

# TECHVISION USA



## MOBILE APPS

FREE MOBILE APPS  
FOR ANDRIOD AND IOS



## FREE TECH SUPPORT

FAST SERVICE SUPPORT

## IB-S2LIR100W2

### 2MP IP Fixed Lens Bullet



- Please use the specified power supply to connect.
- 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, Relative 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 is product instructions not quality warranty. 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.
- When this product is in use, the relevant contents of Microsoft, Apple and Google will be involved in. The pictures and screenshots in this manual are only used to explain the usage of our product. 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 IR water-proof network camera. All pictures and examples used in the manual are for reference only.

# 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.
- 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

### 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.

# Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
<b>2</b>	<b>Network Connection .....</b>	<b>2</b>
2.1	LAN .....	2
2.1.1	Access through IP-Tool .....	2
2.1.2	Directly Access through IE .....	4
2.2	WAN .....	5
<b>3</b>	<b>Live View .....</b>	<b>8</b>
<b>4</b>	<b>Configuration .....</b>	<b>9</b>
4.1	System Configuration .....	9
4.1.1	Basic Information .....	9
4.1.2	Date & Time .....	9
4.1.3	Local Configuration .....	10
4.1.4	Storage .....	10
4.2	Image Configuration .....	12
4.2.1	Display Configuration .....	13
4.2.2	Video/Audio Settings .....	14
4.2.3	OSD Configuration .....	16
4.2.4	Video Mask .....	16
4.2.5	ROI Configuration .....	17
4.3	Alarm Configuration .....	18
4.3.1	Motion Detection .....	18
4.3.2	Other Alarms .....	20
4.3.3	Alarm Server .....	20
4.4	Event Configuration .....	21
4.4.1	Object Removal .....	21
4.4.2	Exception .....	23
4.4.3	Line Crossing .....	24
4.4.4	Intrusion .....	25
4.5	Network Configuration .....	26
4.5.1	TCP/IP .....	26
4.5.2	Port .....	28
4.5.3	Server Configuration .....	28
4.5.4	DDNS Configuration .....	28
4.5.5	802.1x .....	30
4.5.6	RTSP .....	30
4.5.7	UPNP .....	32
4.5.8	Mail Configuration .....	32
4.5.9	FTP .....	33
4.5.10	HTTPS .....	33
4.5.11	QoS .....	35

4.6	Security Configuration.....	35
4.6.1	User Configuration .....	35
4.6.2	Online Video User .....	37
4.6.3	Block and Allow List .....	37
4.6.4	Security Management .....	37
4.7	Maintenance Configuration.....	38
4.7.1	Backup and Restore .....	38
4.7.2	Reboot .....	38
4.7.3	Upgrade .....	39
4.7.4	Operation Log.....	39
<b>5</b>	<b>Search .....</b>	<b>40</b>
5.1	Image Search .....	40
5.2	Video Search.....	42
5.2.1	Local Video Search.....	42
5.2.2	SD Card Video Search.....	43
<b>Appendix.....</b>		<b>45</b>
<b>Appendix 1 Q &amp; A.....</b>		<b>45</b>
<b>Appendix 2 Specifications .....</b>		<b>46</b>

# 1 Introduction

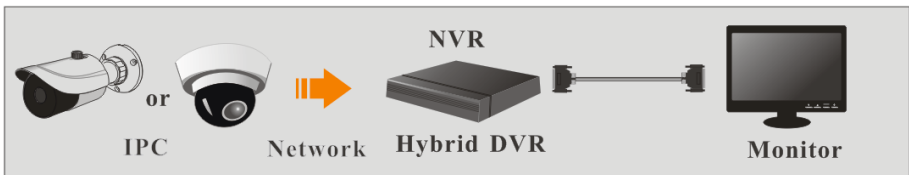
This IP-CAMERA (short for IP-CAM) is designed for high performance CCTV solutions. It adopts state-of-the-art video processing chips, integrated with the most advanced technologies (like video encoding and decoding technology) to make the image transmission more stable and smooth. Moreover, the built-in WEB server of this series improves the performance of the traditional surveillance system so that users can be easy to operate and monitor.

This product is widely used in banks, telecommunication systems, electricity power departments, law systems, factories, storehouses, uptowns, etc. In addition, it is also an ideal choice for surveillance sites with middle or high risks.

## Main Features

- ICR auto switch, true day/night
- 3D DNR, digital WDR, defog, BLC, HLC
- ROI coding
- Support mobile surveillance by smart phones

## Surveillance Application



## 2 Network Connection

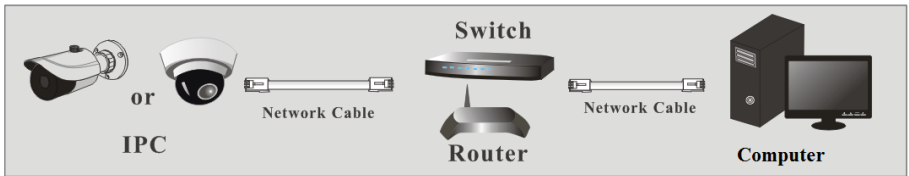
Connect IP-CAM via LAN or WAN. Here only take IE browser for example. The details are as follows:

### 2.1 LAN

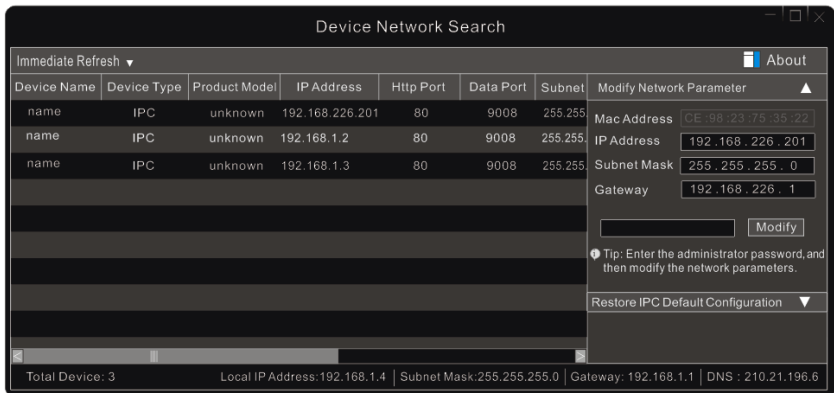
In LAN, there are two ways to access IP-CAM: 1. access through IP-Tool; 2. directly access through IE browser.

#### 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 “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. Then follow directions to install and run the applicable plug-in.

