

GV-BX2802, BX4802

User's Manual





© 2023 GeoVision, Inc. All rights reserved.

Under the copyright laws, this manual may not be copied, in whole or in part, without the written consent of GeoVision.

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>

Trademarks used in this manual: *GeoVision*, the *GeoVision* logo and *GV* series products are trademarks of GeoVision, Inc. *Windows* is the registered trademark of Microsoft Corporation.

June 2023

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



[Warranty]



[Technical Support Policy]

Safety Instruction

- 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 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 in case 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.
- This manual is suitable for face detection network cameras.

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 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

1. FCC compliance

The products have been tested and found in compliance with the council FCC rules and regulations part 15 subpart B. These limits are designed to provide reasonable protection against harmful interference. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. The user will be required to correct the interface at his own expense in case the harmful interference occurs.

2. FCC conditions:

Operation of this product is subject the following two conditions: (1) this device may not cause harmful interface, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CE Information

 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.

Contents

Safety Instruction	1
Contents	1
Chapter 1 Introduction	1
1.1 GV-BX2802	1
1.2 GV-BX4802	1
Chapter 2 Network Connection	2
2.1 LAN	2
2.1.1 Access through IP-Tool	2
2.1.2 Directly Access through IE	4
2.2 WAN	6
Chapter 3 Live View	8
Chapter 4 Network Camera Configuration	10
4.1 System Configuration	10
4.1.1 Basic Information	10
4.1.2 Date and Time	10
4.1.3 Local Config	11
4.1.4 Storage	12
4.2 Image Configuration	14
4.2.1 Display Configuration	14
4.2.2 Video / Audio Configuration	16
4.2.3 OSD Configuration	18
4.2.4 Video Mask	18
4.2.5 ROI Configuration	19
4.2.6 Lens Control	20
4.3 PTZ Configuration	20
4.4 Alarm Configuration	21
4.4.1 Motion Detection	21
4.4.2 Other Alarms	22
4.4.3 Alarm In	24
4.4.4 Alarm Out	25
4.4.5 Alarm Server	26
4.5 Event Configuration	27
4.5.1 Object Abandoned / Missing	27
4.5.2 Video Exception	29
4.5.3 Line Crossing	30
4.5.4 Region Entrance	32
4.5.5 Region Exiting	34
4.5.6 Target Counting by Line	35
4.5.7 Target Counting by Area	38
4.5.8 Region Intrusion	40
4.5.9 Crowd Density	42
4.5.10 Face Detection	44
4.5.11 Heat Map	46
4.6 Network Configuration	48
4.6.1 TCP/IP	48
4.6.2 Port	49
4.6.3 DDNS	49
4.6.4 SNMP	50
4.6.5 802.1x	52
4.6.6 RTSP	52
4.6.7 RTMP	53
4.6.8 UPNP	54
4.6.9 Email	54
4.6.10 FTP	55
4.6.11 HTTP POST	56
4.6.12 HTTPS	57

4.6.13	QoS.....	58
4.7	Security Configuration	59
4.7.1	User Configuration	59
4.7.2	Online User	61
4.7.3	Block and Allow Lists	61
4.7.4	Security Management.....	61
4.8	Maintenance Configuration	63
4.8.1	Backup and Restore	63
4.8.2	Reboot	63
4.8.3	Upgrade.....	64
4.8.4	Operation Log.....	64
Chapter 5	Search.....	65
5.1	Image Search.....	65
5.2	Video Search	67
5.2.1	Local Video Search.....	67
5.2.2	SD Card Video Search	68
Appendix	70
Appendix 1	Troubleshooting	70
Appendix 2	Configuration Requirements and Surrounding Area	72

Chapter 1 Introduction

1.1 GV-BX2802

Main Features

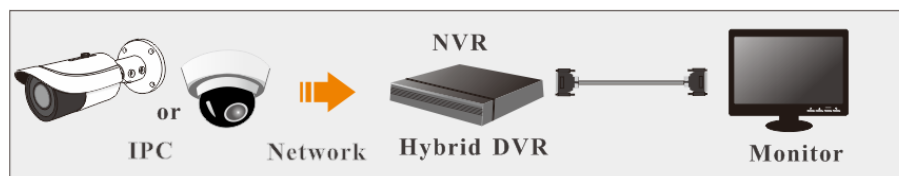
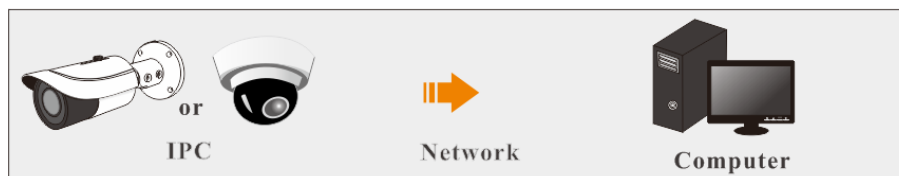
- IR auto switch, true day/night
- 3D DNR, WDR Pro
- BLC, Defog, Anti-flicker, corridor pattern
- ROI coding
- Face detection, line crossing / region intrusion / region entrance / region exiting (human / vehicle classification), video exception detection, heat map, crowd density, target counting, etc.

1.2 GV-BX4802

Main Features

- IR auto switch, true day/night
- 3D DNR, WDR Pro
- BLC, Defog, Anti-flicker, HFR mode, corridor pattern
- ROI coding
- Face detection, line crossing / region intrusion / region entrance / region exiting (human / vehicle classification), video exception detection, heat map, target counting, etc.

Surveillance Application



Chapter 2 Network Connection

System Requirement

For proper operation of the product, the following requirements should be met for your computer.

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 the applicable plug-in will display more functions of the camera.

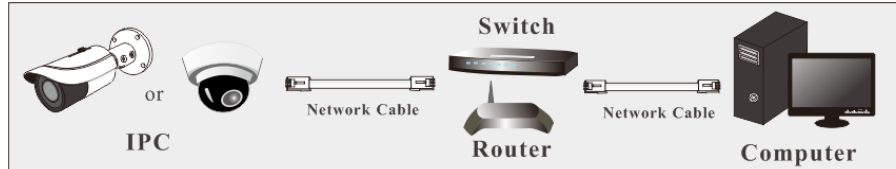
Connect IP-Cam via LAN or WAN. Here only take IE browser for example. The details are as follows:

2.1 LAN


In LAN, there are two ways to access IP-Cam: 1. access through GV-IP Device Utility (V8.9.8 or later); 2. directly access through IE browser.

2.1.1 Access through IP-Tool

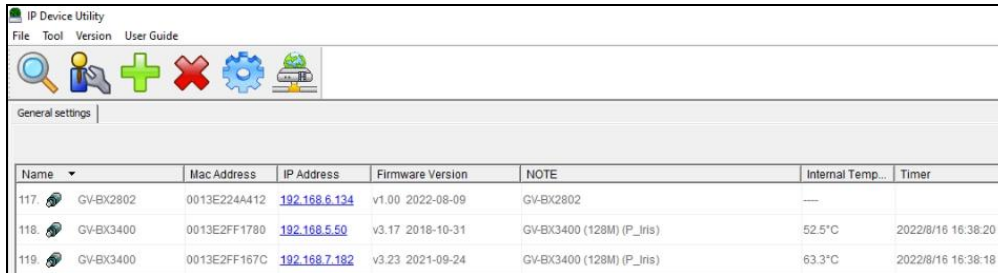
Network connection:



By default, when the camera is connected to LAN 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 accessed IP address to log in from its Web interface.

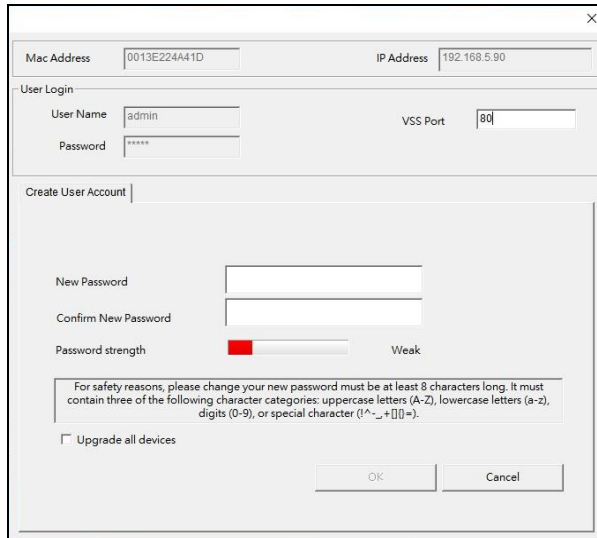
1. Make sure the PC and the camera are connected to the LAN, and **GV-IP Device Utility** (V8.9.8 or later) is installed on the PC from our [website](#).
2. On GV-IP Device Utility window, click the  button to search for the IP devices in the same LAN. Click the **Name** or **Mac Address** column to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

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



Name	Mac Address	IP Address	Firmware Version	NOTE	Internal Temp...	Timer
117. GV-BX2802	0013E224A412	192.168.6.134	v1.00 2022-08-09	GV-BX2802	---	
118. GV-BX3400	0013E2FF1780	192.168.5.50	v3.17 2018-10-31	GV-BX3400 (128M) (P_Iris)	52.5°C	2022/8/16 16:38:20
119. GV-BX3400	0013E2FF167C	192.168.7.182	v3.23 2021-09-24	GV-BX3400 (128M) (P_Iris)	63.3°C	2022/8/16 16:38:18

- For first-time users, you are requested to create a password.



Mac Address: 0013E224A41D IP Address: 192.168.5.90

User Login

User Name: admin VSS Port: 80

Password: *****

Create User Account

New Password:

Confirm New Password:

Password strength: ■ Weak

For safety reasons, please change your new password must be at least 8 characters long. It must contain three of the following character categories: uppercase letters (A-Z), lowercase letters (a-z), digits (0-9), or special character (!^_+[]{}~).

Upgrade all devices

OK Cancel

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

IMPORTANT:

- By default, the Administrator's username is **admin** and cannot be modified.
 - To change the password using GV-IP Device Utility, click on the camera's IP address, and select **Configure > Change Password**. Or you can optionally change the password on the camera's Web interface by clicking **Config→Security→User**; see "Modify User" in *4.7.1 Security Configuration*.
-

2.1.2 Directly Access through IE

The default network settings are as shown below:

IP address: **192.168.0.10**

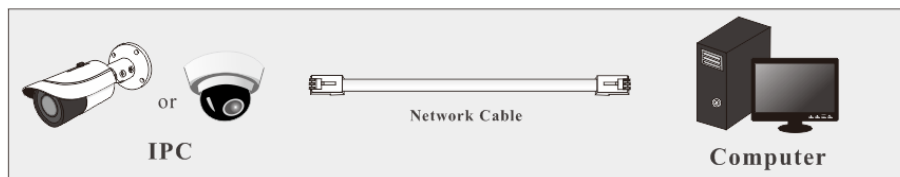
Subnet Mask: **255.255.255.0**

Gateway: **192.168.226.1**

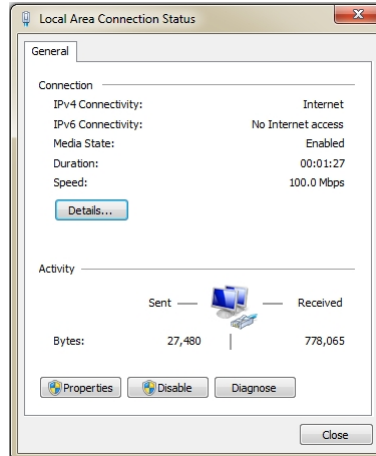
HTTP: **80**

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.

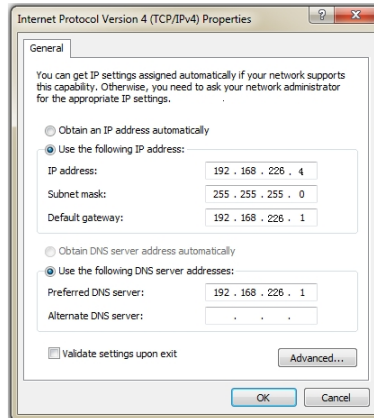


1. Manually set the IP address of the PC and the network segment should be the same as the default settings of the IP camera. Open the network and share center. Click “Local Area Connection” to pop up the following window.



2. Select “Properties” and then select internet protocol according to the actual situation (for example: IPv4).

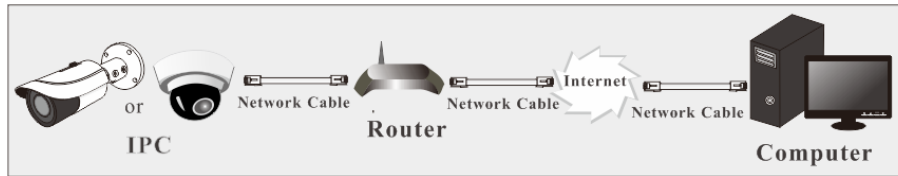
3. Next, click the “Properties” button to set the network of the PC.



4. Open the Web browser and enter the default address of the IP-camera.
5. Follow directions to download and install the plug-in.
6. Enter the default username and password on the login page and click “Login”.

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
<input type="radio"/> Obtain an IP address automatically <input checked="" type="radio"/> 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".

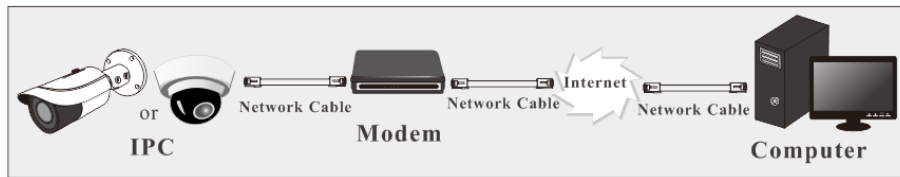
Port Range					
Application	Start	End	Protocol	IP Address	Enable
1	9007	to 9008	Both	192.168.1.201	<input checked="" type="checkbox"/>
2	80	to 81	Both	192.168.1.201	<input checked="" type="checkbox"/>
3	10000	to 10001	Both	192.168.1.166	<input type="checkbox"/>
4	21000	to 21001	Both	192.168.1.166	<input type="checkbox"/>

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:

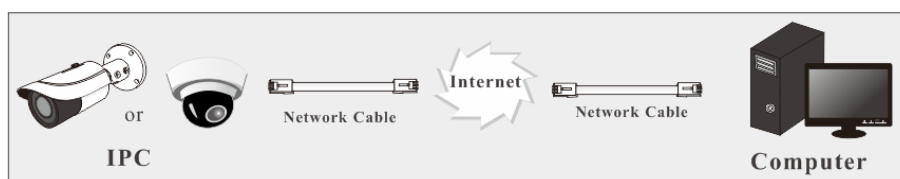
1. Go to Config→Network→Port menu to set the port number.
2. Go to Config →Network→TCP/IP→PPPoE Config menu. Enable PPPoE and then enter the user name and password from your internet service provider.

