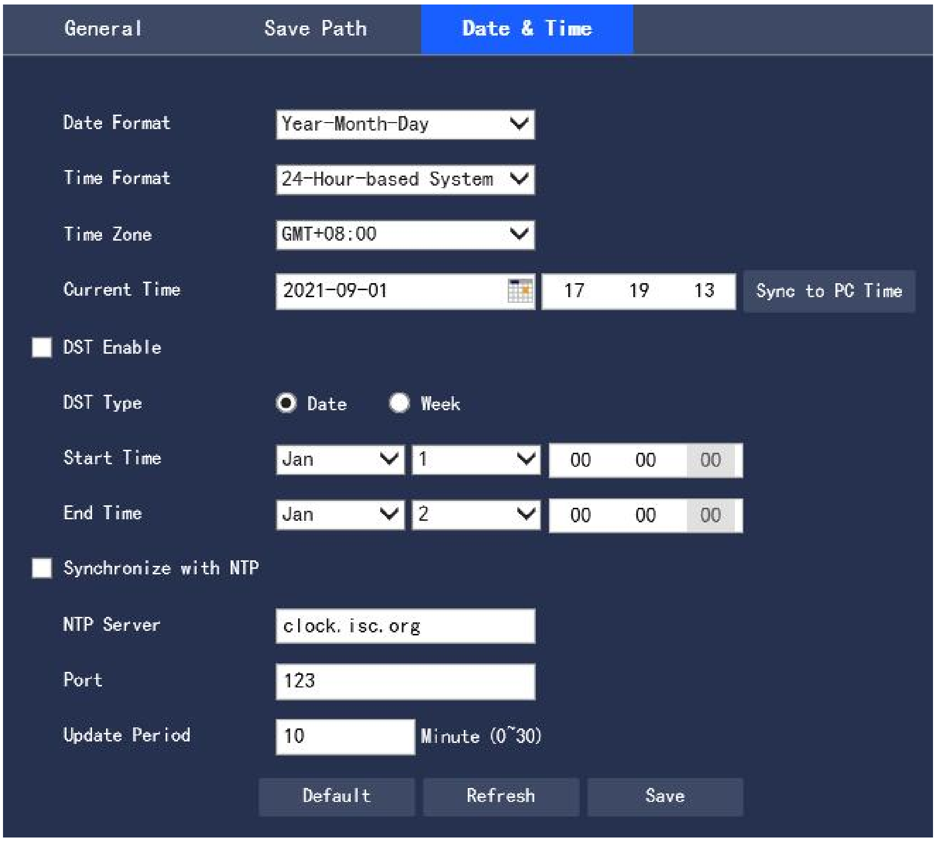
Note: "Administrator" is the login account of PC.

The Image capture and video taking paths of thermal imaging are not displayed in “Save Path”. By default, the suffix of the above paths of the visible light is added with “_Heat”.

Step 3 Click "Save" to complete the configuration.

3.6.1.3 Date &Time

Step 1 Select “Settings > System Management > General > Date & Time”, and the system displays the “Date & Time” interface, as shown in Figure 3.6-3.



Date Format: Year-Month-Day

Time Format: 24-Hour-based System

Time Zone: GMT+08:00

Current Time: 2021-09-01 17 19 13

□ DST Enable

DST Type: ● Date ○ Week

Start Time: Jan 1 00 00 00

End Time: Jan 2 00 00 00

□ Synchronize with NTP

NTP Server: clock. isc. org

Port: 123

Update Period: 10 Minute (0~30)

Figure 3.6-3 Date & Time

Step 2 Configure information of each parameter according to actual needs. Please refer to Table 3.6-2

Parameters	Descriptions
Date Format	Select the display format of corresponding date to be displayed
Time Format	Select the format of corresponding time to be displayed
Time Zone	Set the local time zone
Current Time	Set the current system time of the device

DST Enable	Set the start time and end time of DST, which can be set in the time or week format.
Synchronize with NTP	Set whether to enable the network time synchronization function, and enable it after you check it
NTP Server	Set the address of the time server
Port	Set the port number of the time server
Update Period	The synchronization interval period of the device time

Table 3.6-2 Setting Description of Parameters of “Date & Time”

Step 3 Click “Save” to complete the configuration

3.6.2 User Management

3.6.2.1 User Management

The “Account” interface is only available when the user has the user management authority.

● User name and group name can be set with a maximum length of 15 characters, only letters, numbers and underscores are acceptable.

● The password can be set to 0-32 digits, and only numbers and letters are acceptable. User can also change passwords of other users in addition to changing his/her own password.

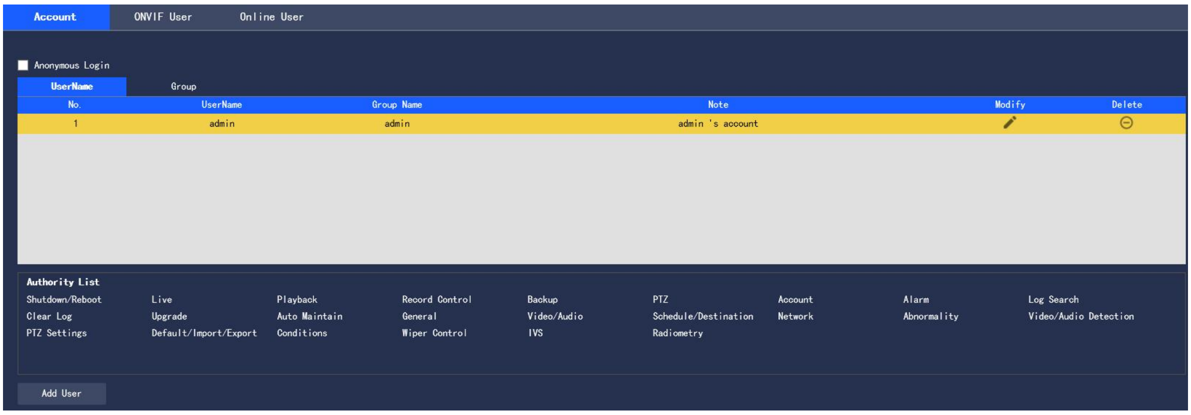
● In the “User Management” interface, the group and user modes are adopted. Both the group name and the user name cannot be duplicate, and one user can only belong to one group.

● The user currently logged in cannot modify his/her own authority.

