



Paramont Cameras

User Manual: PAR 4MP Series

PARAMONT ^{IP}

- This product is intended to be supplied by a Listed Power Unit, marked with 'Limited Power Source', 'LPS' on unit, output rated minimum 12V/2 A or POE 48V/ 350mA or AC24V (depending on models), no more than 2000m altitude of operation and Tma=60 Deg.C.
- As for the modes with PoE function, the function of the ITE being investigated to IEC 60950-1 standard is considered not likely to require connection to an Ethernet network with outside plant routing, including campus environment and the ITE is to be connected only to PoE networks without routing to the outside plant.
- Do not attempt to disassemble the camera; in order to prevent electric shock, do not remove screws or covers.
- There are no user-serviceable parts inside. Please contact the nearest service center as soon as possible if there is any failure.
- Avoid from incorrect operation, shock vibration, heavy pressing which can cause damage to product.
- Do not use corrosive detergent to clean main body of the camera. If necessary, please use soft dry cloth to wipe dirt; for hard contamination, use neutral detergent. Any cleanser for high grade furniture is applicable.
- Avoid aiming the camera directly towards extremely bright objects, such as, sun, as this may damage the image sensor.
- Please follow the instructions to install the camera. Do not reverse the camera, or the reversing image will be received.
- Do not operate it 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 active deterrence 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 really very convenient for users, but this will increase the risk of data leakage when the system automatically forwards ports. Disabling UPnP is recommended when the function is not used in real applications.
- Check the log. If you want to know whether your device has been accessed by unauthorized users or not, you can check the log. The system log will show you which IP addresses were used to log in your system and what was accessed.

Regulatory Information

FCC Information

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

1. FCC compliance


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

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

2. FCC conditions:

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

CE Information

 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.

Table of Contents

1	Introduction	1
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.....	5
3	Live View	8
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.....	11
4.2	Image Configuration.....	14
4.2.1	Display Configuration	14
4.2.2	Video / Audio Configuration	16
4.2.3	OSD Configuration.....	17
4.2.4	Video Mask	18
4.2.5	ROI Configuration.....	19
4.2.6	Lens Control	20
4.3	Alarm Configuration	21
4.3.1	Motion Detection.....	21
4.3.2	Other Alarms	22
4.3.3	Alarm In	24
4.3.4	Alarm Out.....	26
4.3.5	Alarm Server	27
4.3.6	Audio Alarm.....	27
4.3.7	Light Alarm	28
4.4	Event Configuration	28
4.4.1	Exception.....	29
4.4.2	Line Crossing.....	30
4.4.3	Intrusion.....	32
4.4.4	Region Entrance	34
4.4.5	Region Exiting.....	36
4.5	Network Configuration.....	38
4.5.1	TCP/IP	38
4.5.2	Port	39
4.5.3	Server Configuration	40
4.5.4	DDNS	40
4.5.5	SNMP	41

4.5.6	802.1x	43
4.5.7	RTSP	43
4.5.8	UPNP	44
4.5.9	Email	44
4.5.10	FTP	45
4.5.11	HTTPS	46
4.5.12	QoS	47
4.6	Security Configuration	48
4.6.1	User Configuration	48
4.6.2	Online User	49
4.6.3	Block and Allow Lists	50
4.6.4	Security Management	50
4.7	Maintenance Configuration	51
4.7.1	Backup and Restore	51
4.7.2	Reboot	51
4.7.3	Upgrade	52
4.7.4	Operation Log	52
5	Search	53
5.1	Image Search	53
5.2	Video Search	55
5.2.1	Local Video Search	55
5.2.2	SD Card Video Search	56
Appendix		59
Appendix 1 Troubleshooting		59

1 Introduction

Main Features

- Max. resolution : 2592×1520@30fps/25fps
- ICR auto switch, true day/night
- 3D DNR, true WDR
- ROI coding
- Video exception detection, intrusion detection (human/vehicle classification), line crossing detection (human/vehicle classification), region entrance detection (human/vehicle classification), region exiting detection (human/vehicle classification), light and sound alarm
- Support BLC, Defog, Anti-flicker, smart IR, etc.
- Support mobile surveillance by smart phones with iOS and Android OS

Surveillance Application



2 Network Connection

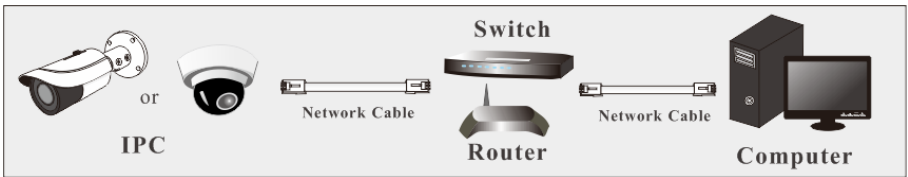
Connect IP-Cam via LAN or WAN. Here only take IE browser for example. The details are as follows:

2.1 LAN

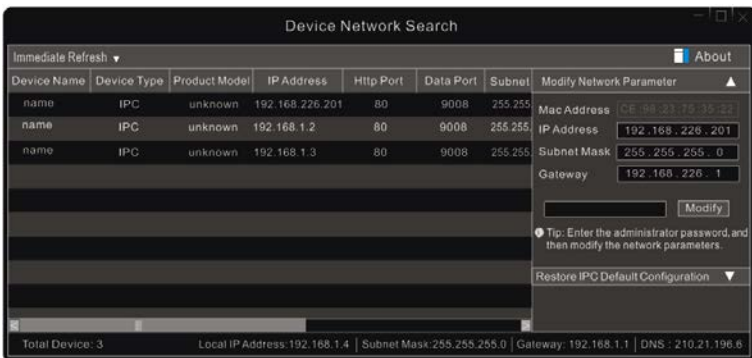
In LAN, there are two ways to access IP-Cam: 1. access through IP-Tool; 2. directly access through IE browser.

2.1.1 Access through IP-Tool

Network connection:



- ① Make sure the PC and IP-Cam are connected to the LAN and the IP-Tool is installed in the PC from the CD.
- ② Double click the IP-Tool icon on the desktop to run this software as shown below:



- ③ Modify the IP address. The default IP address of this camera is 192.168.226.201. Click the information of the camera listed in the above table to show the network information on the right hand. Modify the IP address and gateway of the camera and make sure its network address is in the same local network segment as the computer's. Please modify the IP address of your device according to the practical situation.

For example, the IP address of your computer is 192.168.1.4. So the IP address of the camera shall be changed to 192.168.1.X. After modification, please enter the password of the administrator and click the “Modify” button to modify the setting.



The default password of the administrator is “**123456**”.

④ Double click the IP address and then the system will pop up the IE browser to connect IP-CAM. Follow directions to download, install and run the Active X control.

Enter the username and password in the login window to log in.



The default username is “**admin**”; the default password is “**123456**”.

The system will pop up the above-mentioned textbox to ask you to change the default password. It is strongly recommended to change the default password for account security. If “Do not show again” is checked, the textbox will not appear next time.