IPv4	IPv6	PPPoE Config	IP Change Notification Config
<input checked="" type="checkbox"/> Enable			
User Name		xxxxxxx	
Password		●●●●●	
<input type="button" value="Save"/>			

3. Go to Config →Network→DDNS menu. Before configuring the DDNS, please apply for a domain name first. Please refer to DDNS 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

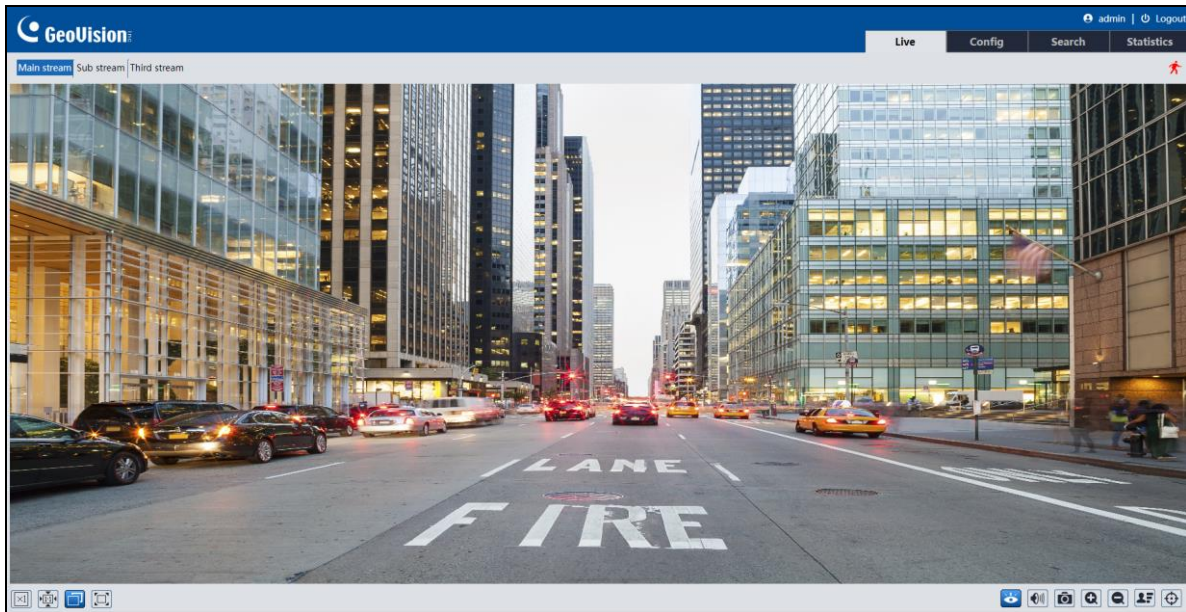


The setup steps are as follow:






























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.

























The following table is the instructions of the icons on the live view interface.




Icon	Description	Icon	Description
	Original size		Sensor alarm indicator
	Fit correct scale		Motion alarm indicator
	Adapt		Color abnormal indicator
	Full screen		Abnormal clarity indicator
	Start/stop live view		Scene change indicator
	Start/stop two-way audio		Line Crossing indicator
	Enable/disable audio		Region Intrusion indicator
	Snapshot		Region Entrance indicator
	Start/stop local recording		Region Exiting indicator
	Zoom in		Face detection indicator
	Zoom out		Target Counting by Line indicator
	PTZ control		Target Counting by Area indicator
	Face Detection		Object detection indicator (object Abandoned/Missing)
	Rule information display		Heat map indicator
	SD card recording indicator		

Note: PTZ control, two-way audio, local recording, and the preview mode switch (real-time / balanced / fluent mode) are not supported in plug-in free live view:


Some cameras can be installed in a compatible external PTZ enclosure through RS485. Click the PTZ icon to reveal the PTZ control panel.

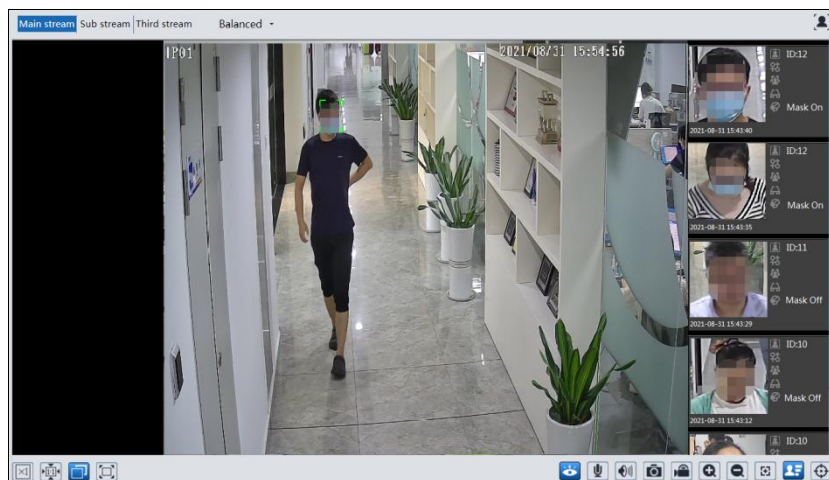
The descriptions of the control panel are as follows:

Icon	Description	Icon	Description
	Move upper left direction		Move upper right direction
	Move up		Stop movement
	Move left		Move right
	Move lower left direction		Move lower right direction
	Move down		Speed adjustment
	Zoom out		Zoom in
	Focus -		Focus +
	Iris -		Iris +
	Auto scan		Wiper
	Light		Radom scan
	Group scan		Preset

Select preset and click  to call the preset. Select and set the preset and then click  to save the position of the preset. Select the set preset and click  to delete it

Face Capture View

1. Go to Config→Event→Face Detection interface. Check “Enable”.
2. Return to the live view interface. Click  to go to the following interface. When there are faces detected, the face pictures will be listed on the right.



Chapter 4 Network Camera Configuration

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

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

4.1 System Configuration

4.1.1 Basic Information

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

Device name	Camera
Product Model	GV-BX2802
Brand	GeoVision
Software Version	5.1.1.0(35754)
Firmware Version	V100_2022_08_09
Software Build Date	2022-08-09
Onvif Version	21.06
MAC	00:13:e2:24:a4:12
About this machine	View
Privacy Statement	View
Open source statement	View

4.1.2 Date and Time

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

Zone
Date and Time

Zone
GMT (Dublin, Lisbon, London, Reykjavik) ▼

DST

Auto DST

Manual DST

Start Time
January ▼
First ▼
Sunday ▼
00 ▼
Hour

End Time
February ▼
First ▼
Monday ▼
00 ▼
Hour

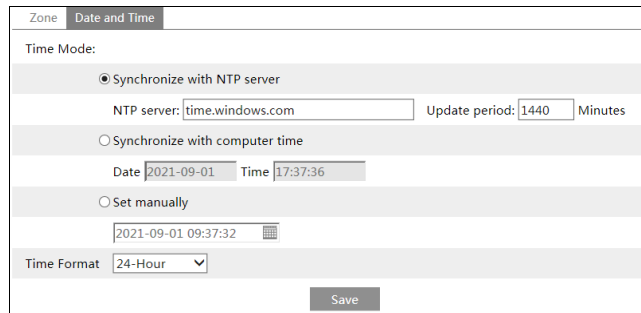
Time Offset
120 Minutes ▼

Save

Select the time zone and DST as required.

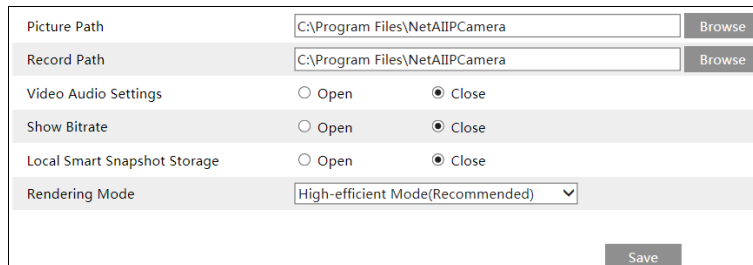
Note: The time zone of the camera and the computer must be the same. It is recommended to modify the time zone of the camera according to the time zone of the computer. If the time zone of the computer is modified, the current web client needs to be closed. Then re-open it and log in again.

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



4.1.3 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 entrance, etc.) will be saved to the local PC.

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

Note:

1. If the performance of your computer is not compatible with the IE client or your computer has no graphics card, low-efficient mode is suggested.
 2. When you access your camera by the web browser without the plug-in, only Show Bitrate can be set in the above interface.
-

4.1.4 Storage

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

Management	Record	Snapshot
Total picture capacity	379 MB	
Picture remaining space	379 MB	
Total recording capacity	3329 MB	
Record remaining space	2816 MB	
State	Normal	
Snapshot Quota	10 %	
Video Quota	90 %	
Changes in the quota ratio need to be formatted before they become effective.		
<input type="button" value="Eject"/> <input type="button" value="Format"/>		

- **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.

4.1.4.1 Schedule Recording Settings

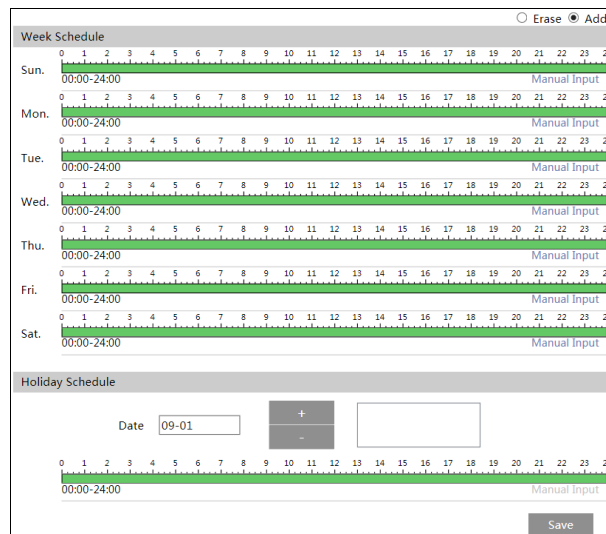
Go to Config→System→Storage→Record to go to the interface as shown below.

Management	Record	Snapshot
Record Parameters		
Record Stream	Main	
Pre Record Time	No Pre Record (H264,H265,MJPEG)	
Cycle Write	Yes	
Timing		
<input checked="" type="checkbox"/> Enable Schedule Record		

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

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

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 enter specific start and end times. This adds more granularities (minutes).

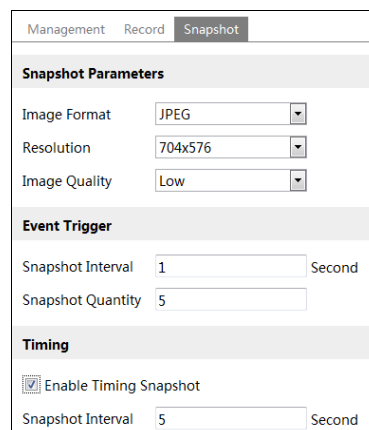
Holiday Schedule

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

Note: Holiday schedule takes priority over weekly schedule.

4.1.4.2 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.

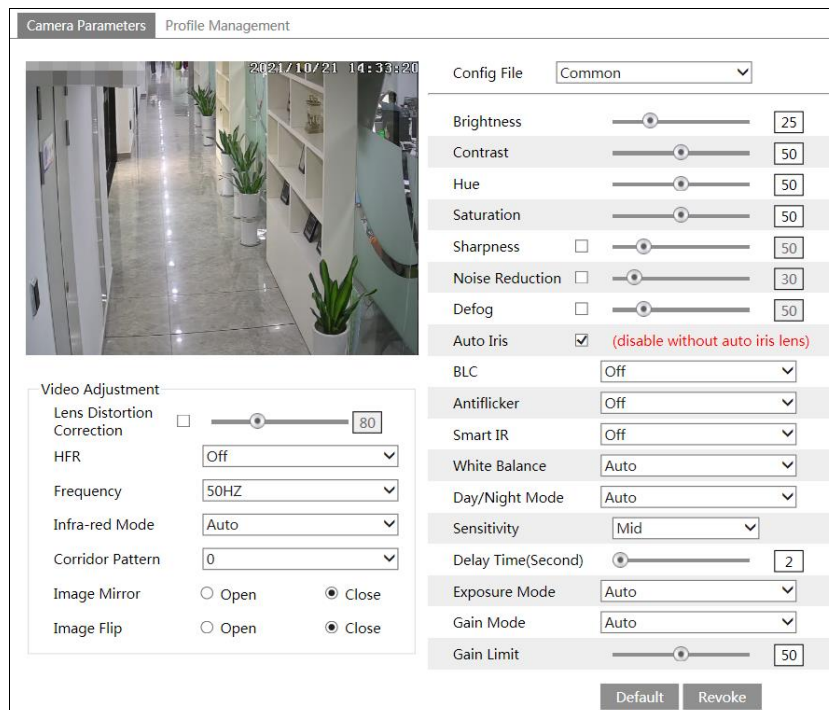
Snapshot Timing

Check the box for “Enable Timing Snapshot” first and set the snapshot interval and schedule. The setup steps of schedule are the same as the schedule recording (See [4.1.4.1 Schedule Recording Settings](#)).

4.2 Image Configuration

4.2.1 Display Configuration

Go to Image→Display Settings 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.

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.

Auto Iris: If your camera is equipped with auto Iris lens, please enable it.

Backlight Compensation (BLC):

- Off: Disables the backlight compensation function. It is the default mode.
- HWDR: 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.
- 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.

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

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.

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

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

Shutter 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.

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.

Frequency: 50Hz and 60Hz can be optional.

HFR: High Frame Rate. If "ON" is selected, the system will restart and the maximum value of the frame rate of the main stream can be set to 60 fps / 50 fps.

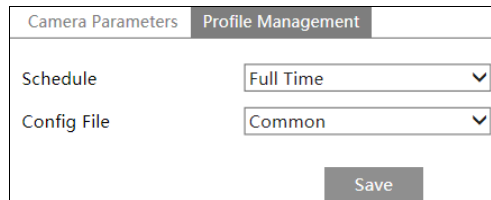
Corridor Pattern: Corridor viewing modes can be used for situations such as long hallways. 0, 90, 180 and 270 are available. The default value is 0.

Image Mirror: Turn the current video image horizontally.

Image Flip: Turn the current video image vertically.

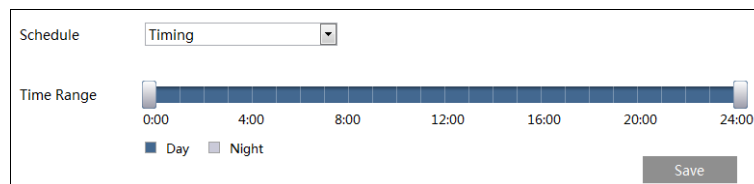
Schedule Settings of Image Parameters

Click the “Profile Management” tab as shown below.



The screenshot shows the 'Profile Management' tab with two dropdown menus: 'Schedule' set to 'Full Time' and 'Config File' set to 'Common'. A 'Save' button is located at the bottom right.

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

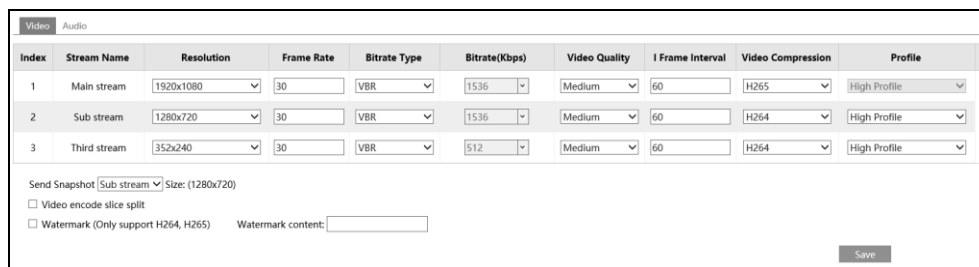


The screenshot shows the 'Timing' schedule configuration. It features a 'Schedule' dropdown set to 'Timing' and a 'Time Range' slider from 0:00 to 24:00. The slider is divided into 'Day' (blue) and 'Night' (grey) segments. A 'Save' button is at the bottom right.

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.

4.2.2 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.



The screenshot shows the 'Video / Audio' configuration interface. It contains a table with columns for Index, Stream Name, Resolution, Frame Rate, Bitrate Type, Bitrate(Kbps), Video Quality, I Frame Interval, Video Compression, and Profile. Below the table are options for 'Send Snapshot', 'Video encode slice split', and 'Watermark'.