Enter the username and password 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**

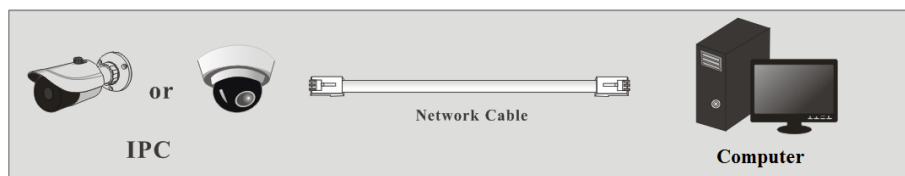
Subnet Mask: **255.255.255.0**

Gateway: **192.168.226.1**

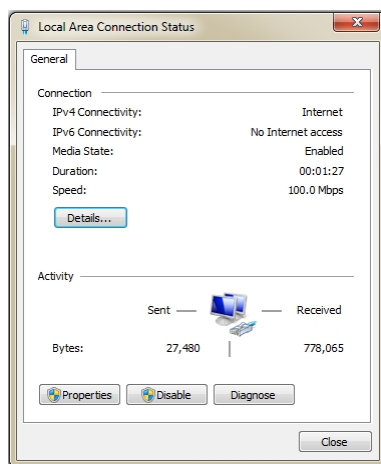
HTTP: **80**

Data port: **9008**

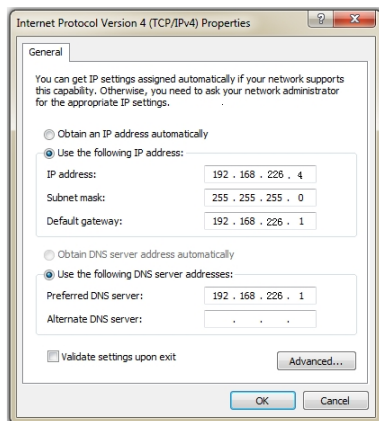
Use the above default settings when logging in the camera for the first time. Directly connect the camera to the computer through the network cable.



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.



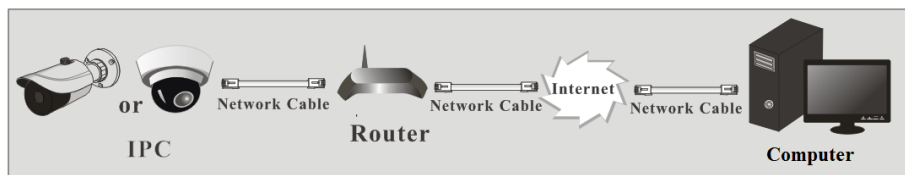
Select “Properties” and then select internet protocol according to the actual situation (for example: IPv4). Next, click “Properties” button to set the network of the PC.



- 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

- ② Go to Config →Network → TCP/IPv4 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		<input type="button" value="Test"/>
Subnet Mask	255.255.255.0		
Gateway	192.168.226.1		
Preferred DNS Server	192.168.226.1		
Alternate DNS Server	8.8.8.8		

- 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".

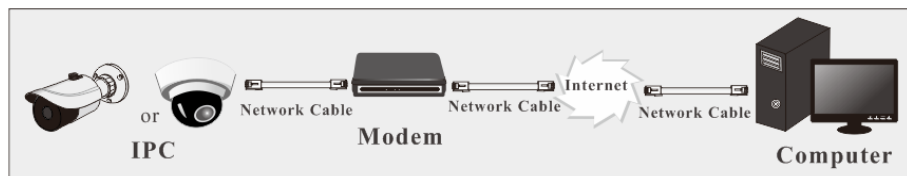
Port Range					
Application	Start	End	Protocol	IP Address	Enable
1	9007	to 9008	Both	192.168.1.201	<input checked="" type="checkbox"/>
2	80	to 81	Both	192.168.1.201	<input checked="" type="checkbox"/>
3	10000	to 10001	Both	192.168.1.166	<input type="checkbox"/>
4	21000	to 21001	Both	192.168.1.166	<input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

Router Setup

- ④ Open the IE browser and enter its WAN IP and http port to access.

### ➤ Access through PPPoE dial-up

Network connection



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

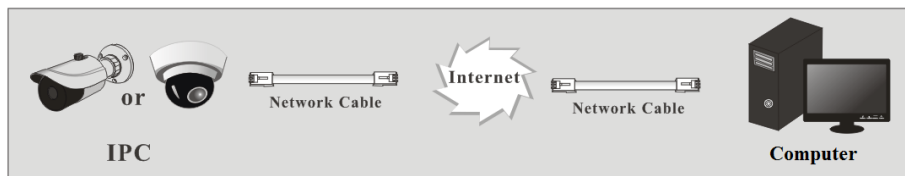
- ① Go to Config→Network→Port menu to set the port number.
- ② Go to Config →Network→TCP/IP→PPPoE Config menu. Enable PPPoE and then enter the user name and password from your internet service provider.

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

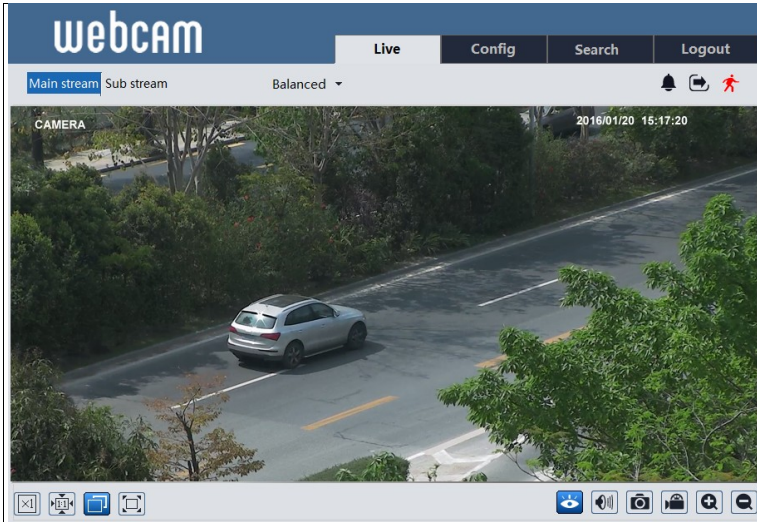


The setup steps are as follow:

















- 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		Zoom in
	Appropriate size		Zoom out
	Auto		Motion alarm indicator
	Full screen		SD card recording indicator
	Start/stop live view		Abnormal clarity indicator
	Snapshot		Line crossing indicator
	Enable/disable audio (only some models support)		Intrusion indicator
	Start/stop record		Scene change 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.

### 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	IPC
Brand	Customer
Software Version	4.2.1.0(29686)
Software Build Date	2021-02-23
Kernel Version	01000009
Hardware Version	1.4-1412128
Onvif Version	20.06
OCX Version	2.0.6.5
MAC	00:18:ae:aa:93:f5

#### 4.1.2 Date & 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 type="checkbox"/> DST					
<input checked="" type="radio"/> Auto DST					
<input type="radio"/> Manual DST					
Start Time	January ▼	First ▼	Sunday ▼	00 ▼	Hour
End Time	Februar ▼	First ▼	Monday ▼	00 ▼	Hour
Time Offset	120 Minutes ▼				
<div>Save</div>					

Select the time zone and DST as desired.

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

Zone	Date and Time
Time Mode:	
<input checked="" type="radio"/> Synchronize with NTP server NTP server: <input type="text" value="time.windows.com"/> Update period: <input type="text" value="1440"/> Minutes	
<input type="radio"/> Synchronize with computer time Date: <input type="text" value="2021-03-09"/> Time: <input type="text" value="11:22:19"/>	
<input type="radio"/> Set manually Date: <input type="text" value="2021-03-09"/> Time: <input type="text" value="03:22:16"/>	
<input type="button" value="Save"/>	

### 4.1.3 Local Configuration

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.

