GeoVision inc
The Vision of Security

GV-IP Thermal Camera

User's Manual

Before attempting to connect or operate this product,
please read these instructions carefully and save this manual for future use.

TMEB-UA-A

Every effort has been made to ensure that the information in this manual is accurate. GeoVision, Inc. makes no expressed or implied warranty of any kind and assumes no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages arising from the use of the information or products contained herein. Features and specifications are subject to change without notice.

GeoVision, Inc.
9F, No. 246, Sec. 1, Neihu Rd.,
Neihu District, Taipei, Taiwan
Tel: +886-2-8797-8377
Fax: +886-2-8797-8335
http://www.geovision.com.tw

August 2022

Scan the following QR codes for product warranty and technical support policy:

[Warranty]

[Technical Support Policy]

Contents

Notes on Safety

- This product is intended to be supplied by a Listed Power Unit, marked with 'Limited Power Source', 'LPS' on unit, output rated minimum 12V/2 A or POE 48V/ 350mA or AC24V (depending on models), no more than 2000m altitude of operation and Tma=60 Deg.C.
- As for the modes with PoE function, the function of the ITE being investigated to IEC 60950-1 standard is considered not likely to require connection to an Ethernet network with outside plant routing, including campus environment and the ITE is to be connected only to PoE networks without routing to the outside plant.
- Do not attempt to disassemble the camera; in order to prevent electric shock, do not remove screws or covers.
- There are no user-serviceable parts inside. Please contact the nearest service center as soon as possible if there is any failure.
- Avoid from incorrect operation, shock vibration, heavy pressing which can cause damage to product.
- Do not use corrosive detergent to clean main body of the camera. If necessary, please use soft dry cloth to wipe dirt; for hard contamination, use neutral detergent. Any cleanser for high grade furniture is applicable.
- Avoid aiming the camera directly towards extremely bright objects, such as, sun, as this may damage the image sensor.
- Please follow the instructions to install the camera. Do not reverse the camera, or the reversing image will be received.
- Do not operate it incase temperature, humidity and power supply are beyond the limited stipulations.
- Keep away from heat sources such as radiators, heat registers, stove, etc.
- Do not expose the product to the direct airflow from an air conditioner.
- This manual is for using and managing the product. We may reserve the rights of amending the typographical errors, inconsistencies with the latest version, software upgrades and product improvements, interpretation and modification. These changes will be published in the latest version without special notification.
- All pictures, charts, images in this manual are only for description and explanation of our products. The ownerships of trademarks, logos and other intellectual properties related to Microsoft, Apple and Google belong to the above-mentioned companies.

Disclaimer

- With regard to the product with internet access, the use of product shall be wholly at your own risks. Our company shall be irresponsible for abnormal operation, privacy leakage or other damages resulting from cyber attack, hacker attack, virus inspection, or other internet security risks; however, Our company will provide timely technical support if necessary.
- Surveillance laws vary from country to country. Check all laws in your local region before using this product for surveillance purposes. We shall not take the responsibility for any consequences resulting from illegal operations.

Cybersecurity Recommendations

- Use a strong password. At least 8 characters or a combination of characters, numbers, and upper- and lower-case letters should be used in your password.
- Regularly change the passwords of your devices to ensure that only authorized users can access the system (recommended time is 90 days).
- It is recommended to change the service default ports (like HTTP-80, HTTPS-443, etc.) to reduce the risk of outsiders being able to access.
- It is recommended to set the firewall of your router. But note that some important ports cannot be closed (like HTTP port, HTTPS port, Data Port).
- It is not recommended to expose the device to the public network. When it is necessary to be exposed to the public network, please set the external hardware firewall and the corresponding firewall policy.
- It is not recommended to use the v1 and v2 functions of SNMP.
- In order to enhance the security of WEB client access, please create a TLS certificate to enable HTTPS.
- Use black and white list to filter the IP address. This will prevent everyone, except those specified IP addresses from accessing the system.
- If you add multiple users, please limit functions of guest accounts.
- If you enable UPnP, it will automatically try to forward ports in your router or modem. It is really very convenient for users, but this will increase the risk of data leakage when the system automatically forwards ports. Disabling UPnP is recommended when the function is not used in real applications.

- Check the log. If you want to know whether your device has been accessed by unauthorized users or not, you can check the log. The system log will show you which IP addresses were used to log in your system and what was accessed.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

1. FCC compliance

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

2. FCC conditions:

- This device complies with part 15 of the FCC Rules. Operation of this product is subject the following two conditions:
- This device may not cause harmful interface.
- This device must accept any interference received, including interference that may cause undesired operation.

CE Information

CE The products have been manufactured to comply with the following directives.

EMC Directive 2014/30/EU

RoHS

The products have been designed and manufactured in accordance with Directive EU RoHS Directive 2011/65/EU and its amendment Directive EU 2015/863 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

2012/19/EU (WEEE directive): The Directive on waste electrical and electronic equipment (WEEE Directive). To improve the environmental management of WEEE, the improvement of collection, treatment and recycling of electronics at the end of their life is essential. Therefore, the product marked with this symbol must be disposed of in a responsible manner.

Directive 94/62/EC: The Directive aims at the management of packaging and packaging waste and environmental protection. The packaging and packaging waste of the product in this manual refers to must be disposed of at designated collection points for proper recycling and environmental protection.

REACH(EC1907/2006): REACH concerns the Registration, Evaluation, Authorization and Restriction of Chemicals, which aims to ensure a high level of protection of human health and the environment through better and earlier identification of the intrinsic properties of chemical substances. The product in this manual refers to conforms to the rules and regulations of REACH. For more information of REACH, please refer to DG GROWTH or ECHA websites.

Installation Requirements for Video Content Analysis

Thermal Detection

- **Human**
  - **Installation Height:** 3 ~ 6 m (9.8 ~ 19.7 ft)
  - **Video Content Analysis Range:** 24 m (78.7 ft) or less
  - **Camera View:** no requirements
  - **Angle of Depression:** 30° ~ 45° recommended
- **Vehicle**
  - **Installation Height:** 3 ~ 6 m (9.8 ~ 19.7 ft)
  - **Video Content Analysis Range:** 35 m (114.8 ft) or less
  - **Camera View:** The camera is facing the direction the traffic is coming from.
  - **Angle of Depression:** 30° ~ 45° recommended

Optical Detection

- **Installation Height:** 2.8 m (9.2 ft) or above
- **Video Content Analysis Range:**
  - Human: 10 m (32.8 ft) or less
  - Car: 20 m (65.6 ft) or less
- **Camera View:** It is recommended to have a front or side view of the vehicle as illustrated below. And no view requirements for human detection.
  - Recommended camera views:

  - Not recommended to use a camera with a large angle of depression

- **Requirements**

1. The best angle of depression for the camera is at about 45°.
2. Auto-focusing function should not be enabled for intrusion detection.
3. Avoid the scenes with many trees or the scenes with various light changes (like many flashing headlights). The ambient brightness of the scenes shouldn’t be too low.
4. The detected objects should not be less than 1% of the entire image and the largest sizes of the detected objects should not be more than 1/8 of the entire image.
5. Make sure cameras can view objects for at least 2 seconds in the detected area for accurate detection.
6. Adequate light and clear scenery are crucial to optical AI detection.

Chapter 1 Introduction

Main Features

Thermal:

- Resolution: 256 × 192
- Temperature range: -20°C ~ 150 °C (-4 °F ~ 302 °F)
- Multi-palette: white hot, black hot, iron oxide red, etc.
- Sound and light warning, temperature exception alarm, fire detection

Optical：

- Resolution: 5 MP (2592 × 1944)
- ICR auto switch, true day/night vision
- 3D DNR, true WDR (120dB), HLC, BLC, Smart IR, distortion image correction, ROI etc.
- AI analytics: Line Crossing, Region Entrance, Region Exiting, Target Counting, Region Intrusion, Face Detection

Chapter 2 Network Connection

Available web browser: IE (plug-in required)/ Firefox/Edge/Safari/Google Chrome
It is recommended to use the latest version of these web browsers.

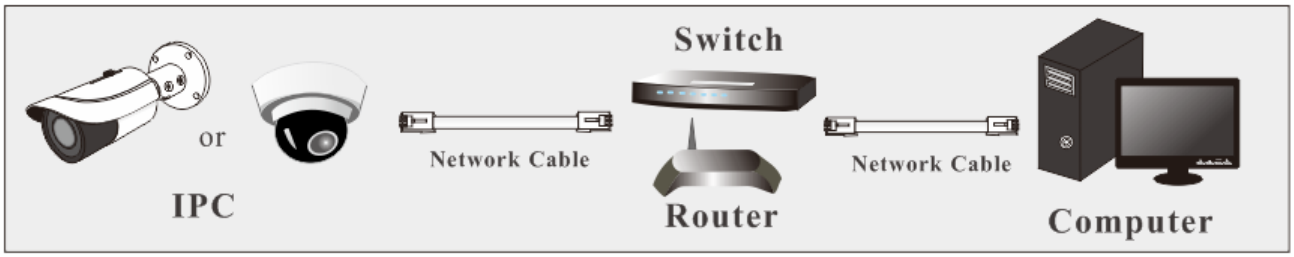
The menu display and operation of the camera may be slightly different by using the browser with plug-in or without plug-in. Installing plug-in will display more functions of the camera.
Connect the camera via LAN or WAN. Here only take IE browser for example. The details are as follows:

2.1 LAN

In LAN, there are two ways to access the camera: 1. access through GV-IP Device Utility; 2. directly access through IE browser.

2.1.1 Access through GV-IP Device Utility

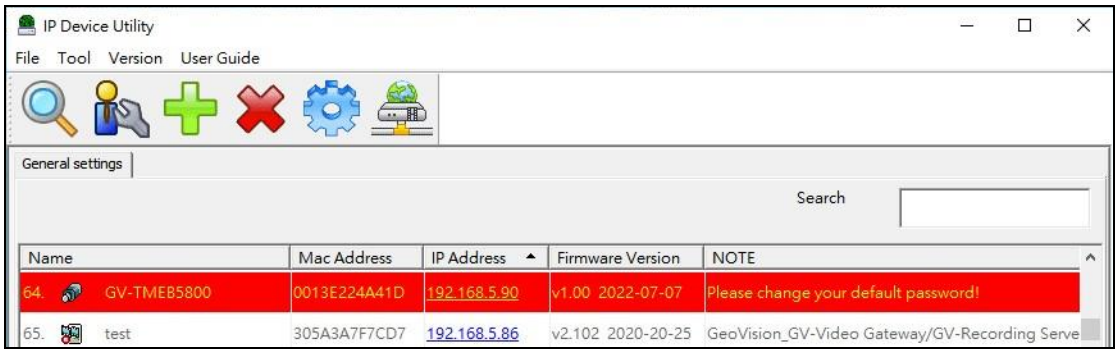
Network connection:



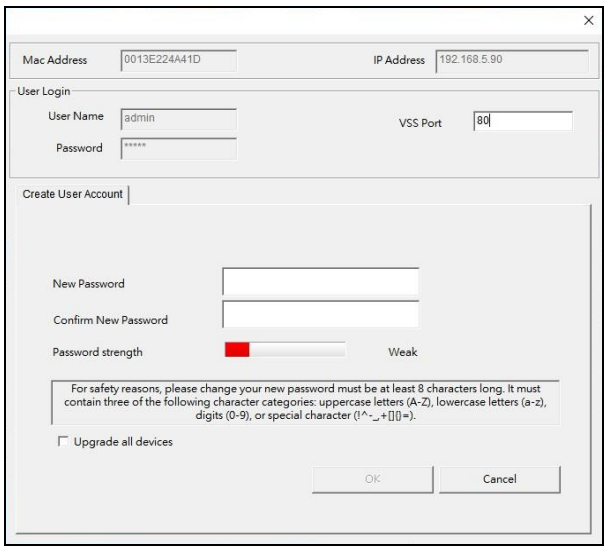
By default, when the camera is connected to LAN a with DHCP server, it is automatically assigned with a dynamic IP address. Follow the steps below to look up its IP address, and use the found IP address to log in its Web interface.

1. Make sure the PC and the camera are connected to the LAN, and **GV-IP Device Utility** (V8.9.8 or later) is installed in the PC from our website.
2. On the GV-IP Utility window, click the button to search for the IP devices connected in the same LAN. Click the **Name** or **Mac Address** column to sort.

3. Find the camera with its Mac Address, and click on its IP address.



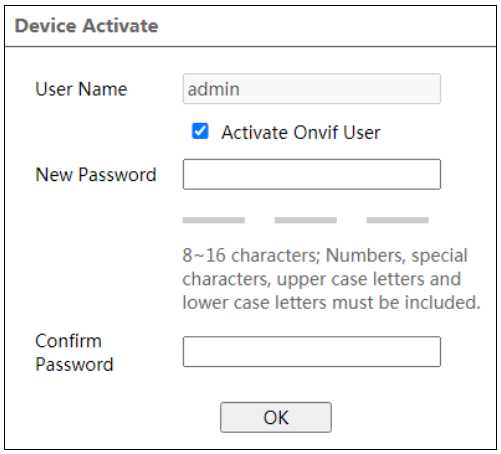
4. For the first-time users, you are requested to set up a password.



5. Type a new password and click **OK**.
6. Click on its IP address again and select **Webpage** to open its Web interface.
7. Type the set password on the login page and click **Login**.

IMPORTANT:

1. By default, the Administrator's username is **admin** and cannot be modified.
2. **The camera has two sets of passwords: one is for Web interface and the other is for the third-party platform connection via ONVIF, e.g. GV-VMS**. GV-IP Device Utility is used to set the ONVIF password. When the first-time user uses GV-IP Device Utility to set a password for the camera, the two sets of passwords are created simultaneously.
3. To change the password **for Web interface**, go to Config > Security > User ; see "Modified User" in *5.6.1 User Configuration*. To change the password **for ONVIF connection**, go Config > Network > Advnaced; see *5.5.4 ONVIF*.
4. If the first-time user accesses the camera's Web interface on the browser directly by using the IP address found in GV-IP Device Utility, the following dialog box will apear.



If "Activate Onvif User" is enabled, the ONVIF user can be activated simultanously for the third-party platform connection via ONVIF, using the default username and set password set above to connect.

2.1.2 Directly Access through IE

The default network settings are as shown below:

IP address: **192.168.0.10**

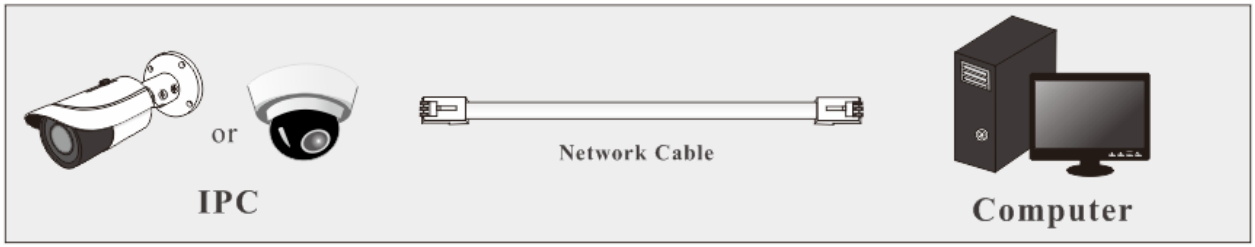
Subnet Mask: **255.255.248.0**

Gateway: **192.168.0.1**

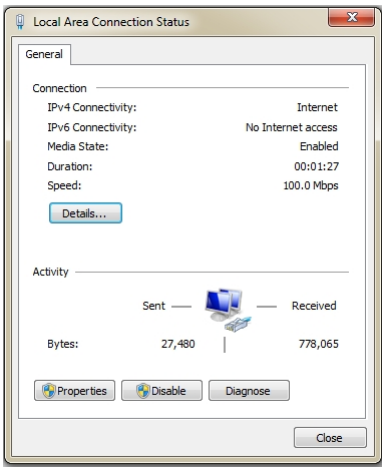
HTTP: **80**

Data port: **9008**

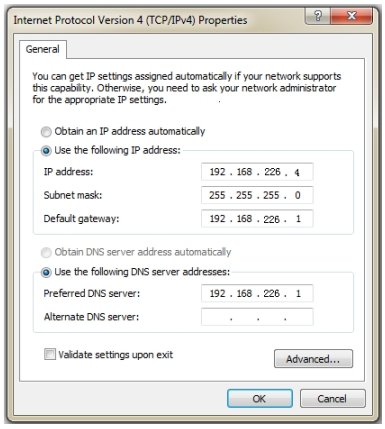
Use the above default settings when logging in the camera for the first time. Directly connect the camera to the computer through network cable.



1. Manually set the IP address of the PC and the network segment should be as the same as the default settings of the camera. Open the network and share center. Click “Local Area Connection” to pop up the following window.



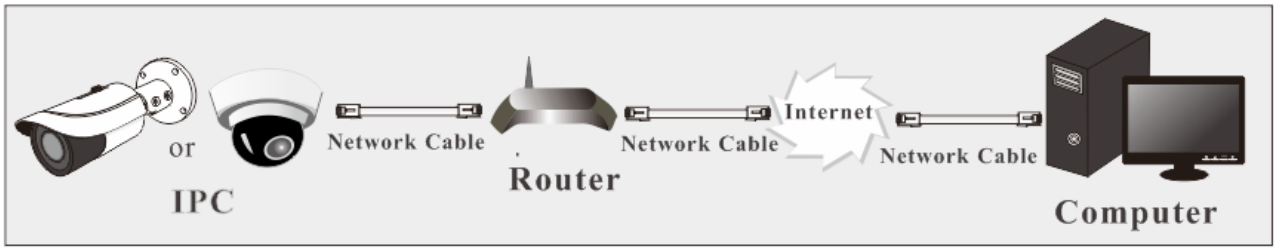
Select “Properties” and then select internet protocol according to the actual situation (for example: IPv4). Next, click the “Properties” button to set the network of the PC.