Index	Stream Name	Resolution	Frame Rate	Bitrate Type	Bitrate(Kbps)	Video Quality	I Frame Interval	Video Compression	Profile
1	Main stream	1920x1080	30	VBR	1536	Medium	60	H265	High Profile
2	Sub stream	1280x720	30	VBR	1536	Medium	60	H264	High Profile
3	Third stream	352x240	30	VBR	512	Medium	60	H264	High Profile

Send Snapshot (Sub stream) Size: (1280x720)
 Video encode slice split
 Watermark (Only support H264, H265) Watermark content:

Three video streams can be adjustable.

Resolution: The size of image.

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

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 bitrate type is set to CBR. The higher the bitrate, the better the image quality will be.

Video Quality: It can be adjusted when the bitrate type 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: MJPEG, H264+, H264, H265 or H265+ are applicable. MJPEG is not available for main stream. If H.265 / H.265+ is chosen, make sure the client system is able to decode H.265 / H.265+. Compared to H.265, H.265+ saves more storage space with the same maximum bitrate in most scenes. Compared to H.264, H.265 reduces the transmission bitrate under the same resolution, frame rate and image quality.

Note: For plug-in free live view, MJPEG is not recommended (if the sub / third stream and MJPEG are selected, no image will be output).

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.



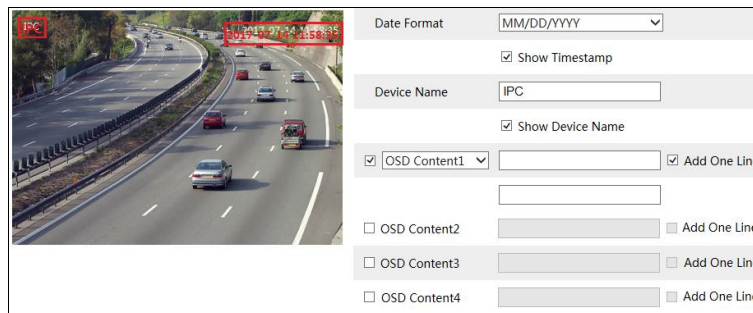
The screenshot shows a configuration window with two tabs: "Video" and "Audio". The "Audio" tab is selected. Inside the window, there is a checked checkbox labeled "Enable". Below it, there are two dropdown menus: "Audio Encoding" with "G711A" selected, and "Audio Type" with "MIC" selected. A "Save" button is located at the bottom right of the configuration area.

Audio Encoding: G711A and G711U are selectable.

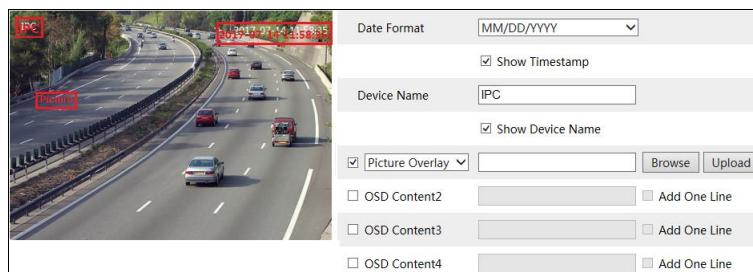
Audio Type: LINE or MIC can be optional.

4.2.3 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.

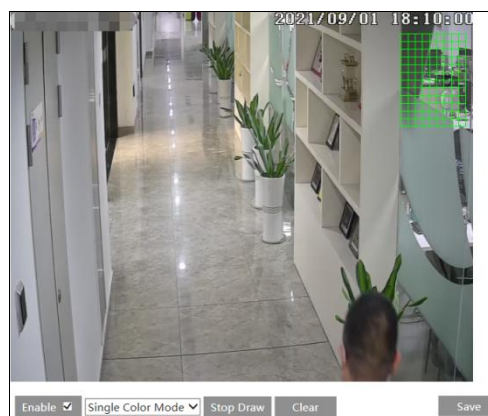


Picture Overlay Settings:

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.

4.2.4 Video Mask

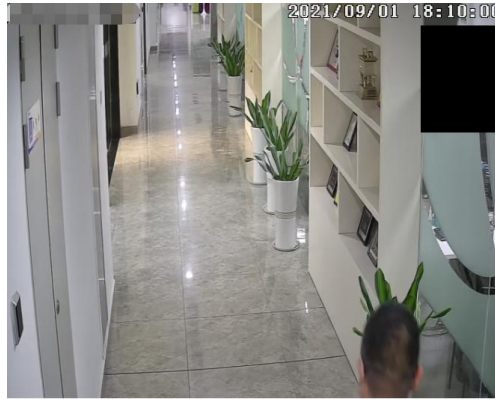
Go to Image→Video Mask interface as shown below. A maximum of 4 zones can be set up.



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 have been drawn as shown as blocked out in the image.

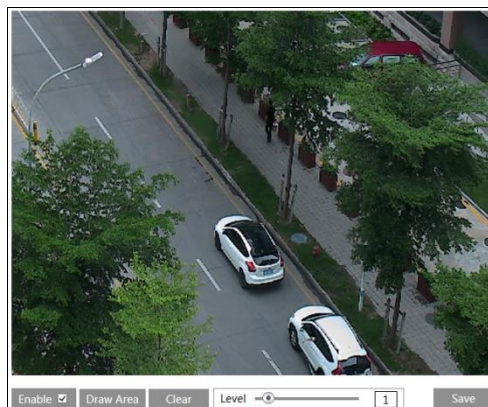


To clear the video mask:

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

4.2.5 ROI Configuration

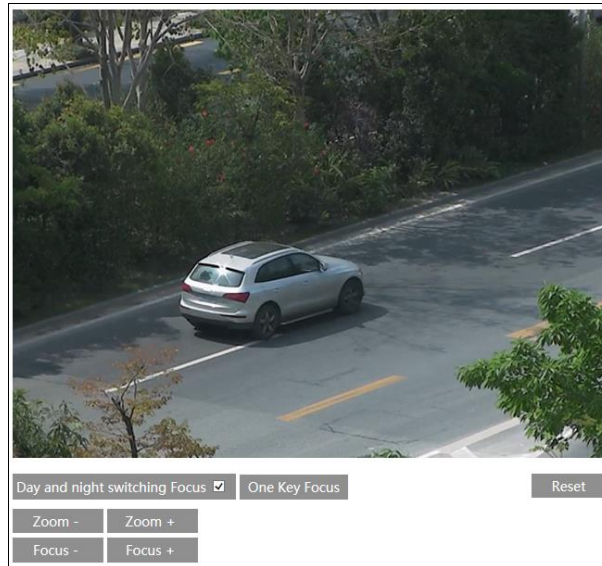
Go to Image→ROI Config interface as shown below. An area in the image can be set as a region of interest. This area will have a higher bitrate than the rest of the image, resulting in better image quality for the identified area.



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.

4.2.6 Lens Control

This function is only available for the model with motorized zoom lens. Within this section, zoom and focus can be controlled. If the image is out of focus after a manual adjustment, one key focus can be used to set the focus automatically. Go to Config→Image→Zoom/Focus interface to set.



4.3 PTZ Configuration

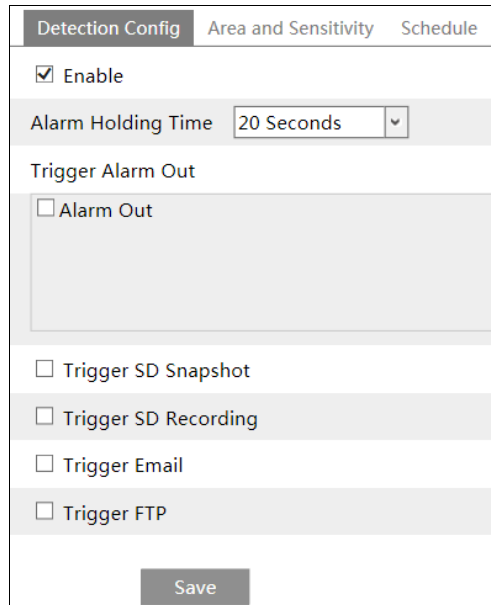
This function is only available for the model with RS485 interface. It can be used with a compatible external PTZ enclosure. Go to PTZ→Protocol interface as shown below.

Protocol	PELCOD ▾
Address	1
Baud-Rate	2400 ▾
Save	

4.4 Alarm Configuration

4.4.1 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 Holding Time: It refers to the interval time between the adjacent motion detections. For instance, if the alarm holding time is set to 20 seconds, once the camera detects a motion, it will go to alarm and would not detect any other motion in 20 seconds. If there is another motion detected during this period, it will be considered as continuous movement; otherwise, it will be considered as a single motion.

Alarm Out: If selected, this would trigger an external relay output that is connected to the camera on detecting a motion based alarm.

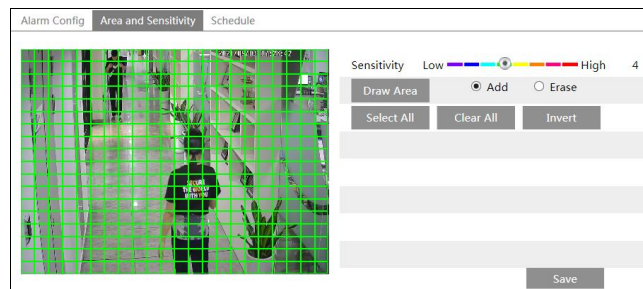
Trigger SD Snapshot: If selected, the system will capture images on motion detection and save the images on an SD card.

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 to the set addresses.

Trigger FTP: If “Trigger FTP” and “Attach Picture” are checked, the captured pictures will be sent into FTP server address. Please refer to [4.6.12 FTP](#) for more details.

- 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.

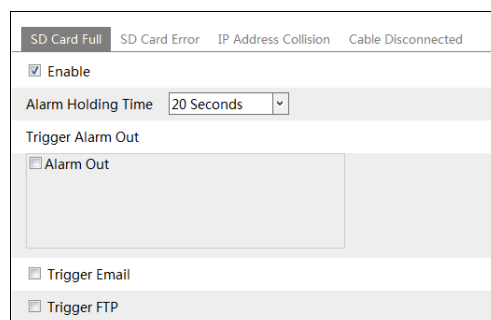
After that, click the “Save” to save the settings.

- Set the schedule for motion detection. The schedule setup steps of the motion detection are the same as the schedule recording setup (See [4.1.4.1 Schedule Recording Settings](#)).

4.4.2 Other Alarms

- SD Card Full**

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

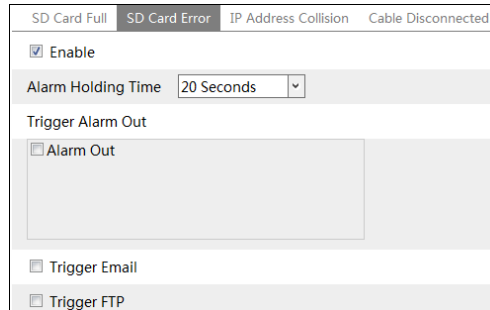


- Click “Enable”.
- Set the alarm holding time and alarm trigger options. The setup steps are the same as motion detection. Please refer to [4.4.1 Motion Detection](#) for details.

- **SD Card Error**

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

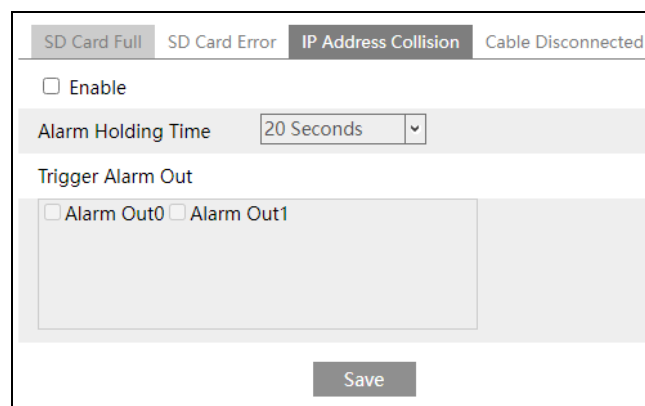
1. Go to Config→Alarm→Anomaly→SD Card Error as shown below.



2. Click “Enable”.
3. Set the alarm holding time and alarm trigger options. Trigger alarm out, Email and FTP. The setup steps are the same as motion detection. Please refer to [4.4.1 Motion Detection](#) for details.

- **IP Address Conflict**

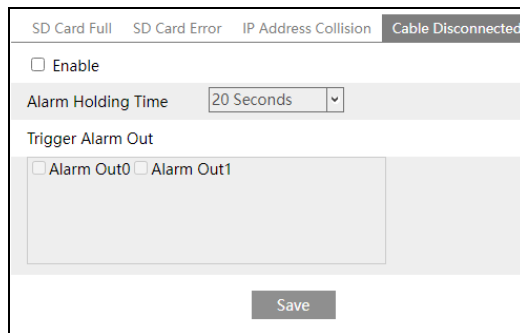
1. Go to Config→Alarm→Anomaly→IP Address Collision as shown below.



2. Click “Enable” 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.

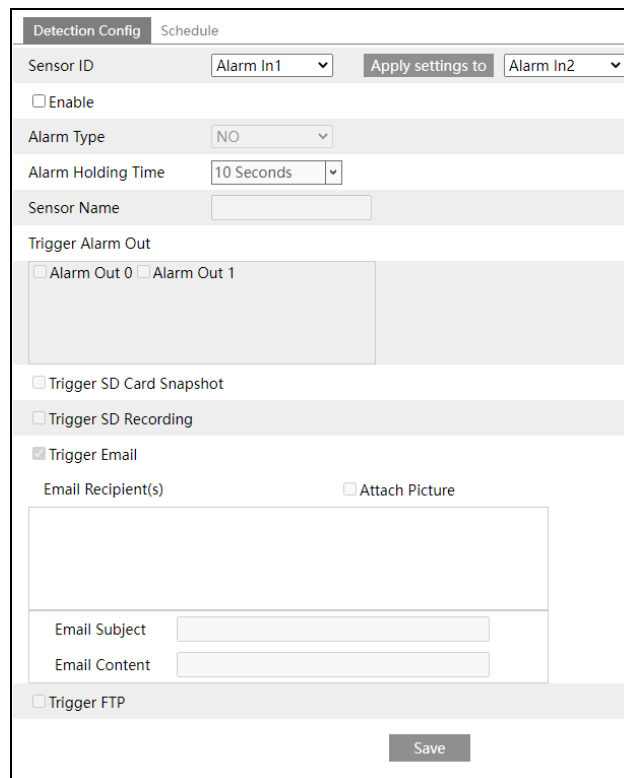


2. Click “Enable” and set the alarm holding time.
3. Trigger alarm out. When the camera is disconnected, the system will trigger the alarm out.

4.4.3 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 motion detection. Please refer to [4.4.1 Motion Detection](#) 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 [4.1.4.1 Schedule Recording Settings](#)).

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

4.4.4 Alarm Out

Go to Config→Alarm→Alarm Out.

Alarm Out Mode	Alarm Linkage	▼
Alarm Out Name	alarmOut1	
Alarm Holding Time	20 Seconds	▼
Alarm Type	NC	▼
Save		

Alarm Out ID: 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.

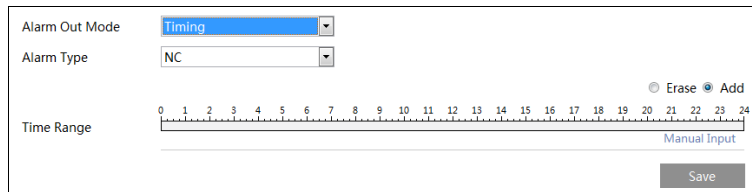
Manual Operation: Having selected this mode, select the alarm type and click “Open” to trigger the alarm out immediately; click “Close” to stop alarm.

Alarm Out Mode	Manual Operation	▼
Alarm Type	NC	▼
Manual Operation	Open	Close
Save		

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.

