

# **TITANIUM 4MP Network Camera**

## **User's Manual**

- 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 face detection network cameras.

# Disclaimer

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

## Cybersecurity Recommendations

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

## 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>9</b>
<b>4</b>	<b>Network Camera Configuration.....</b>	<b>11</b>
4.1	System Configuration .....	11
4.1.1	Basic Information .....	11
4.1.2	Date and Time .....	11
4.1.3	Local Config.....	12
4.1.4	Storage.....	12
4.2	Image Configuration .....	15
4.2.1	Display Configuration .....	15
4.2.2	Video / Audio Configuration .....	18
4.2.3	OSD Configuration.....	19
4.2.4	Video Mask .....	20
4.2.5	ROI Configuration.....	21
4.2.6	Lens Control .....	22
4.3	Alarm Configuration.....	22
4.3.1	Motion Detection.....	22
4.3.2	Other Alarms .....	24
4.3.3	Alarm Server .....	25
4.4	Network Configuration .....	25
4.4.1	TCP/IP.....	25
4.4.2	Port .....	27
4.4.3	Server Configuration .....	27
4.4.4	Onvif.....	28
4.4.5	DDNS .....	28
4.4.6	SNMP .....	29
4.4.7	802.1x.....	30
4.4.8	RTSP.....	31
4.4.9	UPNP.....	32
4.4.10	Email .....	32
4.4.11	FTP.....	33
4.4.12	HTTPS.....	35
4.4.13	QoS.....	36
4.5	Security Configuration.....	37
4.5.1	User Configuration .....	37

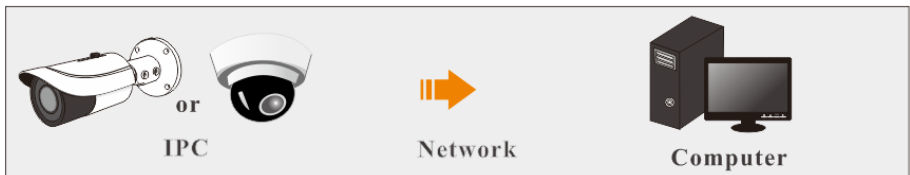
4.5.2	Online User.....	38
4.5.3	Block and Allow Lists .....	39
4.5.4	Security Management .....	39
4.6	Maintenance Configuration.....	40
4.6.1	Backup and Restore .....	40
4.6.2	Reboot .....	41
4.6.3	Upgrade .....	41
4.6.4	Operation Log.....	41
<b>5</b>	<b>Search .....</b>	<b>42</b>
5.1	Image Search .....	42
5.2	Video Search.....	44
5.2.1	Local Video Search.....	44
5.2.2	SD Card Video Search .....	45
<b>Appendix.....</b>		<b>47</b>
<b>Appendix 1 Troubleshooting .....</b>		<b>47</b>

# 1 Introduction

## Main Features

- ICR auto switch, true day/night
- Digital NR, HWDR
- BLC, HLC, Anti-flicker, smart IR, corridor mode, etc.
- ROI coding
- Support mobile surveillance by smart phones with iOS and Android OS

## Surveillance Application





## 2 Network Connection

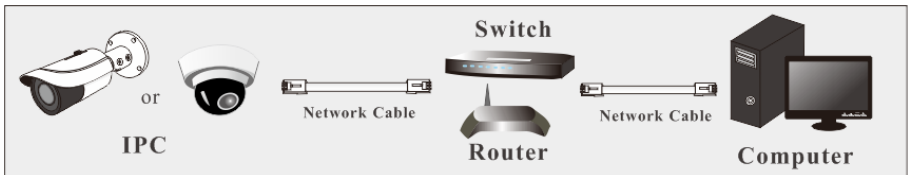
Connect IP-Cam via LAN or WAN. Here only take IE browser for example. The details are as follows:

### 2.1 LAN

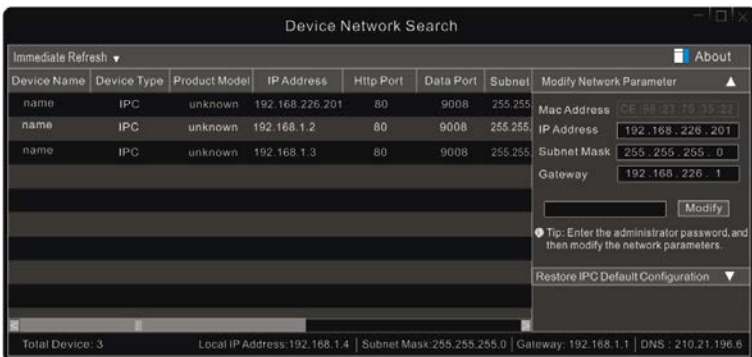
In LAN, there are two ways to access IP-Cam: 1. access through IP-Tool; 2. directly access through IE browser.