Save snapshots to	<input type="text" value="C:\Program Files\NetIPCamera"/>	<input type="button" value="Browse"/>
Save recording files to	<input type="text" value="C:\Program Files\NetIPCamera"/>	<input type="button" value="Browse"/>
Audio Recording	<input type="radio"/> Open <input checked="" type="radio"/> Close	
Bitrate Overlay	<input type="radio"/> Open <input checked="" type="radio"/> Close	

For the model with audio input connector or built-in MIC, there is an option to enable or disable the audio recording.

### 4.1.4 Storage

**This function is only available for the model with SD card slot.**

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

Management	Record	Snapshot
Total picture capacity	<input type="text" value="379 MB"/>	
Picture remaining space	<input type="text" value="379 MB"/>	
Total recording capacity	<input type="text" value="3329 MB"/>	
Record remaining space	<input type="text" value="3072 MB"/>	
State	<input type="text" value="Normal"/>	
Snapshot Quota	<input type="text" value="10"/> %	
Video Quota	<input type="text" value="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 and video quota can be modified as needed.

## ● Schedule Recording Settings

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

Management **Record** Snapshot

**Record Parameters**

Record Stream: Main stream

Pre Record Time: No Pre Record

Cycle Write: Yes

**Timing**

☒ Enable Schedule Record

2. Set record stream, pre-record time and 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.

Week Schedule ○ Erase ● Add

Sun. 00:00-24:00 Manual Input

Mon. 00:00-24:00 Manual Input

Tue. 00:00-24:00 Manual Input

Wed. 00:00-24:00 Manual Input

Thu. 00:00-24:00 Manual Input

Fri. 00:00-24:00 Manual Input

Sat. 00:00-24:00 Manual Input

**Holiday Schedule**

Date: 07-12 Add Delete

00:00-24:00 Manual Input

## 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	
<b>Snapshot Parameters</b>					
Image Format	JPEG				
Resolution	704x576				
Image Quality	Low				
<b>Event Trigger</b>					
Snapshot Interval	1	Second			
Snapshot Quantity	5				
<b>Timing</b>					
<input type="checkbox"/> Enable Timing Snapshot					
Snapshot Interval	5	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.

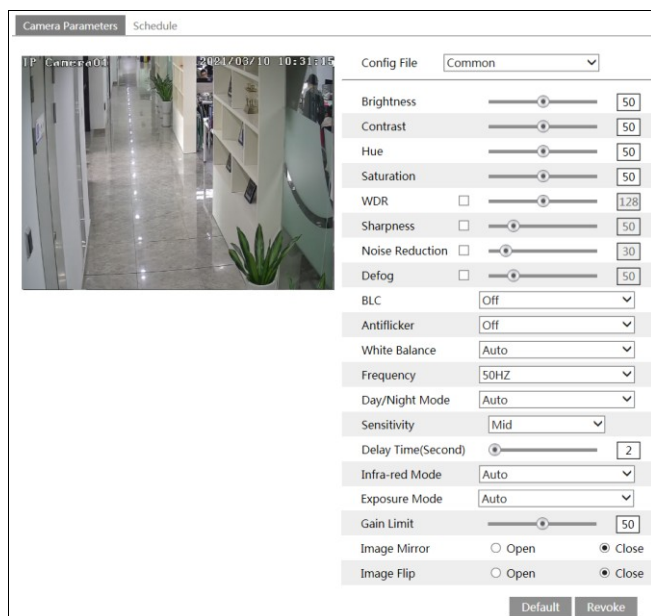
**Timing Snapshot:** Enable timing snapshot first and then set the snapshot interval and schedule. The setup steps of schedule are the same as the schedule recording (See [Schedule Recording](#)).

## 4.2 Image Configuration

Image Configuration includes five submenus: 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 is, the brighter the image is.

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

**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.

**Backlight Compensation (BLC):**

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

of the image in the darkest area will be seen clearly.

**Antiflicker:**

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

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

**Frequency:** 50Hz and 60Hz can be optional.

**Day/night Mode:** Please choose the mode as needed.

**Sensitivity:** High, middle and low can be selected for switching back and forth from day to night modes.

**Infrared Mode:** Choose “ON”, “OFF” and “Auto” (**Some models may not support the infrared mode**).

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

**Gain Limit:** The higher the gain value is, the higher the brightness of the image is and the more noises of the image are.

**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.

The screenshot shows a web interface with two tabs: 'Camera Parameters' and 'Schedule'. The 'Schedule' tab is active. Below the tabs, there are two dropdown menus. The first is labeled 'Schedule' and has 'Full Time' selected. The second is labeled 'Config File' and has 'Common' selected.

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 a 'Timing' configuration window. At the top, a 'Schedule' dropdown is set to 'Timing'. Below it is a 'Time Range' section with a horizontal timeline from 0:00 to 24:00. The timeline is divided into segments. A legend below the timeline indicates that blue segments represent 'Day' and blank segments represent 'Night'. In the current view, the entire timeline is blue. A 'Save' button is located at the bottom right of the window.

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 Timing, the image configuration mode will automatically switch between day and night according to the schedule.

## 4.2.2 Video/Audio Settings

The following interface will be displayed by clicking Config→Image→Video/Audio.

Video
Audio

Index	Stream	Resolution	Frame	Bitrate Type	Bitrate(Kbps)	Video	I Frame	Video	Profile
1	Main stream	1920x1080	25	CBR	3072	Highest	100	H264	High Profile
2	Sub stream	704x576	25	CBR	480	Highest	100	H264	High Profile
3	Third stream	352x288	25	CBR	128	Higher	100	H264	High Profile

Send Snapshot 2 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:** H264/H265 can be selected.

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

**Send Snapshot:** Set the snapshot stream. 2 stands for sub stream, 3 stands for third 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.

Video

Audio

☒ Enable

Audio Encoding
 

G711A

Audio Type
 

LIN

LIN In Volume
 

8

Save

**Audio Encoding:** G711A and G711U are selectable.

**Audio Type:** MIC or LIN

**Note:** Only the model with audio input connector or built-in MIC can set audio encoding and audio type. Additionally, MIC/LIN In volume can be adjustable as needed.

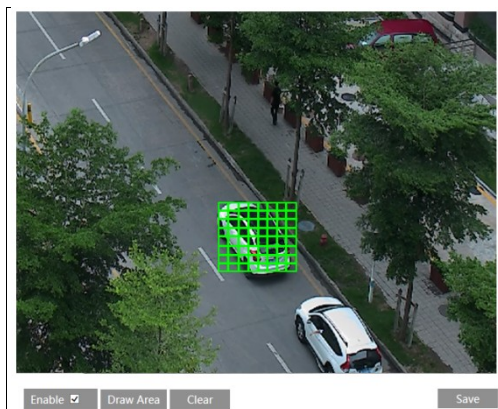
### 4.2.3 OSD Configuration

Go to Config→Image→OSD menu to display the interface as shown below:

Time stamp, device name and OSD can be set up here. After enabling the corresponding display and entering the content, drag them to change their position. Then press the “Save” button to save the settings.