Alarm Out Mode	Day/night switch linkage	▼
Alarm Type	NC	▼
Day	Close	▼
Night	Close	▼

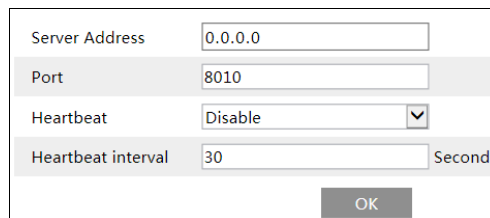
Timing: Select the alarm type. Then click “Add” and drag the mouse on the timeline to set the schedule of alarm out; click “Erase” and drag the mouse on the timeline to erase the set time schedule. After this schedule is saved, the alarm out will be triggered in the specified time.



4.4.5 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.



4.5 Event Configuration

For more accuracy, here are some recommendations for installation.

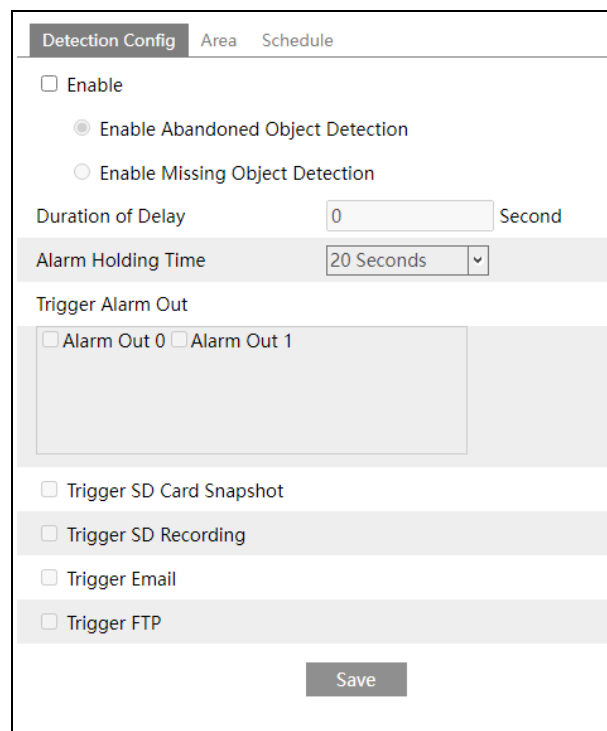
- Cameras should be installed on stable surfaces, as vibrations can affect the accuracy of detection.
- Avoid pointing the camera at the reflective surfaces (like shiny floors, mirrors, glass, lake surfaces and so on).
- Avoid places that are narrow or have too much shadowing.
- Avoid scenario where 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.

4.5.1 Object Abandoned / Missing

Alarms will be triggered when the objects are removed from or left at the pre-defined area.

To set abandoned/missing object detection:

Go to Config→Event→Object Abandoned/Missing interface as shown below.

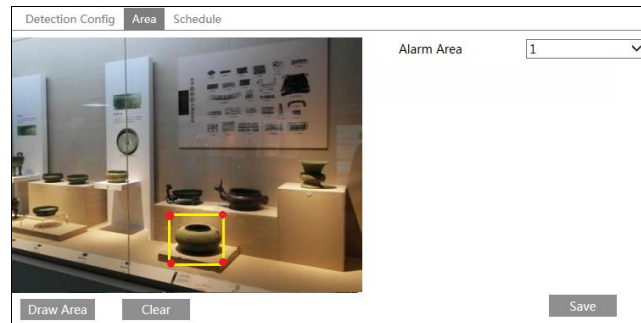


1. Enable abandoned/missing object detection and then select the detection type.

Enable Abandoned Object Detection: Alarms will be triggered if there are items left in the pre-defined area.

Enable Missing Object Detection: Alarms will be triggered if there are items missing in the pre-defined area.

2. Set the alarm holding time and alarm trigger options. The setup steps are the same as motion detection. Please refer to [4.4.1 Motion Detection](#) for details.
3. Click “Save” button to save the settings.
4. Set the alarm area of the abandoned/missing object detection. Click the “Area” tab to go to the interface as shown below.



Set the alarm area number and then enter the desired alarm area name. Only one alarm area 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 (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.

5. Set the schedule of the abandoned/missing object detection. The setup steps of schedule are the same as the schedule recording (See [4.1.4.1 Schedule Recording Settings](#)).

※ The configuration requirements of camera and surrounding areas

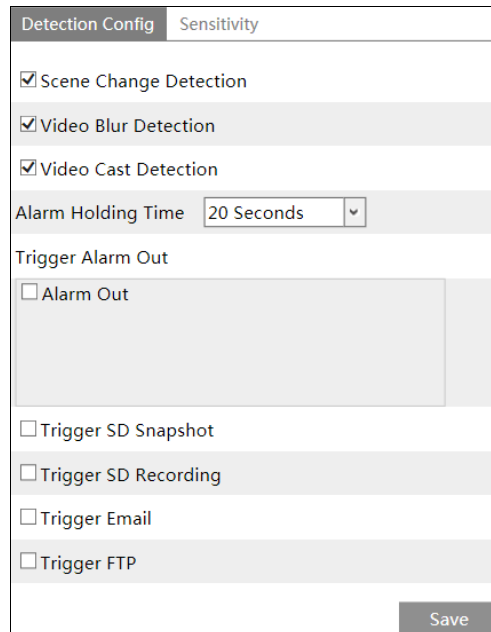
1. The range of the detection object should occupy from 1/50 to 1/3 of the entire image.
2. The detection time of objects in the camera shall be from 3 to 5 seconds.
3. The defined area cannot be covered frequently and continuously (like people and traffic flow).
4. It is necessary for abandoned/missing object detection that the drawn frame must be very close to the margin of the object in enhancing the sensitivity and accuracy of the detection.
5. Abandoned/missing object detection cannot determine the objects’ ownership. For instance, there is an unattended package in the station. Abandoned object detection can detect the package itself but it cannot determine to whom it belongs to.
6. Try not to enable abandoned/missing object detection when light changes greatly in the scene.
7. Try not to enable abandoned/missing object if there are complex and dynamic environments in the scene.
8. Adequate light and clear scenery are very important to abandoned/missing object detection.

4.5.2 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.



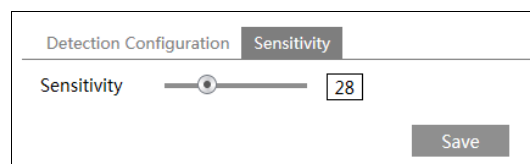
1. Enable the applicable detection that's desired.

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 [4.4.1 Motion Detection](#) 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.

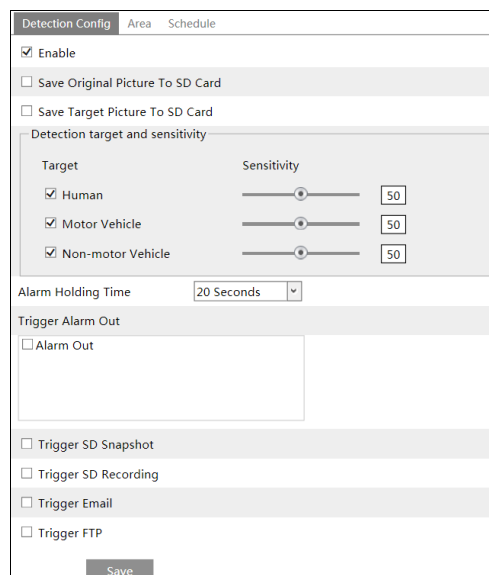
※ **The requirements of camera and surrounding area**

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.

4.5.3 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 alarm and select the snapshot type and the detection target.

Save Original Picture to SD Card: If it is enabled, the detected original 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.

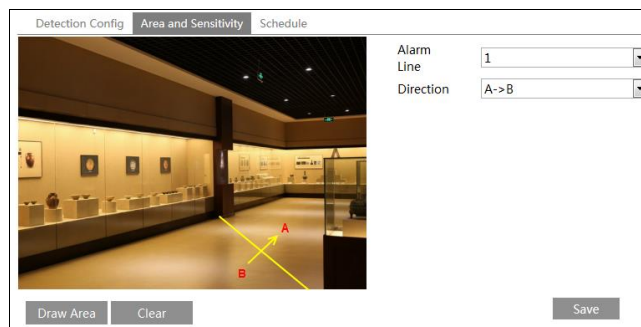
Detection Target:

- **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 motion detection. Please refer to [4.4.1 Motion Detection](#) 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 the intruder/vehicle crosses over the alarm line.

- **A<->B:** The alarm will be triggered when the intruder/vehicle crosses over the alarm line from B to A or from A to B.
- **A->B:** The alarm will be triggered when the intruder/vehicle crosses over the alarm line from A to B.
- **A<-B:** The alarm will be triggered when the intruder/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 [4.1.4.1 Schedule Recording Settings](#)).

※ Configuration of camera and surrounding area

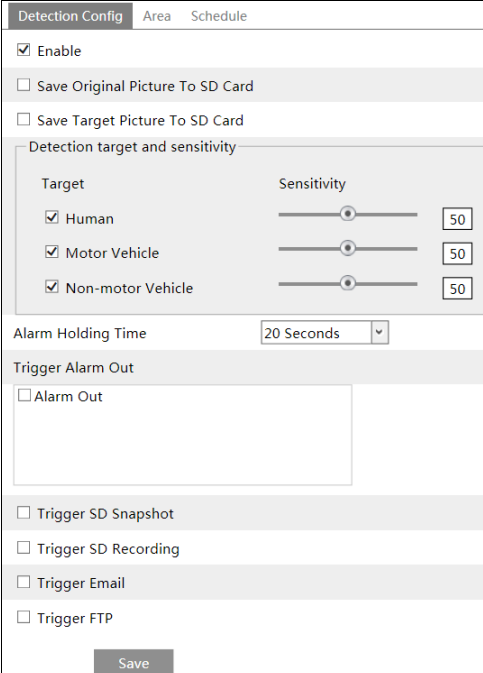
1. Auto-focusing function should not be enabled for line crossing detection.

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.

4.5.4 Region Entrance

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

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



1. Enable region entrance detection and select the snapshot type and the detection target.

Save Original Picture to SD Card: If it is enabled, the detected original pictures will be captured and saved to the SD card when the targets intrude into the pre-defined areas.

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 intrude into the pre-defined areas.

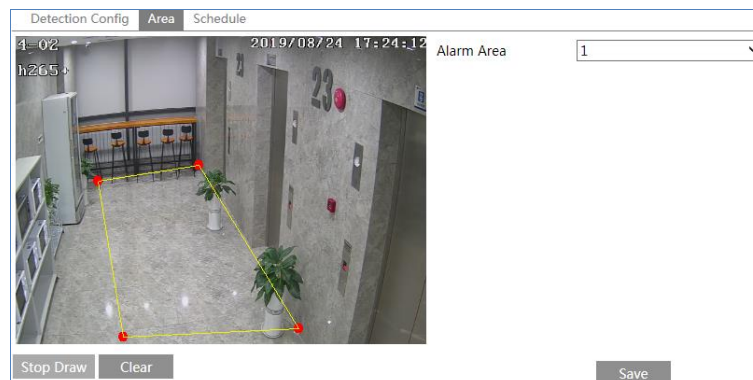
Note: To save snapshots to the local PC, please enable “Local Smart Snapshot Storage” in the local config interface first. To save snapshots to the SD card, please install an SD card first.

Detection Target:

- **Human:** Select it and then alarms will be triggered if someone intrudes into the pre-defined area.
- **Motor Vehicle:** Select it and then alarms will be triggered if a vehicle with four or more wheels (eg. a car, bus or truck) intrudes into the pre-defined area.
- **Non-motor Vehicle:** Select it and then alarms will be triggered if a vehicle with two wheels (eg. a motorcycle or bicycle) intrudes into the pre-defined area.

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 intrusion detection is enabled.

2. Set the alarm holding time and alarm trigger options.
3. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to [4.4.1 Motion Detection](#) for details.
4. Click the “Save” button to save the settings.
5. Set the alarm area of the region entrance 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.

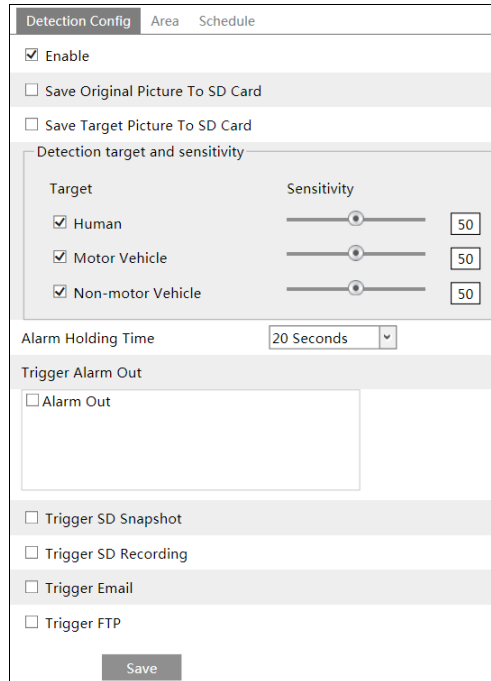
Click the “Draw Area” button and then click around the area where you want to set as the alarm area in the image on the left side (the alarm area should be a closed area). Click the “Stop Draw” button to stop drawing. Click the “Clear” button to delete the alarm area. Click the “Save” button to save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

6. Set the schedule of the region intrusion detection. The setup steps of the schedule are the same as schedule recording setup (See [4.1.4.1 Schedule Recording Settings](#)).

4.5.5 Region Exiting

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

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



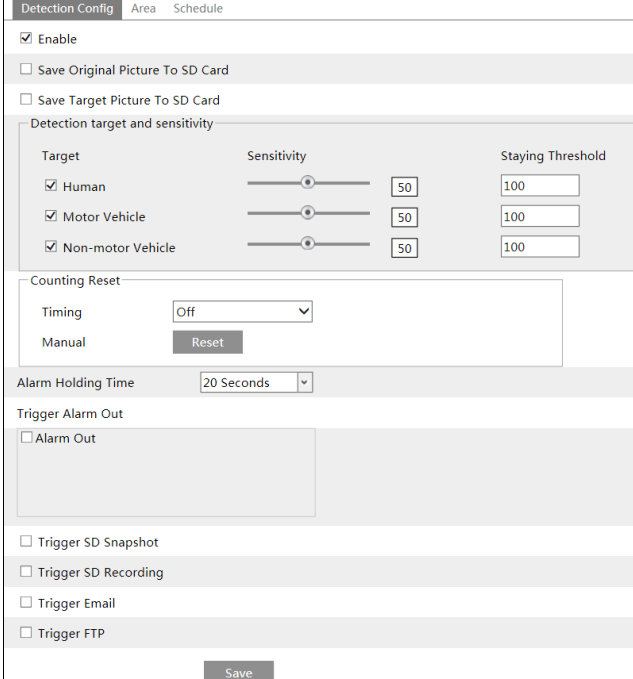
1. Enable region exiting detection and select the snapshot type and the detection target.
2. Set the alarm holding time and alarm trigger options.
3. Set the alarm area of the region exiting detection.
4. Set the schedule of the region exiting detection.

The setup steps of the region exiting detection are the same as the region entrance detection setup (See [4.5.4 Region Entrance](#) for details).

4.5.6 Target Counting by Line

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.



The screenshot shows the 'Detection Config' window with the following settings:

- Enable:**
- Save Original Picture To SD Card:**
- Save Target Picture To SD Card:**
- Detection target and sensitivity:**

Target	Sensitivity	Staying Threshold
<input checked="" type="checkbox"/> Human	50	100
<input checked="" type="checkbox"/> Motor Vehicle	50	100
<input checked="" type="checkbox"/> Non-motor Vehicle	50	100
- Counting Reset:**
 - Timing: Off
 - Manual:
- Alarm Holding Time:** 20 Seconds
- Trigger Alarm Out:** Alarm Out
- Trigger SD Snapshot:**
- Trigger SD Recording:**
- Trigger Email:**
- Trigger FTP:**

A 'Save' button is located at the bottom of the window.