#### 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:



The default IP address of the camera is **192.168.226.201**.

- ③ Double click the IP address and then the system will pop up the IE browser to connect IP-CAM. After you read the privacy statement, check and click “Already Read”. Then activate the device.

### Device Activation

User Name

☒ Activate Onvif User

New Password

8~16 characters; Numbers, special characters, upper case letters and lower case letters must be included.

Confirm Password

OK

Please self-define the password of admin according to the tip.

If “Activate Onvif User” is enabled, the ONVIF user can be activated simultaneously. When you connect the camera through the ONVIF protocol in the third-party platform, you can use the default username and the password set above to connect.

After that, follow directions to download, install and run the Active X control if prompted.

Re-connect your camera via IE browser and then a login box will appear.

Name:

Password:

Stream Type:

Language:

[Forget Password?](#)

Login

Please enter the user name (admin) and password. Then select the stream type and language as needed.

Stream Type: The plug-in free live view only supports 1080P or lower resolution.

The security questions must be set after you click “Login” button. It is very important for you to reset your password. Please remember these answers.

**Safety Question**

Security Question1	<input type="text" value="Your father's name?"/>
Answer	<input type="text"/>
Security Question2	<input type="text" value="Your mother's name?"/>
Answer	<input type="text"/>
Security Question3	<input type="text" value="Your seniors school name?"/>
Answer	<input type="text"/>

If you forget the admin password, you can reset the password by clicking **Forget Password** on the login page. Then you can reset the password by the security questions and answers you set.

You can set the account security question during the activation, or you can go to Config→Security→User, click **Safety Question**, select the security questions and input your answers.

### 2.1.2 Directly Access through IE

The default network settings are as shown below:

IP address: **192.168.226.201**

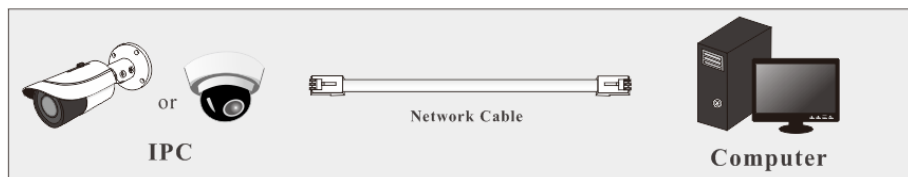
Subnet Mask: **255.255.255.0**

Gateway: **192.168.226.1**

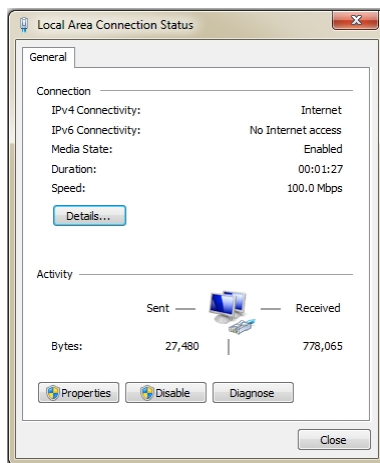
HTTP: **80**

Data port: **9008**

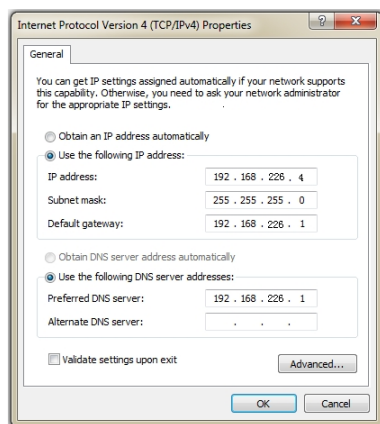
Use the above default settings when logging in the camera for the first time. Directly connect the camera to the computer through network cable.



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.



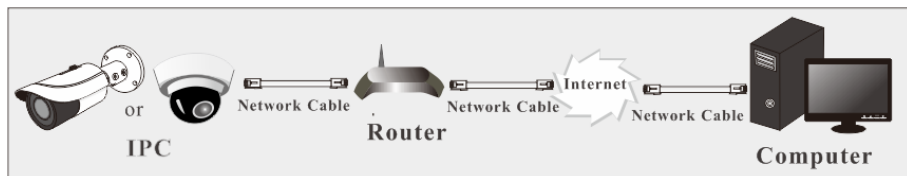
Select “Properties” and then select internet protocol according to the actual situation (for example: IPv4). Next, click the “Properties” button to set the network of the PC.