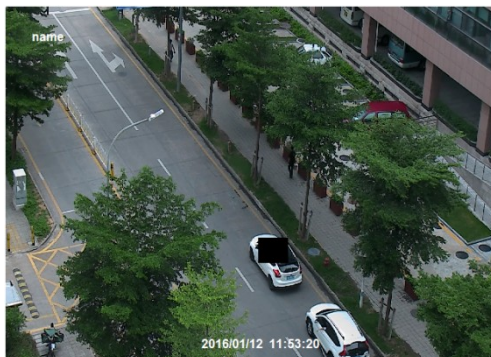
### 4.2.4 Video Mask

Go to Config→Image→Video Mask menu to display the 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 blocked out in the image.

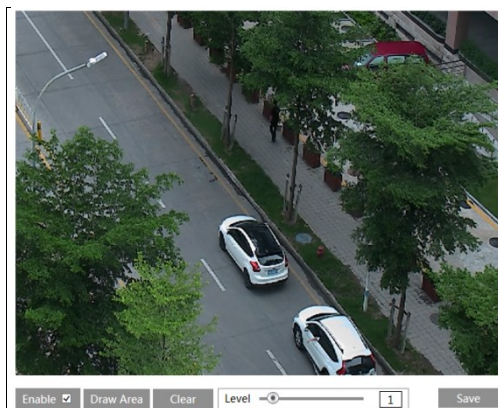


To clear the video mask:

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

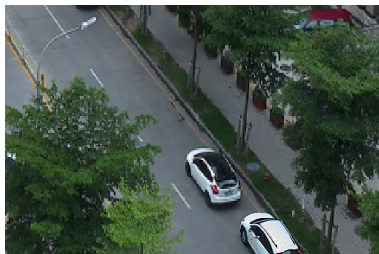
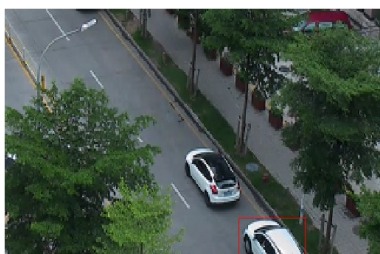
### 4.2.5 ROI Configuration

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.



#### To set up ROI

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.



## 4.3 Alarm Configuration

### 4.3.1 Motion Detection

To set motion detection:

1. Go to Config→Alarm→Motion Detection to set motion detection alarm.
- 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 Config   Area and Sensitivity   Schedule

☒ Enable

Alarm Holding Time   20 Seconds   ▾

☐ Trigger Snap

☐ Trigger SD Recording

☐ Trigger Email

☐ Trigger FTP

Save

Then select the alarm holding time and set the alarm trigger options.

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

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

Alarm Config   Area and Sensitivity   Schedule

Sensitivity   Low   High   4

Draw Area   ☒ Add   ☐ Erase

Select All   Clear All   Invert

Save

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

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

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

3. Set the schedule of the 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.

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

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

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

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

4. Set alarm trigger options. Trigger Email and FTP. The setup steps are the same as motion detection. Please refer to motion detection chapter for details.

### 4.3.3 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	<input type="text"/>
Port	<input type="text" value="0"/>
Heartbeat	<input type="text" value="Disable"/> ▼
Heartbeat interval	<input type="text" value="30"/> Second

## 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 Object Removal

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

To set object removal:

Go to Config→Event→Object Removal interface as shown below.

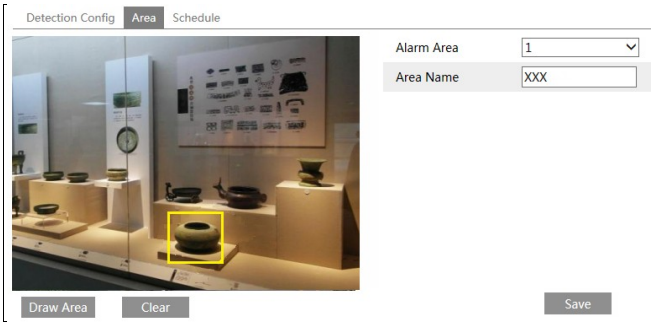
Detection Config	Area	Schedule
<input checked="" type="checkbox"/> Enable		
<input checked="" type="radio"/> Enable Left Detection		
<input type="radio"/> Enable Item Missing Detection		
Alarm Holding Time	<input type="text" value="20"/> Seconds	▼
<input type="checkbox"/> Trigger Snap		
<input type="checkbox"/> Trigger SD Recording		
<input type="checkbox"/> Trigger Email		
<input type="checkbox"/> Trigger FTP		
<input type="button" value="Save"/>		

1. Enable object removal detection and then select the detection type.

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

**Enable Item Missing 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 motion detection chapter for details.
3. Click “Save” button to save the settings.
4. Set the alarm area of the object removal 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 object removal detection. The setup steps of schedule are the same as the schedule recording (See [Schedule Recording](#)).

### ※ 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 object removal 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. Object removal detection cannot determine the objects’ ownership. For instance, there is an unattended package in the station. Object removal detection can detect the package itself but it cannot determine to whom it belongs to.
6. Try not to enable object removal detection when light changes greatly in the scene.
7. Try not to enable object removal detection if there are complex and dynamic environments in the scene.
8. Adequate light and clear scenery are very important to object removal detection.

## 4.4.2 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.

The screenshot shows the 'Detection Config' tab of the Exception detection settings. It contains the following elements:

- Scene change detection:** A checked checkbox.
- Video blur detection:** An unchecked checkbox.
- Alarm Holding Time:** A dropdown menu currently set to '20 Seconds'.
- Trigger Snap:** An unchecked checkbox.
- Trigger SD Recording:** An unchecked checkbox.
- Trigger Email:** An unchecked checkbox.
- Trigger FTP:** An unchecked checkbox.
- Save:** A button at the bottom right.

1. Enable “Video blur detection”.

**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.

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

3. Click “Save” to save the settings.

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

The screenshot shows the 'Sensitivity' tab of the Exception detection settings. It contains the following elements:

- Sensitivity:** A slider control with a circular knob and a text input box next to it containing the value '28'.
- Save:** A button at the bottom right.

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 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.

## 4.4.3 Line Crossing

**Line Crossing:** Alarms will be triggered if someone or something crosses the pre-defined alarm lines.

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

1. Enable line crossing alarm.
2. Set the alarm holding time and choose the alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection chapter for details.
3. Click “Save” to save the settings.
4. 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. Only 1 line can be added.

**Direction:** A<->B, A->B and A<-B are optional. This indicates the direction of the intruder who crosses over the alarm line that would trigger the alarm.

**A<->B:** The alarm will be triggered when the intruder crosses over the alarm line from B to A

or from A to B.

**A->B:** The alarm will be triggered when the intruder crosses over the alarm line from A to B.

**A<-B:** The alarm will be triggered when the intruder crosses over the alarm line from B to A.

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

5. Set the schedule of the line crossing alarm. The schedule setup steps of the line crossing detection 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.