2.1.2 Directly Access through IE

The default network settings are as shown below:

IP address: **192.168.226.201**

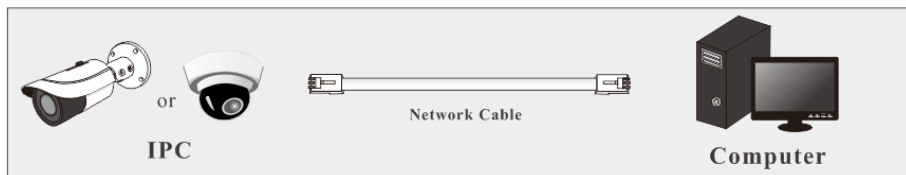
Subnet Mask: **255.255.255.0**

Gateway: **192.168.226.1**

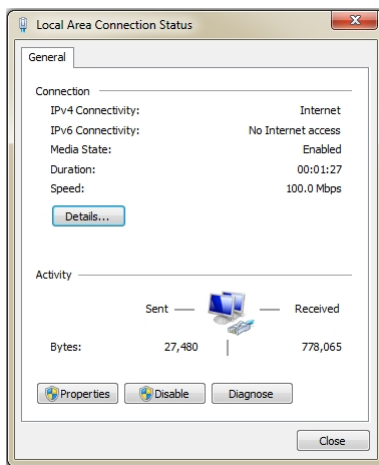
HTTP: **80**

Data port: **9008**

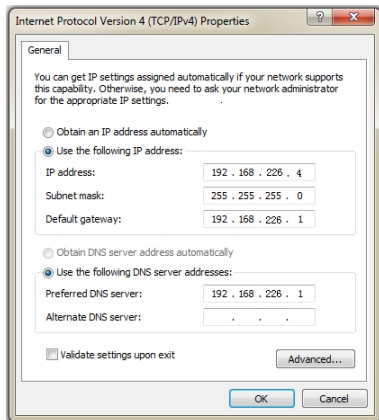
Use the above default settings when logging in the camera for the first time. Directly connect the camera to the computer through network cable.



① Manually set the IP address of the PC and the network segment should be as 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.



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



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

2.2 WAN

➤ Access through the router or virtual server



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

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

Port Setup

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

IPv4	IPv6	PPPoE Config	IP Change Notification Config
<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”.

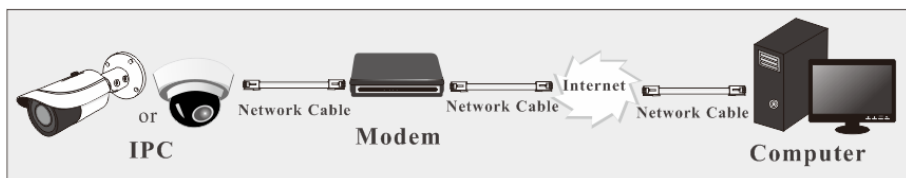
Port Range					
Application	Start	End	Protocol	IP Address	Enable
1	9007	to 9008	Both	192.168.1.201	<input checked="" type="checkbox"/>
2	80	to 81	Both	192.168.1.201	<input checked="" type="checkbox"/>
3	10000	to 10001	Both	192.168.1.166	<input type="checkbox"/>
4	21000	to 21001	Both	192.168.1.166	<input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

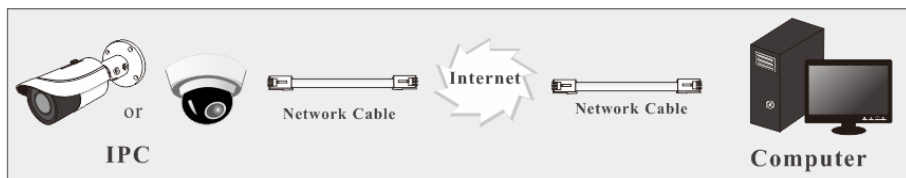
- ① Go to Config→Network→Port menu to set the port number.
- ② Go to Config →Network→TCP/IP→PPPoE Config menu. Enable PPPoE and then enter the user name and password from your internet service provider.

IPv4	IPv6	PPPoE Config	IP Change Notification Config
<input checked="" type="checkbox"/> Enable			
User Name		<input type="text" value="xxxxxxx"/>	
Password		<input type="password" value="•••••"/>	
<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

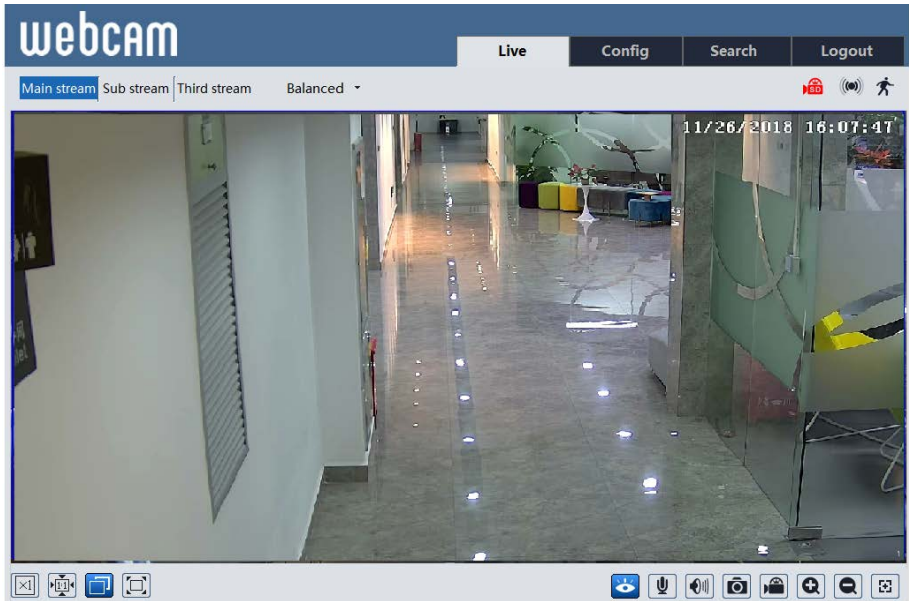


The setup steps are as follow:



















- 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.





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		Focus/Zoom adjustment (only available for the models with motorized lens)
	Fit correct scale		SD card recording indicator
	Auto (fill the window)		Color abnormal indicator
	Full screen		Abnormal clarity indicator
	Start/stop live view		Scene change indicator
	Start/stop two-way audio		Sensor alarm indicator
	Enable/disable audio		Motion alarm indicator
	Snapshot		Line crossing indicator
	Start/stop local recording		Region entrance indicator

Icon	Description	Icon	Description
	Zoom in		Region exiting indicator
	Zoom out		Intrusion indicator

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

In full screen mode, double click on the mouse to exit or press the ESC key on the keyboard. Click AZ control button to show AZ control panel. The descriptions of the control panel are as follows:

Icon	Description	Icon	Description
	Zoom -		Zoom +
	Focus -		Focus +
	One key focus (used when image is out of focus after manual adjustment)		

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	IPC
Product Model	XXXXXXXX-PA
Brand	Customer
Software Version	5.0.1.0(22431)
Software Build Date	2021-08-11
Kernel Version	0303014D
Hardware Version	1.5-1524532
Onvif Version	20.12
Video Structured Version	1.1.1
OCX Version	2.1.8.8
MAC	00:18:ae:00:93:dc

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)
<input checked="" type="checkbox"/> DST	
<input checked="" type="radio"/> Auto DST	
<input type="radio"/> Manual DST	
Start Time	January First Sunday 00 Hour
End Time	February First Monday 00 Hour
Time Offset	120 Minutes

Select the time zone and DST as required.

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

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, the local smart snapshot storage can be enabled or disabled here.

4.1.4 Storage

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

- **SD Card Management**

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

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

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

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

● **Schedule Recording Settings**

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

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

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

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

Weekly schedule

Set the alarm time from Monday to Sunday for a single week. Each day is divided in one hour

increments. Green means scheduled. Blank means unscheduled.

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

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

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

Day schedule

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

Note: Holiday schedule takes priority over weekly schedule.