- 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	<input type="text" value="80"/>
HTTPS Port	<input type="text" value="443"/>
Data Port	<input type="text" value="9008"/>
RTSP Port	<input type="text" value="554"/>

### 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	<input type="text" value="192.168.226.201"/>	<input type="button" value="Test"/>	
Subnet Mask	<input type="text" value="255.255.255.0"/>		
Gateway	<input type="text" value="192.168.226.1"/>		
Preferred DNS Server	<input type="text" value="210.21.196.6"/>		
Alternate DNS Server	<input type="text" value="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".

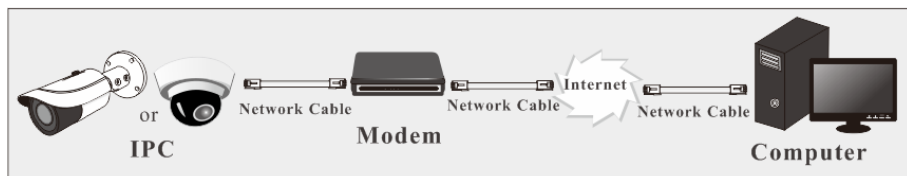
Port Range					
Application	Start	End	Protocol	IP Address	Enable
1	9007	to 9008	Both	192.168.1.201	<input checked="" type="checkbox"/>
2	80	to 81	Both	192.168.1.201	<input checked="" type="checkbox"/>
3	10000	to 10001	Both	192.168.1.166	<input type="checkbox"/>
4	21000	to 21001	Both	192.168.1.166	<input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

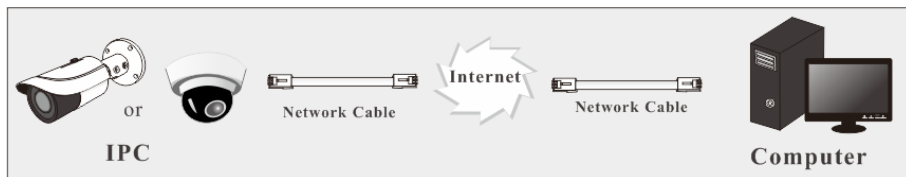
- ① Go to Config→Network→Port menu to set the port number.
- ② Go to Config →Network→TCP/IP→PPPoE Config menu. Enable PPPoE and then enter the user name and password from your internet service provider.

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

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

➤ **Access through static IP**

Network connection

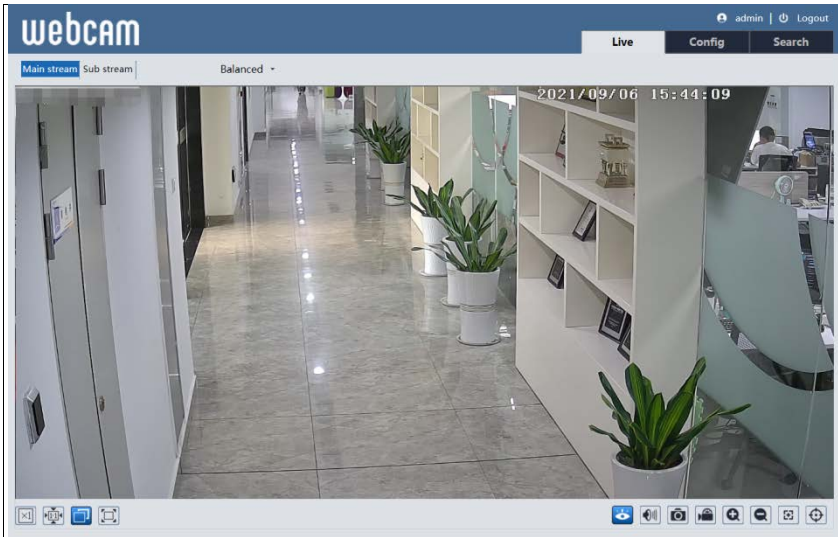


The setup steps are as follow:















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

### 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		Start/stop local recording
	Fit correct scale		Zoom in
	Auto (fill the window)		Zoom out
	Full screen		AZ control (only available for the model with motorized zoom lens )
	Start/stop live view		Rule information display
	Enable/disable audio		SD card recording indicator
	Snapshot		Motion alarm indicator






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

\*Plug-in free live view: the local recording is not supported and the preview mode switch (real-time/balanced/fluent mode) is not available too.