● A default user “admin” is provided during initialization, which is a high-authority user by default during delivery.

3.6.2.1.1 User

In “Settings > System Management > User Management > Account > User Name”, you can check “Anonymous Login”, and click “Enable”, “Add User”, “Delete User” and “Modify User Password” for operations. The configuration interface is shown in Figure 3.6-4.



□ Anonymous Login

No.	UserName	Group Name	Note	Modify	Delete
1	admin	admin	admin 's account	✎	⊖

Authority List

Shutdown/Reboot	Live	Playback	Record Control	Backup	PTZ	Account	Alarm	Log Search
Clear Log	Upgrade	Auto Maintain	General	Video/Audio	Schedule/Destination	Network	Abnormality	Video/Audio Detection
PTZ Settings	Default/Import/Export	Conditions	Wiper Control	IVS	Radiometry			

Figure 3.6-4 User Management

Anonymous Login

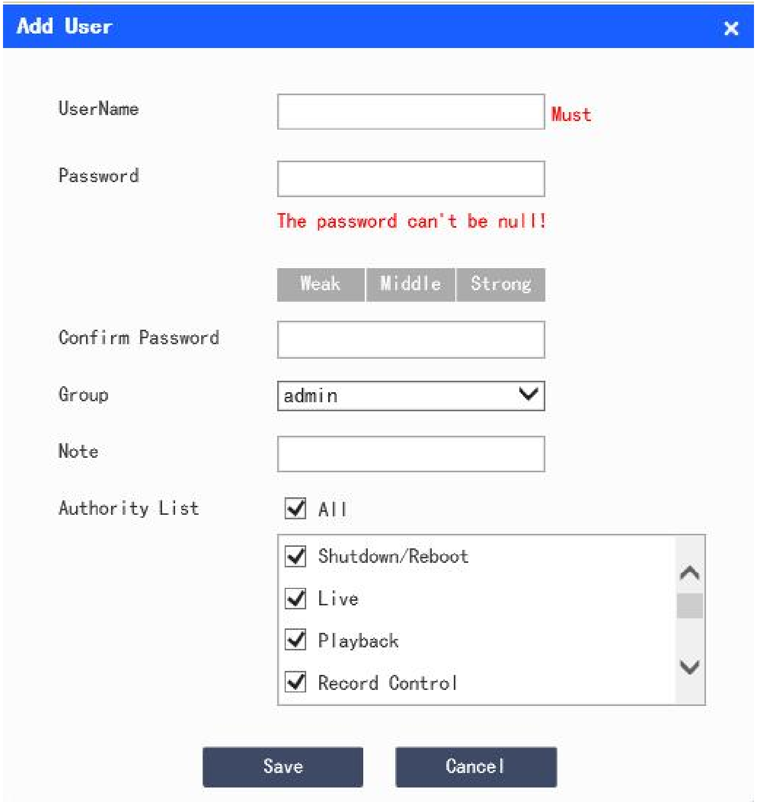
When you check “Anonymous Login”, you can log in to the device anonymously without entering a user name or password after entering IP. The anonymously logged-in user has only the preview authority listed in the “Authority List”. When you log in to the device in an anonymous way, you can log in to it with other user accounts by clicking “Log Out”.

Add User

Control of adding group users and setting users

Note: The user with the highest authority “admin” in the system cannot be deleted by default.

Step 1 Click “Add User”, and the system pops up the “Add User” interface, as shown in Figure 3.6-5



Add User

UserName: Must

Password: The password can't be null!

Weak | Middle | Strong

Confirm Password

Group: admin

Note

Authority List: ☑ All

- ☑ Shutdown/Reboot
- ☑ Live
- ☑ Playback
- ☑ Record Control

Figure 3.6-5 Add User

Step 2 Enter the user name and password, select a user group, and select the authority

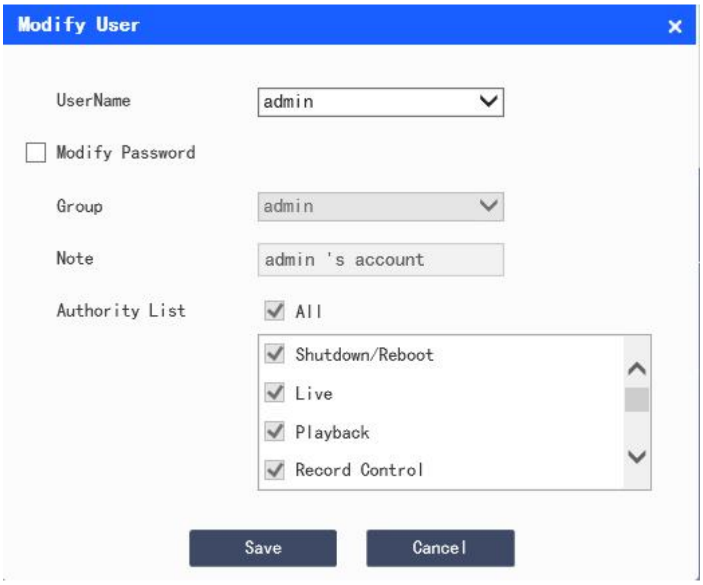
● Once the required group is selected, the user's authority can only be a subset of the group, and cannot exceed the authority attribute of the group.

● In order to facilitate managing the accounts, it is recommended that common users have lower authorities than senior ones when the user defines the authority.

Step 3 Click "Save" to complete the configuration

Modify User

Step 1 Click the corresponding ✏ of the user to be modified, and the system pops up the "Modify User" interface, as shown in Figure 3.6-6