● Snapshot Settings

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

Management Record **Snapshot**

Snapshot Parameters

Image Format

Resolution

Image Quality

Event Trigger

Snapshot Interval Second

Snapshot Quantity

Timing

Enable Timing Snapshot

Snapshot Interval Second

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

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

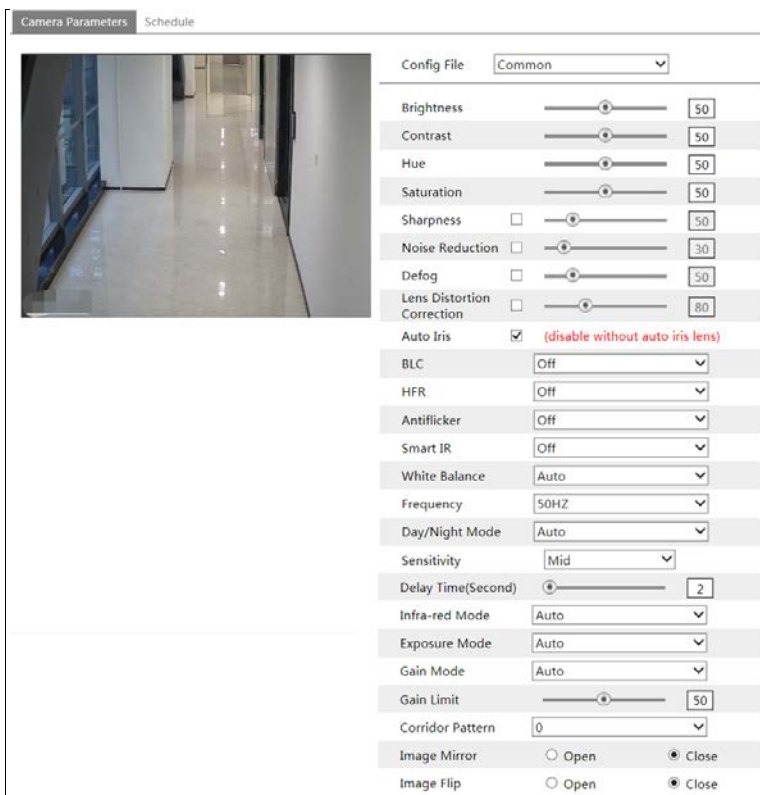
Timing Snapshot: Enable timing snapshot first and then set the snapshot interval and schedule. The setup steps of schedule are the same as the schedule recording (See [Schedule Recording](#)).

4.2 Image Configuration

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

4.2.1 Display Configuration

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



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

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

Hue: Set the total color degree of the image.

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

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

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

Defog: Activating this function and setting an appropriate value as needed in foggy, dusty,

smoggy or rainy environment to get clear images.

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

Auto Iris: If your camera is auto Iris, 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.

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

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

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

Antiflicker:

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

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

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

Frequency: 50Hz and 60Hz can be optional.

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

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

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

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. The video resolution should be 1080P or below if this function is used.

Image Mirror: Turn the current video image horizontally.

Image Flip: Turn the current video image vertically.

Schedule Settings of Image Parameters:

Click the "Schedule" tab as shown below.

Camera Parameters **Schedule**

Schedule: Full Time

Config File: Common


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.

Schedule: Timing

Time Range: 0:00 to 24:00

Day (blue bar) Night (blank bar)

Save

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.

Video **Audio**

Index	Stream	Resolution	Frame	Bitrate	Bitrate(Kbps)	Video	I Frame	Video	Profile
1	Main str...	2560x1440	25	CBR	4096	High	100	H264	High Profile
2	Sub strea...	704x576	25	CBR	480	High	100	H264	High Profile
3	Third str...	352x288	25	CBR	128	High	100	H264	High Profile

Send Snapshot: Sub stream Size: (704x576)

Video encode slice split

Watermark (H264 , H265) Watermark content:

Save

Three video streams can be adjustable.

Resolution: The size of image.

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

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

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

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

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

Video Compression: MJPEG, H264+, H264, H265 or H265+ can be optional. 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.

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 active. Below the tabs, there is a checked checkbox labeled 'Enable'. Underneath, there are three dropdown menus: 'Audio Encoding' with 'G711A' selected, 'Audio Type' with 'MIC' selected, and 'Speaker' with 'Warning' selected. A 'Save' button is located at the bottom right of the configuration area.

Please check “Enable” as needed.

Audio Encoding: G711A and G711U are selectable.

Audio Type: LIN. LIN/MIC can be selected if the model supports built-in microphone.

Speaker: Talkback or Warning can be optional. If “Talkback” is selected, the built-in speaker will be used to output sound for two-way talk. If “Warning” is selected, the built-in speaker will be used to output the pre-defined audio alarm.

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.

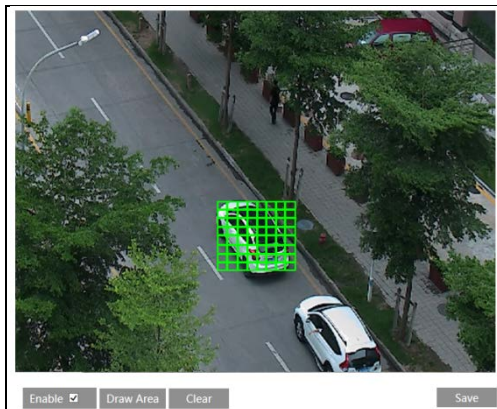


Picture Overlay Settings:

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.

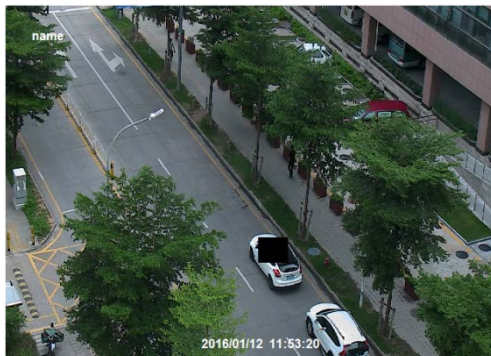
4.2.4 Video Mask

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.

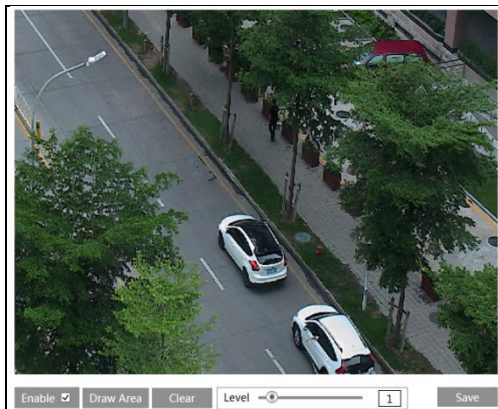


To clear the video mask:

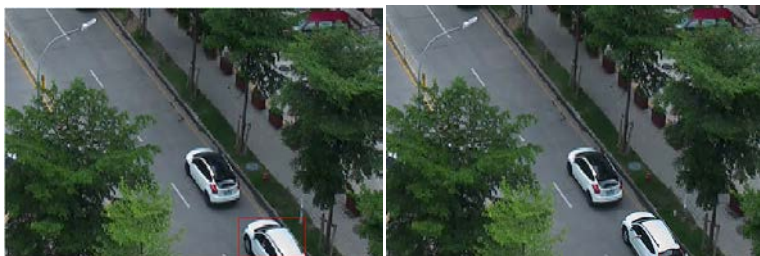
Click the “Clear” button to delete the current video mask area.