2. Open the IE browser and enter the default address of the camera and confirm.
3. Follow directions to download and install the Active X control.
4. Enter the username and password in the login window and then enter to view.

2.2 WAN

➢ **Access through the router or virtual server**



1. Make sure the camera is connected to the local network and then log in the camera via LAN and go to Config→Network→Port menu to set the port number.

HTTP Port	80
HTTPS Port	443
Data Port	9008
RTSP Port	554

Port Setup

2. Go to Config →Network→TCP/IP menu to modify the IP address.

IPv4 | IPv6 | PPPoE Config | IP Change Notification Config

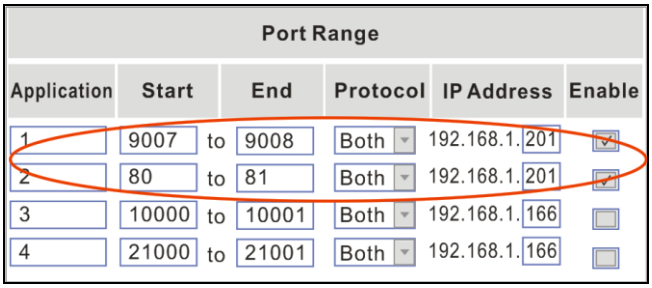
○ Obtain an IP address automatically

◉ Use the following IP address

IP Address	192.168.226.201	Test
Subnet Mask	255.255.255.0	
Gateway	192.168.226.1	
Preferred DNS Server	210.21.196.6	
Alternate DNS Server	8.8.8.8	

IP Setup

3. Go to the router's management interface through IE browser to forward the IP address and port of the camera in the "Virtual Server".

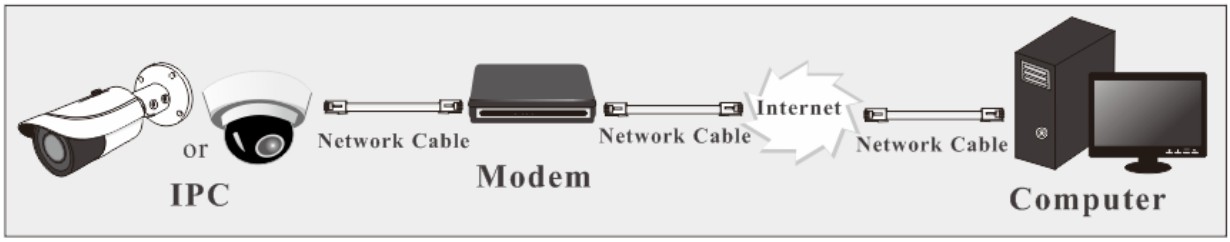


Router Setup

4. Open the IE browser and enter its WAN IP and http port to access. (for example, if the http port is changed to 81, please enter "192.198.1.201:81" in the address bar of web browser to access).

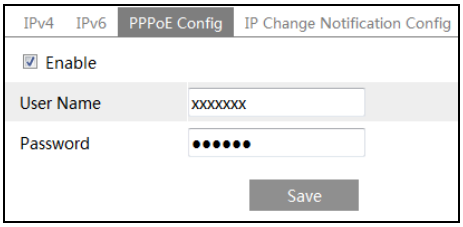
➢ **Access through PPPoE dial-up**

Network connection



Access the camera through PPPoE auto dial-up. The setup steps are as follow:

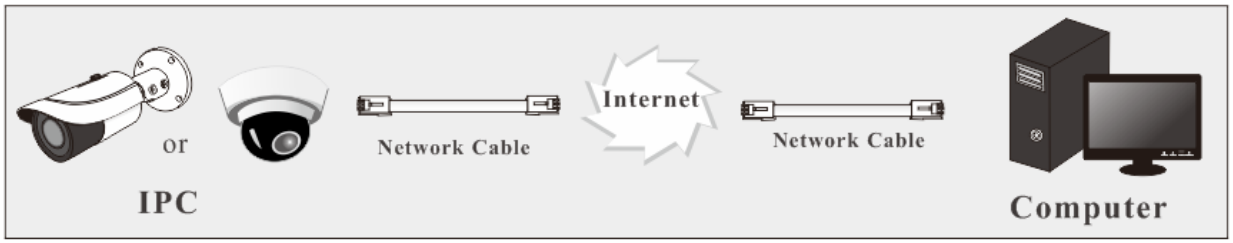
1. Go to Config→Network→Port menu to set the port number.
2. Go to Config →Network→TCP/IP→PPPoE Config menu. Enable PPPoE and then enter the user name and password from your internet service provider.



3. Go to Config →Network→DDNS menu. Before configuring the DDNS, please apply for a domain name first. Please refer toDDNS configuration for detail information.
4. Open the IE browser and enter the domain name and http port to access.

➢ **Access through static IP**

Network connection

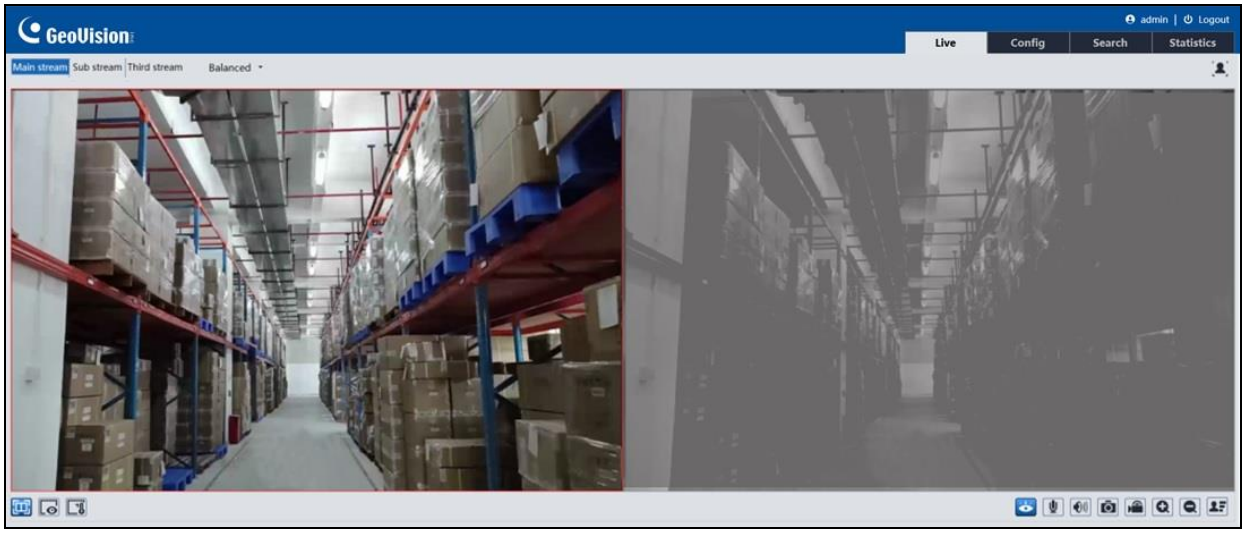


The setup steps are as follow:

1. Go to Config→Network→Port menu to set the port number.
2. Go to Config →Network→TCP/IP menu to set the IP address. Check “Use the following IP address” and then enter the static IP address and other parameters.
3. Open the IE browser and enter its WAN IP and http port to access.

Chapter 3 Live View

After logging in, the following window will be shown.



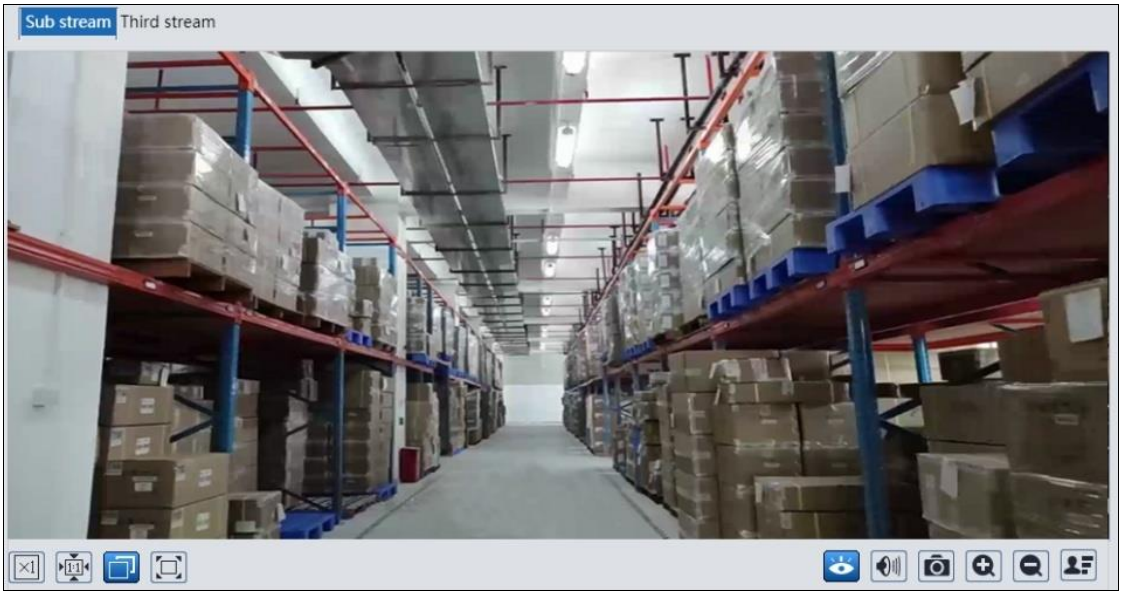
IMPORTANT: It is required to use **IE** or **Edge IE mode** to access thermal images.

Icon	Description	Icon	Description
	Visible light image and thermal image display		Fire detection indicator
	Visible light image display		Temperature indicator
	Thermal image display		SD card recording indicator
	Start/stop live view		Color abnormal indicator
	Start/stop two-way audio		Abnormal clarity indicator
	Enable/disable audio		Scene change indicator
	Snapshot		Sensor alarm indicator
	Start/stop local recording		Motion alarm indicator
	Zoom in		Line crossing indicator
	Zoom out		Intrusion indicator
	Face Detection		Region entrance indicator
	Face detection indicator		Region exiting indicator

*Those smart alarm indicators will flash only when the camera supports those functions and the corresponding events are enabled.

Plug-in free live view:

When the main stream is set over 1080P, only the sub stream or the third stream tab can be displayed on the interface by default.



Icon	Description	Icon	Description
	Original size		Auto (fill the window)
	Fit correct scale		Full screen

In full screen mode, double click on the mouse to exit or press the ESC key on the keyboard.

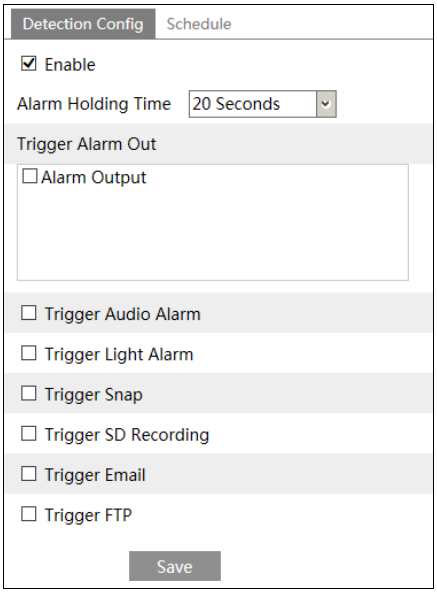
Note: Plug-in free view doesn't support thermal images.

Chapter 4 Fire Detection and Temp Measurement

4.1 Fire Detection

Fire Detection: Alarms will be triggered when the camera detects the fire source.

Click Config→Fire Detection to enter the following interface.



1. Click “Enable” and set the alarm holding time.
2. Set alarm trigger options.

Alarm Out: If selected, this would trigger an external relay output that is connected to the camera when the fire source is detected.

Trigger Audio Alarm: If selected, the warning voice will be uttered when the fire source is detected. (Please set the warning voice first. See Audio Alarm for details).

Trigger Light Alarm: If selected, the light of the camera will flash when the fire source is detected. (Please set the light flashing time and frequency first. See Light Alarm for details).

Trigger Snap: If selected, the system will capture images when the fire source is detected and save the images on an SD card.

Trigger SD Recording: If selected, video will be recorded on an SD card when the fire source is detected.

Trigger Email: If “Trigger Email” and “Attach Picture”are checked (email address must be set first in the Email configuration interface), the captured pictures and triggered event will be sent into those addresses.

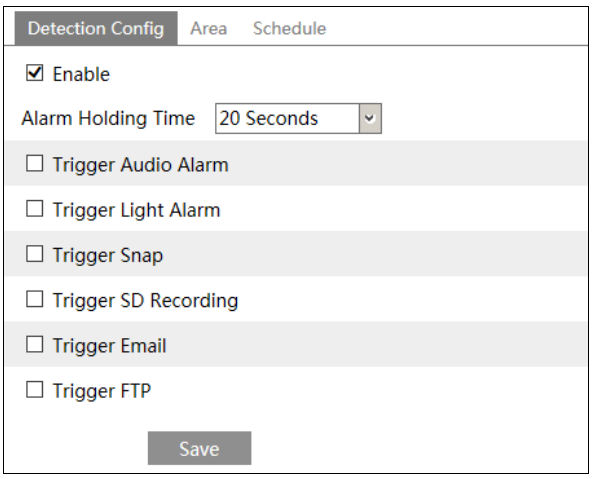
Trigger FTP: If “Trigger FTP” and “Attach Picture” are checked, the captured pictures will be sent into FTP server address. Refer to FTP configuration chapter for more details.

3. Click “Save” button to save the settings.
4. Set the schedule of the fire detection. The setup steps of the schedule are the same as the schedule recording setup. (See Schedule Recording).

4.2 Temperature Measurement

Temperature Measurement: When detecting the temperature of the pre-defined point/line/area exceeds the temperature threshold value, alarms will be triggered.

Click Config→Temperature measurement to enter the following interface.



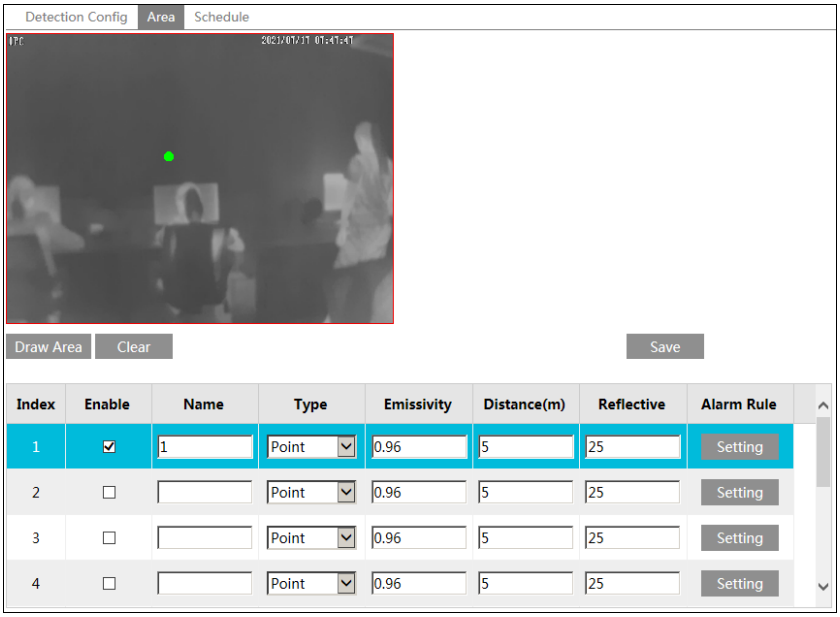
1. Click “Enable” and set the alarm holding time.
2. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to Fire Detection chapter for details.
3. Set thermography rule. Click the “Area” tab to go to the following interface.

The thermography rule type includes Point, Line Area.

Point setting: After the type is set to “Point”, click “Draw Area” and then drag the mouse in the image on the left side to move the point. Click the “Stop Draw” button to stop drawing. Up to 10 points can be set in the above interface.

Line setting: After the type is set to “Line”, click “Draw Area” and then drag the mouse in the image on the left side to draw a line. Click the “Stop Draw” button to stop drawing. To ensure the accuracy of temperature measurement, it is recommended to set not more than two lines at the same time.

Area setting: Click the “Draw Area” button and then click around the area where you want to set as the alarm area in the image on the left side (the alarm area should be a closed area). Click the “Stop Draw” button to stop drawing. Click the “Clear” button to delete the alarm area. Click the “Save” button to save the settings. To ensure the accuracy of temperature measurement, it is recommended to set not more than two areas at the same time.

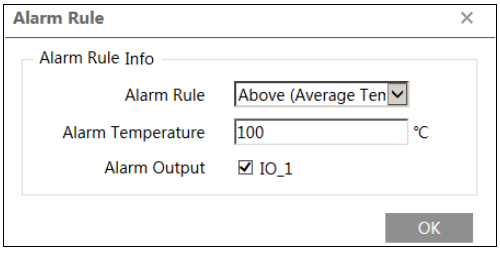


Emissivity: Set the emissivity of the target. The emissivity of each object is different. Please refer to Common Material Emissivity for details.

Distance: The distance between the target and the camera.