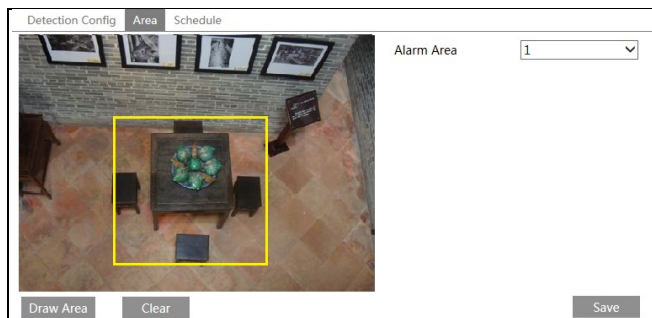
## 4.4.4 Intrusion

**Intrusion:** Alarms will be triggered if someone or something intrudes into the pre-defined areas.

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

Detection Config	Area	Schedule
<input checked="" type="checkbox"/> Enable		
Alarm Holding Time		20 Seconds ▾
<input type="checkbox"/> Trigger Snap		
<input type="checkbox"/> Trigger SD Recording		
<input type="checkbox"/> Trigger Email		
<input type="checkbox"/> Trigger FTP		

1. Enable region intrusion detection alarm.
2. Set the alarm holding time and choose the alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection chapter for details.
3. Click “Save” to save the settings.
4. 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. Only one alarm area can be added. Click “Draw Area” and then draw a rectangle in the image on the left side. Click “Stop Draw” to stop drawing. Click “Clear” to delete the alarm area. Click “Save” to save the settings.

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

### ※ Configuration requirements of camera and surrounding area

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

## 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.



**1. 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.

**2. 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, a new IP address will be sent to the appointed mailbox automatically.

**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. 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: Optional. 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. It can be changed to any port which is not occupied.

RTSP Port: The default port is 554. It can be changed to any port which is not occupied.

### 4.5.3 Server Configuration

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

<input type="checkbox"/> Enable	
Server Port	0
Server Address	
Device ID	1

1. Check “Enable”.
2. Check the IP address and auto report 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, input the remaining information of the device in the ECMS/NVMS. After that, the system will auto allot a device ID. Please check it in the ECMS/NVMS.
3. Input the above-mentioned server address, server port and device ID in the responding boxes. Click “Save” button to save the settings.



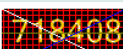
### 4.5.4 DDNS Configuration

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="mintdns"/>
Server Address	<input type="text" value="www.dvrdydns.com"/>
User Name	<input type="text"/>
Password	<input type="password"/>
Domain	<input type="text"/>

2. Apply for a domain name. Take [www.dvrdydns.com](http://www.dvrdydns.com) for example. Input [www.dvrdydns.com](http://www.dvrdydns.com) in the IE address bar to visit its website. Then click “Registration” button.

NEW USER REGISTRATION	
USER NAME	<input type="text" value="xxxx"/>
PASSWORD	<input type="password" value="•••••"/> 
PASSWORD CONFIRM	<input type="password" value="•••••"/>
FIRST NAME	<input type="text" value="xxx"/>
LAST NAME	<input type="text" value="xxx"/>
SECURITY QUESTION.	<input type="text" value="My first phone number."/> 
ANSWER	<input type="text" value="xxxxxxxx"/>
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.

<i>You must create a domain name to continue.</i>	
Domain name must start with (a-z, 0-9). Cannot end or start, but may contain a hyphen and is not case-sensitive.	
<input type="text" value="dvrdydns.com"/>	<input type="button" value="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.dvrdyns.com

Last Update: *Not yet updated* IP Address: 210.21.229.138

Create additional domain names

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

### 4.5.5 802.1x

IEEE802.X is an access control protocol. The setting steps are as follows:

☒ 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.

### 4.5.6 RTSP

Go to Config→Network→RTSP.

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

**Audio:** Having entered the main/sub stream in a VLC player, the video and audio will play automatically. (it is only available for the model with audio input connector or built-in MIC)

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.

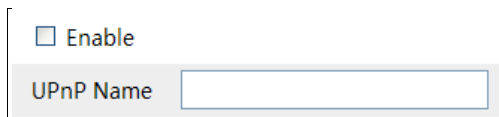
3. Avoid the use of the same multicast address in the same local network.

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.

### 4.5.7 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.



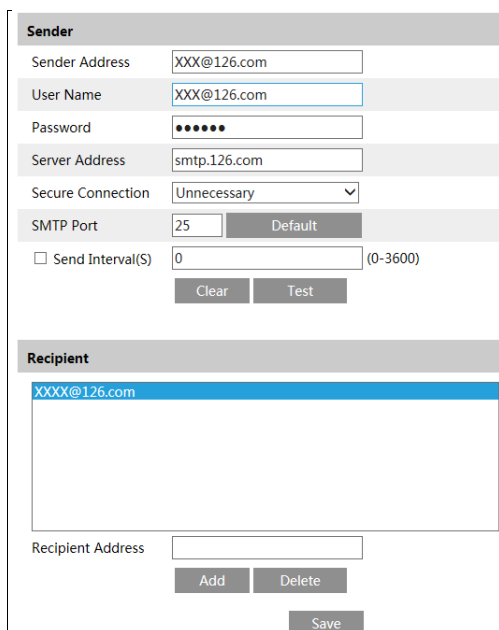
☐ Enable

UPnP Name

### 4.5.8 Mail Configuration

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

User Name

Password

Server Address

Secure Connection  ▼

SMTP Port

☐ Send Interval(S)  (0-3600)

**Recipient**

Recipient Address

**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.

### 4.5.9 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	Server Address	Port	User Name	Upload Path
<div> <div> Add FTP </div> <div> <div> Server Name <input type="text"/> </div> <div> Server Address <input type="text"/> </div> <div> Upload Path <input type="text" value="Example/Dir/folder"/> </div> <div> Port <input type="text" value="21"/> </div> <div> User Name <input type="text"/> </div> <div> Password <input type="password"/> </div> <div> <input type="checkbox"/> Anonymous </div> <div> <div>OK</div> <div>Cancel</div> </div> </div> </div>				

Add

Modify

Delete

Test

Save

**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.

### 4.5.10 HTTPS

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

Go to Config→Network→HTTPS as shown below.

☒ Enable

Certificate installed: C=CN, ST=GD, L=SZ, O=embeddedsoftware [Delete]

Attribute: Issued to: C=CN, ST=GD, L=SZ, O=embeddedsoftware, OU=IPC, H=localhost, E=com.cn, Issuer: C=CN, ST=GD, L=SZ, O=embeddedsoftware, OU=IPC, H=localhost, E=com.cn, Validity date: 2017-07-26 01:02:07 ~ 2022-07-26 01:02:07

[Save]

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.

☒ Enable

Installation type: ☒ Have signed certificate, install directly  
☐ Create a private certificate  
☐ Create a certificate request

Install certificate: [Browse] [Install]

[Save]

\* 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.

☒ Enable

Installation type: ☐ Have signed certificate, install directly  
☒ Create a private certificate  
☐ Create a certificate request

Create a private certificate: [Create]

[Save]

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.

☒ Enable

Installation type: ☐ Have signed certificate, install directly  
☐ Create a private certificate  
☒ Create a certificate request

Create a certificate request: [Create] [Download] [Delete]

[Save]



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.