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.

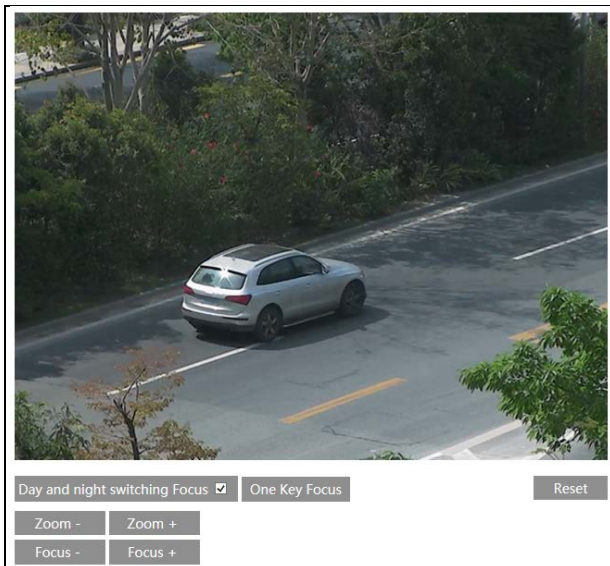


1. Check “Enable” and then click the “Draw Area” button.
2. Drag the mouse to set the ROI area.
3. Set the level.
4. Click the “Save” button to save the settings.



4.2.6 Lens Control

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 Alarm Configuration

4.3.1 Motion Detection

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

Alarm Config
Area and Sensitivity
Schedule

Enable

Alarm Holding Time ▼

Trigger Alarm Out

Alarm Out

Trigger Audio Alarm

Trigger SD Snap

Trigger SD Recording

Trigger Email

Trigger FTP

Save

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

Alarm Out: If selected, this would trigger an external relay output that is connected to the camera on detecting a motion based alarm (This function is only available for the models with the alarm output interface).

Trigger Audio Alarm: If selected, the warning voice will be uttered on detecting a motion based alarm. (Please set the warning voice first. See [Audio Alarm](#) for details).

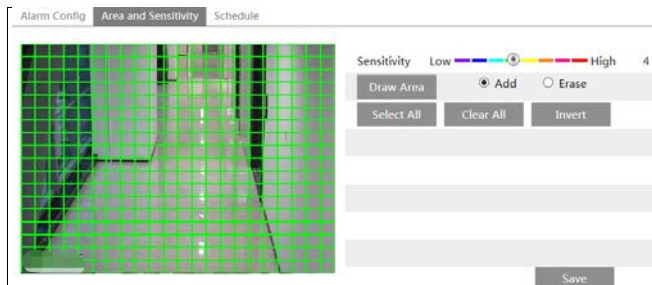
Trigger SD Snap: If selected, the system will capture images on motion detection and save the images on an SD card.

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

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

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

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



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

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

Select “Erase” and drag the mouse to clear motion detection area.

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

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

4.3.2 Other Alarms

- **SD Card Full**

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

SD Card Full | SD Card Error | IP Address Collision | Cable Disconnected

Enable

Alarm Holding Time: 20 Seconds

Trigger Alarm Out

Alarm Out

Trigger Email

Trigger FTP

Save

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

● **SD Card Error**

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

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

SD Card Full | SD Card Error | IP Address Collision | Cable Disconnected

Enable

Alarm Holding Time: 20 Seconds

Trigger Alarm Out

Alarm Out

Trigger Email

Trigger FTP

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

● **IP Address Conflict**

This function is only available for the models with Alarm Out interface.

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

SD Card Full SD Card Error **IP Address Collision** Cable Disconnected

Enable

Alarm Holding Time 20 Seconds ▾

Trigger Alarm Out

Alarm Out

Save

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

● **Cable Disconnection**

This function is only available for the models with Alarm Out interface.

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

SD Card Full SD Card Error IP Address Collision **Cable Disconnected**

Enable

Alarm Holding Time 20 Seconds ▾

Trigger Alarm Out

Alarm Out

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.

4.3.3 Alarm In

This function is only available for the models with Alarm In interface.

To set sensor alarm (alarm in):

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

The screenshot shows the 'Alarm Config' tab in a web interface. It includes the following elements:

- Alarm Config** (selected) and **Schedule** tabs.
- Enable**
- Alarm Type**: A dropdown menu currently set to **NO**.
- Alarm Holding Time**: A dropdown menu currently set to **20 Seconds**.
- Sensor Name**: An empty text input field.
- Trigger Alarm Out** section:
 - Alarm Out**
- Other trigger options (all unchecked):
 - Trigger Audio Alarm**
 - Trigger Light Alarm**
 - Trigger SD Snap**
 - Trigger SD Recording**
 - Trigger Email**
 - Trigger FTP**
- Save** button at the bottom right.

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

Alarm Out: If selected, this would trigger an external relay output that is connected to the camera when the sensor alarm is triggered (**This function is only available for the models with Alarm Out interface**).

Trigger Audio Alarm: If selected, the warning voice will be uttered when the sensor alarm is triggered. (Please set the warning voice first. See [Audio Alarm](#) for details).

Trigger Light Alarm: If selected, the light of the camera will flash when the sensor alarm is triggered. (Please set the light flashing time and frequency first. See [Light Alarm](#) for details).

Trigger SD Snap: If selected, the system will capture images when the sensor alarm is triggered and save the images on an SD card.

Trigger SD Recording: If selected, video will be recorded on an SD card when the sensor alarm is triggered.

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

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

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

4. Set the schedule of the sensor alarm. The setup steps of the schedule are the same as the schedule recording setup. (See [Schedule Recording](#)).

4.3.4 Alarm Out

This function is only available for the models with Alarm Out interface.

Go to Config→Alarm→Alarm Out.

Alarm Out Mode	Alarm Linkage
Alarm Out Name	alarmOut1
Alarm Holding Time	20 Seconds
Alarm Type	NO
Save	

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.

Alarm Out Mode:

Alarm Type:

Time Range:

Erase Add

Manual Input:

Save

4.3.5 Alarm Server

Go to Alarm→Alarm Server interface as shown below.

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

Server Address:

Port:

Heartbeat:

Heartbeat interval: Second

4.3.6 Audio Alarm

Go to Alarm→Audio Alarm interface as shown below.

Voice Configuration

Warning voice:

Voice:

Warning Times: times

Volume:

OK

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

Voice Configuration

Warning voice:

Voice:

Warning Times: times

Volume: 100

Upload Audio

Upload Path:

Audio Name:

Tips: audio format (WAV, 8000Hz, monophonic, 16bit , less than 300K)

Audio List:

- ② Select the voice and then set the warning times and volume as needed.
Warning times: it ranges from 1 to 50.
- ③ Click “OK” to save the settings.

4.3.7 Light Alarm

Go to Alarm→Light Alarm interface as shown below.
Set the flashing time and frequency of the light.

Flashing Time: Second

Flashing Frequency:

Flashing time: the flashing time ranges from 1 second to 60 seconds.
Flashing Frequency: three options- low, middle and high

4.4 Event Configuration

For more accuracy, here are some recommendations for installation.

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

- At any time of day or night, please make sure the image of the camera is clear and with adequate and even light, avoiding overexposure or too much darkness on both sides.