Modify User

UserName: admin

□ Modify Password

Group: admin

Note: admin 's account

Authority List: ☑ All

- ☑ Shutdown/Reboot
- ☑ Live
- ☑ Playback
- ☑ Record Control

Figure 3.6-6 Modify User

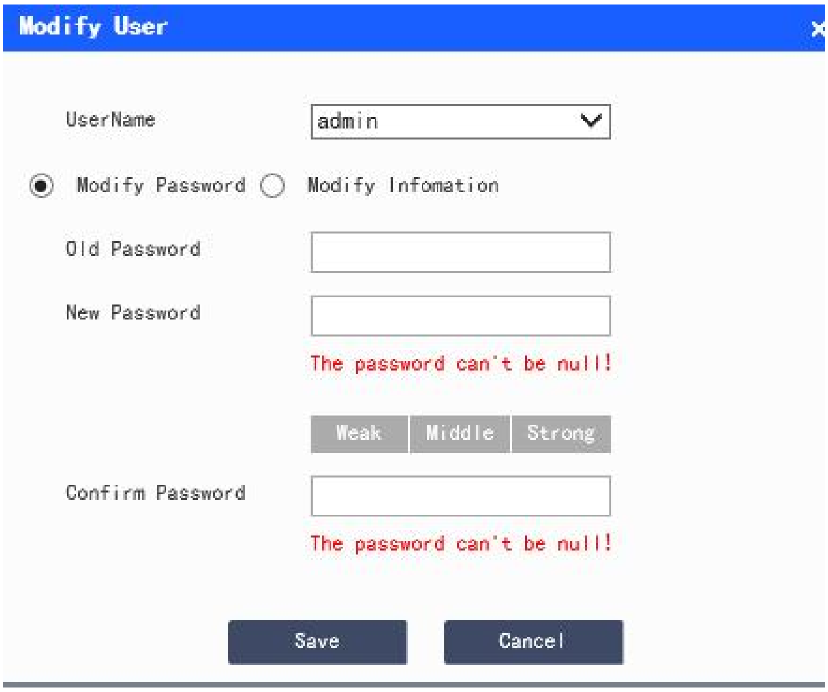
Step 2 Modify the user information according to actual needs

Step 3 Click “Save” to complete the configuration

Modify Password

Step 1 Check the “Modify Password” check box

Step 2 Enter the old password, and enter the new password and confirm it



Modify User

UserName: admin

● Modify Password ○ Modify Infomation

Old Password

New Password

The password can't be null!

Confirm Password

The password can't be null!

Figure 3.6-7 Modify Password

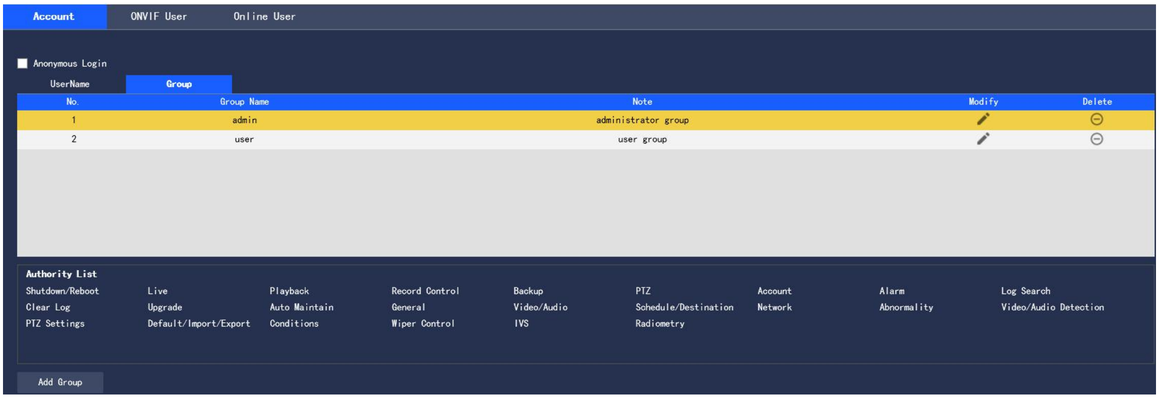
Step 3 Click “Save” to complete the configuration.

Delete User

You can delete the user by clicking the corresponding ⊖ of the user to be deleted.

3.6.2.1.2 User Group

In “Settings > System Management > User Management > Account > Group”, you can click “Add Group”, “Delete Group” and “Modify Group Password” for operations. The operating interface is shown in Figure 3.6-8.



No.	Group Name	Note	Modify	Delete
1	admin	administrator group	✎	⊖
2	user	user group	✎	⊖

Authority List

Shutdown/Reboot	Live	Playback	Record Control	Backup	PTZ	Account	Alarm	Log Search
Clear Log	Upgrade	Auto Maintain	General	Video/Audio	Schedule/Destination	Network	Abnormality	Video/Audio Detection
PTZ Settings	Default/Import/Export	Conditions	Wiper Control	IVS	Radiometry			

Figure 3.6-8 Settings of “Group”

Add Group

For specific operations, please refer to “3.6.2.1.1 User”

Modify Group

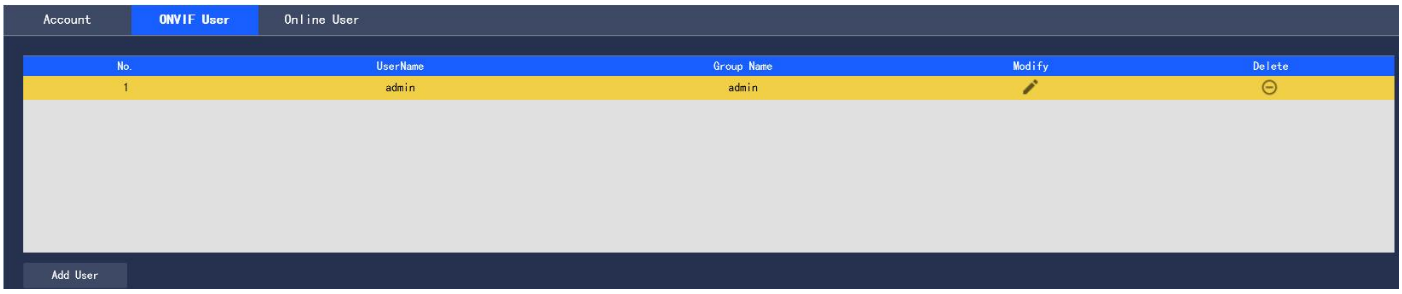
For specific operations, please refer to “3.6.2.1.1 User”

Delete User Group

For specific operations, please refer to “3.6.2.1.1 User”

3.6.2.2 ONVIF User

In “Settings > System Management > User Management > Onvif User”, you can view the information of users currently logged in through ONVIF, as shown in Figure 3.6-9.