## 4.5.11 QoS

QoS (Quality of Service) function is used to provide different quality of services for various network applications. Under 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

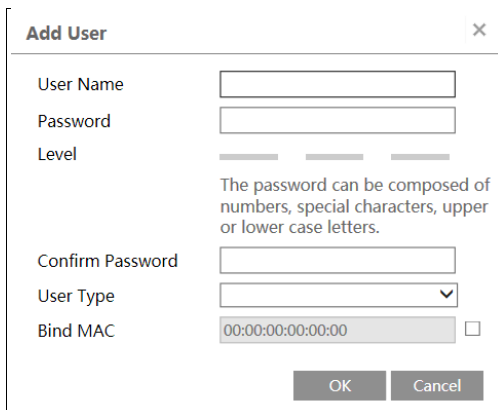
### 4.6.1 User Configuration

Go to Config→Security.

<div>Add</div> <div>Modify</div> <div>Delete</div>			
Index	User Name	User Type	Binding MAC
1	admin	Administrator	

#### Add user:

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



**Add User** [X]

User Name

Password

Level

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

Confirm Password

User Type

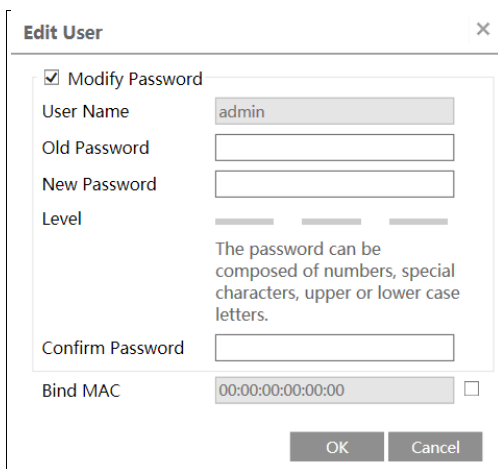
Bind MAC  ☐

OK Cancel

2. Enter user name in “User Name” textbox.
3. Enter letters or numbers in “Password” and “Confirm Password” textbox.
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.



**Edit User** [X]

☒ Modify Password

User Name

Old Password

New Password

Level

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

Confirm Password

Bind MAC  ☐

OK Cancel

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 Video User

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

## 4.6.3 Block and Allow List

Go to Config→Security→Block and Allow Lists.

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.

## 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.

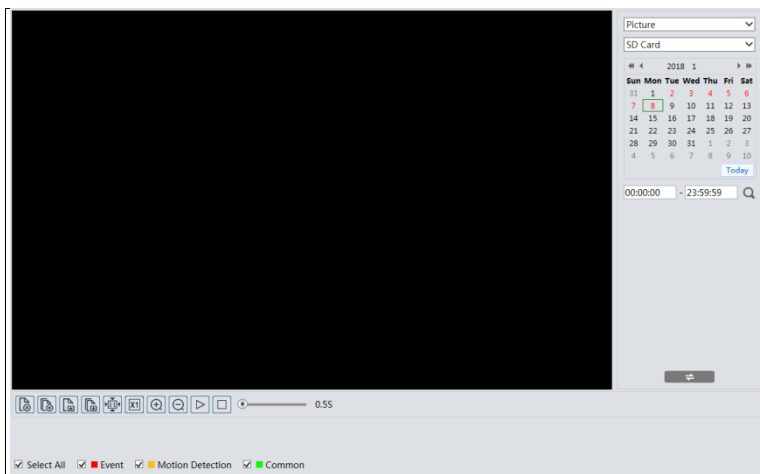




Click  to return to the previous interface.

### ● SD Card Image Search












This function is only available for the model with SD card slot.

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.

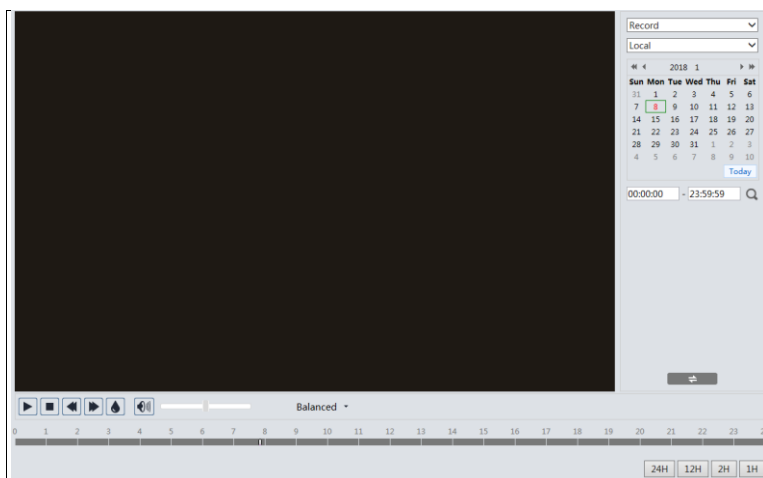
The descriptions of the buttons are shown as follows.


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.






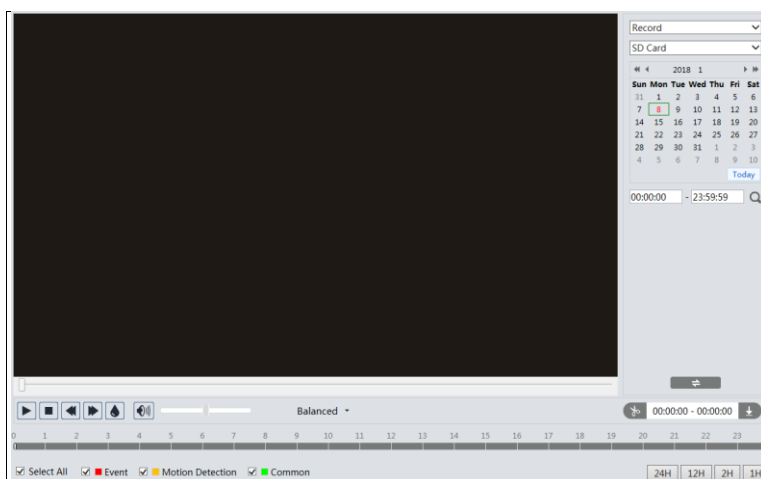
Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button
	Stop button		Speed down
	Speed up		Watermark display
	Enable / disable audio; drag the slider to adjust the volume after enabling audio .		

### 5.2.2 SD Card Video Search

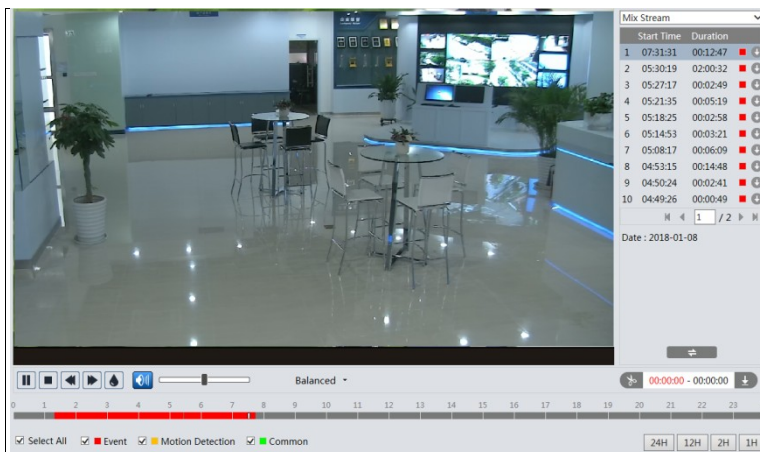
Click Search to go to the interface as shown below. Videos that were recorded on the SD card can be played in this interface.