4.4.1 Exception

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

To set exception detection:

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

Detection Config Sensitivity

Scene Change Detection

Video Blur Detection

Video Cast Detection

Alarm Holding Time 20 Seconds

Trigger Alarm Out

Alarm Out

Trigger Audio Alarm

Trigger SD Snap

Trigger SD Recording

Trigger Email

Trigger FTP

Save

1. Enable the applicable detection that's desired.

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

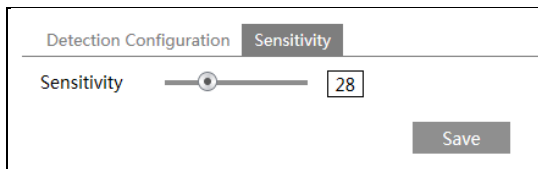
Video Blur Detection: Alarms will be triggered if the video becomes blurry.

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

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

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

4. Set the sensitivity of the exception detection. Click “Sensitivity” tab to go to the interface as shown below.



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

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

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

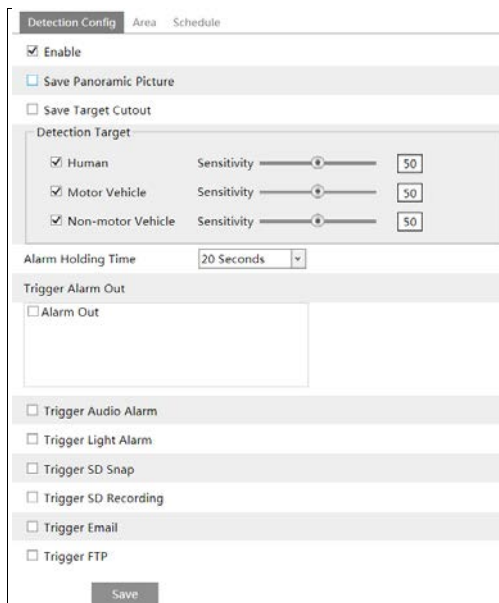
The sensitivity value of Video Cast Detection: The higher the value is, the more sensitive the system responds to the obscuring of the image.

※ The requirements of camera and surrounding area

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

4.4.2 Line Crossing

Line Crossing: Alarms will be triggered if the target crosses the pre-defined alarm lines. Go to Config→Event→Line Crossing interface as shown below.



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

Save Panoramic Picture: If it is enabled, the detected panoramic pictures will be captured and saved to the SD card when there are targets detected.

Save Target Cutout: If it is enabled, the detected target cutout pictures will be captured and saved to the SD card when there are targets detected.

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 and enable “Trigger Snap” 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.

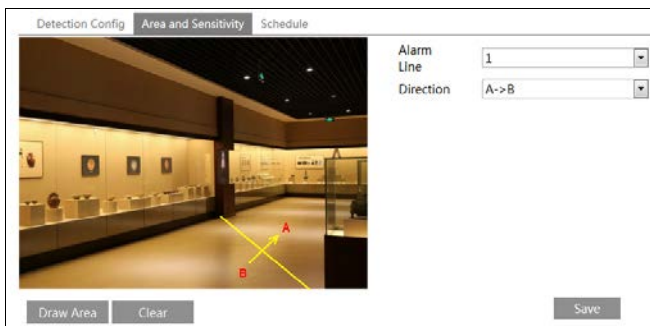
All of the three types of objects can be selected simultaneously. Please select the detection objects as needed. If no object/target is selected, alarms will not be triggered even if line crossing detection is enabled.

2. Set the alarm holding time.

3. Set alarm trigger options. The setup steps are the same as alarm in (sensor alarm) detection. Please refer to [Alarm IN](#) chapter for details.

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

5. Set area and sensitivity of the line crossing alarm. Click the “Area and Sensitivity” tab to go to the interface as shown below.



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

Direction: A<->B, A->B and A<-B optional. This indicates the direction of 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 [Schedule Recording](#)).

※ Configuration of camera and surrounding area

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

4.4.3 Intrusion

Intrusion: Alarms will be triggered if the target intrudes and loiters in 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→Intrusion interface as shown below.

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

Save Panoramic Picture: If it is enabled, the detected panoramic pictures will be captured and saved to the SD card when there are targets detected.

Save Target Cutout: If it is enabled, the detected target cutout pictures will be captured and saved to the SD card when there are targets detected.

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 and enable “Trigger Snap” first.

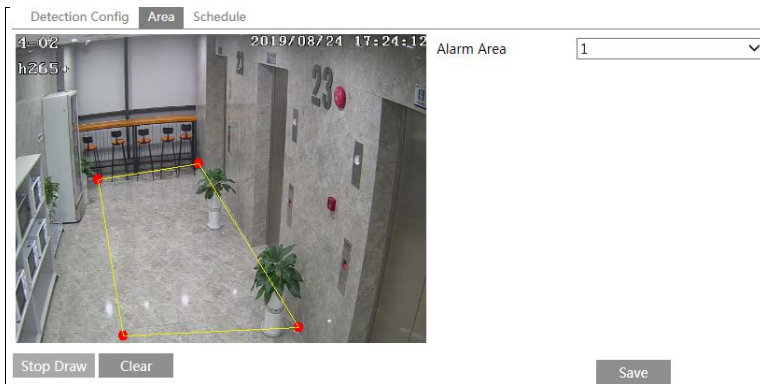
Detection Target: See [4.4.2 Line Crossing --Detection Target](#) for details.

2. Set the alarm holding time.

3. Set alarm trigger options. The setup steps are the same as alarm in (sensor alarm) detection. Please refer to [Alarm IN](#) chapter for details.

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

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



Set the alarm area number on the right side. Up to 4 alarm areas can be added.

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

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

※ Configuration requirements of camera and surrounding area

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

4.4.4 Region Entrance

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

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

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

- Enable:**
- Save Panoramic Picture:**
- Save Target Cutout:**
- Detection Target:**
 - Human:** Sensitivity: 50
 - Motor Vehicle:** Sensitivity: 50
 - Non-motor Vehicle:** Sensitivity: 50
- Alarm Holding Time:** 20 Seconds
- Trigger Alarm Out:** Alarm Out
- Trigger Audio Alarm:**
- Trigger Light Alarm:**
- Trigger SD Snap:**
- Trigger SD Recording:**
- Trigger Email:**
- Trigger FTP:**

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

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

Save Panoramic Picture: If it is enabled, the detected panoramic pictures will be captured and saved to the SD card when there are targets detected.

Save Target Cutout: If it is enabled, the detected target cutout pictures will be captured and saved to the SD card when there are targets detected.

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 and enable “Trigger Snap” first.

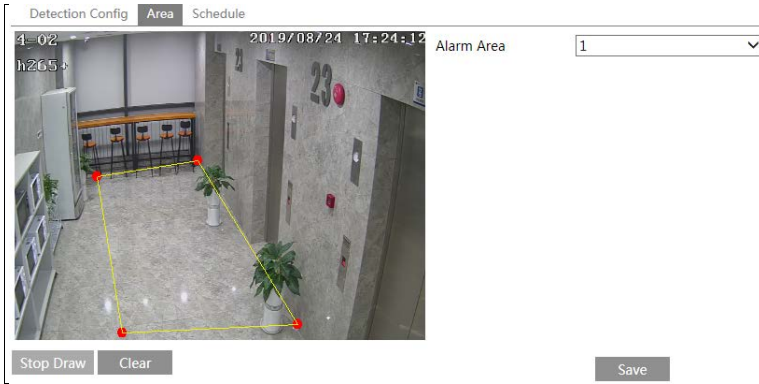
Detection Target: See [4.4.2 Line Crossing --Detection Target](#) for details.

2. Set the alarm holding time.

3. Set alarm trigger options. The setup steps are the same as alarm in (sensor alarm) detection. Please refer to [Alarm IN](#) chapter 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.