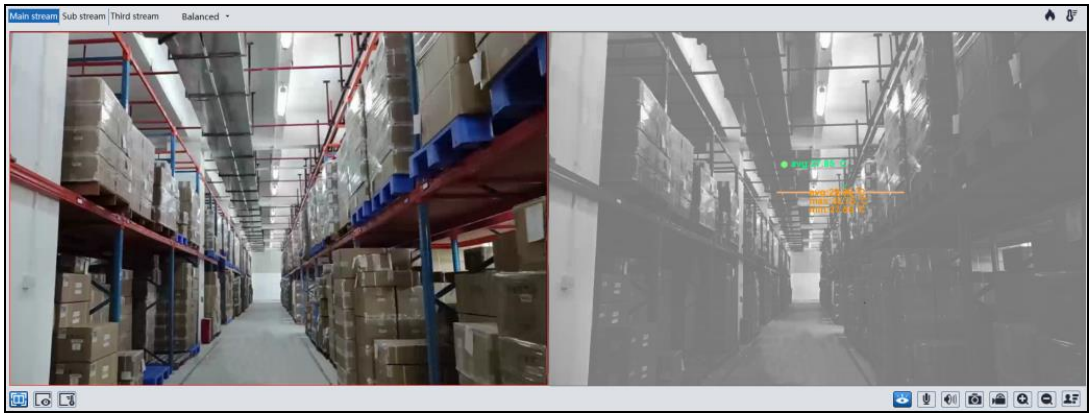
Reflective: If there is any object with high emissivity in the scene, set the reflective temperature to correct the ambient temperature. The reflective temperature should be set the same as the temperature of the high emissivity object.

4. Click “Setting” to set the alarm rule.



Set the alarm rule, alarm temperature and alarm output. For example, select Alarm Rule as Above (Average Temperature), set the alarm temperature to 100°C and check alarm output. Then alarms will be triggered when the average temperature of the target is higher than 100°C

5. Click “Live” to view the temperature and rule information.



Requirements of Fire detection and temperature measurement

1. The thermal camera should be used in a stable indoor environment without wind. Please make sure the monitoring field is far away from any objects that could produce airflow.
2. The lens of the camera shouldn’t face the sun to avoid the damage of the sensor.
3. The thermal camera should be installed in the highest position of the detection area and the camera should face the detected object.

Chapter 5 Other Configurations

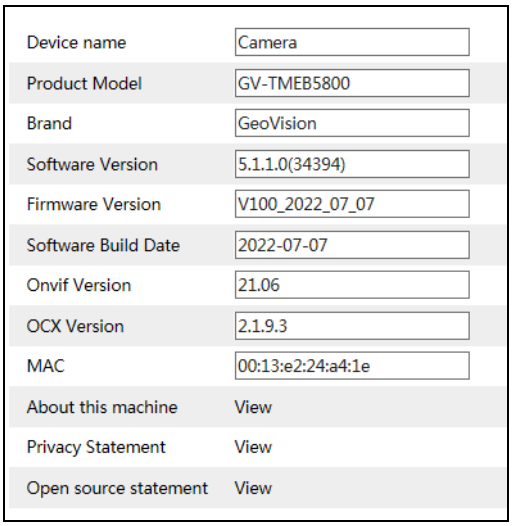
In the Webcam client, choose “Config” to go to the configuration interface.

Note: Wherever applicable, click the “Save” button to save the settings.

5.1 System Configuration

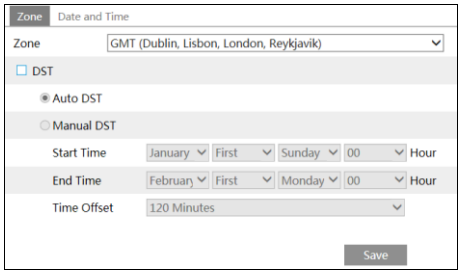
5.1.1 Basic Information

In the “Basic Information” interface, the system information of the device is listed.



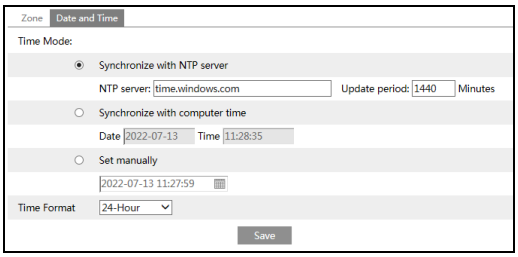
5.1.2 Date and Time

Go to Config→System→Date and Time. Please refer to the following interface.



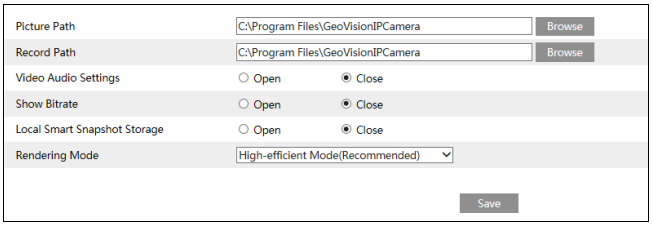
Select the time zone and DST as required.

Click the “Date and Time” tab to set the time mode.



5.1.3 Local Config

Go to Config→System→Local Config to set up the storage path of captured pictures and recorded videos on the local PC. There is also an option to enable or disable the bitrate display in the recorded files.



Additionally, “Local smart snapshot storage” can be enabled or disabled here. If enabled, the captured pictures triggered by smart events (like line crossing detection, region intrusion, etc.) will be saved to the local PC.

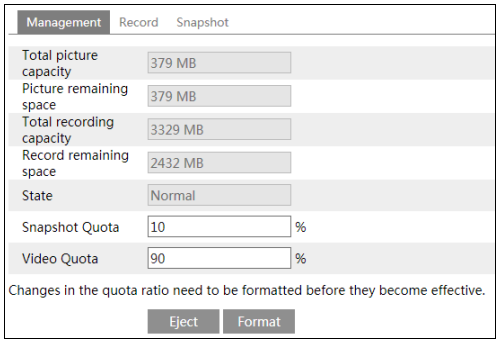
Rendering Mode: High-efficient mode, compatible mode or low-efficient mode can be optional.

If the performance of your computer is not compatible with the web client or your computer has no graphics card, low-efficient mode is suggested.

Note: when you access your camera by the web browser without the plug-in, only Show Bitrate can be set in the above interface.

5.1.4 Storage

Go to Config→System→Storage to go to the interface as shown below.



- **SD Card Management**

Click the “Format” button to format the SD card. All data will be cleared by clicking this button.

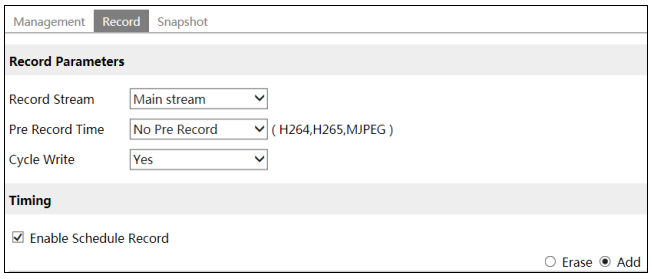
Click the “Eject” button to stop writing data to SD card. Then the SD card can be ejected safely.

Snapshot Quota: Set the capacity proportion of captured pictures on the SD card.

Video Quota: Set the capacity proportion of record files on the SD card.

- **Schedule Recording Settings**

1. Go to Config→System→Storage→Record to go to the interface as shown below.



2. Set record stream, pre-record time, cycle writing.

Pre Record Time: Set the time to record before the actual recording begins.

3. Set schedule recording. Check “Enable Schedule Record” and set the schedule.

Weekly schedule

Set the alarm time from Monday to Sunday for a single week. Each day is divided in one hour increments. Green means scheduled. Blank means unscheduled.

“Add”: Add the schedule for a special day. Drag the mouse to set the time on the timeline.

“Erase”: Delete the schedule. Drag the mouse to erase the time on the timeline.

Manual Input: Click it for a specific day to enterspecific start and end times. This adds more granularities (minutes).

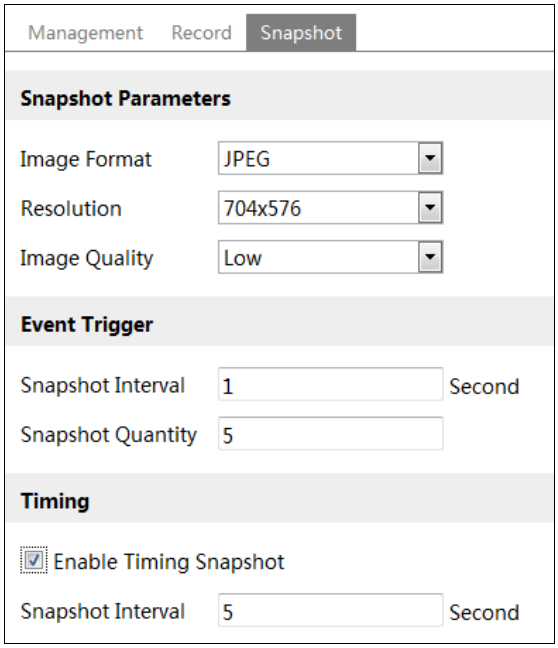
Day schedule

Set the alarm time for alarm a special day, such as a holiday.

Note: Holiday schedule takes priority over weekly schedule.

- **Snapshot Settings**

Go to Config→System→Storage→Snapshot to go to the interface as shown below.



Set the format, resolution and quality of the image saved on the SD card and the snapshot interval and quantity and the timing snapshot here.

Snapshot Quantity: The number you set here is the maximum quantity of snapshots. The actual quantity of snapshots may be less than this number. Supposing the occurrence time of an alarm event is less than the time of capturing pictures, the actual quantity of snapshots is less than the set quantity of snapshots.

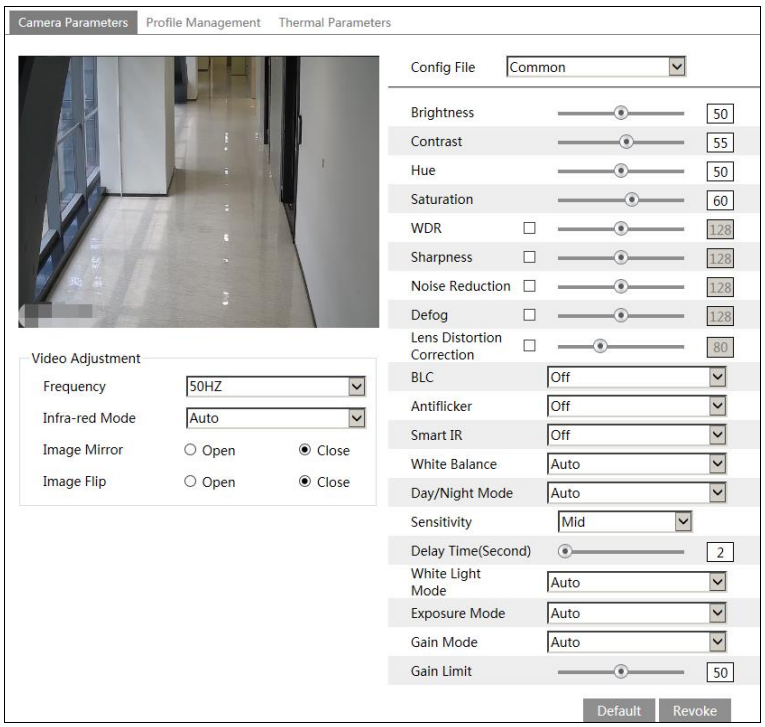
Timing Snapshot: Enable timing snapshot first and then set the snapshot interval and schedule. The setup steps of schedule are the same as the schedule recording (See Schedule Recording).

5.2 Image Configuration

Image Configuration includes Display, Video/Audio, OSD, Video Mask and ROI Config.

5.2.1 Display Configuration

Go to Image→Display interface as shown below. The image's brightness, contrast, hue and saturation and so on for common, day and night mode can be set up separately. The image effect can be quickly seen by switching the configuration file.



Brightness: Set the brightness level of the camera's image.

Contrast: Set the color difference between the brightest and darkest parts.

Hue: Set the total color degree of the image.

Saturation: Set the degree of color purity. The purer the color, the brighter the image is.

WDR: WDR can adjust the camera to provide a better image when there are both very bright and very dark areas simultaneously in the field of the view by lowering the brightness of the bright area and increasing the brightness of the dark area.

Recording will be stopped for a few seconds while the mode is changing from non-WDR to WDR mode.

Sharpness: Set the resolution level of the image plane and the sharpness level of the image edge.

Noise Reduction: Decrease the noise and make the image more thorough. Increasing the value will make the noise reduction effect better but it will reduce the image resolution.

Defog: Activating this function and setting an appropriate value as needed in foggy, dusty, smoggy or rainy environment to get clear images.

Lens Distortion Correction: When the image appears distortion to some extent, please enable this function and adjust the level according to the actual scene to correct the distortion.

Backlight Compensation (BLC):

- Off: disables the backlight compensation function. It is the default mode.
- HLC: lowers the brightness of the entire image by suppressing the brightness of the image's bright area and reducing the size of the halo area.
- BLC: If enabled, the auto exposure will activate according to the scene so that the object of the image in the darkest area will be seen clearly.

Antiflicker:

- Off: disables the anti-flicker function. This is used mostly in outdoor installations.
- 50Hz: reduces flicker in 50Hz lighting conditions.
- 60Hz: reduces flicker in 60Hz lighting conditions.

Smart IR: Choose "ON" or "OFF". This function can effectively avoid image overexposure so as to make the image more realistic. The higher the level is, the more overexposure compensation will be given.

White Balance: Adjust the color temperature according to the environment automatically.

Day/Night Mode: Choose "Auto", "Day", "Night" or "Timing".

White Light Mode: "OFF", "Manual" or "Auto" is optional. In low illumination condition, this mode can be enabled.

Exposure Mode: Choose "Auto" or "Manual". If manual is chosen, the digital shutter speed can be adjusted.

Gain Mode: Choose "Auto" or "Manual". If "Auto" is selected, the gain value will be automatically adjusted (within the set gain limit value) according to the actual situation. If "Manual" is selected, the gain value shall be set manually. The higher the value is, the brighter the image is.

Frequency: 50Hz and 60Hz can be optional.

Infrared Mode: Choose "Auto", "On" or "Off". Some modes may not support this mode.

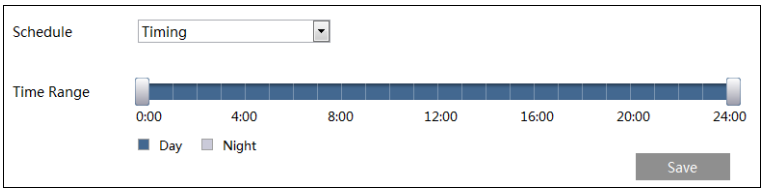
Image Mirror: Turn the current video image horizontally.

Image Flip: Turn the current video image vertically.

Schedule Settings of Image Parameters:

Click the “Profile Management” tab as shown below.

Set full time schedule for common, day, night mode and specified time schedule for day and night. Choose “Schedule” in the drop-down box of schedule as shown below.

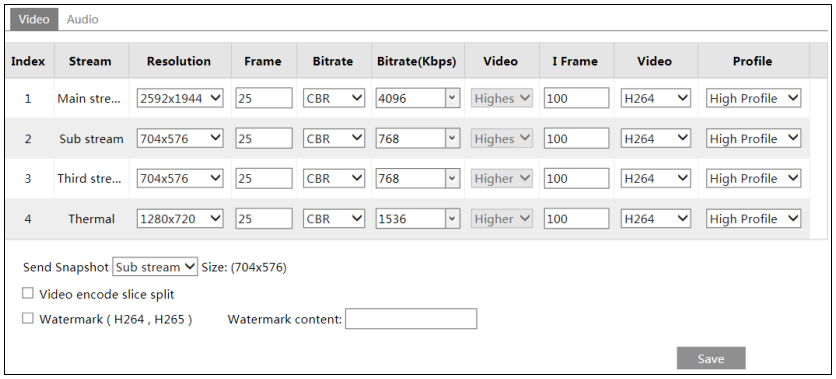


Drag “” icons to set the time of day and night. Blue means day time and blank means night time. If the current mode of camera parameters is set to schedule, the image configuration mode will automatically switch between day and night according to the schedule.

Thermal Parameter Settings: Click the “Thermal Parameters” tab to set the thermal color.

5.2.2 Video / Audio Configuration

Go to Image→Video / Audio interface as shown below. In this interface, set the resolution, frame rate, bitrate type, video quality and so on subject to the actual network condition.



Four video streams can be adjustable.

Resolution: The size of image.

Frame rate: The higher the frame rate, the video is smoother.

Bitrate type: CBR and VBR are optional. Bitrate is related to image quality. CBR means that no matter how much change is seen in the video scene, the compression bitrate will be kept constant. VBR means that the compression bitrate will be adjusted according to scene changes. For example, for scenes that do not have much movement, the bitrate will be kept at a lower value. This can help optimize the network bandwidth usage.

Bitrate: it can be adjusted when the mode is set to CBR. The higher the bitrate, the better the image quality will be.

Video Quality: It can be adjusted when the mode is set to VBR. The higher the image quality, the more bitrate will be required.

I Frame interval: It determines how many frames are allowed between a “group of pictures”. When a new scene begins in a video, until that scene ends, the entire group of frames (or pictures) can be considered as a group of pictures. If there is not much movement in the scene, setting the value higher than the frame rate is fine, potentially resulting in less bandwidth usage. However, if the value is set too high, and there is a high frequency of movement in the video, there is a risk of frame skipping.

Video Compression: Select JPEG, H264, or H265. MJPEG is not available for main stream. If H.265 is chosen, make sure the client system is able to decode H.265. Compared to H.264, H.265 reduces the transmission bitrate under the same resolution, frame rate and image quality.

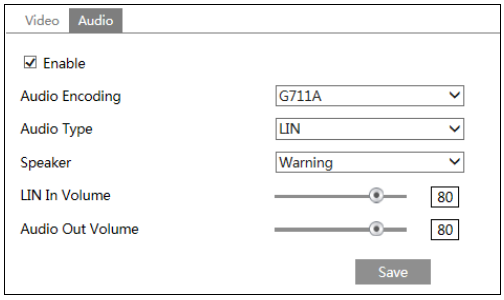
Profile: For H.264. Baseline, main and high profiles are selectable.