No.	UserName	Group Name	Modify	Delete
1	admin	admin	✎	⊖

Figure 3.6-9 ONVIF User

Add User

For specific operations, please refer to “3.6.2.1.1 User”

Modify User

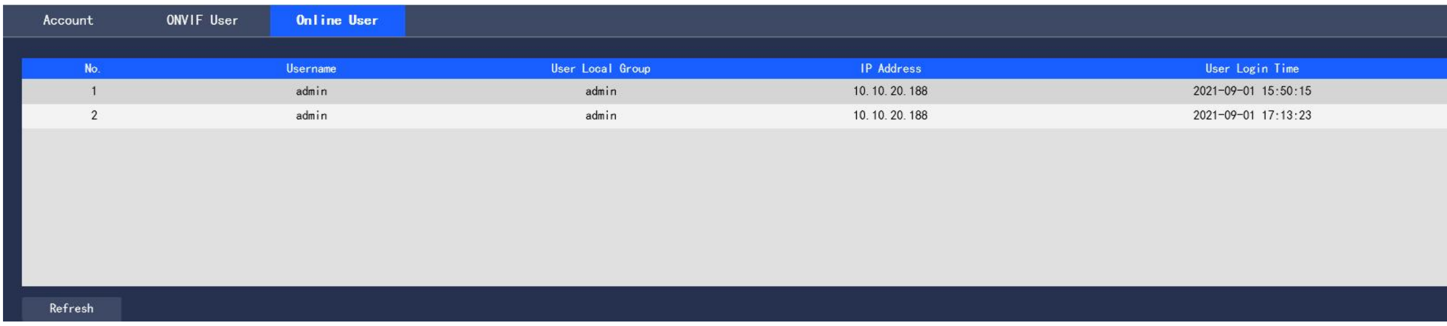
For specific operations, please refer to “3.6.2.1.1 User”

Delete User

For specific operations, please refer to “3.6.2.1.1 User”

3.6.2.3 Online User

In “Settings > System Management > Account> Online User”, you can view the information of users currently logged in to WEB, as shown in Figure 3.6-10.



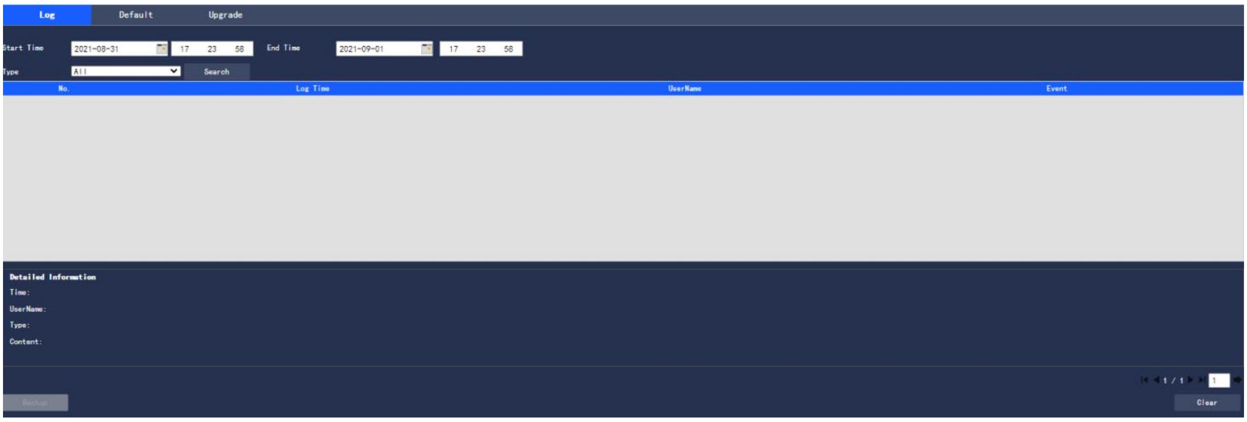
No.	Username	User Local Group	IP Address	User Login Time
1	admin	admin	10.10.20.188	2021-09-01 15:50:15
2	admin	admin	10.10.20.188	2021-09-01 17:13:23

Figure 3.6-10 Online User

3.6.3 System Maintenance

3.6.3.1 System Log

In “Settings > System Management > System Maintenance > Log”, you can view the user’s operation information on the device and some system information, as shown in Fig. 3.6-11. For the description of parameters, please refer to Table 3.6-3



Start Time 2021-08-31 17 23 58
End Time 2021-09-01 17 23 58
Type All

No.	Log Time	UserName	Event

Detailed Information
Time:
UserName:
Type:
Content:

Figure 3.6-11 System Log

Parameters	Descriptions
Start Time	The start time of the log to be searched
End Time	The end time of the log to be searched
Type	For types of log information, system operation, configuration operation, data management, alarm event, video taking operation, user management and log clearing are available.
Search	First, you can set the start time and end time of the log to be searched, and select the log type. When you click “Search”, the system will dynamically display the number of searched entries. When you click “Stop”, the system will stop searching logs, and display the number of searched entries and the period area.
Detailed Information	Click “Log Record” to display the details of the log
Clear	Clear all the log information of the device. The log information cannot be

	cleared by categories however.
Backup	Back up the searched system log information to the PC currently used by the user

Table 3.6-3 Description of Parameters of “Log”

The meanings of different log types are as follows:

● System operation: including application startup, abnormal exit, exit, application restart, device shutdown/restart, device restart and system upgrade

● Configuration operation: including saving and deleting configuration files

● Data operation: including setting of hard disk type, data clearing, hot swap, FTP status and video taking mode

● Event operation (record the video detection, intelligence, alarm, abnormality and other events): including the start time and end time of the event

● Video taking operation: including file access, file access error and file query

● User Management (record User Management modification and login and logout of user): including login, logout, adding user, deleting user, modifying user, adding group, deleting group and modifying group

● Clear log: clear the log

3.6.3.2 Default

In “Settings > System Management > System Maintenance > Default”, you can click “Manual Reboot” to restart the device, and click “Default” to restore some of the device settings to default values. The configuration interface is shown in Figure 3.6-12.

When multiple devices share the same configuration method, you can rapidly configure the above multiple devices by importing and exporting configuration files.