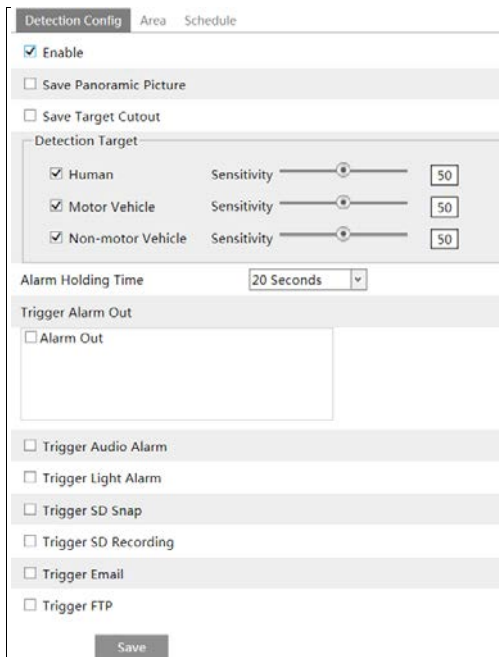
6. Set the schedule of the region entrance detection. The setup steps of the schedule are the same as schedule recording setup (See [Schedule Recording](#)).

* The configuration requirements of camera and surrounding area are the same as intrusion detection.

4.4.5 Region Exiting

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

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



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

Save Panoramic Picture: If it is enabled, the detected panoramic pictures will be captured and saved to the SD card when there are targets detected.

Save Target Cutout: If it is enabled, the detected target cutout pictures will be captured and saved to the SD card when there are targets detected.

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 and enable “Trigger Snap” first.

Detection Target: See [4.4.2 Line Crossing --Detection Target](#) for details.

2. Set the alarm holding time.

3. Set alarm trigger options. The setup steps are the same as alarm in (sensor alarm) detection. Please refer to [Alarm IN](#) chapter for details.

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

5. Set the alarm area of the region exiting 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.

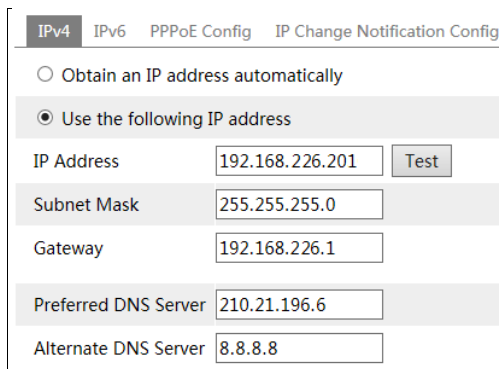
6. Set the schedule of the region exiting detection. The setup steps of the schedule are the same as schedule recording setup (See [Schedule Recording](#)).

* The configuration requirements of camera and surrounding area are the same as intrusion detection.

4.5 Network Configuration

4.5.1 TCP/IP

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



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

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

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

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

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.

IPv4	IPv6	PPPoE Config	IP Change Notification Config
<input type="checkbox"/> Trigger Email			
<input type="checkbox"/> Trigger FTP			
Save			

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.

4.5.2 Port

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

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

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.

4.5.3 Server Configuration

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

Enable
 Server Port:
 Server Address:
 Device ID:

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

4.5.4 DDNS

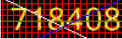
If the camera is set up with a DHCP connection, DDNS should be set for the internet.

1. Go to Config→Network→ DDNS.

Port Server **DDNS** SNMP B02.1X RTSP UPnP Email FTP HTTPS QoS
 Enable
 Server Type:
 User Name:
 Password:
 Domain:

2. Apply for a domain name. Take www.dvr dyndns.com for example.
 Enter www.dvr dyndns.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	 New Captcha <input type="text"/> Enter the text you see above
<input type="button" value="Submit"/> <input type="button" value="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

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

Search by Domain

Click a name to edit your domain settings.

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

Last Update: Not yet updated! IP Address: 210.21.229.139
[Create address/dns domain name]

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

4.5.5 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" value="public"/>
Write SNMP Community	<input type="text" value="private"/>
Trap Address	<input type="text" value="192.168.226.201"/>
Trap Port	<input type="text" value="162"/>
Trap community	<input type="text" value="public"/>
SNMP v3	
<input type="checkbox"/> Enable SNMPv3	
Read User Name	<input type="text" value="public"/>
Security Level	<input type="text" value="auth, priv"/>
Authentication Algorithm	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Authentication Password	<input type="text" value="••••••••"/>
Private-key Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES
Private-key Algorithm	<input type="text" value="••••••••"/>
Write User Name	<input type="text" value="private"/>
Security Level	<input type="text" value="auth, priv"/>
Authentication Algorithm	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Authentication Password	<input type="text" value="••••••~"/>
Private-key Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES
Private-key Algorithm	<input type="text" value="••••~"/>
Other Settings	
SNMP Port	<input type="text" value="161"/>
<input type="button" value="Save"/>	

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.

4.5.6 802.1x

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 and EAPOL version: Please use the default settings.

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

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

Note:1. This camera support 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.

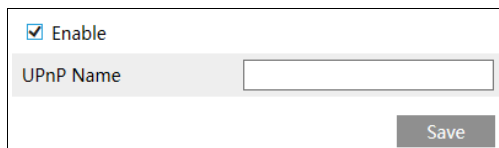
4. When playing the video through the multicast streams in a VLC player, please pay attention to the mode of the VLC player. If it is set to TCP mode, the video cannot be played.

5. If the coding format of the video of the main stream is MJPEG, the video may be disordered at some resolutions.

4.5.8 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.



Enable

UPnP Name

Save

4.5.9 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	
Sender Address	<input type="text" value="XXX@126.com"/>
User Name	<input type="text" value="XXX@126.com"/>
Password	<input type="password" value="•••••"/>
Server Address	<input type="text" value="smtp.126.com"/>
Secure Connection	<input type="text" value="Unnecessary"/>
SMTP Port	<input type="text" value="25"/> <input type="button" value="Default"/>
<input type="checkbox"/> Send Interval(S)	<input type="text" value="0"/> (0-3600)
<input type="button" value="Clear"/> <input type="button" value="Test"/>	
Recipient	
<input type="text" value="XXXX@126.com"/>	
<input type="text"/>	
Recipient Address	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Delete"/>	
<input type="button" value="Save"/>	

Sender Address: sender’s e-mail address.

User name and password: sender’s user name and password.

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.

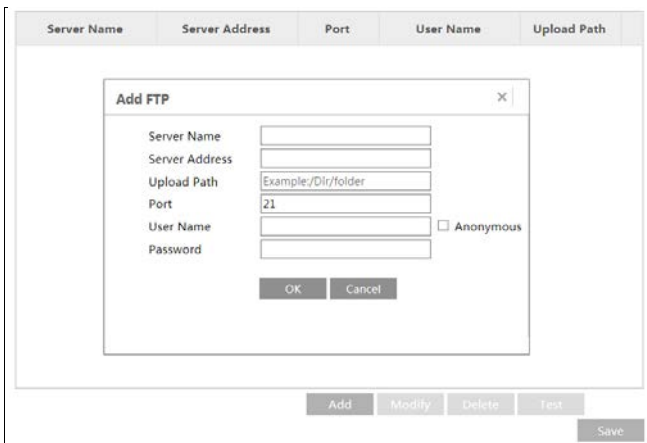
Click the “Test” button to test the connection of the account.

Recipient Address: receiver’s e-mail address.

4.5.10 FTP

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

Go to Config→Network →FTP.



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.