Send Snapshot: Set the snapshot stream.

Video encode slice split: If this function is enabled, smooth image can be gotten even though using the low-performance PC.

Watermark: When playing back the local recorded video in the search interface, the watermark can be displayed. To enable it, check the watermark box and enter the watermark text.

Click the “Audio” tab to go to the interface as shown below.



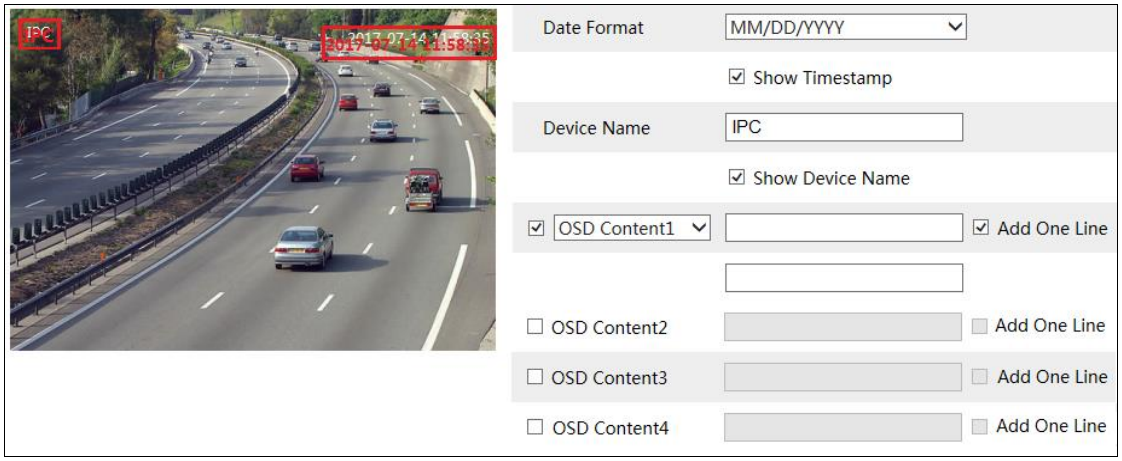
Audio Encoding: G711A and G711U are selectable.

Audio Type: Select LIN for external microphone, or MIC for build-in microphone.

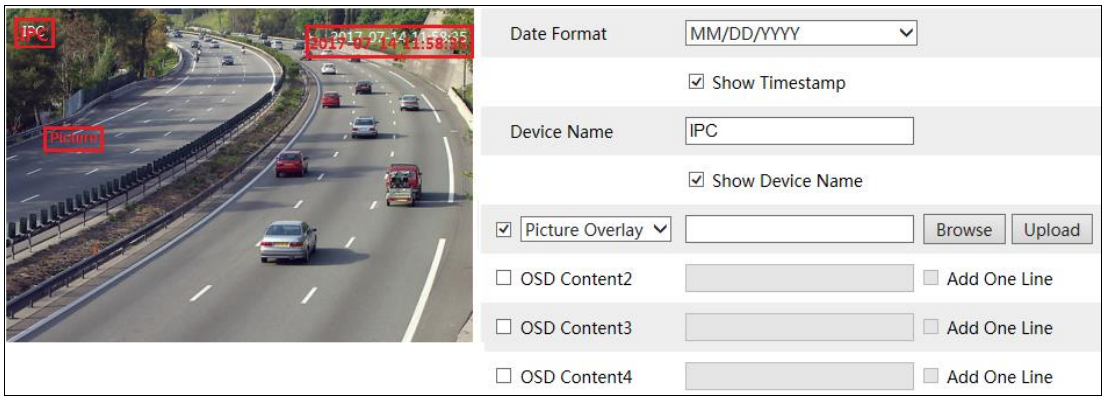
Speaker: Choose warning voice or talkback as needed.

5.2.3 OSD Configuration

Go to Image→OSD interface as shown below.



Set time stamp, device name, OSD content and picture overlap here. After enabling the corresponding display and entering the content, drag them to change their position. Then click the “Save” button to save the settings.



Picture Overlay Settings:

Check “OSD Content1”, choose “Picture Overlay” and click “Browse” to select the overlap picture. Then click “Upload” to upload the overlap picture. The pixel of the image shall not exceed 200*200, or it cannot be uploaded.

5.2.4 Video Mask

Go to Image→Video Mask interface as shown below. A maximum of 4 zones can be set up.

To set up video mask:

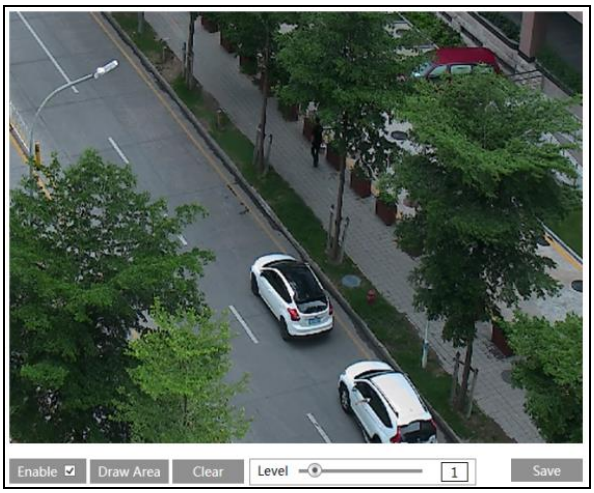
1. Enable video mask.
2. Click the “Draw Area” button and then drag the mouse to draw the video mask area.
3. Click the “Save” button to save the settings.
4. Return to the live to verify that the area has been drawn as shown as blocked out in the image.

To clear the video mask:

Click the “Clear” button to delete the current video mask area.

5.2.5 ROI Configuration

Go to Image→ROI Config interface as shown below. An area in the image can be set as a region of interest. This area will have a higher bitrate than the rest of the image, resulting in better image quality for the identified area.

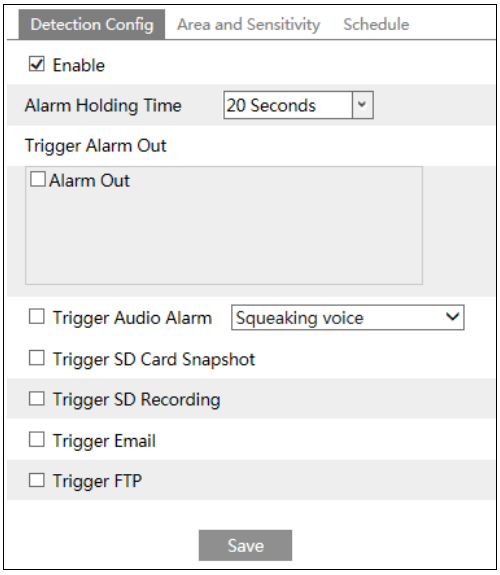


1. Check “Enable” and then click the “Draw Area” button.
2. Drag the mouse to set the ROI area.
3. Set the level.
4. Click the “Save” button to save the settings.

5.3 Alarm Configuration

5.3.1 Motion Detection

Go to Alarm→Motion Detection to set motion detection alarm.



1. Check “Enable” check box to activate motion-based alarms. If unchecked, the camera will not send out any signals to trigger motion-based recording to the NVR or CMS, even if there is motion in the video.

Alarm Out: If selected, this would trigger an external relay output that is connected to the camera on detecting a motion- based alarm (some models may support two alarm output interfaces. Please select alarm out according to the actual situation).

Trigger Audio Alarm: If selected, the warning voice will be uttered on motion detection. (Please set the warning voice first. See Audio Alarm for details).

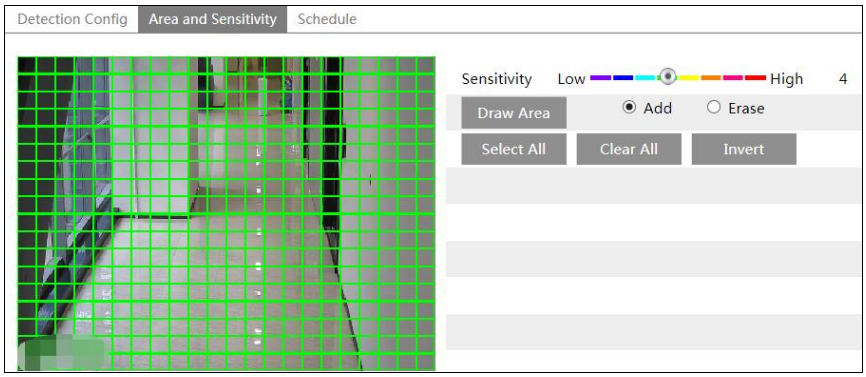
Trigger SD Snapshot: If selected, the system will capture images on motion detection and save the images on an SD card.

Trigger SD Recording: If selected, video will be recorded on an SD card on motion detection.

Trigger Email: If “Trigger Email” and “Attach Picture “are checked (email address must be set first in the Email configuration interface), the captured pictures and triggered event will be sent into those addresses.

Trigger FTP: If “Trigger FTP” is checked, the captured pictures will be sent into FTP server address. Please refer to FTP configuration chapter for more details.

2. Set motion detection area and sensitivity. Click the “Area and Sensitivity” tab to go to the interface as shown below.



Move the “Sensitivity” scroll bar to set the sensitivity. Higher sensitivity value means that motion will be triggered more easily.

Select “Add” and click “Draw”. Drag the mouse to draw the motion detection area; Select “Erase” and drag the mouse to clear motion detection area.

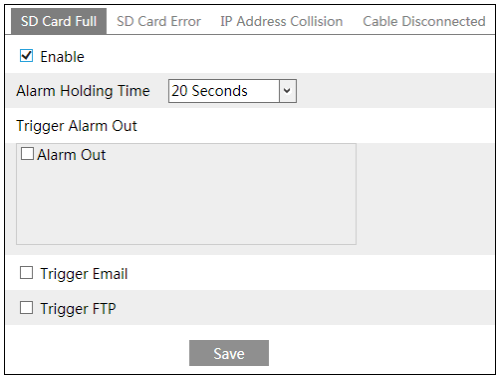
After that, click the “Save” to save the settings.

3. Set the schedule for motion detection. The schedule setup steps of the motion detection are the same as the schedule recording setup (See Schedule Recording).

5.3.2 Other Alarms

- **SD Card Full**

1. Go to Config→Alarm→Anomaly→SD Card Full.

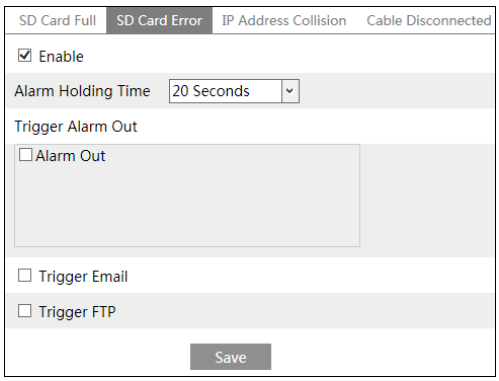


2. Click “Enable” and set the alarm holding time.
3. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection chapter for details.

- **SD Card Error**

When there are some errors in writing SD card, the corresponding alarms will be triggered.

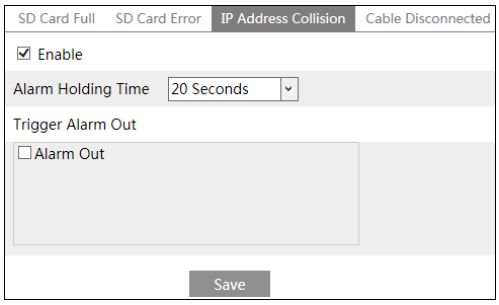
1. Go to Config→Alarm→Anomaly→SD Card Error as shown below.



2. Click “Enable” and set the alarm holding time.
3. Set alarm trigger options. Trigger alarm out, Email and FTP. The setup steps are the same as motion detection. Please refer to motion detection chapter for details.

- **IP Address Conflict**

1. Go to Config→Alarm→Anomaly→IP Address Collision as shown below.

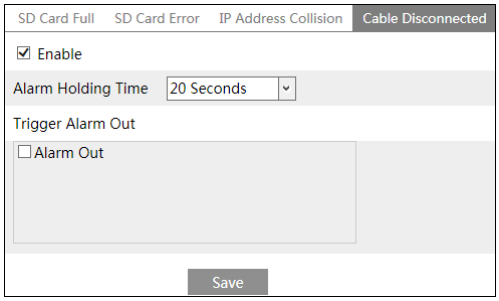


2. Click “Enable alarm” and set the alarm holding time.
3. Trigger alarm out. When the IP address of the camera conflicts with the IP address of other devices, the system will trigger the alarm out.

-

Cable Disconnection

1. Go to Config→Alarm→Anomaly→Cable Disconnected as shown below.



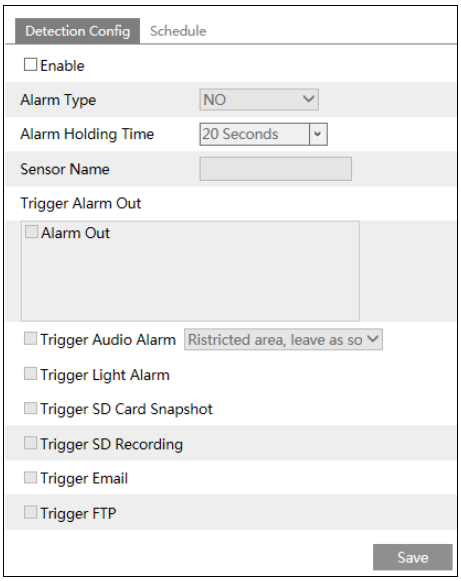
2. Click “Enable” and set the alarm holding time.

3. Trigger alarm out. When the camera is disconnected, the system will trigger the alarm out.

5.3.3 Alarm In

To set sensor alarm (alarm in):

Go to Config→Alarm→Alarm In interface as shown below.

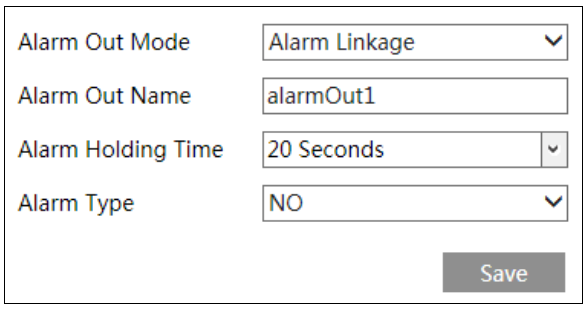


1. Click “Enable” and set the alarm type, alarm holding time and sensor name.
2. Set alarm trigger options. The setup steps are the same as fire detection. Please refer to Fire Detection chapter for details.
3. Click “Save” button to save the settings.
4. Set the schedule of the sensor alarm. The setup steps of the schedule are the same as the schedule recording setup. (See Schedule Recording).

If there are two sensors, please select the sensor ID. Click “Apply settings to” to quickly apply the settings to the other alarm input.

5.3.4 Alarm Out

This function is only available for some models. Go to Config→Alarm→Alarm Out.

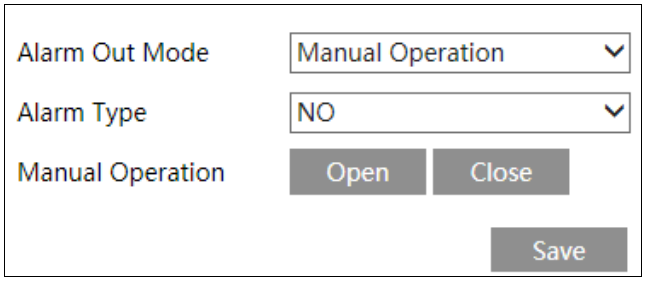


Alarm Out ID: Some models may support two alarm output interfaces. The alarm out can be set respectively by selecting alarm out ID.

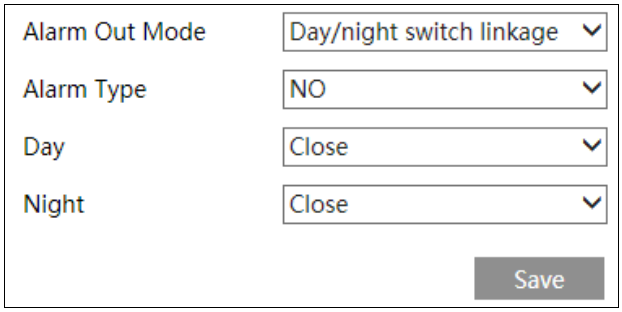
Alarm Out Mode: Alarm linkage, manual operation, day/night switch linkage and timing are optional.

Alarm Linkage: Having selected this mode, select alarm out name, alarm holding time at the "Alarm Holding Time" pull down list box and alarm type.

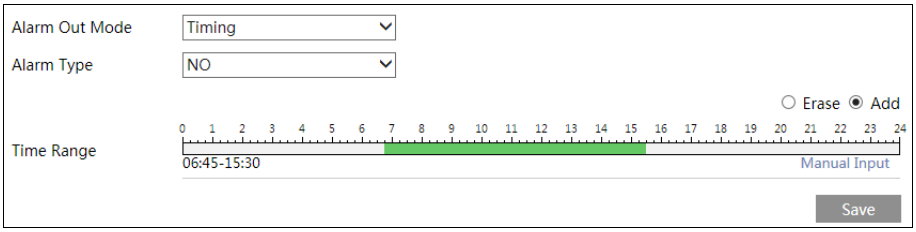
Manual Operation: Having selected this mode, select the alarm type and click "Open" to trigger the alarm out immediately; click "Close" to stop alarm.



Day/Night Switch Linkage: Having selected this mode, select the alarm type and then choose to open or close alarm out when the camera switches to day mode or night mode.