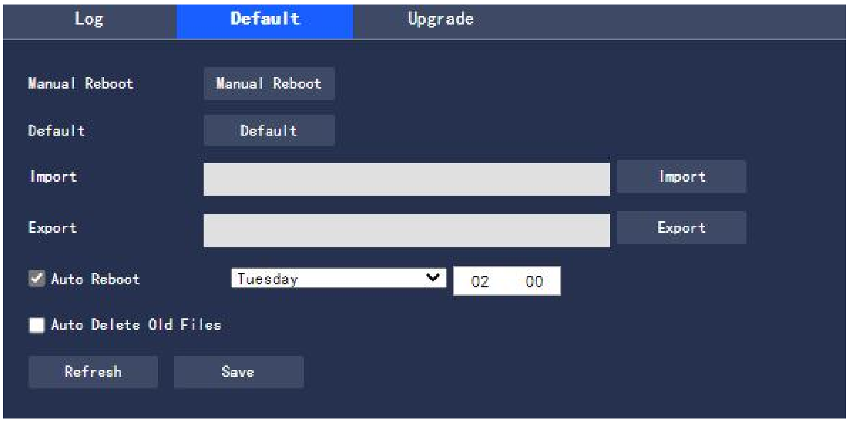
Step 1 Select the “Settings > System Management > System Maintenance > Default” interface on the Web side of a device, as shown in Figure 3.6-12

Step 2 Click “Export” to export the configuration file (.backup file) to local

Step 3 Click “Import” in the “Import/Export” interface of the WEB side to be configured with device, and import the configuration file into the system, and the device will be configured.

User can set to automatically reboot the system or delete a file. To automatically reboot the system, you need to set the period and time, being 02:00 every Tuesday by default. To automatically delete an old file, you need to set the period of the file, and delete the file within a certain period.

Step 1 Select the “Settings > System Management > System Maintenance > Default” interface, as shown in Figure 3.6-12.



☑ Auto Reboot Tuesday 02 00

□ Auto Delete Old Files

Figure 3.6-12 Default

Step 2 Configure information of each parameter according to actual needs. For the description of parameters, please refer to Table 3.6-4

Parameter	Description
Auto Reboot	Set the reboot time of the device after you check it
Auto Delete Old Files	After you check it, you can customize the period for deleting files, ranging from 1 day to 31 days.

Table 3.6-4 Description of Parameters of “Auto Maintenance”

Step 3 Click “Save” to make the configuration effective

Note: Some settings will not be restored to default values.

3.6.3.3 Firmware Upgrade

You can upgrade the firmware in “Settings > System Management > System Maintenance > Upgrade”. The configuration interface is shown in Figure 3.6-13.

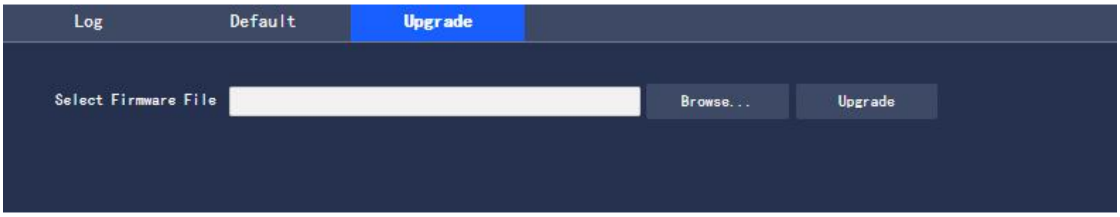


Figure 3.6-13 Firmware Upgrade

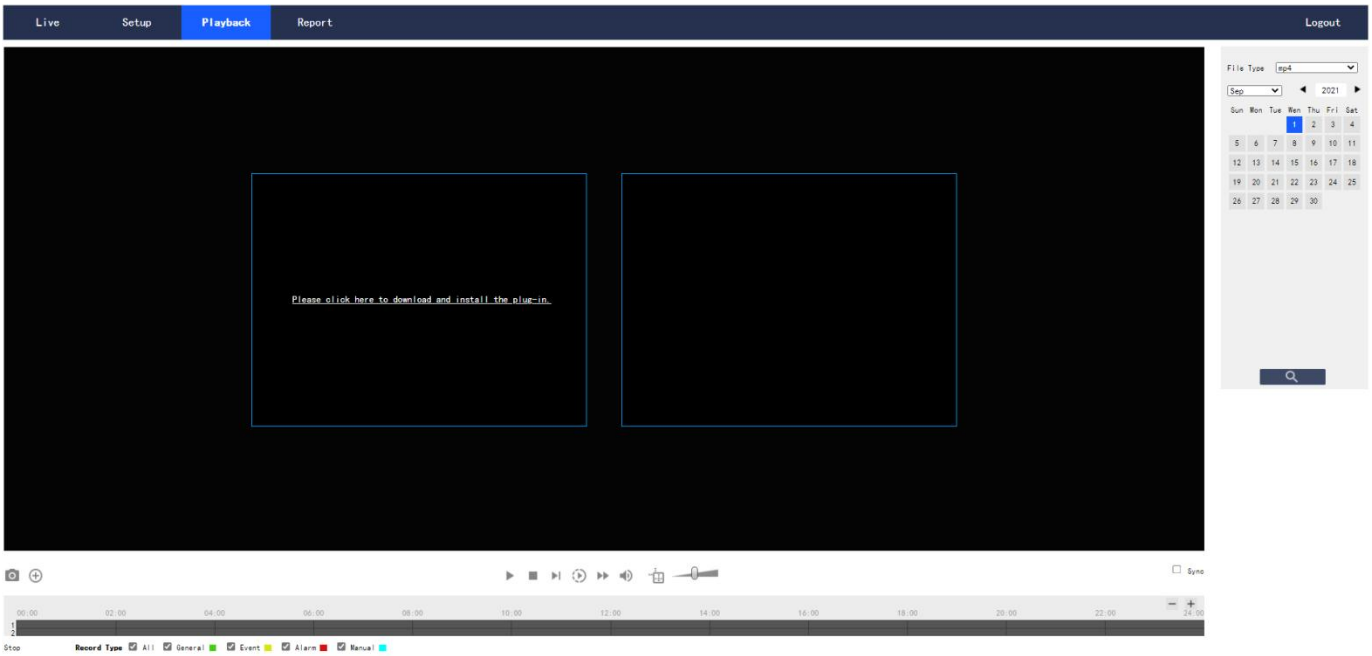
When upgrading the firmware, you can click “Browse…” to select the file to be upgraded, and click “Upgrade” to upgrade the firmware. Files to be upgraded belong to the “*.bin” type.

4 Playback

Saved videos and pictures can be played back in the “Playback” interface.

● Before playback, you are required to make sure that there are video takings and pictures stored in the local SD card.