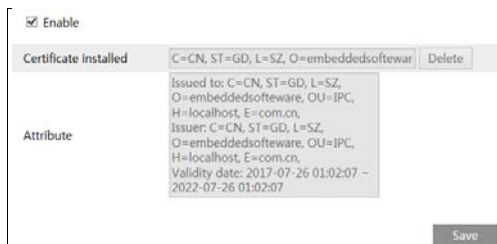
Port: The port of the FTP server.

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

4.5.11 HTTPS

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

Go to Config → Network → HTTPS as shown below.

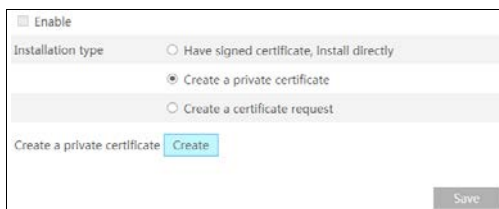


There is a certificate installed by default as shown above. Enable this function and save it. Then the camera can be accessed by entering https://IP: https port via the web browser (eg. https://192.168.226.201:443).

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

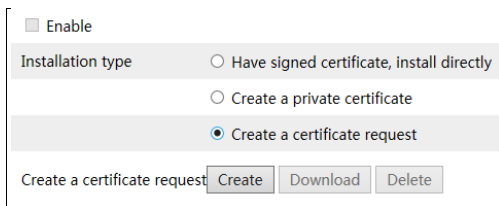


- * If there is a signed certificate, click “Browse” to select it and then click “Install” to install it.
- * Click “Create a private certificate” to enter the following creation interface.



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

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



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

4.5.12 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	13
Alarm DSCP	35
Manager DSCP	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 speaking, the larger the number is, the higher the priority is.

4.6 Security Configuration

4.6.1 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.

Add User ✕

User Name

Password

Level

The password can be composed of numbers, special characters, upper or lower case letters.

Confirm Password

User Type

Bind MAC

2. Enter user name in “User Name” textbox.

3. Enter the password in the “Password” and “Confirm Password” textbox. Please set the password according to the requirement of the password security level (Go to Config→Security→Security Management→Password Security interface to set the security level).

4. Choose the user type. Administrator has all permissions. Normal user can only view the

live video. Advanced user has the same permissions as an Administrator except for; user, backup settings, factory reset, and upgrading the firmware.

5. Enter the MAC address of the PC in “Bind MAC” textbox.

If this option is enabled, only the PC with the specified MAC address can access the camera for that user.

6. 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 and MAC address if necessary 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. Enter computer’s MAC address as necessary.

6. Click the “OK” button to save the settings.

Note: To change the access level of a user, the user must be deleted and added again with the new access level.

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.

4.6.2 Online User

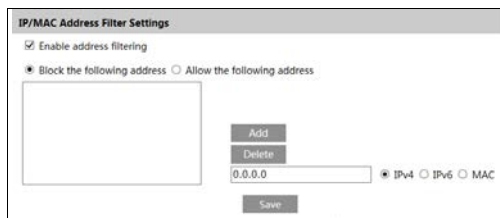
Go to Config→Security→Online User to view the user who is viewing the live video.

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).

4.6.3 Block and Allow Lists

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



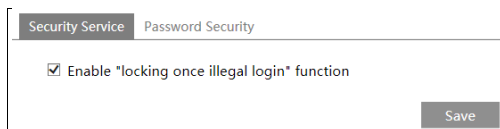
The setup steps are as follows:

Check the “Enable address filtering” check box.

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

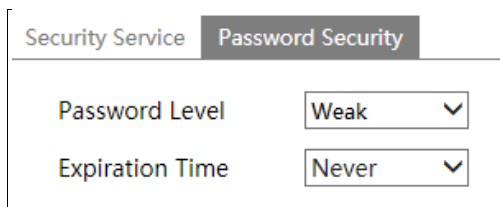
4.6.4 Security Management

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



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

- Password Security



Please set the password level and expiration time as needed.

Password Level: Weak, Medium or Strong.

Weak level: Numbers, special characters, upper or lower case letters can be used. You can

choose one of them or any combination of them when setting the password.

Medium Level: 9~15 characters, including at least two of the following categories: numbers, special characters, upper case letters and lower case letters.

Strong Level: 9~15 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.

4.7 Maintenance Configuration

4.7.1 Backup and Restore

Go to Config→Maintenance→Backup & Restore.

Import Setting

Path

Export Settings

Default Settings

Keep

Network Config

Security Configuration

Image Configuration

- **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.

4.7.2 Reboot

Go to Config→Maintenance→Reboot.

Click the “Reboot” button to reboot the device.

Timed Reboot Setting:

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

4.7.3 Upgrade

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

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

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

4.7.4 Operation Log

To query and export log:

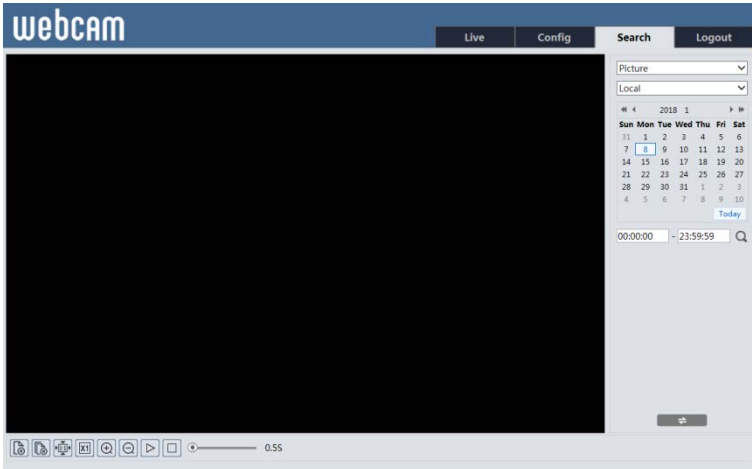
1. Go to Config→Maintenance→Operation Log.

Index	Time	Main Type	Sub Type	User Name	Login IP
1	2015-07-14 11:15:18	Operation	Log in	admin	192.168.12.53
2	2015-07-14 11:12:02	Exception	Disconnected		192.168.12.53
3	2015-07-14 19:12:17	Exception	Disconnected		192.168.12.52


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.