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

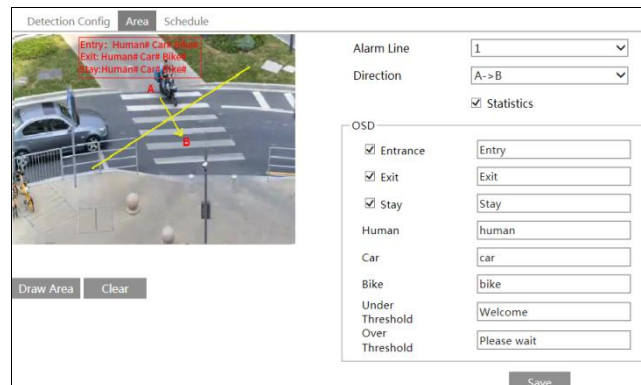
Detection Target: Select the target to calculate. Human, motor vehicle and motorcycle/bicycle can be selected.

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/car/bike counting.

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

- Set the alarm line. 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.

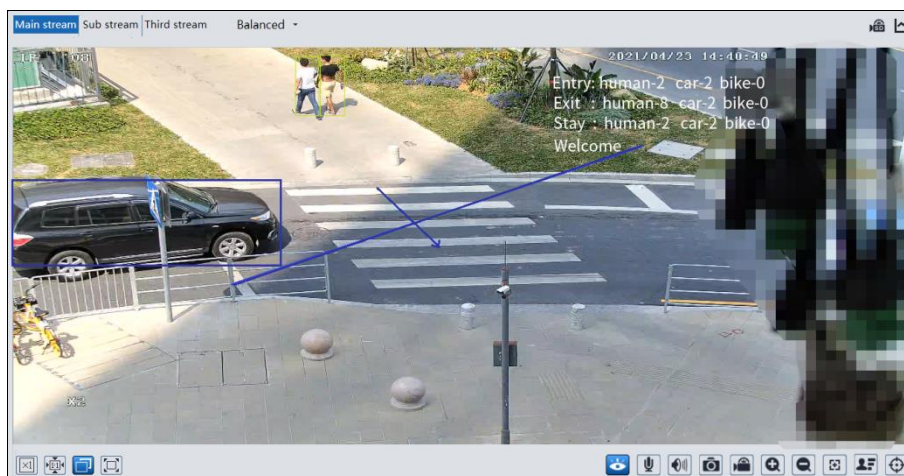
Statistics: If enabled, you can see the statistical information in the live view interface. If disabled, the statistical information will not be displayed in the live view interface.

The statistical OSD information can be customized as needed.

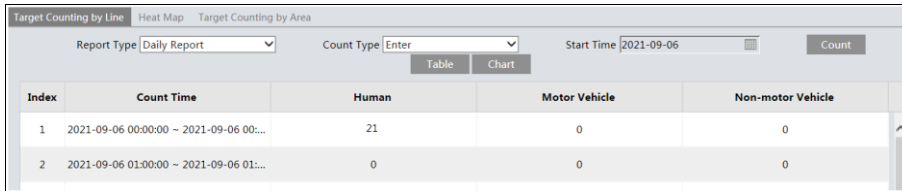
Click the “Draw Area” button and then drag the mouse to draw a line in the image. Check “Statistics” and then move the red box to change the position of the statistical information displayed on the screen. Click the “Stop Draw” button to stop drawing. Click the “Clear” button to delete the lines.

Click the “Save” button to save the settings.

- Set the schedule of the target counting by line. The setup steps of the schedule are the same as schedule recording setup (See [4.1.4.1 Schedule Recording Settings](#)).
- View the statistical information in the live view interface.



9. View the statistical information of target counting by line. Click Statistics→Target Counting by Line to enter the following interface.

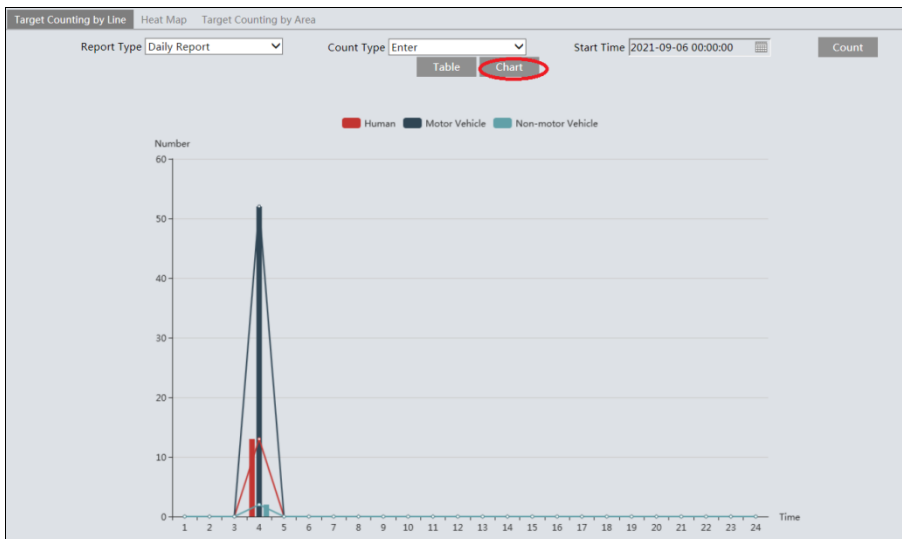


Index	Count Time	Human	Motor Vehicle	Non-motor Vehicle
1	2021-09-06 00:00:00 ~ 2021-09-06 00:...	21	0	0
2	2021-09-06 01:00:00 ~ 2021-09-06 01:...	0	0	0

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.

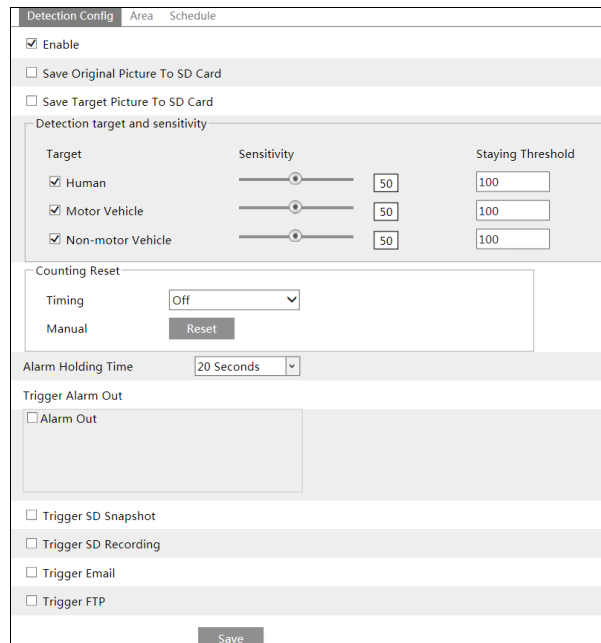
Select the start time and then click “Count”. Then the counting result will display in the statistic result area. Click Table or Statistics to display the result in different way.



4.5.7 Target Counting by Area

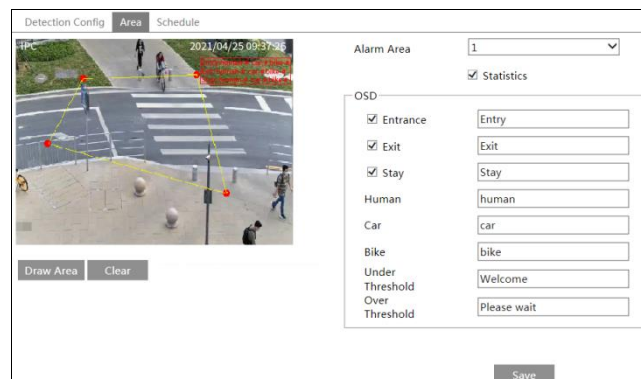
This function is to calculate the number of the people or vehicles intruding into the pre-defined area through detecting, tracking and counting the shapes of the people or vehicles.

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



The screenshot shows the 'Detection Config' window with the 'Area' tab selected. The 'Enable' checkbox is checked. There are options for 'Save Original Picture To SD Card' and 'Save Target Picture To SD Card', both unchecked. Under 'Detection target and sensitivity', three targets are listed: 'Human', 'Motor Vehicle', and 'Non-motor Vehicle', all with checked checkboxes. Each target has a sensitivity slider set to 50 and a 'Staying Threshold' input field set to 100. The 'Counting Reset' section has 'Timing' set to 'Off' and a 'Manual' button labeled 'Reset'. 'Alarm Holding Time' is set to '20 Seconds'. There are checkboxes for 'Trigger Alarm Out', 'Trigger SD Snapshot', 'Trigger SD Recording', 'Trigger Email', and 'Trigger FTP', all of which are currently unchecked. A 'Save' button is at the bottom.

2. Enable target counting by area, select the snapshot type, the detection target, counting reset and alarm linkages. The setup steps are the same as the target counting by line.
3. Set the statistic area. Click the “Area” tab to go to the interface as shown below.



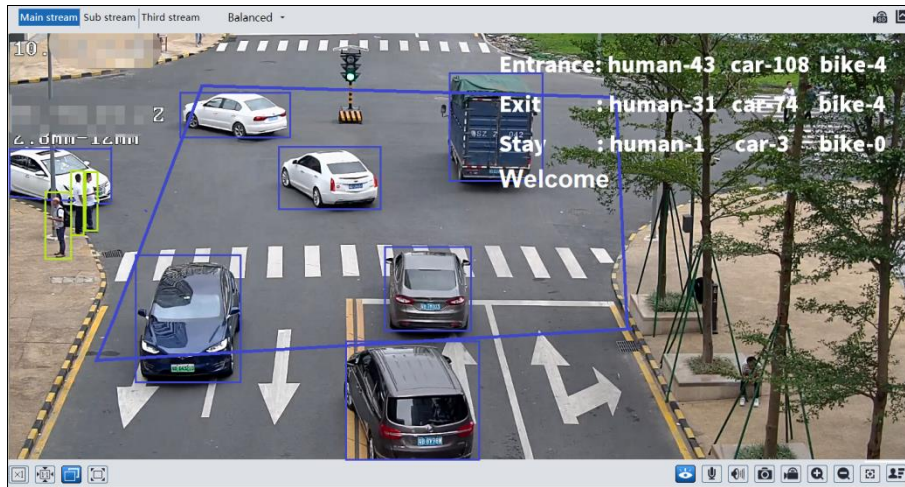
The screenshot shows the 'Area' configuration interface. On the left, there is a video feed showing a street scene with a yellow polygon drawn around a crosswalk area. Below the video are 'Draw Area' and 'Clear' buttons. On the right, there is a configuration panel. 'Alarm Area' is set to '1'. The 'Statistics' checkbox is checked. Under the 'OSD' section, there are checkboxes for 'Entrance', 'Exit', and 'Stay', all checked. Each has a corresponding text input field: 'Entrance' (Entry), 'Exit' (Exit), and 'Stay' (Stay). Below these are input fields for 'Human' (human), 'Car' (car), 'Bike' (bike), 'Under Threshold' (Welcome), and 'Over Threshold' (Please wait). A 'Save' button is at the bottom right.

Select the alarm area number on the right side. Only one alarm area 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.

4. Set the schedule of the target counting by area. The setup steps of the schedule are the same as schedule recording setup (See [4.1.4.1. Schedule Recording Settings](#)).

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



6. View the statistical information of target counting by area. Click Statistics→Target Counting by Area to enter the following interface.

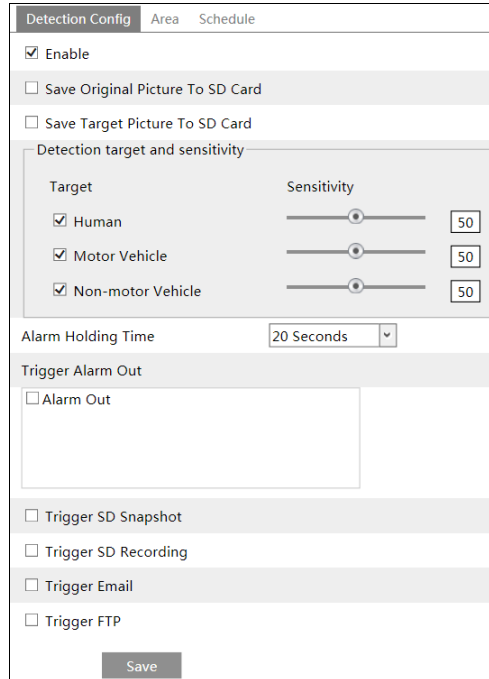
Target Counting by Line					Heat Map					Target Counting by Area										
Report Type			Daily Report			Count Type			Enter			Start Time			2021-09-06			Count		
			Table			Chart														
Index	Count Time		Human	Motor Vehicle		Non-motor Vehicle														
1	2021-09-06 00:00:00 – 2021-09-06 00:...		21	0		0														
2	2021-09-06 01:00:00 – 2021-09-06 01:...		0	0		0														

Please select Report Type, Count Type and Count Time as needed. Then click “Count” to search the statistic result. Click “Statistics” to view the statistic result intuitively.

4.5.8 Region Intrusion

Region 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.

Save Original Picture to SD Card: If it is enabled, the detected original pictures will be captured and saved to the SD card when the targets intrude into the pre-defined areas.

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 intrude into the pre-defined areas.

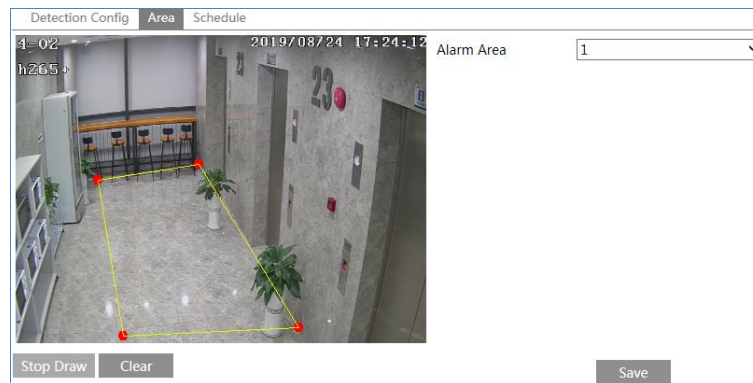
Note: To save snapshots to the local PC, please enable “Local Smart Snapshot Storage” in the local config interface first. To save snapshots to the SD card, please install an SD card first.

Detection Target:

- **Human:** Select it and then alarms will be triggered if someone intrudes into the pre-defined area.
- **Motor Vehicle:** Select it and then alarms will be triggered if a vehicle with four or more wheels (eg. a car, bus or truck) intrudes into the pre-defined area.
- **Non-motor Vehicle:** Select it and then alarms will be triggered if a vehicle with two wheels (eg. a motorcycle or bicycle) intrudes into the pre-defined area.

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 intrusion detection is enabled.

2. 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.
4. Click the “Save” button to save the settings.
5. Set the alarm area of the region 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 region intrusion detection. The setup steps of the schedule are the same as schedule recording setup (See [4.1.4.1 Schedule Recording Settings](#)).