Click the “Playback” tab, and the system will display the “Playback” interface, as shown in Figure 4-1


File Type mp4

Sep 2021

Please click here to download and install the plug-in.

Record Type ☑ All ☑ General 🟩 ☑ Event 🟨 ☑ Alarm 🟥 ☑ Manual 🟦

Figure 4-1 “Playback” Interface

4.1 Video Playback

Select the file type as “mp4”, and the system will display the interface as shown in Figure 4.1-1. For the description of parameters, please refer to Table 4.1-1

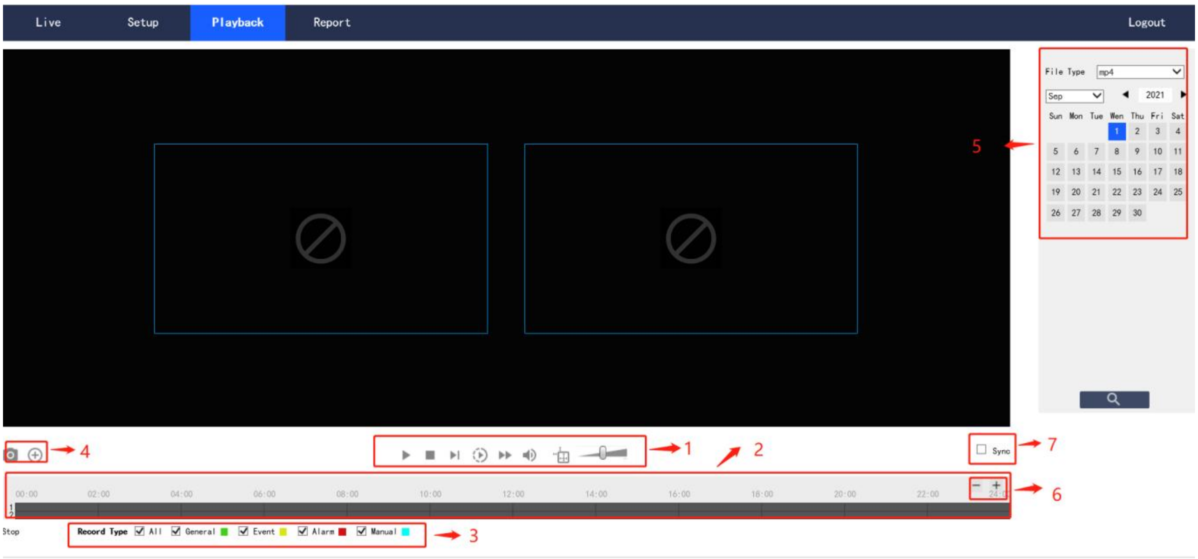

Live
Setup
Playback
Report
Logout
File Type
mp4
Sep
2021
Sun Mon Tue Wen Thu Fri Sat
5
Sync
7
6
4
1
2
Stop
Record Type ☑ All ☑ General 🟩 ☑ Event 🟨 ☑ Alarm 🟥 ☑ Manual 🟦
3

Figure 4.1-1 “Video Playback” Interface

No.	Description
1	Play function bar
2	Progress bar
3	Video taking type bar
4	Miscellaneous function bar
5	Playback file bar
6	Progress bar time format bar
7	Progress synchronization

Table 4.1-1 Description of Parameters of “Video Playback”

4.1.1 Play function

The play function bar is shown in Figure 4.1-2. For the description of parameters, please refer to Table 4.1-2

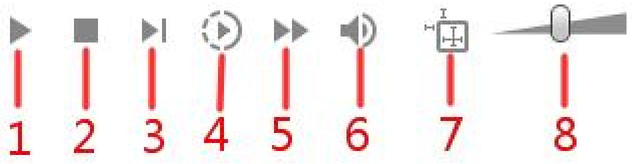


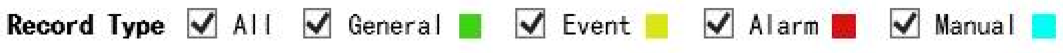
Figure 4.1-2 Play Function Bar

Parameters	Descriptions
1 Play	When this button is displayed, it indicates that the video taking is paused or not played. Click it to switch to the normal play state
2 Stop playing	Click it to stop playing the video taking
3 Next frame	Click it to skip to the next frame to play
4 Slow play	Click it to slow down
5 Fast play	Click it to speed up
6 Mute	When this button is displayed, it indicates that it is currently in the mute state. Click it to switch to the normal sound state
7 Regulation information	Click it to display the intelligent rule line in “Video Taking Playback”
8 Volume	Click the left mouse button to adjust the video taking volume

Table 4.1-2 Description of Parameters in the Play Function Bar

4.1.2 Video Taking Type

After selecting a video taking file, only the selected file will be displayed in the progress bar and file list. The “Video Taking Type” interface is shown in Figure 4.1-3



Record Type ☑ All ☑ General 🟩 ☑ Event 🟨 ☑ Alarm 🟥 ☑ Manual 🟦

Figure 4.1-3 Video Taking Type

4.1.3 Miscellaneous Function

The miscellaneous function bar is shown in Figure 4.1-4. For the description of parameters, please refer to Table 4.1-3

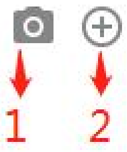


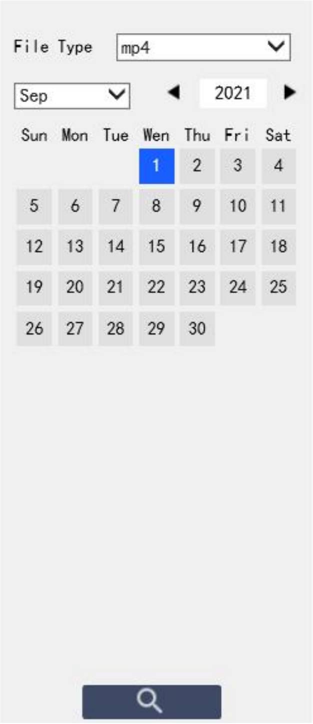
Figure 4.1-4 Miscellaneous Function Bar

Parameters	Descriptions
1 Image capture	Click the button to conduct image capture of the video, and save the pictures in the set path.
2 Partial zoom	● Click the button, and select any area by frame to zoom when the picture is in the original state. For any picture that is not in the original state, the zoomed area can be dragged within a certain range, which will be resumed to the original state by clicking the right mouse button. ● Click the button, and zoom in and out the picture by scrolling the mouse wheel.