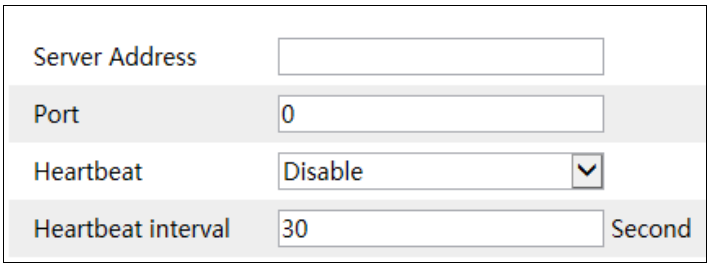
Timing: Select the alarm type. Then click “Add” and drag the mouse on the timeline to set the schedule of alarm out; click “Erase” and drag the mouse on the timeline to erase the set time schedule. After this schedule is saved, the alarm out will be triggered in the specified time.



5.3.5 Alarm Server

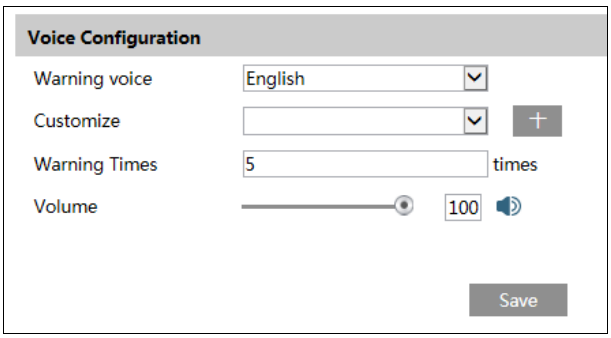
Go to Alarm→Alarm Server interface as shown below.

Set the server address, port, heartbeat and heartbeat interval. When an alarm occurs, the camera will transfer the alarm event to the alarm server. If an alarm server is not needed, there is no need to configure this section.

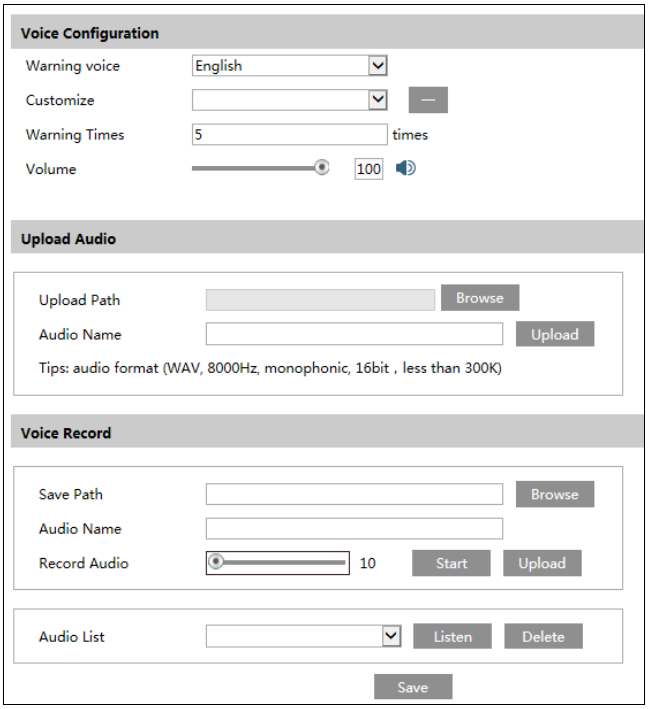


5.3.6 Audio Alarm

Go to Alarm→Audio Alarm interface as shown below.



1. Select the warning voice. If you want to customize the voice content, you can choose “Customize”. Click “Browse” to choose the audio file you want to upload and then enter the audio name. Finally, click “Upload” to upload the audio file. Note that the format of the audio file must meet the requirement (see Tips), or it will not be uploaded. After you upload the audio file, you can select the audio name from the audio list and click “Listen” to listen to it. Click “Delete” to delete the audio.



You can also record your own voice in the above interface and then upload.

- Insert the microphone into your PC.
- Click “Browse” to choose the save path of the audio you want to record.
- Set the record audio volume and then click “Start” to start recording your voice.
- Click “Upload” to upload your customized voice.

2. Select the voice and then set the warning times and volume as needed.

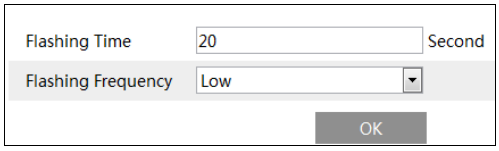
Warning times: it ranges from 1 to 50.

3.Click “OK” to save the settings.

5.3.7 Light Alarm

Go to Alarm→Light Alarm interface as shown below.

Set the flashing time and frequency of the light.



Flashing time: the flashing time ranges from 1 second to 60 seconds.

Flashing Frequency: three options- low, middle and high.

5.4 Event Configuration

For more accuracy, here are some recommendations for installation.

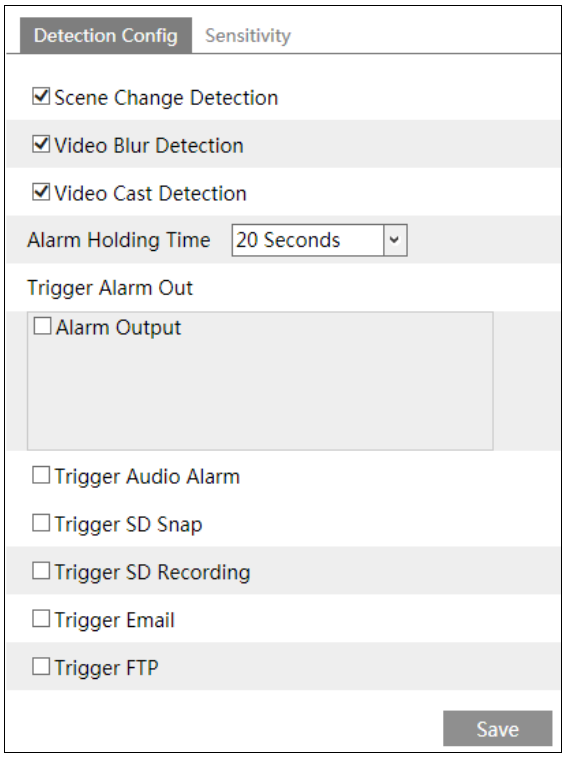
- Cameras should be installed on stable surfaces, as vibrations can affect the accuracy of detection.
- Avoid pointing the camera at the reflective surfaces (like shiny floors, mirrors, glass, lake surfaces and so on).
- Avoid places that are narrow or have too much shadowing.
- Avoid scenario where the object's color is similar to the background color.
- At any time of day or night, please make sure the image of the camera is clear and with adequate and even light, avoiding overexposure or too much darkness on both sides.

5.4.1 Video Exception

This function can detect changes in the surveillance environment affected by the external factors.

To set exception detection:

Go to Config→Event→Video Exception interface as shown below.



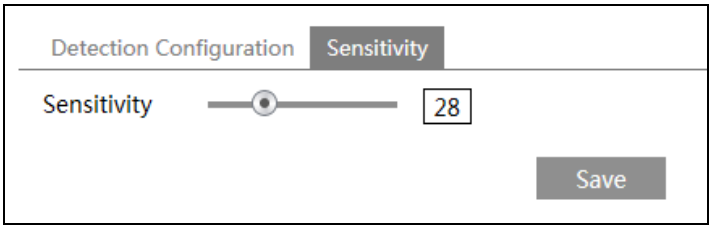
1. Enable the applicable detection that's desired.

Scene Change Detection: Alarms will be triggered if the scene of the monitor video has changed.

Video Blur Detection: Alarms will be triggered if the video becomes blurry.

Video Cast Detection: Alarms will be triggered if the video becomes obscured.

2. Set the alarm holding time and alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection chapter for details.
3. Click "Save" button to save the settings.
4. Set the sensitivity of the exception detection. Click "Sensitivity" tab to go to the interface as shown below.



Drag the slider to set the sensitivity value or directly enter the sensitivity value in the textbox. Click "Save" button to save the settings.

The sensitivity value of Scene Change Detection: The higher the value is, the more sensitive the system responds to the amplitude of the scene change.

The sensitivity value of Video Blur Detection: The higher the value is, the more sensitive the system responds to the blurriness of the image.

The sensitivity value of Video Cast Detection: The higher the value is, the more sensitive the system responds to the obscuring of the image.

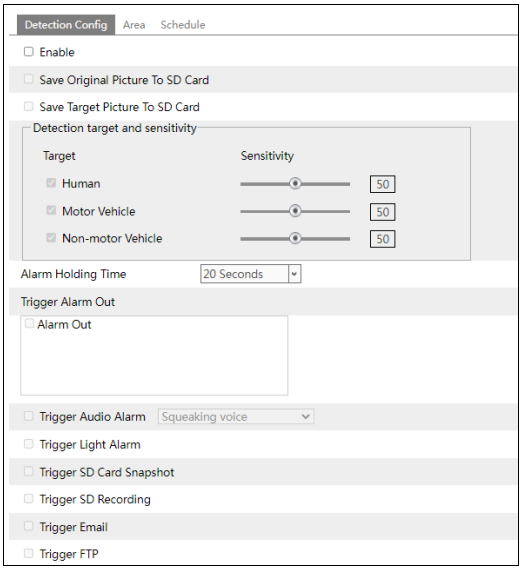
※ The requirements of camera and surrounding area

1. Auto-focusing function should not be enabled for exception detection.
2. Try not to enable exception detection when light changes greatly in the scene.
3. Please contact us for more detailed application scenarios.

5.4.2 Line Crossing

Line Crossing: Alarms will be triggered if the target crosses the pre-defined alarm lines.

Go to Config→Event→Line Crossing interface as shown below.



1. Enable line crossing detection and select the snapshot type and the detection target.

Save Original Picture to SD Card: If it is enabled, the detected pictures will be captured and saved to the SD card when the targets cross the alarm line.

Save Target Picture to SD Card: If it is enabled, the detected target cutout pictures will be captured and saved to the SD card when the targets cross the alarm line.

Note: To save snapshots to the local PC, please enable “Local Smart Snapshot Storage” in the local config interface first. To save snapshots to the SD card, please install an SD card first.

Detection Target:

Human: Select it and then alarms will be triggered if someone crosses the pre-defined alarm lines.

Motor Vehicle: Select it and then alarms will be triggered if a vehicle with four or more wheels (eg. a car, bus or truck) crosses the pre-defined alarm lines.

Non-motor Vehicle: Select it and then alarms will be triggered if a vehicle with two wheels (eg. a motorcycle or bicycle) crosses the pre-defined alarm lines.

All of the three types of objects can be selected simultaneously. Please select the detection objects as needed. If no object/target is selected, alarms will not be triggered even if line crossing detection is enabled.

2. Set the alarm holding time.
3. Set alarm trigger options. The setup steps are the same as fire detection. Please refer to FireDetection chapter for details.
4. Click “Save” button to save the settings.
5. Set area and sensitivity of the line crossing alarm. Click the “Area and Sensitivity” tab to go to the interface as shown below.

Set the alarm line number and direction. Up to 4 lines can be added. Multiple lines cannot be added simultaneously.

Direction：A<->B, A->B and A<-B optional. This indicates the direction of someone or a vehicle crosses over the alarm line.

A<->B: Alarms will be triggered when someone or a vehicle crosses over the alarm line from B to A or from A to B.

A->B: Alarms will be triggered when someone or a vehicle crosses over the alarm line from A to B.

A<-B: Alarms will be triggered when someone or a vehicle crosses over the alarm line from B to A.

Click the “Draw Area” button and then drag the mouse to draw a line in the image. Click the “Stop Draw” button to stop drawing. Click the “Clear” button to delete the lines. Click the “Save” button to save the settings.

6. Set the schedule of the line crossing alarm. The setup steps of the schedule are the same as the schedule recording setup (See Schedule Recording).

※ Configuration of camera and surrounding area

1. Auto-focusing function should not be enabled for line crossing detection.

2. Avoid the scenes with many trees or the scenes with various light changes (like many flashing headlights). The ambient brightness of the scenes shouldn’t be too low.

3. Cameras should be mounted at a height of 2.8 meters or above.

4. Keep the mounting angle of the camera at about 45°.

5. The detected objects should not be less than 1% of the entire image and the largest sizes of the detected objects should not be more than 1/8 of the entire image.

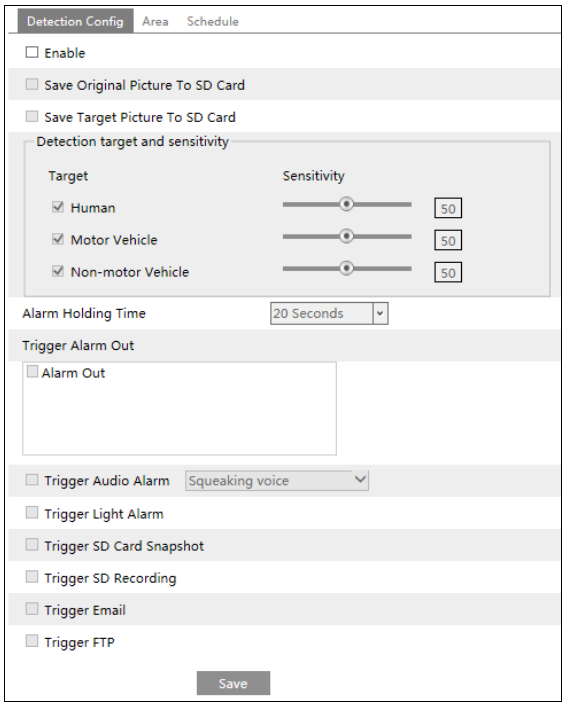
6. Make sure cameras can view objects for at least 2 seconds in the detected area for accurate detection.

7. Adequate light and clear scenery are crucial for line crossing detection.

5.4.3 Region Intrusion

Intrusion: Alarms will be triggered if the target intrudes into the pre-defined areas. This function can be applicable to important supervision places, danger areas and prohibited areas, like military administrative zones, high danger areas, no man's areas, etc.

Go to Config→Event→Region Intrusion interface as shown below.



1. Enable intrusion detection and select the snapshot type and the detection target.

2. Set the alarm holding time.

3. Set alarm trigger options. The setup steps are the same as fire detection. Please refer to Fire Detection chapter for details.

4. Click the “Save” button to save the settings.

5. Set the alarm area of the intrusion detection. Click the “Area” tab to go to the interface as shown below.

Set the alarm area number on the right side. Up to 4 alarm areas can be added.
Click the “Draw Area” button and then click around the area where you want to set as the alarm area in the image on the left side (the alarm area should be a closed area). Click the “Stop Draw” button to stop drawing. Click the “Clear” button to delete the alarm area. Click the “Save” button to save the settings.

6. Set the schedule of the intrusion detection. The setup steps of the schedule are the same as schedule recording setup (See Schedule Recording).

※ Configuration requirements of camera and surrounding area

1. Auto-focusing function should not be enabled for intrusion detection.
2. Avoid the scenes with many trees or the scenes with various light changes (like many flashing headlights). The ambient brightness of the scenes shouldn’t be too low.
3. Cameras should be mounted at a height of 2.8 meters or above.
4. Keep the mounting angle of the camera at about 45°.
5. The detected objects should not be less than 1% of the entire image and the largest sizes of the detected objects should not be more than 1/8 of the entire image.
6. Make sure cameras can view objects for at least 2 seconds in the detected area for accurate detection.
7. Adequate light and clear scenery are crucial to intrusion detection.

5.4.4 Region Entrance

Region Entrance: Alarms will be triggered if the target enters the pre-defined areas.

Go to Config→Event→Region Entrance interface. The setup steps of the region entrance are the same as Intrusion setup (See Region Intrusion for details).

5.4.5 Region Exiting

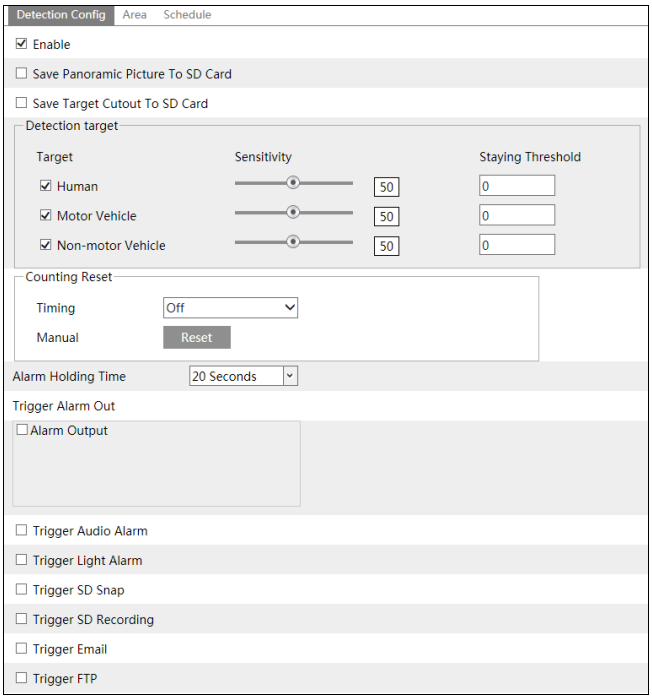
Region Exiting: Alarms will be triggered if the target exits from the pre-defined areas.

Go to Config→Event→Region Exiting interface. The setup steps of the region exiting are the same as Region Intrusion setup (See Region Intrusion for details).

5.4.6 Target Counting

This function is to calculate the number of the people or vehicles crossing the alarm line through detecting, tracking and counting the shapes of the people or vehicles.

1. Go to Config→Event→Target Counting by Line as shown below.



2. Enable target counting and select the snapshot type and the detection target.

Detection Target: Select the target to calculate. Human, motor vehicle and non-motor vehicle can be selected.