※ Configuration requirements of camera and surrounding area

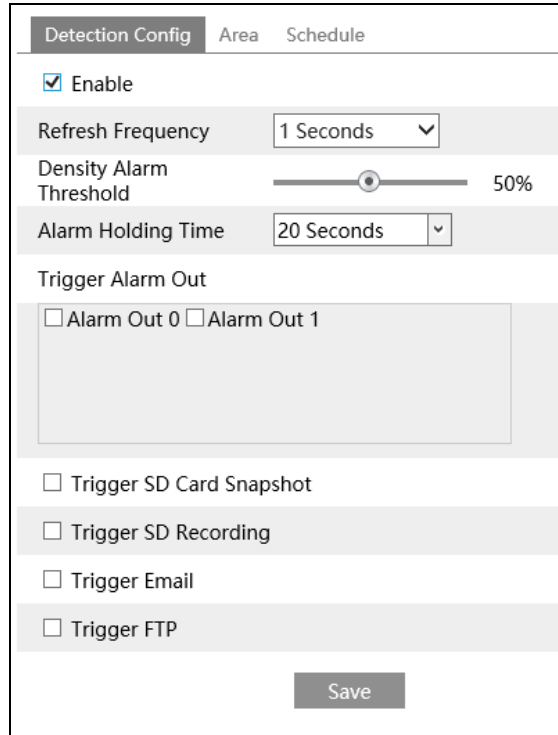
1. Auto-focusing function should not be enabled for region intrusion detection.
2. Avoid the scenes with many trees or the scenes with various light changes (like many flashing headlights). The ambient brightness of the scenes shouldn't be too low.
3. Cameras should be mounted at a height of 2.8 meters 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 region intrusion detection.

4.5.9 Crowd Density

Crowd Density function is to detect the number of people in the surveillance scene. Alarms will be triggered when crowd density exceeds the set threshold. Note that this function is only applicable to GV-BX2802.

The setting steps are as follows:

1. Go to Config→Event→Crowd Density as shown below.



2. Enable the crowd density detection function.

Refresh Frequency: Select the frequency for refreshing crowd density data.

Density Alarm Threshold: Set the crowd density threshold to trigger the alarm.

Set alarm holding time and alarm trigger options. The alarm trigger setup steps are the same as motion detection setup. Please refer to [4.4.1 Motion Detection](#) for details.

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

4. Set the alarm area of crowd density detection. Click the “Area” tab to go to the interface as shown below.



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.

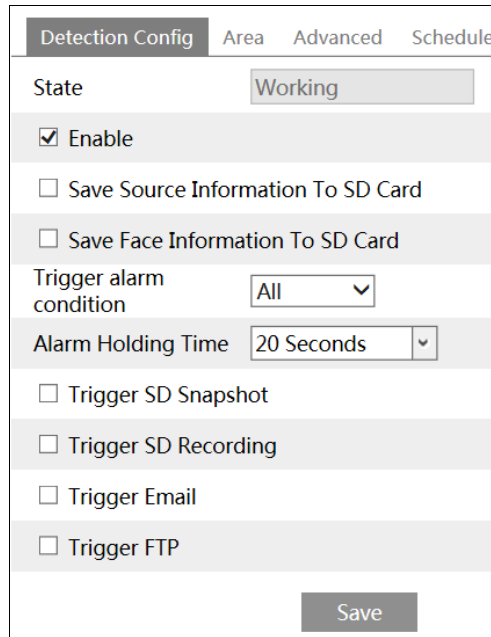
6. Set the schedule of the region intrusion detection. The setup steps of the schedule are the same as schedule recording setup (See [4.1.4.1 Schedule Recording Settings](#)).

4.5.10 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 to SD Card: if checked, the whole picture will be saved to the local PC or SD card when detecting a face.

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

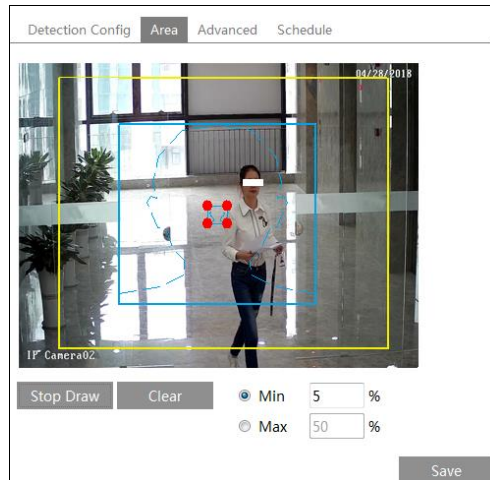
Note: To save images to the local PC, please enable the local smart snapshot storage first (Config→System→Local Config). To save images to the SD card, please install an SD card first.

3. Set alarm holding time and alarm trigger options. The alarm trigger setup steps are the same as motion detection setup. Please refer to [4.4.1 Motion Detection](#) chapter for details.

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

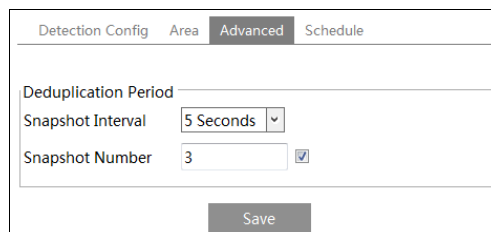
- All: Alarms will be triggered when the camera detects a face (with/without a mask).
- Mask off: Alarms will be triggered when the detected person is not wearing a mask on the face.

4. Set 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.

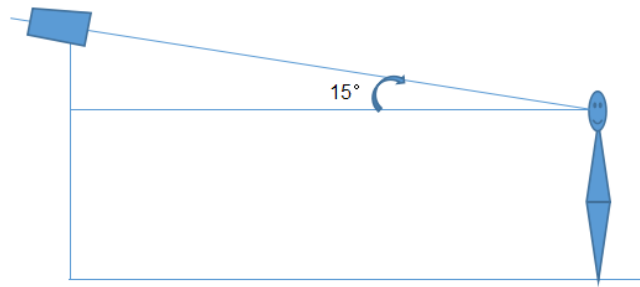
Snapshot Number: If the snapshot number is enabled and set (eg. 3), the camera will capture the same target once every 5 seconds and it will capture this target 3 times at most during its continuous tracking period. If the snapshot number is disabled, the camera will capture the same target once every 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 [4.1.4.1 Schedule Recording Settings](#)).

※ **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 2.0 m to 3.5 m, adjustable according to the focal-length of different lenses and object distances.

- The depression angle of the camera shall be less than or equal to 15°.

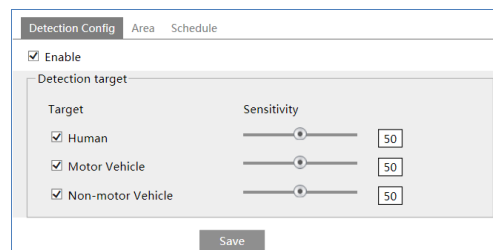


- The object distance depends on the focal-length of the lens mounted in the camera.
- To ensure the accuracy of face detection, the requirements for face capture are: left or right turn angle is less than about 30°; pitching angle is less than 20°.
- The following scenes are not applicable, like crowded scenes (airport, railway station, square, etc), backlight scenes, crossroads and so on.

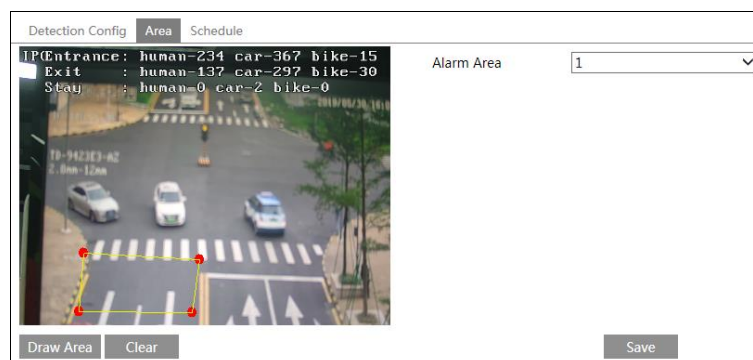
4.5.11 Heat Map

Heat Map is to display the flow distribution of people/vehicles in pre-defined areas by different colors.

- Enable Heat Map, set snapshot type and detection target type as needed.

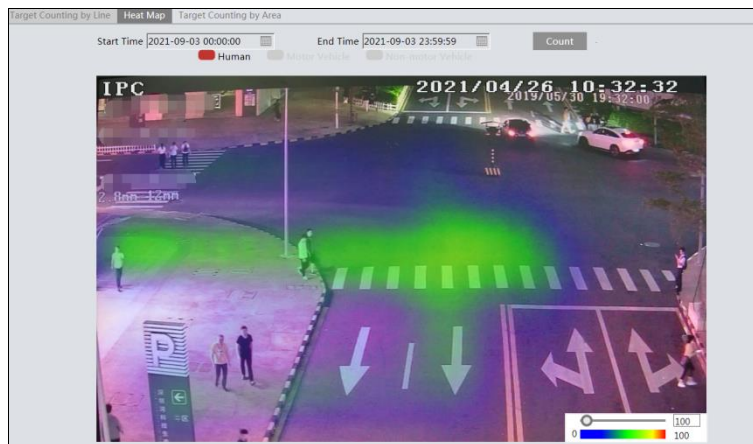


- Set heat map display area. Up to 4 areas can be set.



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.

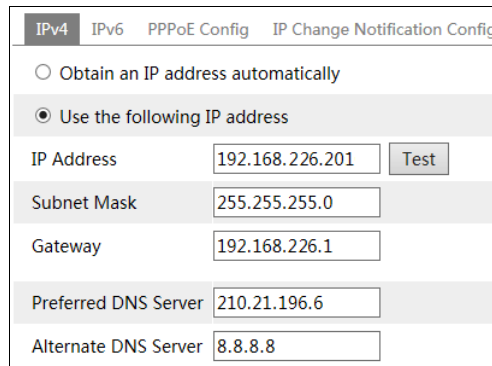
3. Set the schedule of heat map. The setup steps of the schedule are the same as schedule recording setup (See [4.1.4.1 Schedule Recording Settings](#)).
4. View the heat map data (click Statistics→Heat Map). Set the start time and the end time. Click “Count” to view the heat map as shown below. The default heat map is people flow data display. Click “Motor Vehicle” or “Non-motor Vehicle” to view the corresponding data.



4.6 Network Configuration

4.6.1 TCP/IP

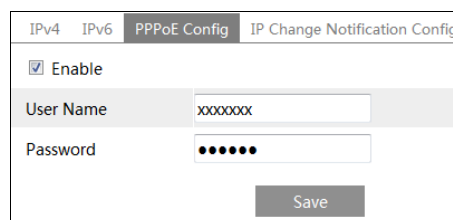
Go to Config→Network→TCP/IP interface as shown below. There are two ways for network connection.



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.

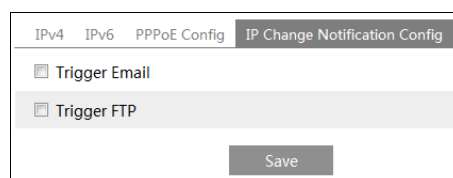
Test: Test the effectiveness of the IP address by clicking this button.

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.

4.6.2 Port

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

HTTP Port	<input type="text" value="80"/>
HTTPS Port	<input type="text" value="443"/>
Data Port	<input type="text" value="9008"/>
RTSP Port	<input type="text" value="554"/>
Persistent connection Port	<input type="text" value="8080"/> <input checked="" type="checkbox"/> Enable
WebSocket Port	<input type="text" value="7681"/>

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.

4.6.3 DDNS

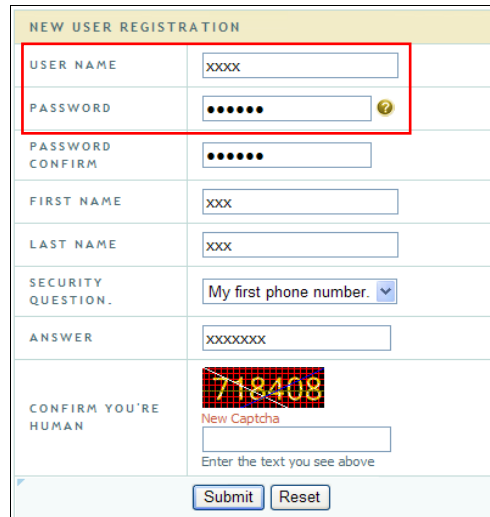
If the camera is set up with a DHCP connection, DDNS should be set for the internet.

1. Go to Config→Network→ DDNS.

<input checked="" type="checkbox"/> Enable
Server Type <input type="text" value="www.dyndns.com"/>
User Name <input type="text"/>
Password <input type="text"/>
Domain <input type="text"/>

2. Apply for a domain name. Take www.dvrddns.com for example.

Enter www.dvrddns.com in the IE address bar to visit its website. Then Click the “Registration” button.



NEW USER REGISTRATION

USER NAME: [xxxx]

PASSWORD: [.....] ⓘ

PASSWORD CONFIRM: [.....]

FIRST NAME: [xxx]

LAST NAME: [xxx]

SECURITY QUESTION: [My first phone number.]

ANSWER: [xxxxxxx]

CONFIRM YOU'RE HUMAN: [718408] New Captcha

Enter the text you see above

[Submit] [Reset]

Create domain name.

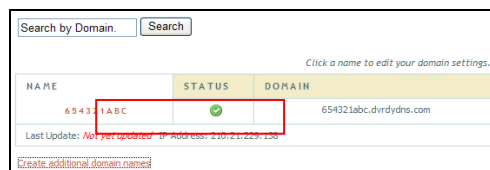


You must create a domain name to continue.

Domain name must start with (a-z, 0-9). Cannot end or start, but may contain a hyphen and is not case-sensitive.

[] dvrddns.com [Request Domain]

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



Search by Domain: [] Search

Click a name to edit your domain settings.

NAME	STATUS	DOMAIN
654321ABC	✓	654321abc.dvrddns.com

Last Update: Not yet updated IP Address: 207.21.229.138

[Create additional domain names](#)

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

4.6.4 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.

SNMP v1/v2	
<input type="checkbox"/> Enable SNMPv1	
<input type="checkbox"/> Enable SNMPv2	
Read SNMP Community	<input type="text"/>
Write SNMP Community	<input type="text"/>
Trap Address	<input type="text" value="..."/>
Trap Port	<input type="text" value="0"/>
Trap community	<input type="text"/>
SNMP v3	
<input type="checkbox"/> Enable SNMPv3	
Read User Name	<input type="text"/>
Security Level	<input type="text" value="auth,priv"/>
Authentication Algorithm	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Authentication Password	<input type="text"/>
Private-key Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES
Private-key Algorithm	<input type="text"/>
Write User Name	<input type="text"/>
Security Level	<input type="text" value="auth,priv"/>
Authentication Algorithm	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Authentication Password	<input type="text"/>
Private-key Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES
Private-key Algorithm	<input type="text"/>
Other Settings	
SNMP Port	<input type="text" value="0"/>

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.

4.6.5 802.1x

If it is enabled, the camera's data can be protected. When the camera is connected to the network protected by the IEEE802.1x, user authentication is needed.

<input checked="" type="checkbox"/> Enable	
Protocol Type	EAP_MD5
EAPOL Version	1
User Name	test
Password	•••••
Confirm Password	•••••

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 / EAPOL version: Please use the default settings.

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

4.6.6 RTSP

Go to Config→Network→RTSP.

<input checked="" type="checkbox"/> Enable	
Port	554
Address	rtsp://IP or domain name:port/profile1
	rtsp://IP or domain name:port/profile2
	rtsp://IP or domain name:port/profile3
Multicast address	
Main stream	239.0.0.0 50554 <input type="checkbox"/> Automatic start
Sub stream	239.0.0.1 51554 <input type="checkbox"/> Automatic start
Third stream	239.0.0.2 52554 <input type="checkbox"/> Automatic start
Audio	239.0.0.3 53554 <input type="checkbox"/> Automatic start
<input type="checkbox"/> Allow anonymous login (No username or password required)	
Save	

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".

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 “Automatic Start” is enabled, the multicast received data should be added into a VLC player to play the video.