Table 4.1-3 Description of Parameters of “Miscellaneous Function”

4.1.4 Playback File

The date displayed in blue in the calendar indicates that there are video takings or pictures for the current date, as shown in Figure 4.1-5. For the description of parameters, please refer to Table 4.1-4



File Type mp4

Sep ◀ 2021 ▶

Sun	Mon	Tue	Wen	Thu	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

Figure 4.1-5 Playback File (1)

Parameters	Descriptions
File Type	● Select “mp4” to play back the video taking ● Select “jpg” to play back the picture
Source	Default SD card

Table 4.1-4 Description of Parameters of "Playback File" (1)

The configuration steps are as follows:

Step 1 Click the date in blue, and the progress bar of the video taking file with color will be displayed on the time axis.

Among them, “green” represents ordinary video takings, “yellow” motion detection video takings, “red” alarm video takings, and “blue” manual video takings.

Step 2 Click a certain time position in the progress bar area of the record file to play the video taking file starting from this time point in the “Playback” interface

The progress bar is shown in Figure 4.1-6.

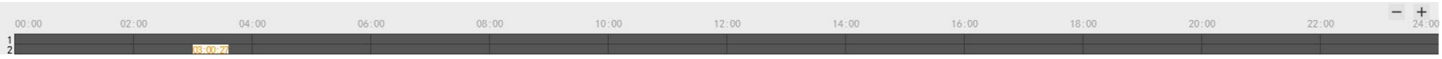


Figure 4.1-6 Progress Bar of video taking File

Step 3 Check “Sync” to set the visible light and thermal imaging playback video takings as synchronous. The synchronization box is shown in Figure 4.1-7.

□ synchronization

Figure 4.1-7 Synchronization Box

Step 4 Select the channel.

- Select “Channel 1” to display the visible light playback file
- Select “Channel 2” to display the thermal imaging playback file

Step 5 Click the query icon 🔍 of the file list. The video taking file of the selected date will be displayed in the list.

The list of playback files is shown in Figure 4.1-8. For the description of parameters, please refer to Table 4.1-5

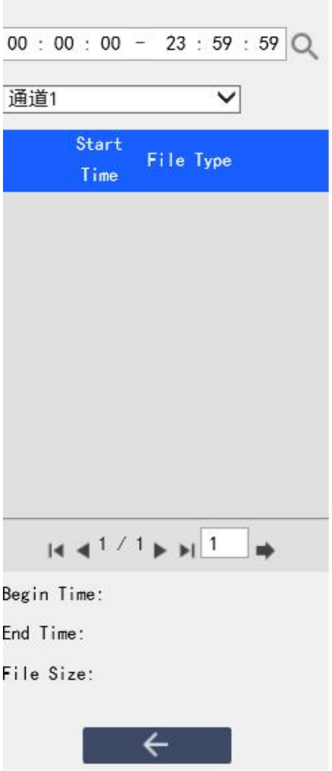


Figure 4.1-8 Playback File (2)

Parameters	Descriptions
🔍	Search, indicating to search all video taking files between the input start time and the end time of the selected date
⤓	Click the download icon to save the video taking file in the set download path of playback file
←	Click it to return to the calendar page, and you can re-select the time for operation

Table 4.1-5 Description of Parameters of "Playback File" (2)

4.1.5 Progress Bar Time Format

The interface of progress bar format is shown in Figure 4.1-9. Every time you click “+”, the progress bar will be changed from display in the 24-hour mode, to the display of video takings of 2 hours, 1 hour, and half an hour of the video taking. You can click “-” successively to change back to the 24-hour mode.

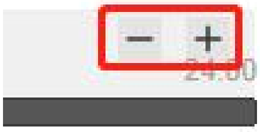


Figure 4.1-9 Progress Bar Time Format

5 View Report

With the report function, you can view the historical temperature data saved in the Micro SD card of the device as per certain rules (e.g. period).

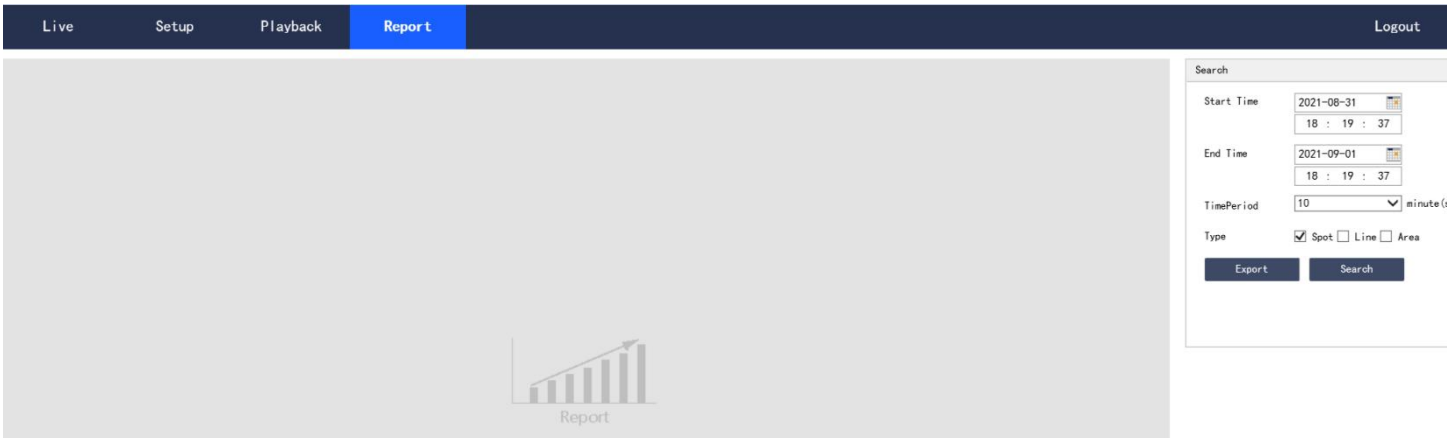
Prerequisites

Temperature measurement rules (including spot, line and area) have been set.

The device has been inserted into the SD card.

Operating Steps

Step 1 Click the “Report” page, and the system displays the “Report” interface, as shown in Figure 5-1.