Staying Threshold: When the targets (human/vehicle) staying in the specified area exceed the threshold, alarms will be triggered.

Counting Reset: The current number of the target counting can be reset. You can choose to reset the counting daily, weekly or monthly. Click “Reset” to manually reset the current number of crossing line people/motor vehicle/non-motor vehicle counting.

3. Set alarm trigger options. The setup steps are the same as fire detection. Please refer to Fire Detection chapter for details.
4. Set the area of the target counting. Click the “Area” tab to go to the interface as shown below.

Set the alarm line number and direction. Only one alarm line can be added.

Direction：A->B and A<-B can be optional. The direction of the arrow is entrance.

Statistics: If enabled, you can see the statistical information in the live view interface. If disabled, the statistical information will not be displayed in the live view interface.

The statistical OSD information can be customized as needed.

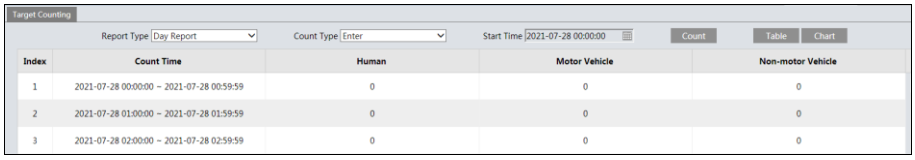
Click the “Draw Area” button and then drag the mouse to draw a line in the image. Check “Statistics” and then move the red box to change the position of the statistical information displayed on the screen. Click the “Stop Draw” button to stop drawing. Click the “Clear” button to delete the lines.

Click the “Save” button to save the settings.

5. Set the schedule of the target counting. The setup steps of the schedule are the same as schedule recording setup (See Schedule Recording).

6. View the statistical information in the live view interface.

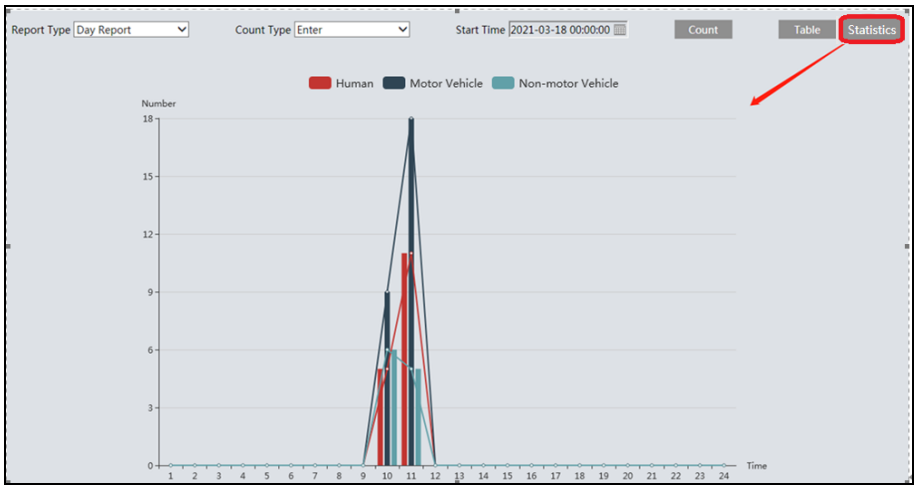
7. View the statistical information of target counting by line crossing. Click “Statistics” to enter the following interface.



Select the report type. Daily report, weekly report, monthly report and annual report are selectable.

Select the count type. Enter or leave can be optional.

Select the start time and then click “Count”. Then the counting result will display in the statistic result area. Click Table or Statistics to display the result in different ways.

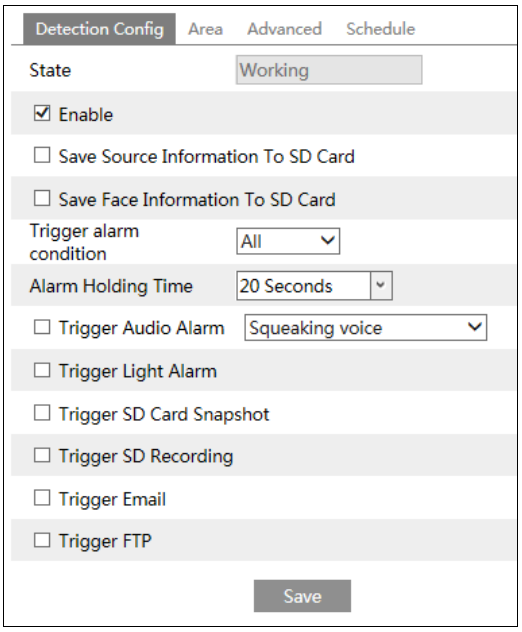


5.4.7 Face Detection

Face detection function is to detect the face appearing in the surveillance scene. Alarms will be triggered when a face is detected.

The setting steps are as follows:

1. Go to Config→Event→Face Detection as shown below.



2. Enable the face detection function.

Save Source Information: if checked, the whole picture will be saved to the SD card when detecting a face.

Save Face Information: if checked, the captured face picture will be saved to the SD card when detecting a face.

Note: To save images to the local PC, please enable the local smart snapshot storage first (Config→System→Local Config). To save images to the SD card, please install an SD card first.

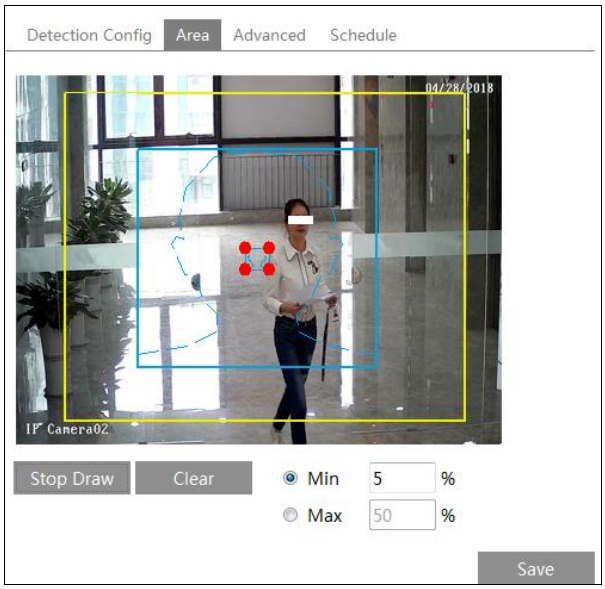
Trigger alarm condition: all alarms or mask off can be selectable.

All alarms: Alarms will be triggered when the camera detects a face (with/without a mask).

Mask off: Alarms will be triggered when the detected person is not wearing a mask on the face.

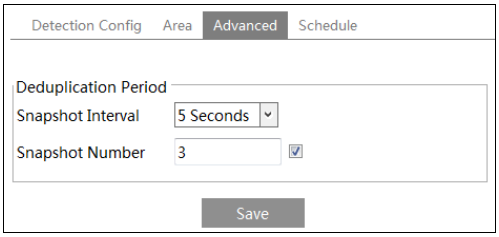
3. Set the alarm holding time and alarm trigger options. The alarm trigger setup steps are the same as fire detection setup. Please refer to Fire Detection chapter for details.

4. Set the alarm detection area.



Click “Draw Area” and drag the border lines of the rectangle to modify its size. Move the rectangle to change its position. Click “Stop Draw” to stop drawing the area. Click “Clear” to clear the area. Then set the detectable face size by defining the maximum value and the minimum value (The default size range of a single face image occupies from 3% to 50% of the entire image).

5. Advanced settings. Choose the snapshot interval and number as needed to avoid capturing multiple similar pictures in a very short period of time.



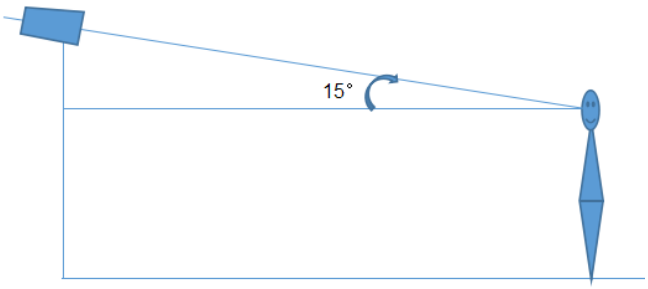
Snapshot Interval: If 5 seconds is selected, the camera will capture the same target once every 5 seconds during its continuous tracking period.

Snapshot Number: If the snapshot number is enabled and set (eg. 3), the camera will capture the same target once every 5 seconds and it will capture this target 3 times at most during its continuous tracking period. If the snapshot number is disabled, the camera will capture the same target once every 5 seconds until the target disappears in the detected area.

6. Set the schedule of the face detection. The setup steps of the schedule are the same as schedule recording setup (See Schedule Recording).

※ Configuration requirements of camera and surrounding area

1. Cameras must be installed in the area with stable and adequate light sources.
2. The installation height ranges from 2.0m to 3.5m, adjustable according to the focal-length of different lenses and object distances.
3. The depression angle of the camera shall be less than or equal to 15°.

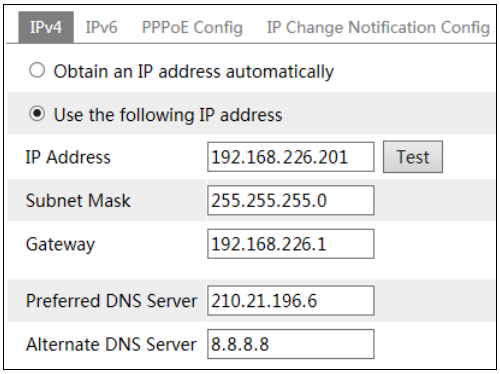


4. The object distance depends on the focal-length of the lens mounted in the camera.
5. To ensure the accuracy of face detection, the captured faces are only allowed to deviate less than 30° leftward or rightward or 20° upward or downward.
6. The following scenes are not applicable, like crowded scenes (airport, railway station, square, etc), backlight scenes, crossroads and so on.

5.5 Network Configuration

5.5.1 TCP/IP

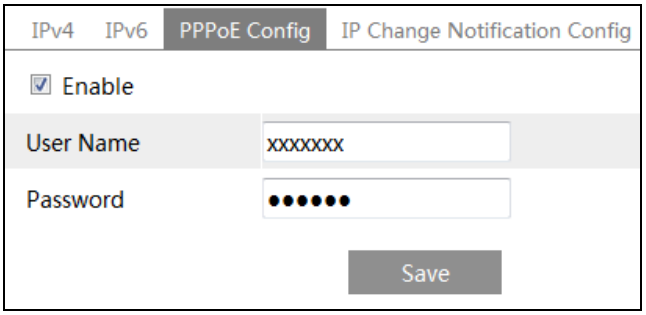
Go to Config→Network→TCP/IP interface as shown below. There are two ways for network connection.



Use IP address (take IPv4 for example): There are two options for IP setup: obtain an IP address automatically by DHCP and use the following IP address. Please choose one of the options as needed.

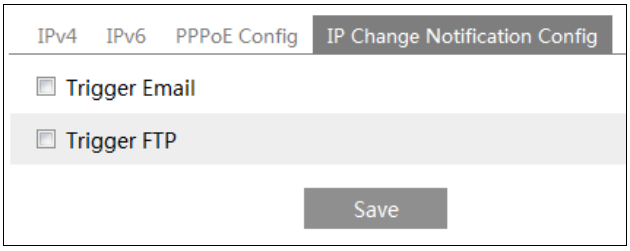
Test: Test the effectiveness of the IP address by clicking this button.

Use PPPoE: Click the “PPPoE Config” tab to go to the interface as shown below. Enable PPPoE and then enter the user name and password from your ISP.



Either method of network connection can be used. If PPPoE is used to connect internet, the camera will get a dynamic WAN IP address. This IP address will change frequently. To be notified, the IP change notification function can be used.

Click “IP Change Notification Config” to go to the interface as shown below.

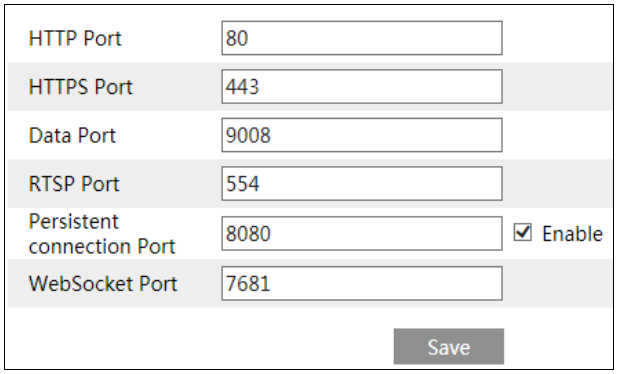


Trigger Email: when the IP address of the device is changed, the new IP address will be sent to the email address that has been set up.

Trigger FTP: when the IP address of the device is changed, the new IP address will be sent to FTP server that has been set up.

5.5.2 Port

Go to Config→Network→Port interface as shown below. HTTP port, Data port and RTSP port can be set.



HTTP Port: The default HTTP port is 80. It can be changed to any port which is not occupied.

HTTPS Port: The default HTTPs port is 443. It can be changed to any port which is not occupied.

Data Port: The default data port is 9008. Please change it as necessary.

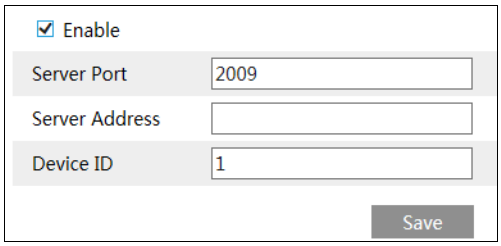
RTSP Port: The default port is 554. Please change it as necessary.

Persistent Connection Port: The port is used for a persistent connection of the third-party platform to push smart data, like face pictures.

WebSocket Port: Communication protocol port for plug-in free preview.

5.5.3 Server Configuration

This function is mainly used for connecting network video management system.



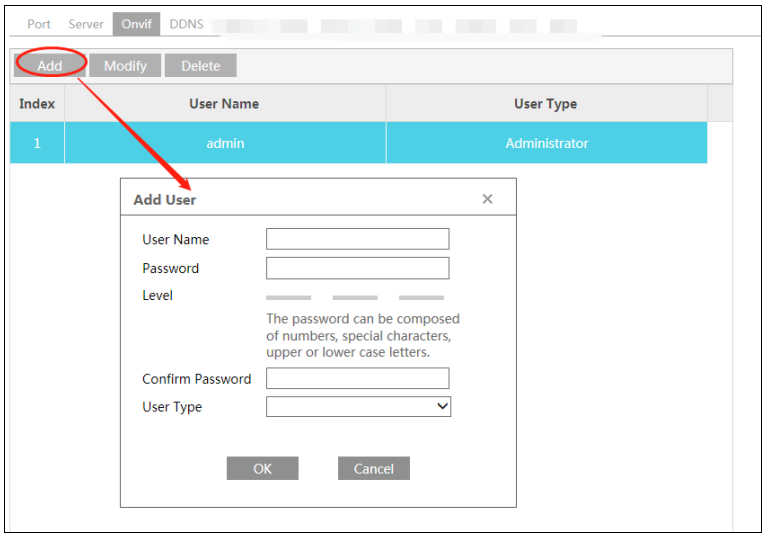
1. Check “Enable”.
2. Check the IP address and port of the transfer media server in the ECMS/NVMS. Then enable the auto report in the ECMS/NVMS when adding a new device. Next, enter the remaining information of the device in the ECMS/NVMS. After that, the system will automatically allot a device ID. Please check it in the ECMS/NVMS.
3. Enter the above-mentioned server address, server port and device ID in the corresponding boxes. Click the “Save” button to save the settings.

5.5.4 Onivf

The camera can be searched and connected to the third-party platform via ONVIF/RTSP protocol.

If “Activate Onvif User” is enabled in the device activation interface, the ONVIF user can be activated simultanously. When you connect the camera through the ONVIF protocol in the third-party platform, you can use this onvif user to connect.

You can also add new users in the Onvif interface.

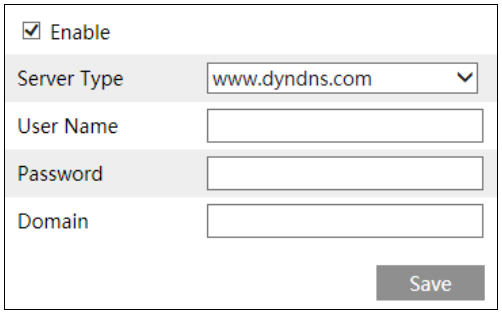


Note: when adding the device to the third-party platform with ONVIF/RTSP protocol, please use the onvif user in the above interface.

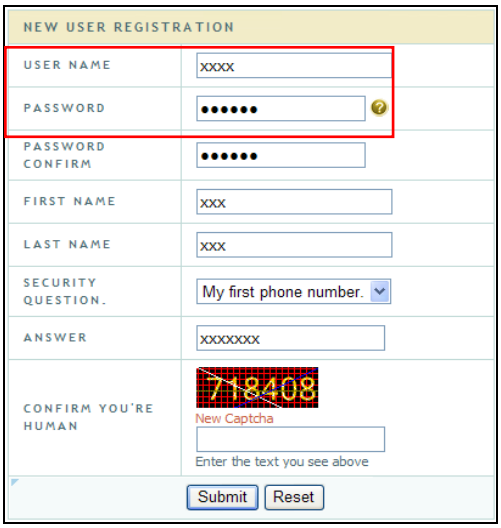
5.5.5 DDNS

If the camera is set up with a DHCP connection, DDNS should be set for the internet.