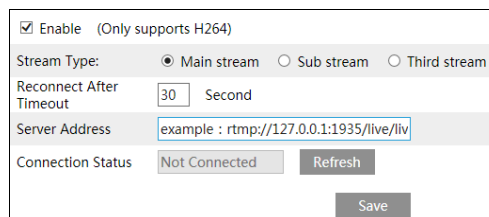
Note:

1. This camera supports local play 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.
-

4.6.7 RTMP

You can access the third-party (like YouTube) to realize video live view through RTMP protocol.

Go to Config→Network→RTMP.



<input checked="" type="checkbox"/> Enable (Only supports H264)
Stream Type: <input checked="" type="radio"/> Main stream <input type="radio"/> Sub stream <input type="radio"/> Third stream
Reconnect After Timeout: <input type="text" value="30"/> Second
Server Address: <input type="text" value="example : rtmp://127.0.0.1:1935/live/liv"/>
Connection Status: <input type="button" value="Not Connected"/> <input type="button" value="Refresh"/>
<input type="button" value="Save"/>

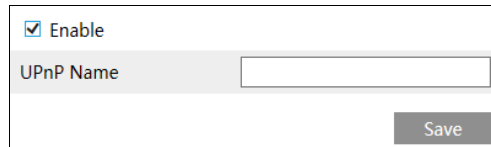
Check “Enable”, select stream type, set the reconnection time after timeout and server address as needed.

Server address: Enter the server address allocated by the third-party server.

After that, click “Save” to save the settings. Then click “Refresh” to view the connection status.

4.6.8 UPNP

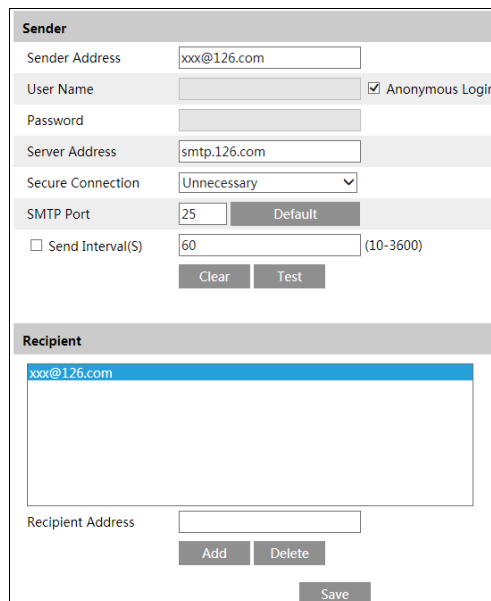
If this function is enabled, the camera can be quickly accessed through the LAN.
Go to Config→Network→UPnP. Enable UPNP and then enter UPnP name.



4.6.9 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.

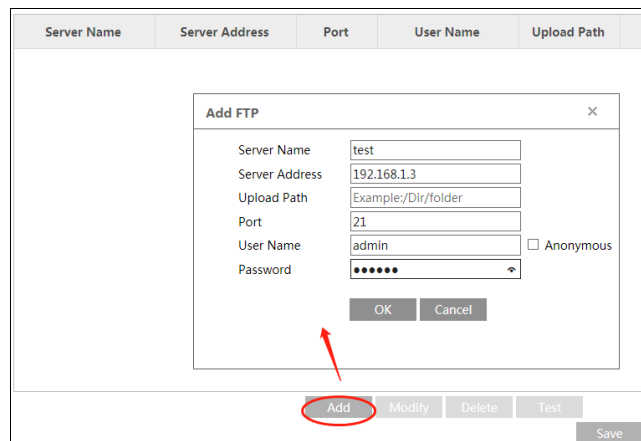
Click the “Test” button to test the connection of the account.

Recipient Address: Receiver’s e-mail address.

4.6.10 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.

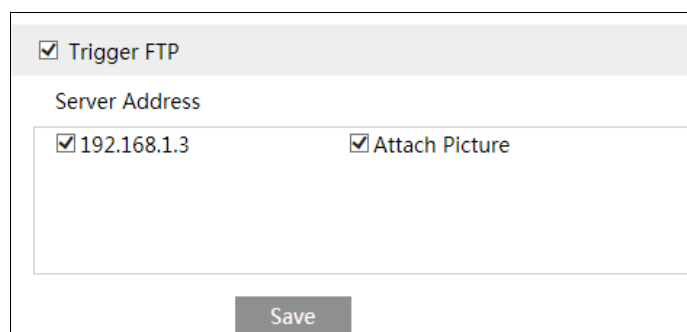
Server Address: The IP address or domain name of the FTP.

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.



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 Abandoned/Missing
AVD	Video Exception
VFD	Face Detection
AOIENTRY	Region Entrance
AOILEAVE	Region Exiting
PASSLINECOUNT	Target Counting by Line
TRAFFIC	Target Counting by Area
SDFULL	SD Full
SDERROR	SD Error

TXT file content:

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

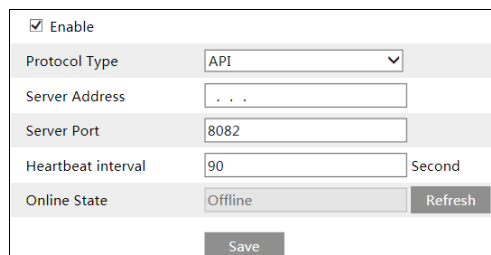
For example:

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

4.6.11 HTTP POST

Go to Config→Network →HTTP POST interface.

Check “Enable”, select protocol type and then set the server address (IP address/domain name), server port and heartbeat interval.



Server Address: The IP address/domain name of the third-party platform.

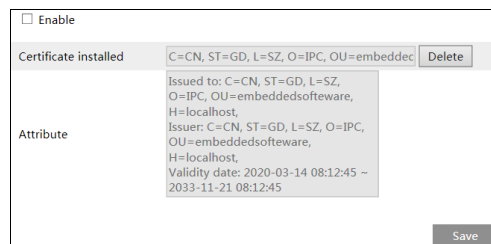
Server Port: The server port of the third-party platform.

After the above parameters are set, click “Save” to save the settings. Then the camera will automatically connect the third-party platform. The online state can be viewed in the above interface. After the camera is successfully connected, it will send the alarm information (HTTP format) to the third-party platform once the smart alarm is triggered. The alarm information includes target tracing coordinates, target features, the captured original/target image (like the captured face picture, motor vehicle picture) and so on.

4.6.12 HTTPS

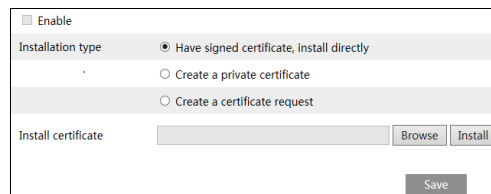
HTTPS provides authentication of the web site and protects user privacy.

Go to Config → Network → HTTPS as shown below.



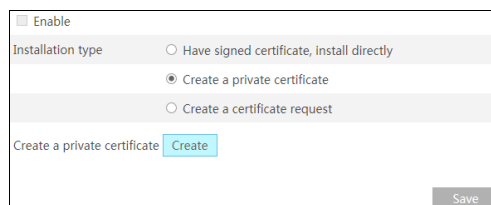
There is a certificate installed by default as shown above. Enable this function and save it. Then the camera can be accessed by entering https://IP: https port via the web browser (e. g. https://192.168.226.201:443).

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.

<input type="checkbox"/> Enable
Installation type
<input type="radio"/> Have signed certificate, install directly
<input type="radio"/> Create a private certificate
<input checked="" type="radio"/> Create a certificate request
Create a certificate request <input type="button" value="Create"/> <input type="button" value="Download"/> <input type="button" value="Delete"/>

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.

4.6.13 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	<input type="text" value="13"/>
Alarm DSCP	<input type="text" value="35"/>
Manager DSCP	<input type="text" value="53"/>

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

4.7 Security Configuration

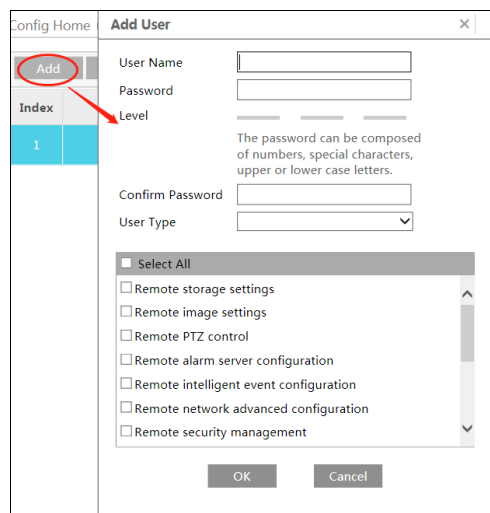
4.7.1 User Configuration

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

Add Modify Delete			
Index	User Name	User Type	Binding MAC
1	admin	Administrator	

Add user:

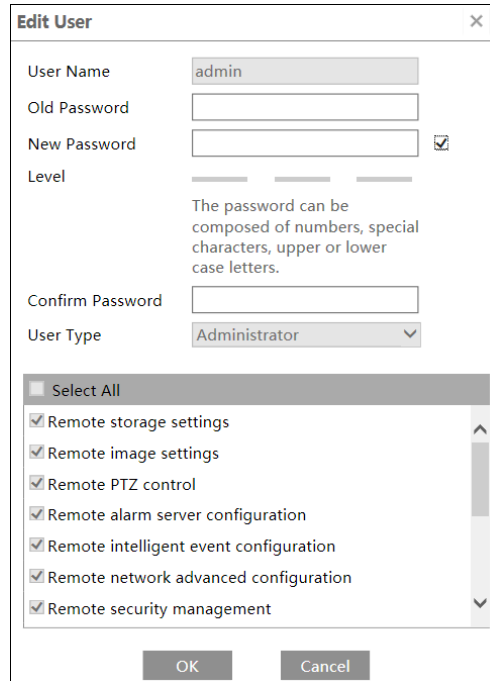
1. Click the “Add” button to pop up the following textbox.



2. Enter user name in the “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.



3. Enter the old password of the user in the “Old Password” text box.
4. Enter the new password in the “New password” and “Confirm Password” text box.
5. Select the user permissions for advanced or normal user.
6. Click the “OK” button to save the settings.

Note: When the password level is set to “Strong”, the password cannot be set the same as the previous five.

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 Settings: Set the questions and answers for admin to reset the password after you forget the password.

4.7.2 Online User

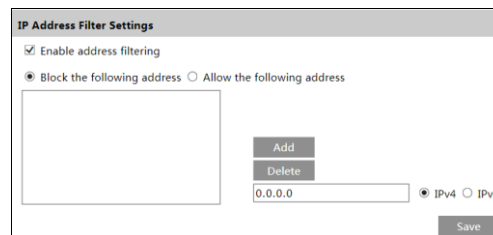
Go to Config→Security→Online User to view the user who is viewing the live video.

Index	Client Address	Port	User Name	User Type	
1	192.168.17.232	55760	admin	Administrator	Kick Out

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

4.7.3 Block and Allow Lists

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



The screenshot shows the 'IP Address Filter Settings' window. It has a title bar with 'IP Address Filter Settings'. Inside, there is a checked checkbox for 'Enable address filtering'. Below it, there are two radio buttons: 'Block the following address' (selected) and 'Allow the following address'. A large empty text box is provided for entering IP addresses. To the right of this box are 'Add' and 'Delete' buttons. Below the text box is an input field containing '0.0.0.0'. To the right of the input field are radio buttons for 'IPv4' (selected) and 'IPv6'. A 'Save' button is located at the bottom right of the form.

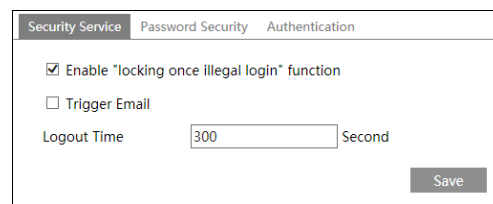
The setup steps are as follows:

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.

4.7.4 Security Management

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



The screenshot shows the 'Security Management' window. It has a title bar with 'Security Service', 'Password Security', and 'Authentication'. The 'Authentication' tab is active. Inside, there is a checked checkbox for 'Enable “locking once illegal login” function'. Below it is an unchecked checkbox for 'Trigger Email'. There is a 'Logout Time' label followed by an input field containing '300' and the word 'Second'. A 'Save' button is located at the bottom right of the form.

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.

- **Password Security**

Security Service	Password Security	Authentication
Password Level	Weak	▼
Expiration Time	Never	▼
<input type="button" value="Save"/>		

Please set the password level and expiration time as needed.

Password Level: Weak, Medium or Strong.

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

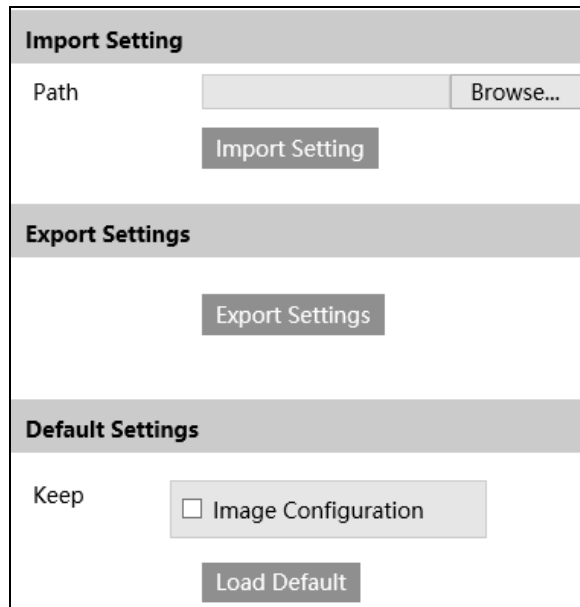
HTTP Authentication: Basic or Token is selectable.

Security Service	Password Security	Authentication
HTTP Authentication	Basic	▼
<input type="button" value="Save"/>		

4.8 Maintenance Configuration

4.8.1 Backup and Restore

Go to Config→Maintenance→Backup & Restore.



The screenshot shows a web interface for 'Backup and Restore' configuration. It is divided into three sections: 'Import Setting', 'Export Settings', and 'Default Settings'. The 'Import Setting' section has a 'Path' input field with a 'Browse...' button and an 'Import Setting' button. The 'Export Settings' section has an 'Export Settings' button. The 'Default Settings' section has a 'Keep' section with an unchecked checkbox for 'Image Configuration' and a 'Load Default' button.

- **Import & Export Settings**

Configuration settings of the camera can be exported from 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 the default factory settings except those you want to keep.

4.8.2 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.

4.8.3 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. Enter the correct password and then the device will restart automatically

IMPORTANT: Do not close the browser or disconnect the camera from the network during the upgrade.