Start Time 2021-08-31 18 : 19 : 37

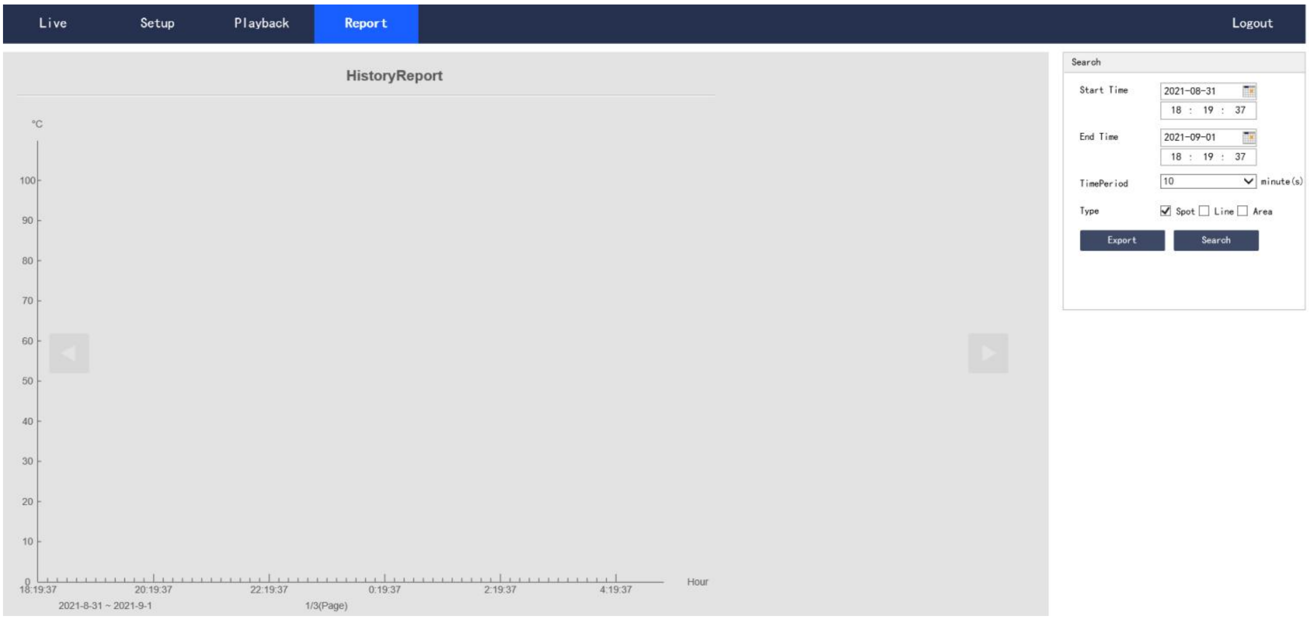
End Time 2021-09-01 18 : 19 : 37

TimePeriod 10 minute(

Type ☑ Spot ☐ Line ☐ Area

Figure 5-1 Report

Step 2 Set the query conditions and click “Search”, and the system displays the queried temperature data, as shown in Figure 5-2.



Start Time 2021-08-31 18 : 19 : 37

End Time 2021-09-01 18 : 19 : 37

TimePeriod 10 minute(s)

Type ☑ Spot ☐ Line ☐ Area

Figure 5-2 Query Results of Report

6 Logout

Click “Log out” to log out the system, and the system will pop up the interface as shown in Figure 6-1. To enter the system again, you need to log in it again.

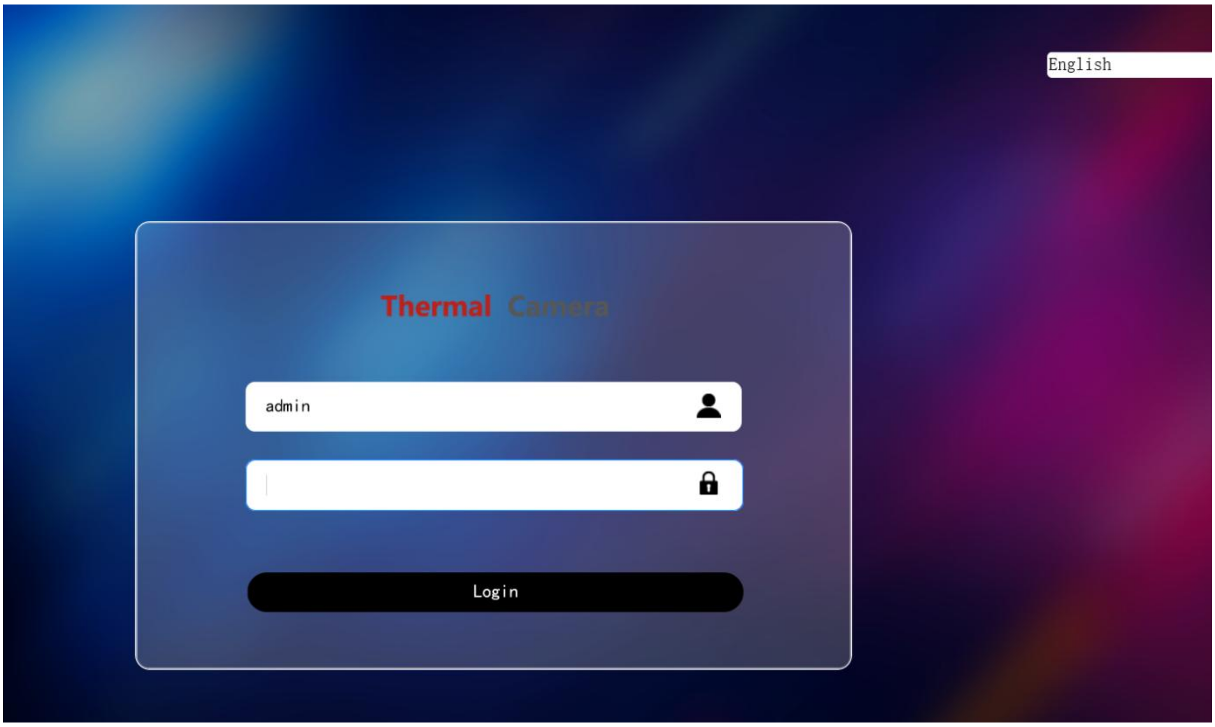


Figure 6-1 Logout Interface