**Note:** This function is only available for the model with SD card slot.

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...	<a href="#">Favorites</a>	<a href="#">Open</a>
<div> <span>Set up</span> <span>D:\Favorites</span> <span>Clear List</span> <span>Close</span> </div>						

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 Q & A

### Q: How to find my password if I forget it?

A: Reset the device to the default factory settings.

Default IP: 192.168.226.201

User name: admin

Password: 123456

### Q: Fail to connect devices through IE browser, why?

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

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

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

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

Note: Default IP: 192.168.226.201, mask number: 255.255.255.0

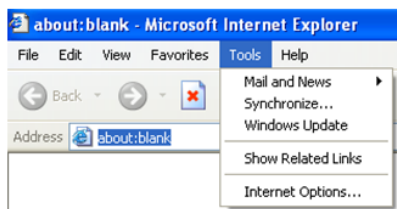
### Q: IP tool cannot search devices, why?

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

### Q: IE cannot download ActiveX control. How can I do?

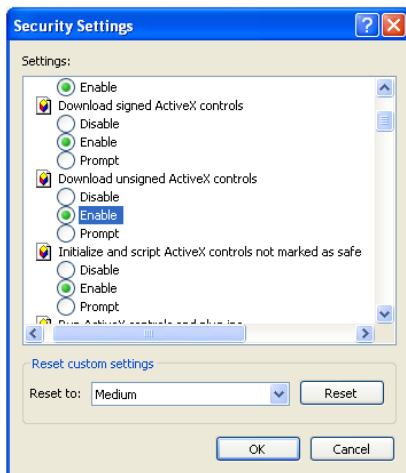
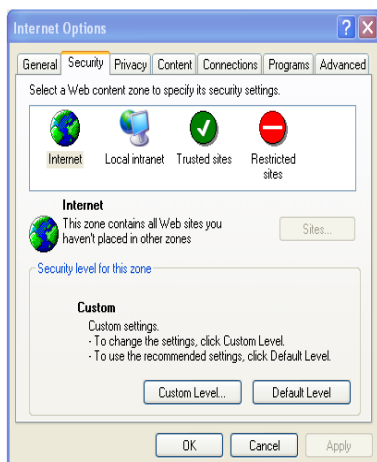
a. IE browser blocks ActiveX. Please try as below.

① Open IE browser. Click Tools-----Internet Options....



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


③ Enable all the sub options under “ActiveX controls and plug-ins”.







④ Then click OK to finish setup.



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

## Appendix 2 Specifications

Specification /Model		 <b>IR Water-proof Bullet Network Camera</b>
Camera	Image Sensor	1/2.8 " CMOS
	Image Size	1920×1080
	Electronic Shutter	1s~1/100000s
	Iris Type	Fixed Iris
	Min. Illumination	0.0035lux@F1.2, AGC ON; 0 lux with IR 0.009lux@F1.6, AGC ON; 0 lux with IR
	Lens	2.8 mm @F1.6, H.FoV: 105.4°, V.FoV:72.9°, D.FoV:112.8° 3.6 mm @F1.6, H.FoV: 87.3°, V.FoV:56.5°, D.FoV:95.2°
	Lens Mount	M12
	Day&Night	ICR
	WDR	Digital WDR
	Digital NR	3D DNR
	Angle Adjustment	Pan: 0°~360°; Tilt: 0°~80°; Rotation: 0°~360°
Image	Video Compression	H.264/H.265
	H.265 Type	Main Profile @Leve4.1 High Tier
	Video Bit Rate	64Kbps~6Mbps
	Resolution	1080P (1920 × 1080), 720P (1280×720), D1, CIF, 480×240
	Main Stream	60Hz: 1080P/720P(1~30fps); 50Hz: 1080P /720P(1~25fps)
	Sub Stream	60Hz: D1/CIF (1~30fps); 50Hz: D1/CIF (1~25fps)
	Third Stream	60Hz: D1/CIF/ 480×240 (1~30fps); 50Hz: D1/CIF/ 480×240 (1~25fps)
	Image Settings	Saturation, Brightness, Hue, Contrast, Wide Dynamic, Sharpness, NR, Defog, BLC, HLC, etc. adjustable through client or web browser
Interfaces	ROI	Support
	Network	RJ45
	Audio	1CH audio input
	Reset	Yes
	Storage	Built-in micro SD card slot; up to 128GB
Fuction	Remote Monitoring	Web browser, CMS remote control
	Online Connection	Support simultaneous monitoring for up to 3 users and multi-stream transmission
	Network Protocol	UDP, IPv4, IPv6, DHCP, NTP, RTSP, DDNS, SMTP, 802.1X, UPnP, FTP, HTTPS, HTTP, QoS
	Interface Protocol	ONVIF
	Storage	Network remote storage; micro SD card storage
	Smart Alarm	Motion alarm; scene change detection, video blur detection; intrusion detection; line crossing detection, object removal detection
Others	IR Distance	20~30 m
	Protection Grade	IP67
	Power	DC12V/PoE
	Power Consumption	< 5.5W
	Operating Environment	Temperature: -30°C~60°C; Humidity: <95% (non-condensing)
	Dimension (mm)	167.5×74.5×74.5
	Weight	Approx. 0.39KG
	Installation	Wall mounting; ceiling mounting

Specification /Model		 IR Water-proof Bullet Network Camera	 IR Water-proof Bullet Network Camera
Camera	Image Sensor	1/2.8 " CMOS	
	Image Size	1920×1080	
	Electronic Shutter	1s~1/100000s	
	Iris Type	Fixed Iris	
	Min. Illumination	0.0035lux@F1.2, AGC ON; 0 lux with IR 0.009lux@F1.6, AGC ON; 0 lux with IR	
	Lens	2.8 mm @F1.6, H.FoV: 105.4°, V.FoV:72.9°, D.FoV:112.8° 3.6 mm @F1.6, H.FoV: 87.3°, V.FoV:56.5°, D.FoV:95.2° 2.8~12mm@F1.4, H.FoV: 88-34.8°, V.FoV:57-20°, D.FoV:96-39.6°	
	Lens Mount	M12 and Ø14 optional	
	Day&Night	ICR	
	WDR	Digital WDR	
	Digital NR	3D DNR	
	Angle Adjustment	Pan: 0°~360°; Tilt: 0°~90°; Rotation: 0°~360°	
Image	Video Compression	H.264/H.265	
	H.265 Type	Main Profile @Leve4.1 High Tier	
	Video Bit Rate	64Kbps~6Mbps	
	Resolution	1080P (1920 × 1080), 720P (1280×720), D1, CIF, 480×240	
	Main Stream	60Hz: 1080P/720P(1~30fps); 50Hz: 1080P /720P(1~25fps)	
	Sub Stream	60Hz: D1/CIF (1~30fps); 50Hz: D1/CIF (1~25fps)	
	Third Stream	60Hz: D1/CIF/ 480×240 (1~30fps); 50Hz: D1/CIF/ 480×240 (1~25fps)	
	Image Settings	Saturation, Brightness, Hue, Contrast, Wide Dynamic, Sharpness, NR, Defog, BLC, HLC, etc. adjustable through client or web browser	
	ROI	Support	
Interfaces	Network	RJ45	
	Audio	1CH audio input	
	Reset	Yes	
	Storage	Built-in micro SD card slot, up to 128GB	
Fuction	Remote Monitoring	Web browser, CMS remote control	
	Online Connection	Support simultaneous monitoring for up to 3 users and multi-stream transmission	
	Network Protocol	UDP, IPv4, IPv6, DHCP, NTP, RTSP, DDNS, SMTP, 802.1X, UPnP, FTP, HTTPS, HTTP, QoS	
	Interface Protocol	ONVIF	
	Storage	Network remote storage	
	Smart Alarm	Motion alarm; scene change detection, video blur detection; intrusion detection; line crossing detection, object removal detection	
Others	IR Distance	30~50 m	
	Protection Grade	IP67	
	Power	DC12V/PoE	
	Power Consumption	< 7W	
	Operating Environment	Temperature: -30°C~60°C; Humidity: < 95% (non-condensing)	
	Dimension (mm)	217.7×80.5×80.3	218.1×79.5×70.4
	Weight	Approx. 0.65KG	
	Installation	Wall mounting; ceiling mounting	