4.8.4 Operation Log

To query and export log:

1. Go to Config→Maintenance→Operation Log.

Index	Time	Main Type	Sub Type	User Name	Login IP	Hostname
1	2021-09-06 03:1...	Operation	Log in	admin	10.20.52.7	
2	2021-09-06 03:1...	Operation	Log in	admin	10.20.52.7	

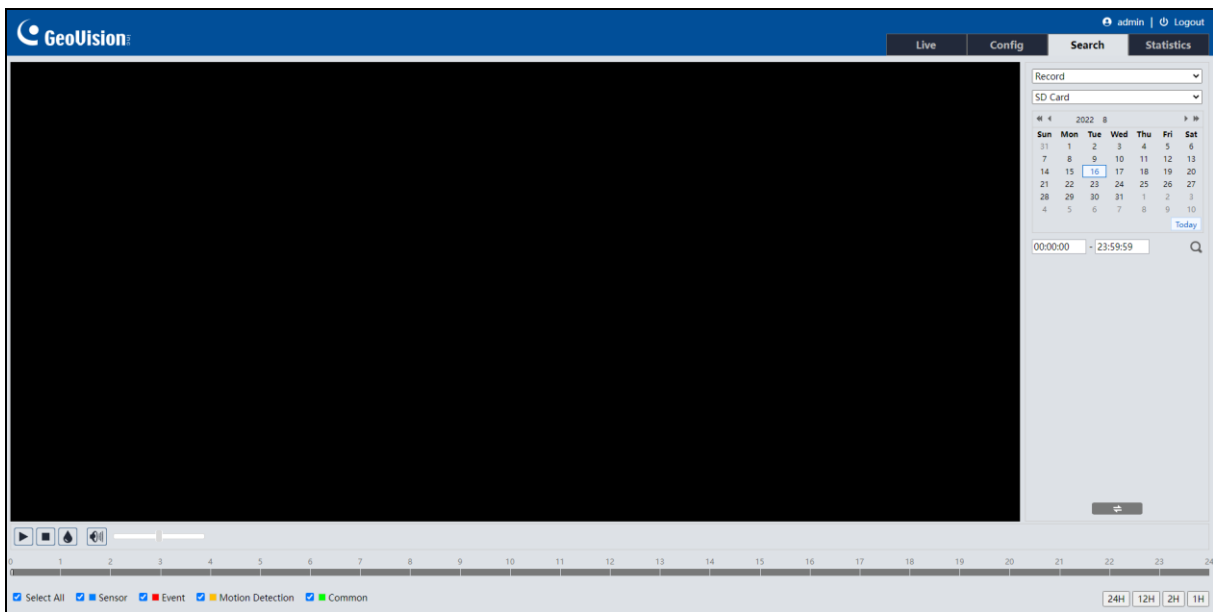
2. Select the main type, sub type, start and end time.
3. Click “Search” to view the operation log.
4. Click “Export” to export the operation log.

Chapter 5 Search


5.1 Image Search

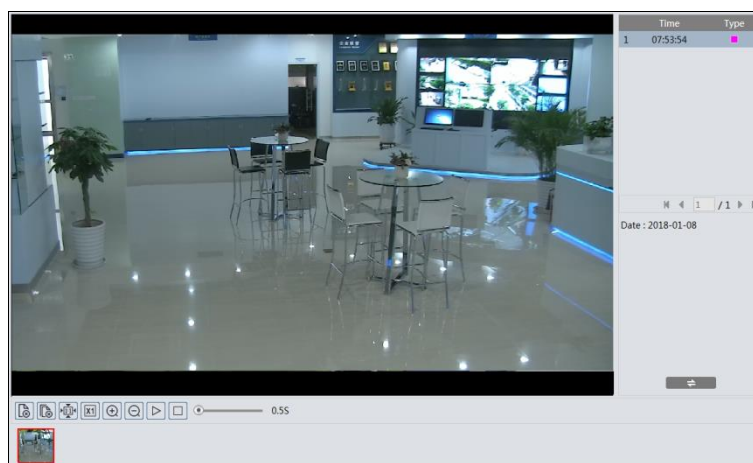
Click Search to go to the interface as shown below. Images that are saved on the SD card can be found here.


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



- **Local Image Search**

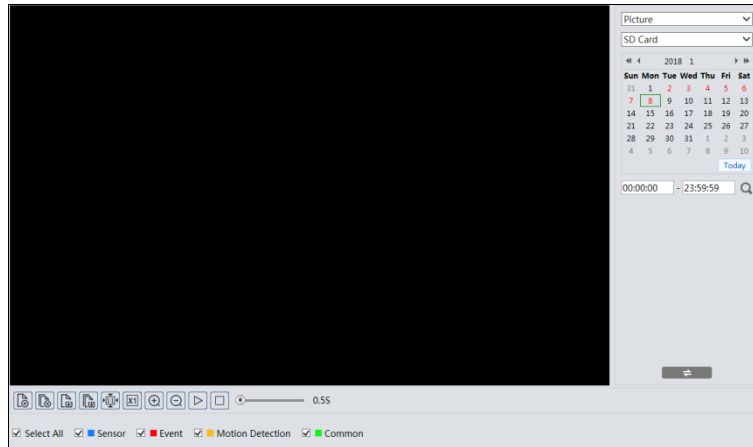
1. Choose “Picture”—“Local”.
2. Set time: Select date and choose the start and end time.
3. Click  to search the images.
4. Double click a file name in the list to view the captured photos as shown above.





Click  to return to the previous interface.

- **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.

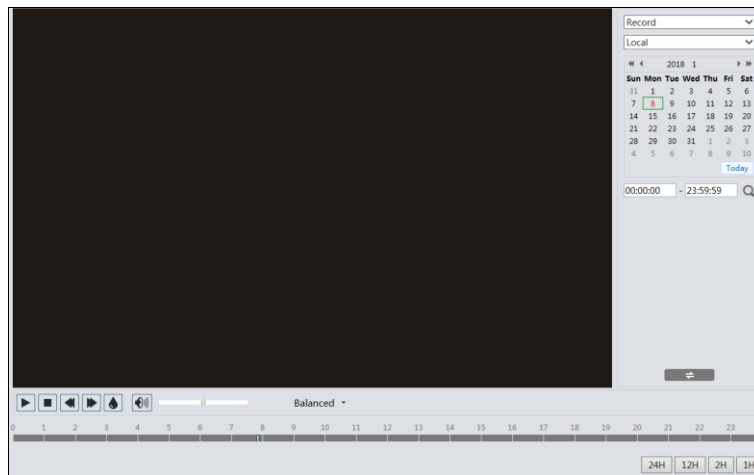
Icon	Description	Icon	Description
	Close: Select an image and click this button to close the image.		Close all: Click this button to close all images.
	Save: Click this button to select the path for saving the image on the PC.		Save All: Click this button to select the path for saving all pictures on the PC.
	Proper 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.
	Play speed: Play speed of the slide show.		


5.2 Video Search

5.2.1 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.

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




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.

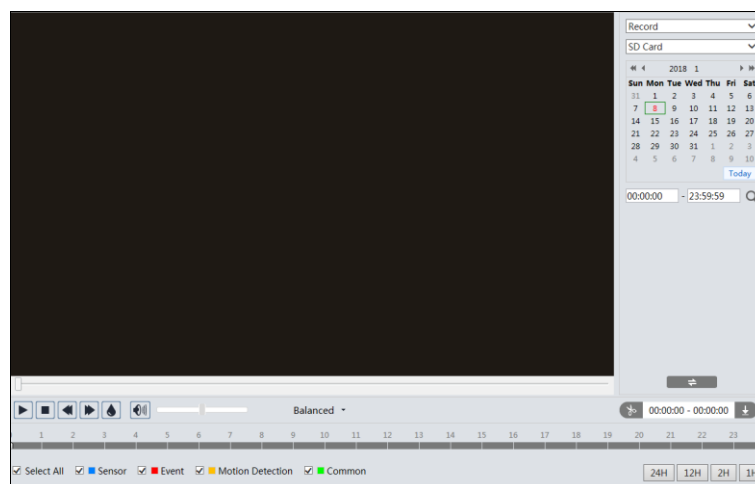


Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button
	Stop button		Speed down
	Speed up		Watermark display
	Enable / disable audio; drag the slider to adjust the volume after enabling audio.		

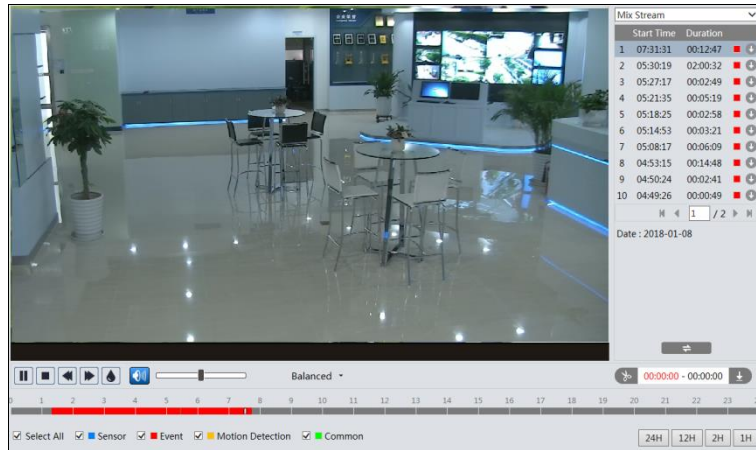
5.2.2 SD Card Video Search

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 in the above interface via the plug-in free browser. Additionally, for plug-in free playback, playback mode switch (balanced / real-time / fluent mode) and downloading functions are not supported too.

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 the  button to set the end time.
5. Click  to download the video file in the PC.

Index	Process	Record	Start Time	End Time	Path	Operate
1	100%	Cut	2018-01-16 01:1...	2018-01-16 01:1...	Favorites	Open

Set up D:\Favorites Clear List Close

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.

Appendix

Appendix 1 Troubleshooting

How to find the password?

A: The password for **admin** can be reset through “Edit Safety Question” function.

Click “Forget Password?” on the login page and enter the corresponding answer of the selected question in the popup window. After you correctly answer all questions, you can reset the password for **admin**. If you forget the answer of the question, this way will be invalid, please contact your dealer for help.

B: The passwords of other users can be reset by **admin**.

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.

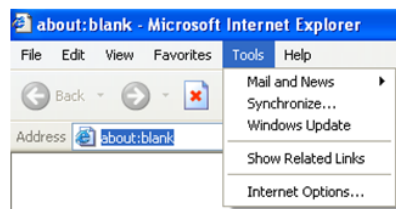
IP tool cannot search devices.

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

IE cannot download the plug-in.

A. IE browser may be set up to block plug-ins. Follow the steps below.

1. Open IE browser and then click Tools→Internet Options.

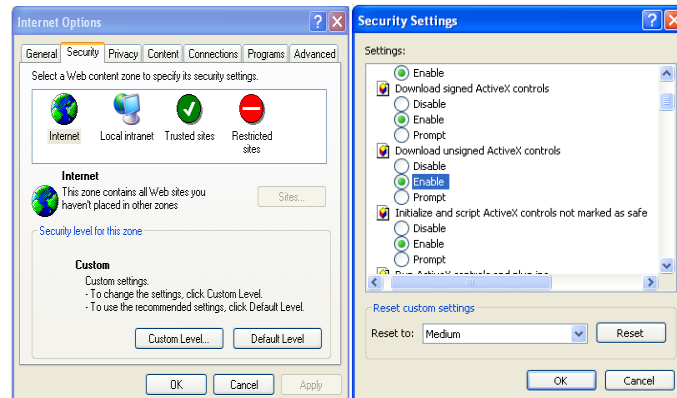


2. Select Security→Custom Level.

3. Enable all the options under the plug-ins.

4. Click OK to finish setup.

B. Other plug-ins or anti-virus blocks the plug-in. 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 Configuration Requirements and Surrounding Area

1. Auto-focusing function should not be enabled. Enabling auto-focusing may cause significant changes in the picture, leading to temporary algorithm interruption.
2. Try to avoid excessive obstruction from trees, while also avoiding excessive variations in lighting conditions in the scene, such as frequent and excessive car headlights, etc., to improve the accuracy of intelligent functions. The brightness of the scene should not be too low, as excessively dim scenes will reduce the accuracy of alarms. Adequate lighting and clear scenery are important conditions.
3. The optimal overhead angle for the camera is between 30 degrees and 45 degrees (see outdoor installation diagram for 12mm lens).

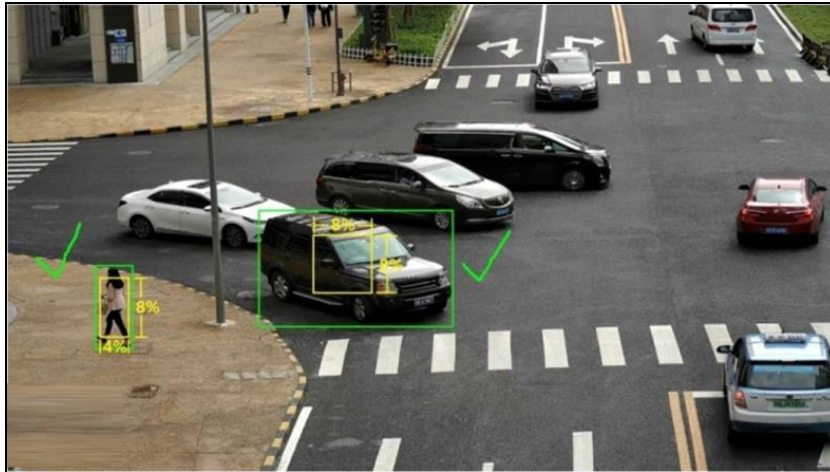
For pedestrians: It is necessary to include the upper body, with the head and torso.

For vehicles: The downward angle should not be too large (not exceeding the recommended angle). Oblique and horizontal views are preferred over downward views, and it is recommended to install the camera with an oblique view.

4. When the camera is detecting, the target should spend at least about 2 seconds passing through the detection area.
5. Not suitable for scenes with significant changes in lighting.
6. Adjust the camera so that the area needing protection is positioned as centrally as possible within the field of view. There should be no obstructions in the main thoroughfare areas. Try to exclude swaying obstructions such as trees, bushes, flags, etc., from the detection area.
7. Please adjust the camera's installation position or focal length so that the targets of interest in the frame meet certain size requirements. Optimal target recognition sizes:

Percentage	Human	Motor Vehicle	Motorcycle/Bicycle
Minimum (Width x Height)	4% x 8%	8% x 8%	4% x 4%
Maximum (Width x Height)	50%x 50%	50%x 50%	50%x 50%

The proportion here refers to the ratio of the target's width to the width of the frame. For example, in a resolution of 1920x1080, the minimum resolution for a person would be 80x160 ($w=1920 \times 4\%=80$, $h=1920 \times 8\%=160$).



Correct example: The target meets the minimum size requirements. The yellow box in the image represents the minimum detection box.

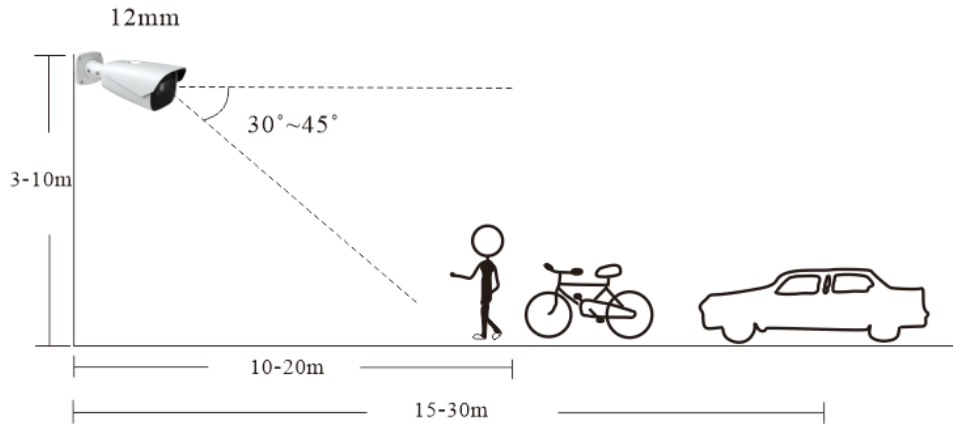


Incorrect example: The target does not meet the minimum size requirements. The yellow box in the image represents the minimum detection box.

8. Installation suggestion:

Outdoor mounting: The optimal detection distance varies due to different focal length. Please refer to the following table.

Focal Length	Installation Height(m)	Human/Motorcycle/Bicycle		Motor Vehicle	
		Maximum Distance(m)	Optimal Distance(m)	Maximum Distance(m)	Optimal Distance(m)
2.8 mm	3-10	8	4-8	15	10-15
3.6 mm	3-10	10	5-10	20	15-20
12 mm	3-10	25	10~20	35	15~30
22 mm	3-10	45	30~40	70	20~50



Example for 12mm focal length

Indoor Mounting