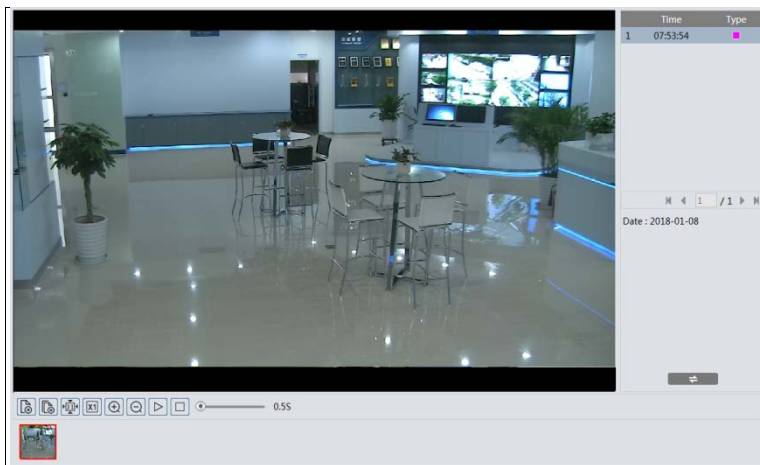
5.1 Image Search


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



● Local Image Search

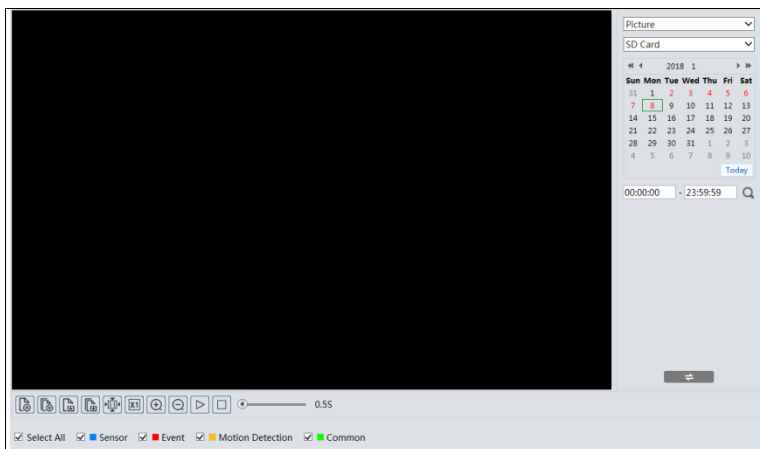
1. Choose “Picture”—“Local”.
2. Set time: Select date and choose the start and end time.
3. Click  to search the images.
4. Double click a file name in the list to view the captured photos as shown above.





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.

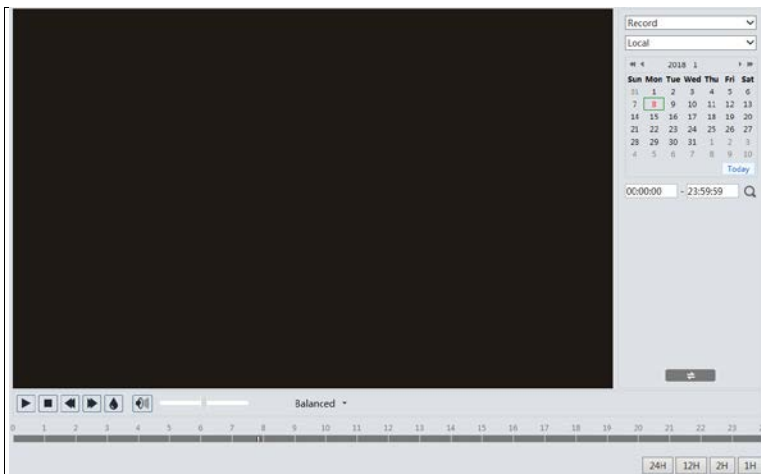
The descriptions of the buttons are shown as follows.

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.
	Fit size: Click to fit the image on the screen.		Actual size: Click this button to display the actual size of the image.
	Zoom in: Click this button to digitally zoom in.		Zoom out: Click this button to digitally zoom out.
	Slide show play: Click this button to start the slide show mode.		Stop: Click this button to stop the slide show.
	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.




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.

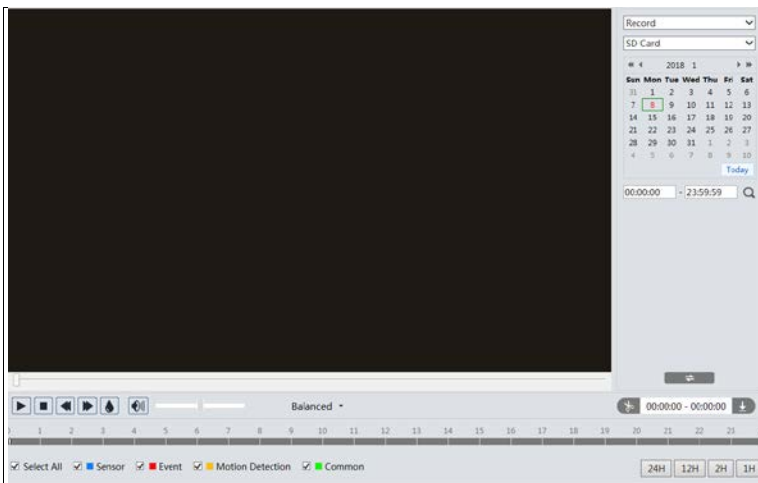


Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button
	Stop button		Speed down
	Speed up		Watermark display
	Enable / disable audio; drag the slider to adjust the volume after enabling audio.		

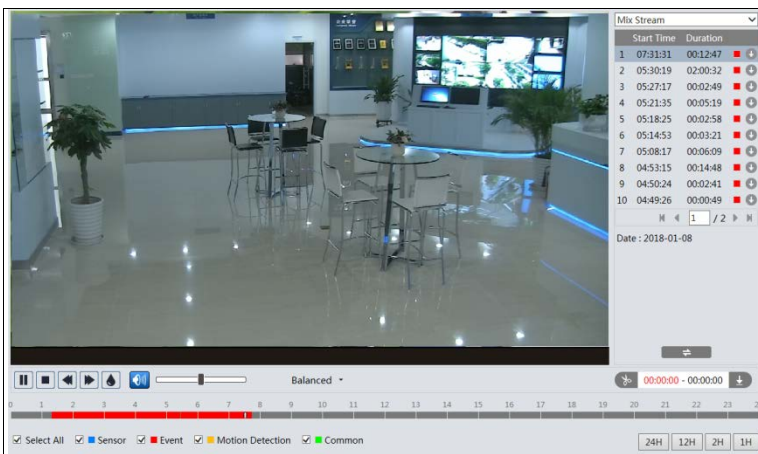
5.2.2 SD Card Video Search

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.



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

Video clip and downloading

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

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 1 Troubleshooting

How to find the password?

A: Reset the device to the default factory settings.

Default IP: 192.168.226.201; User name: admin; Password: 123456

Fail to connect devices through IE browser.

A: Network is not well connected. Check the connection and make sure it is connected well.

B: IP address is not available. Reset the IP address.

C: Web port number has been changed: contact administrator to get the correct port number.

D: Exclude the above reasons. Restore to default setting by IP-Tool.

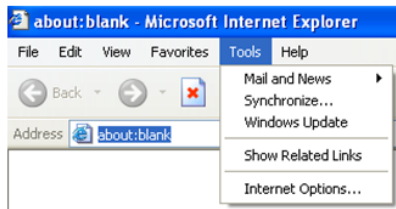
IP tool cannot search devices.

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

IE cannot download ActiveX control.

A. IE browser may be set up to block ActiveX. Follow the steps below.

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

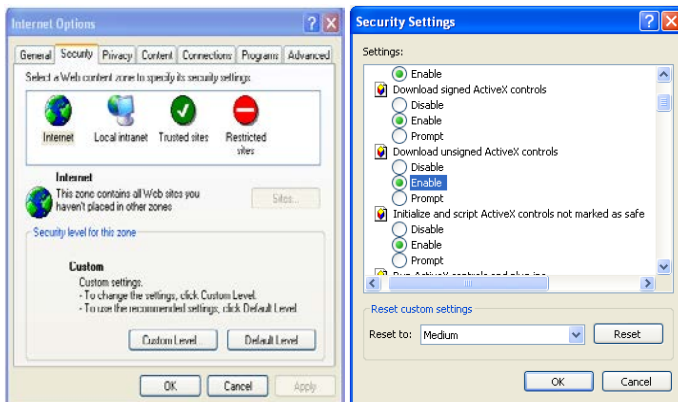


② Select Security-----Custom Level....

③ Enable all the options under "ActiveX controls and plug-ins".

④ Click OK to finish setup.

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



No sound can be heard.

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

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