Specification /Model		 IR Water-proof Dome Network Camera	 IR Water-proof Dome Network Camera
Camera	Image Sensor	1/2.8 " CMOS	
	Image Size	1920×1080	
	Electronic Shutter	1s~1/100000s	
	Auto Iris	Fixed Iris	
	Min. Illumination	0.0035lux@F1.2, AGC ON; 0 lux with IR 0.009lux@F1.6, AGC ON; 0 lux with IR	
	Lens	2.8 mm @F1.6, H.FoV: 105.4°, V.FoV:72.9°, D.FoV:112.8° 3.6 mm @F1.6, H.FoV: 87.3°, V.FoV:56.5°, D.FoV:95.2°	
	Lens Mount	M12	
	Day&Night	ICR	
	WDR	Digital WDR	
	Digital NR	3D DNR	
	Angle Adjustment	Pan: 0°~360°; Tilt: 0°~75°; Rotation: 0°~360°	Pan: 0°~360°; Tilt: 0°~90°; Rotation: 0°~360°
Image	Video Compression	H.264/H.265	
	H.265 Type	Main Profile @Leve4.1 High Tier	
	Video Bit Rate	64Kbps~6Mbps	
	Resolution	1080P (1920 × 1080), 720P (1280×720), D1, CIF, 480×240	
	Main Stream	60Hz: 1080P/720P(1~30fps); 50Hz: 1080P /720P(1~25fps)	
	Sub Stream	60Hz: D1/CIF (1~30fps); 50Hz: D1/CIF (1~25fps)	
	Third Stream	60Hz: D1/CIF/ 480×240 (1~30fps); 50Hz: D1/CIF/ 480×240 (1~25fps)	
	Image Settings	Saturation, Brightness, Hue, Contrast, Wide Dynamic, Sharpness, NR, Defog, BLC, HLC, etc. adjustable through client or web browser	
	ROI	Support	
Interfaces	Network	RJ45	
	Audio	1CH built-in MIC	
	Reset	Yes	
	Storage	Built-in micro SD card slot, up to 128GB	
Fuction	Remote Monitoring	Web browser, CMS remote control	
	Online Connection	Support simultaneous monitoring for up to 3 users and multi-stream transmission	
	Network Protocol	UDP, IPv4, IPv6, DHCP, NTP, RTSP, DDNS, SMTP, 802.1X, UPnP, FTP, HTTPS, HTTP, QoS	
	Interface Protocol	ONVIF	
	Storage	Network remote storage, micro SD card storage	
	Smart Alarm	Motion alarm; scene change detection, video blur detection; intrusion detection; line crossing detection, object removal detection	
Others	IR Distance	20~30 m	
	Protection Grade	IP67	
	Power	DC12V (PoE power supply optional)	
	Power Consumption	< 5.5W	
	Operating Environment	Temperature: -30°C~60°C; Humidity: < 95% (non-condensing)	
	Dimension (mm)	Ø 94.6×82.8	Ø 108 × 95.7
	Weight (net)	Approx. 0.45KG	Approx. 0.47KG
	Installation	Ceiling mounting (wall mounting available with junction box and bracket)	

Specification /Model		 IR Water-proof Dome Network Camera	 IR Water-proof Dome Network Camera
Camera	Image Sensor	1/2.8 " CMOS	
	Image Size	1920×1080	
	Electronic Shutter	1s~1/100000s	
	Auto Iris	Fixed Iris	
	Min. Illumination	0.0035lux@F1.2, AGC ON; 0 lux with IR 0.009lux@F1.6, AGC ON; 0 lux with IR	
	Lens	2.8~12mm@F1.4, H.FoV: 88~34.8°, V.FoV:57~20°, D.FoV:96~39.6°	
	Lens Mount	Ø14	
	Day&Night	ICR	
	WDR	Digital WDR	
	Digital NR	3D DNR	
	Angle Adjustment	Pan: 0°~360°; Tilt: 0°~80°; Rotation: 0°~360°	
Image	Video Compression	H.264/H.265	
	H.265 Type	Main Profile @Leve4.1 High Tier	
	Video Bit Rate	64Kbps~6Mbps	
	Resolution	1080P (1920 × 1080), 720P (1280×720), D1, CIF, 480×240	
	Main Stream	60Hz: 1080P/720P(1~30fps); 50Hz: 1080P /720P(1~25fps)	
	Sub Stream	60Hz: D1/CIF (1~30fps); 50Hz: D1/CIF (1~25fps)	
	Third Stream	60Hz: D1/CIF/ 480×240 (1~30fps); 50Hz: D1/CIF/ 480×240 (1~25fps)	
	Image Settings	Saturation, Brightness, Hue, Contrast, Wide Dynamic, Sharpness, NR, Defog, BLC, HLC, etc. adjustable through client or web browser	
	ROI	Support	
Interfaces	Network	RJ45	
	Audio	1CH built-in MIC	
	Reset	Yes	
	Storage	Built-in micro SD card slot, up to 128GB	
Fuction	Remote Monitoring	Web browser, CMS remote control	
	Online Connection	Support simultaneous monitoring for up to 3 users and multi-stream transmission	
	Network Protocol	UDP, IPv4, IPv6, DHCP, NTP, RTSP, DDNS, SMTP, 802.1X, UPnP, FTP, HTTPS, HTTP, QoS	
	Interface Protocol	ONVIF	
	Storage	Network remote storage, micro SD card storage	
	Smart Alarm	Motion alarm; scene change detection, video blur detection; intrusion detection; line crossing detection, object removal detection	
Others	IR Distance	30~50 m	
	Protection Grade	IP67	
	Power	DC12V/PoE	
	Power Consumption	< 7.5W	
	Operating Environment	Temperature: -30°C~60°C; Humidity: < 95% (non-condensing)	
	Dimension (mm)	Ø111.5×99.6	Ø130×110
	Weight (net)	Approx.0.64KG	Approx. 0.65KG
	Installation	Ceiling mounting (wall mounting available with junction box and bracket)	