1. Go to Config→Network→ DDNS.

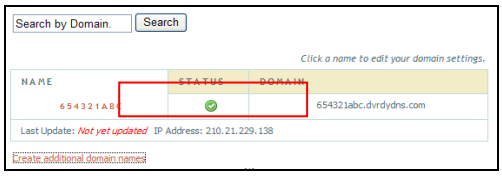


2. Apply for a domain name. Take www.dvrdyndns.com for example. Enterwww.dvrdydns.com in the IE address bar to visit its website. Then Click the “Registration” button.



Create domain name.

After the domain name is successfully applied for, the domain name will be listed as below.

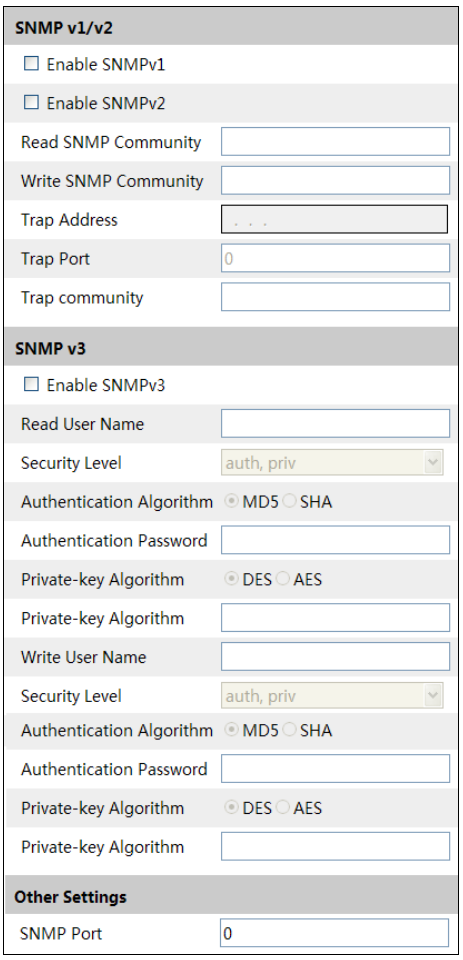


3. Enter the username, password, domain you apply for in the DDNS configuration interface.
4. Click the “Save” button to save the settings.

5.5.6 SNMP

To get camera status, parameters and alarm information and remotely manage the camera, the SNMP function can be used. Before using SNMP, please install an SNMP management tool and set the parameters of the SNMP, such as SNMP port, trap address.

1. Go to Config→Network→SNMP.

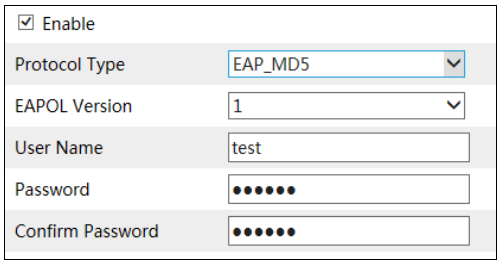


2. Check the corresponding version checkbox (Enable SNMPv1, Enable SNMPv2, Enable SNMPv3) according to the version of the SNMP software that will be used.
3. Set the values for “Read SNMP Community”, “Write SNMP Community”, “Trap Address”, “Trap Port” and so on. Please make sure the settings are the same as that of the SNMP software.

Note: Please use the different version in accordance with the security level you required. The higher the version is, the higher the level of the security is.

5.5.7 802.1x

If it is enabled, the camera's data can be protected. When the camera is connected to the network protected by the IEE802.1x, user authentication is needed.



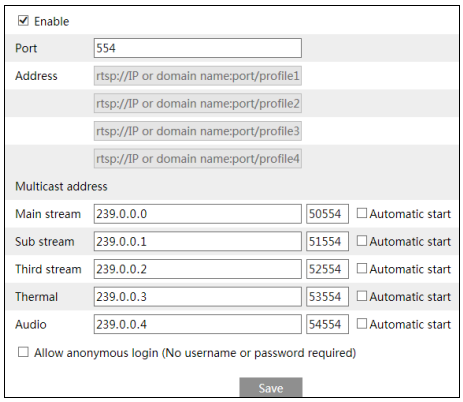
To use this function, the camera shall be connected to a switch supporting 802.1x protocol. The switch can be reckoned as an authentication system to identify the device in a local network. If the camera connected to the network interface of the switch has passed the authentication of the switch, it can be accessed via the local network.

Protocol type and EAPOL version: Please use the default settings.

User name and password: The user name and password must be the same with the user name and password applied for and registered in the authentication server.

5.5.8 RTSP

Go to Config→Network→RTSP.



Select "Enable" to enable the RTSP function.

Port: Access port of the streaming media. The default number is 554.

RTSP Address: The RTSP address (unicast)format that can be used to play the stream in a media player.

Multicast Address

Main stream: The address format is

"rtsp://IP address: rtsp port/profile1?transportmode=mcast".

Sub stream: The address format is

"rtsp://IP address: rtsp port/profile2?transportmode=mcast".

Third stream: The address format is

"rtsp://IP address: rtsp port/profile3?transportmode=mcast".

Thermal stream: The address format is

"rtsp://IP address: rtsp port/profile4?transportmode=mcast".

Audio: Having entered the main/sub stream in a VLC player, the video and audio will play automatically.

If "Allow anonymous login…" is checked, there is no need to enter the username and password to view the video.

If "auto start" is enabled, the multicast received data should be added into a VLC player to play the video.

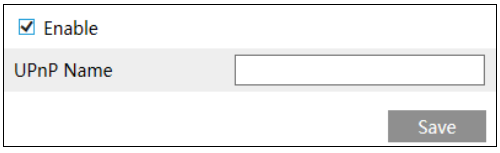
Note:

1. This camera supports local playback through a VLC player. Enter the RTSP address (unicast or multicast, eg. rtsp://192.168.226.201:554/profile1?transportmode=mcast) in a VLC player to realize the simultaneous play with the web client.
2. The IP address mentioned above cannot be the address of IPv6.
3. Avoid the use of the same multicast address in the same local network.
4. When playing the video through the multicast streams in a VLC player, please pay attention to the mode of the VLC player. If it is set to TCP mode, the video cannot be played.
5. If the coding format of the video of the main stream is MJPEG, the video may be disordered at some resolutions.

5.5.9 UPNP

If this function is enabled, the camera can be quickly accessed through the LAN.

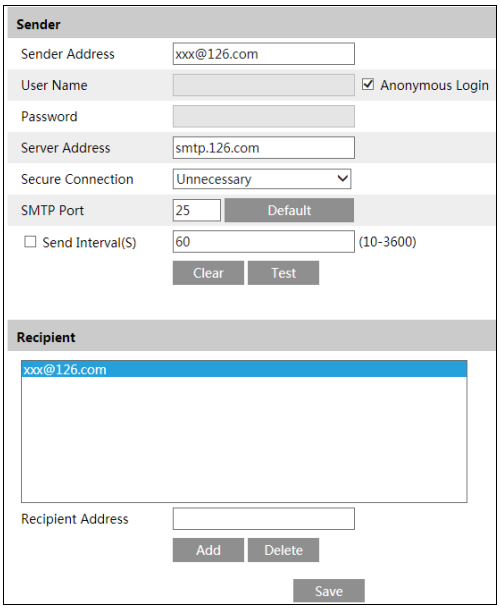
Go to Config→Network→UPnP. Enable UPNP and then enterUPnP name.



5.5.10 Email

If you need to trigger Email when an alarm happens or IP address is changed, please set the Email here first.

Go to Config→Network →Email.



Sender Address: sender's e-mail address.

User name and password: sender's user name and password (you don't have to enter the username and password if "Anonymous Login" is enabled).

Server Address: The SMTP IP address or host name.

Select the secure connection type at the "Secure Connection" pull-down list according to what's required.

SMTP Port: The SMTP port.

Send Interval(S): The time interval of sending email. For example, if it is set to 60 seconds and multiple motion detection alarms are triggered within 60 seconds, they will be considered as only one alarm event and only one email will be sent. If one motion alarm event is triggered and then another motion detection alarm event is triggered after 60 seconds, two emails will be sent. When different alarms are triggered at the same time, multiple emails will be sent separately.

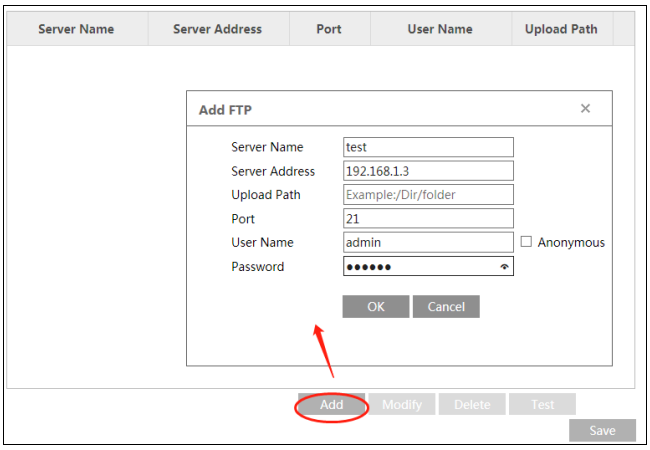
Click the "Test" button to test the connection of the account.

Recipient Address: receiver's e-mail address.

5.5.11 FTP

After an FTP server is set up, captured pictures from events will be uploaded to the FTP server.

1. Go to Config→Network →FTP.



2. Click “Add” to add the information of the FTP. After that, click “Save” to save the settings.

Server Name: The name of the FTP server.

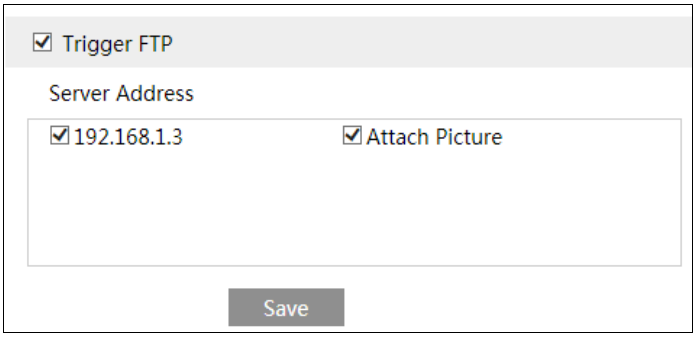
Server Address: The IP address or domain name of the FTP.

Upload Path: The directory where files will be uploaded to.

Port: The port of the FTP server.

User Name and Password: The username and password that are used to login to the FTP server.

3. In the event setting interface (like intrusion, line crossing, etc.), trigger FTP as shown below.



Please refer to 4.1.4 Storage-Snapshot Setting for the parameter settings of the sending snapshots

Rule of FTP storage path: /device MAC address/event type/date/time/

For example: a face detection alarm occurs

FTP file path：\00-18-ae-a8-da-2a\VFD\2021-01-09\14\

Event name table:

File Name	Event Type
IP	IP address change
MOTION	Motion Detection
SENSOR	Sensor Alarm
TRIPWIRE	Line Crossing Detection
PERIMETER	Region Intrusion Detection
OSC	Object Left/Missing
AVD	Video Exception
CDD	Crowd Density Detection
VFD	Face Recognition
VEHICE	License Plate Recognition
AOIENTRY	Region Entering
AOILEAVE	Region Exiting
PASSLINECOUNT	Target Counting by Line Crossing
TRAFFIC	Target Counting by Region Intrusion
SDFULL	SD Full
SDERROR	SD Error

Jpg imagenaming rule:

Event type_Year(4digits)-Month(2digits)-Day(2 digits)-Hour(2 digits)-Minute(2 digits)-Second(2 digits)-Millisecond(3 digits)_index(3digits).jpg

Description:

1. Event type: refers to the above table.
2. Zero shall be added if the digits are insufficient.

For example: MOTION_2021-03-16-16-20-07-529_032.jpg

Txt file naming rule:

Event type_Year(4digits)-Month(2digits)-Day(2 digits)-Hour(2 digits)-Minute(2 digits)-Second(2 digits)-Millisecond(3 digits)_index(3digits).txt

TXT file content:

device name: xxx mac: device MAC address Event Type time:

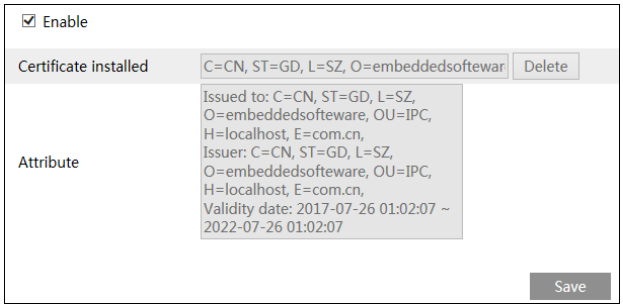
For example: device name: IPC mac: 00-18-ae-a8-da-2a MOTION time: 2021-03-16 12:20:07

Correspondence between txt file and jpeg file: the index of the txt file and jpeg file will be named as the same when the event is triggered each time.

5.5.12 HTTPS

HTTPs provides authentication of the web site and protects user privacy.

Go to Config→Network→HTTPS as shown below.

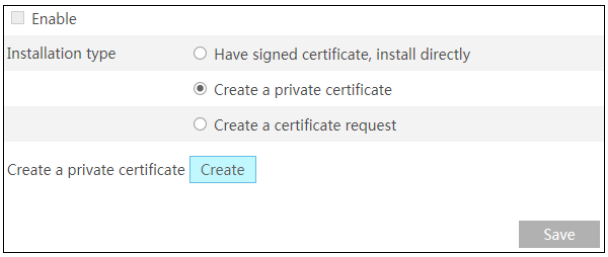


There is a certificate installed by default as shown above. Enable this function and save it. Then the camera can be accessed by entering https://IP: https port via the web browser (eg. https://192.168.226.201:443).

A private certificate can be created if users don't want to use the default one. Click "Delete" to cancel the default certificate. Then the following interface will be displayed.

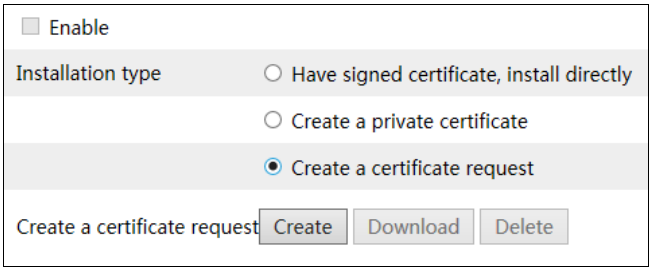
If there is a signed certificate, click "Browse" to select it and then click "Install" to install it.

Click “Create a private certificate” to enter the following creation interface.



Click the “Create” button to create a private certificate. Enter the country (only two letters available), domain (camera’s IP address/domain), validity date, password, province/state, region and so on. Then click “OK” to save the settings.

* Click “Create a certificate request” to enter the following interface.

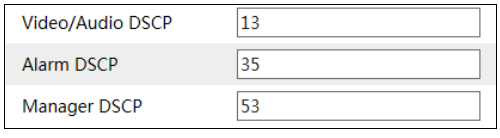


Click “Create” to create the certificate request. Then download the certificate request and submit it to the trusted certificate authority for signature. After receiving the signed certificate, import the certificate to the device.

5.5.13 QoS

QoS (Quality of Service) function is used to provide different quality of services for different network applications. With the deficient bandwidth, the router or switch will sort the data streams and transfer them according to their priority to solve the network delay and network congestion by using this function.

Go to Config→Network→QoS.



Video/Audio DSCP: The range is from 0 to 63.

Alarm DSCP: The range is from 0 to 63.

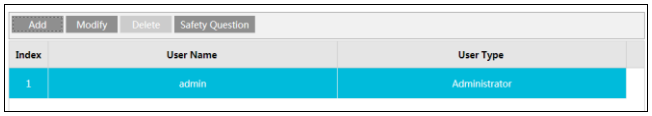
Manager DSCP: The range is from 0 to 63.

Generally speaking, the larger the number is, the higher the priority is.

5.6 Security Configuration

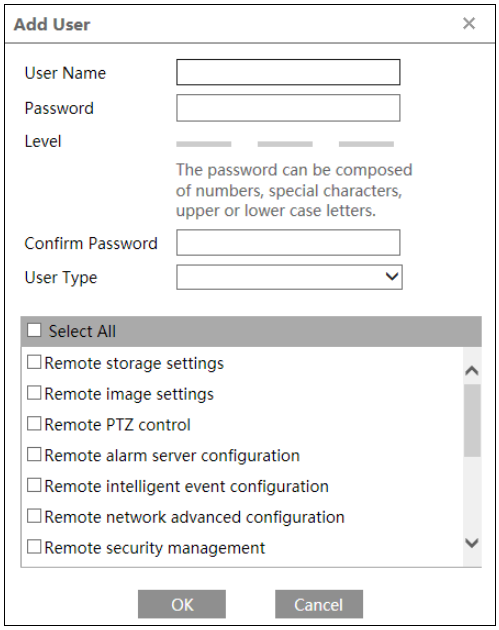
5.6.1 User Configuration

Go to Config→Security→User interface as shown below.



Add user:

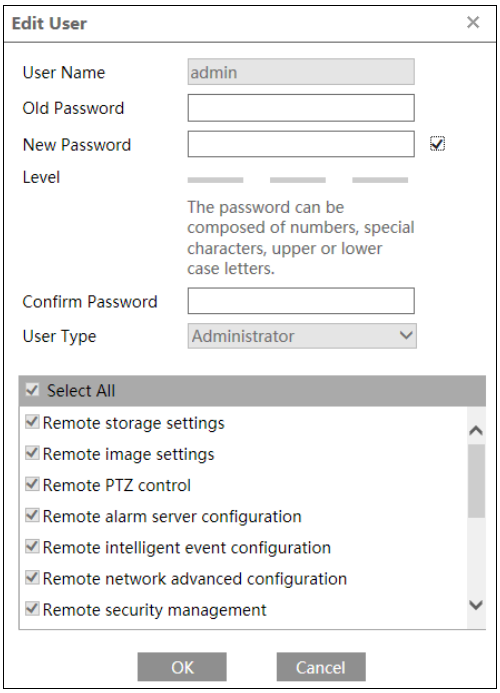
1. Click the “Add” button to pop up the following textbox.



2. Enter user name in “User Name” textbox.
3. Enter the password in the “Password” and “Confirm Password” textbox. Please set the password according to the requirement of the password security level (Go to Config→Security→Security Management→Password Security interface to set the security level).
4. Choose the user type and select the desired user permissions.
5. Click the “OK” button and then the newly added user will be displayed in the user list.

Modify user:

1. Select a user to modify password in the user configuration list box.
2. The “Edit user” dialog box pops up by clicking the “Modify” button.



Admin can modify its password and change the user type and permission of other users here.

Other users only can modify their password in this interface.

Delete user:

1. Select the user to be deleted in the user configuration list box.
2. Click the “Delete” button to delete the user.

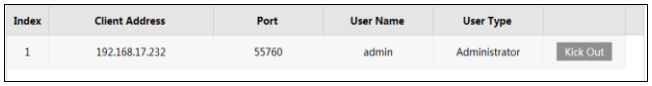
Note: The default administrator account cannot be deleted.

Safety Question

You can set the safety questions and answers here for the default admin user.

5.6.2 Online User

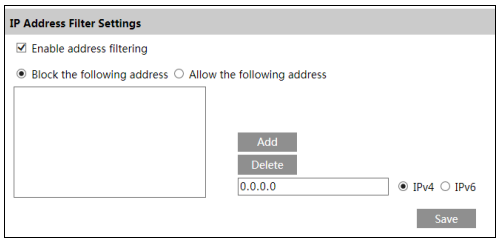
Go to Config→Security→Online User to view the user who is viewing the live video.



An administrator user can kick out all the other users (including other administrators).

5.6.3 Block and Allow Lists

Go to Config→Security→Block and Allow Lists as shown below.



The setup steps are as follows:

Check the “Enable address filtering” check box.

Select “Block/Allow the following address”, IPv4/IPv6 and then enter IP address in the address box and click the “Add” button.

5.6.4 Security Management

Go to Config→Security→Security Management as shown below.

In order to prevent against malicious password unlocking, “locking once illegal login” function can be enabled here. If this function is enabled, login failure after trying six times will make the login interface locked. The camera can be logged in again after a half hour or after the camera reboots.

Trigger Email: if enabled, e-mail will be sent when logging in/out or illegal login lock occurs.

Logout time: Set the logout time as needed. For example: 3600s, you will be automatically logged out after 3600s and then you need to enter the username and password again to log in.

Password Security

Please set the password level and expiration time as needed.

Password Level: Weak, Medium or Strong.

Weak level: Numbers, special characters, upper- or lower-case letters can be used. You can choose one of them or any combination of them when setting the password.

Medium Level: 8~16 characters, including at least two of the following categories: numbers, special characters, upper case letters and lower-case letters.

Strong Level: 8~16 characters. Numbers, special characters, upper case letters and lower-case letters must be included.

For your account security, it is recommended to set a strong password and change your password regularly.

HTTP Authentication: Basic or Token is selectable.

5.7 Maintenance Configuration

5.7.1 Backup and Restore

Go to Config→Maintenance→Backup & Restore.

- **Import & Export Settings**

Configuration settings of the camera can be exported form a camera into another camera.

1. Click “Browse” to select the save path for import or export information on the PC.
2. Click the “Import Setting” or “Export Setting” button.

- **Default Settings**

Click the “Load Default” button to restore all system settings to factory default, except the Image settings (see 5.2 Image Configuration for details) you want to keep.

5.7.2 Reboot

Go to Config→Maintenance→Reboot.

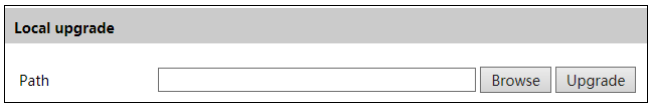
Click the “Reboot” button to reboot the device.

Timed Reboot Setting:

If necessary, the camera can be set up to reboot on a time interval. Enable “Time Settings”, set the date and time and then click the “Save” button to save the settings.

5.7.3 Upgrade

Go to Config→Maintenance→Upgrade. In this interface, the camera firmware can be updated.



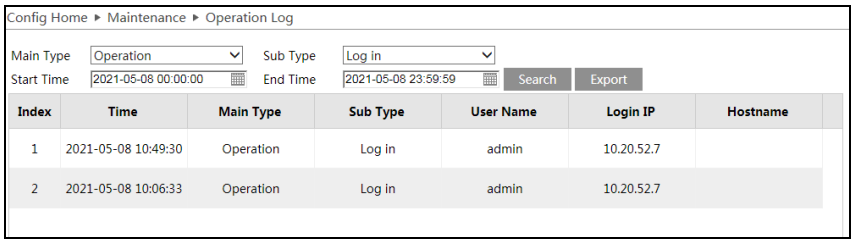
1. Click the “Browse” button to select the save path of the upgrade file
2. Click the “Upgrade” button to start upgrading the firmware.
3. The device will restart automatically.

Caution! Do not close the browser or disconnect the camera from the network during the upgrade.

5.7.4 Operation Log

To query and export log:

1. Go to Config→Maintenance→Operation Log.



2. Select the main type, sub type, start and end time.
3. Click “Search” to view the operation log.
4. Click “Export” to export the operation log.

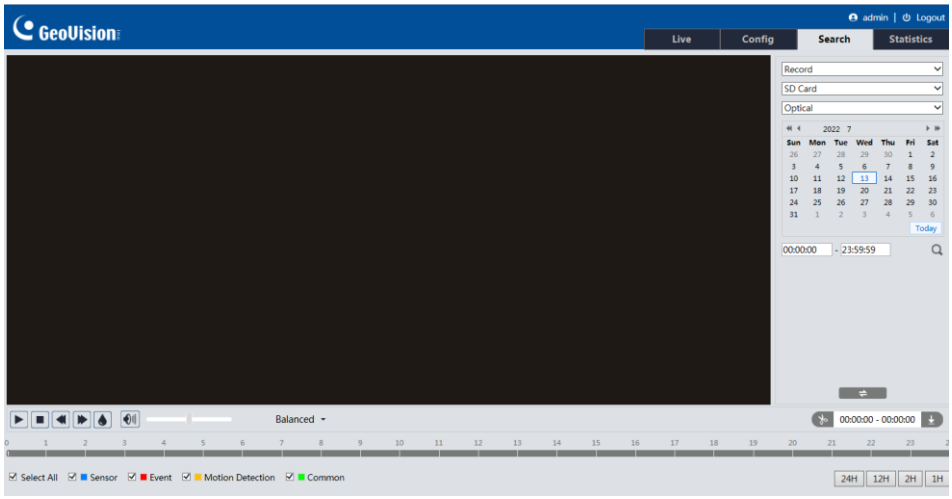
Chapter 6 Search

6.1 Image Search

Click Search to go to the interface as shown below. Images that are saved on the SD card or saved locally to the PC can be found here.

- **Local Image Search**

1. Choose “Picture” > “Local”.



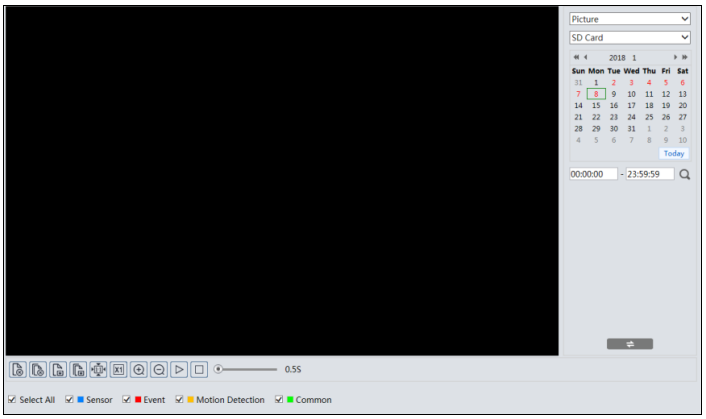
2. Set time: Select date and choose the start and end time.
3. Click to search the images.
4. Double click a filename in the list to view the captured photos as shown below.

Click to return to the previous interface.

Note: When using the plug-in free browser, the local images cannot be searched.

- **SD Card Image Search**

1. Choose “Picture” > “SD Card”.



2. Set time: Select date and choose the start and end time.
3. Choose the alarm events at the bottom of the interface.
4. Click to search the images.
5. Double click a file name in the list to view the captured photos.

Click to return to the previous interface.

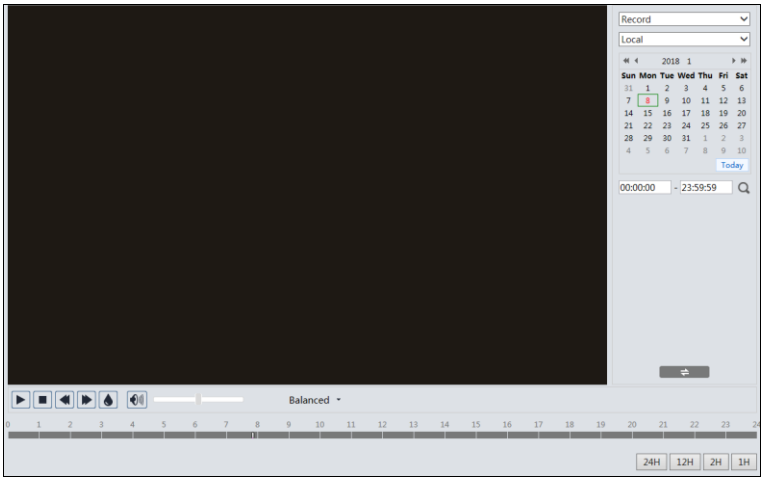
The descriptions of the buttons are shown as follows.

Icon	Description	Icon	Description
	Close: Select an image and click this button to close the image.		Close all: Click this button to close all images.
	Save: Click this button to select the path for saving the image on the PC.		Save all: Click this button to select the path for saving all pictures on the PC.
	Fit size: Click to fit the image on the screen.		Actual size: Click this button to display the actual size of the image.
	Zoom in: Click this button to digitally zoom in.		Zoom out: Click this button to digitally zoom out.
	Slide show play: Click this button to start the slide show mode.		Stop: Click this button to stop the slide show.
5.5S	Play speed: Play speed of the slide show.		

6.2 Video Search

6.2.1 Local Video Search

Click Search to go to the interface as shown below. Videos were recorded locally to the PC can be played in this interface.



1. Choose “Record” > “Local”.
2. Set search time: Select the date and choose the start and end time.
3. Click to search the images.
4. Double click on a file name in the list to start playback.

Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button
	Stop button		Speed down

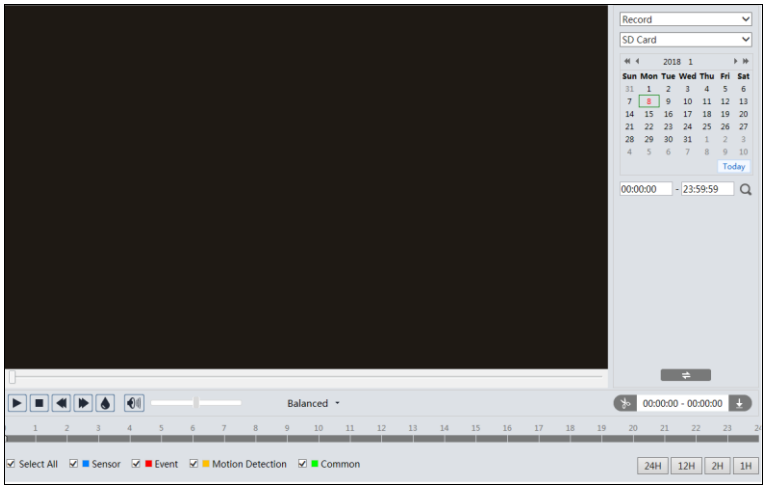
Icon	Description	Icon	Description
	Speed up		Watermark display
	Enable / disable audio; drag the slider to adjust the volume after enabling audio.		

Note: When using the plug-in free browser, the local videos cannot be searched.

6.2.2 SD Card Video Search

Click Search to go to the interface as shown below. Videos that were recorded on the SD card can be played in this interface.

1. Choose “Record” > “SD Card”.
2. Set search time: Select the date and choose the start and end time.
3. Click to search the images.



4. Select the alarm events at the bottom of the interface.
5. Select mix stream (video and audio stream) or video stream as needed.

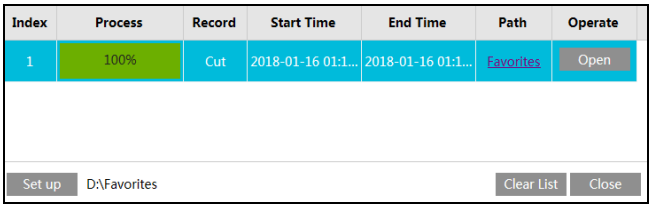
6. Double click on a file name in the list to start playback.

Note: and cannot be displayed when videos are played via the plug-in free browser.

The time table can be shown in 24H/12H/2H/1H format by clicking the corresponding buttons.

Video clip and downloading

1. Search the video files according to the above-mentioned steps.
2. Select the start time by clicking on the time table.
3. Click to set the start time and then this button turns blue ( ).
4. Select the end time by clicking on the time table. Then click to set the end time.
5. Click to download the video file in the PC.



Click “Set up” to set the storage directory of the video files.

Click “Open” to play the video.

Click “Clear List” to clear the downloading list.

Click “Close” to close the downloading window.

Integration with GV-VMS

For how to connect to GV-VMS, see *GV-TMBE5800 Quick Start Guide*.

Note: It is only supported by GV-VMS V17.4.5 / V18.3.1 with patch files or later versions.

Appendix

Appendix 1 Troubleshooting

How to find the password?

Click “Forget Password” and then answer the security questions to reset the password.

Fail to connect devices through IE browser.

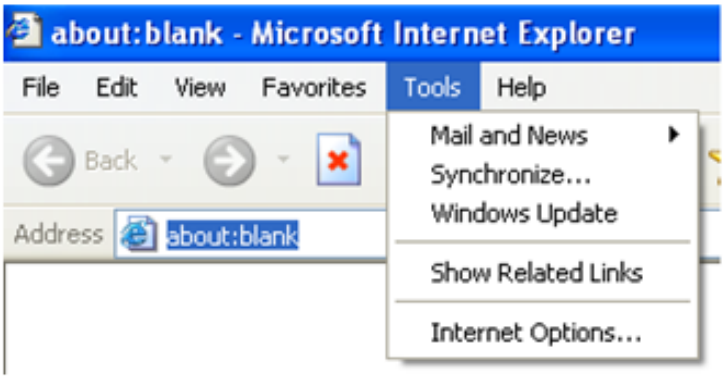
A. Network is not well connected. Check the connection and make sure it is connected well.
B. IP address is not available. Reset the IP address.
C. Web port number has been changed: contact administrator to get the correct port number.
D. Exclude the above reasons. Restore to default setting by IP-Tool.

IP tool cannot search devices.

It may be caused by the anti-virus software in your computer. Please exit it and try to search device again.

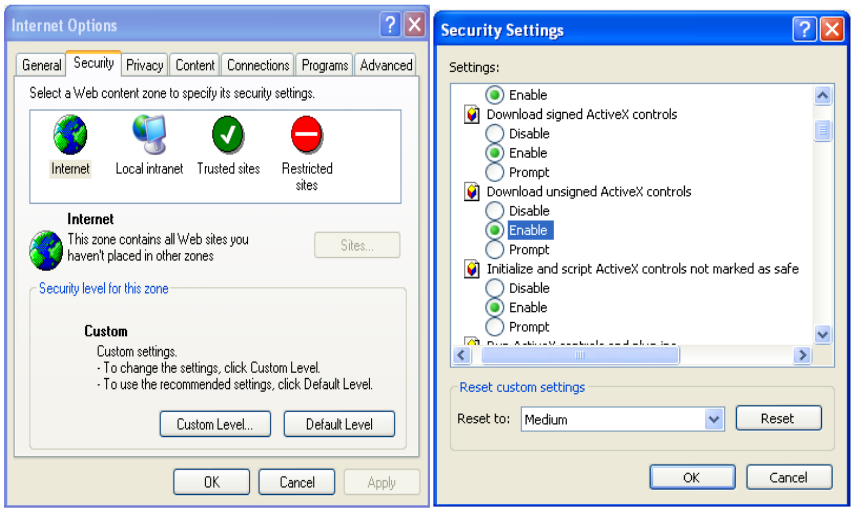
IE cannot download ActiveX control.

A. IE browser may be set up to block ActiveX. Follow the steps below.
   1. Open IE browser and then click Tools-----Internet Options.



   2. Select Security------Custom Level….
   3. Enable all the options under “ActiveX controls and plug-ins”.
   4. Click OK to finish setup.

B. Other plug-ins or anti-virus blocks ActiveX. Please uninstall or close them.



No sound can be heard.

A. Audio input device is not connected. Please connect and try again.

B. Audio function is not enabled at the corresponding channel. Please enable this function.

Appendix 2 Common Material Emissivity

Material	Emissivity	Material	Emissivity
Human Skin	0.98	Brick	0.95
Printed Circuit Board	0.91	Sand	0.90
Concrete	0.95	Soil	0.92
Ceramic	0.92	Cloth	0.98
Rubber	0.95	Hard Paperboard	0.90
Paint	0.93	White Paper	0.90
Wood	0.85	Water	0.96
Pitch	0.96	Flame	0.2~0.3

The material emissivity is also affected by the surface of the material.

Material Surface	Emissivity
Rough	0.95
Slightly Rough	0.8
Slightly Smooth	0.6
Smooth	0.3