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	
Brand	Customer
Software Version	5.1.1.0(23143)
Software Build Date	2021-09-07
Onvif Version	20.12
OCX Version	2.1.9.4
MAC	00:48:af:53:4d:92
About this machine	<a href="#">View</a>
Privacy Statement	<a href="#">View</a>

#### 4.1.2 Date and Time

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

Zone

Date and Time

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

☐ DST

☒ Auto DST

☐ Manual DST

Start Time January ▼ First ▼ Sunday ▼ 00 ▼ Hour

End Time February ▼ First ▼ Monday ▼ 00 ▼ Hour

Time Offset 120 Minutes ▼

Save

Select the time zone and DST as required.

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

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

### 4.1.3 Local Config

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

Additionally, “Local smart snapshot storage” can be enabled or disabled here. If enabled, the captured pictures triggered by smart events will be saved to the local PC.

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

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

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

### 4.1.4 Storage

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

Management	Record	Snapshot
Total picture capacity	379 MB	
Picture remaining space	379 MB	
Total recording capacity	3329 MB	
Record remaining space	2816 MB	
State	Normal	
Snapshot Quota	10 %	
Video Quota	90 %	

Changes in the quota ratio need to be formatted before they become effective.

## ● 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.

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

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.

☐ Erase   ☒ Add

Week Schedule

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Sun.																									
	Manual Input																								
Mon.																									
	Manual Input																								
Tue.																									
	Manual Input																								
Wed.																									
	Manual Input																								
Thu.																									
	Manual Input																								
Fri.																									
	Manual Input																								
Sat.																									
	Manual Input																								

Holiday Schedule

Date

09-01

+

-

0

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

Manual Input

Save

## 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 checked="" 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

### 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.

Camera Parameters

Profile Management



Video Adjustment

Frequency

50HZ

Infra-red Mode

Auto

Corridor Pattern

0

Image Mirror

☐ Open
 ☒ Close

Image Flip

☐ Open
 ☒ Close

Config File

Common

Brightness

50

Contrast

50

Hue

50

Saturation

50

Sharpness

☐

128

Noise Reduction

☐

128

BLC

Off

Antiflicker

Off

Smart IR

Off

White Balance

Auto

Day/Night Mode

Auto

Sensitivity

Mid

Delay Time(Second)

2

Exposure Mode

Auto

Gain Mode

Auto

Gain Limit

50

Default

Revoke

**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.

**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.

**Note:** HWDR and corridor pattern cannot be enabled simultaneously. If HWDR is enabled, the corridor pattern will be disabled.

- HLC: lowers the brightness of the entire image by suppressing the brightness of the image's bright area and reducing the size of the halo area.

- BLC: If enabled, the auto exposure will activate according to the scene so that the object

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

**Antiflicker:**

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

**Smart IR:** Choose “ON” or “OFF”. This function can effectively avoid image overexposure and underexposure by controlling the brightness of the IR lights according to the actual conditions to make the image more realistic. Please enable it as needed.

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

**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 according to the actual situation. If “Manual” is selected, the gain value shall be set manually. The higher the value is, the brighter the image is.

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

**Infra-red Mode:** Choose “Auto”, “ON” or “OFF”.

**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.

**Note:** HWDR and corridor pattern cannot be enabled simultaneously. If the corridor pattern is enabled, HWDR function will be disabled.

**Image Mirror:** Turn the current video image horizontally.

**Image Flip:** Turn the current video image vertically.

**Note:** For some items (like HWDR), if selected/enabled, the camera will reboot automatically. After that, clicking “Default” button will not take effect.

Schedule Settings of Image Parameters:


Click the “Profile Management” tab as shown below.

The screenshot shows the 'Profile Management' tab selected. Under the 'Schedule' dropdown, 'Full Time' is chosen. Under the 'Config File' dropdown, 'Common' is chosen. A 'Save' button is visible at the bottom right of the settings area.

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

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



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

## 4.2.2 Video / Audio Configuration

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

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

Send Snapshot

Sub stream

Size: (704x576)

☐ Video encode slice split

☐ Watermark ( H264 , H265 )

Watermark content:

Save

Two 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. MJPEG is not available for main stream. If H.265/H.265+ is chosen, make sure the client system is able to decode H.265/H.265+. Compared to H.265, H.265+ saves more storage space with the same maximum bitrate in most scenes. Compared to H.264, H.265 reduces the transmission bitrate under the same resolution, frame rate and image quality.

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


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

**Send Snapshot:** Set the snapshot stream.

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

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

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



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

**Audio Type:** LIN or MIC can be optional.

**LIN IN/MIC IN Volume:** LIN IN Volume can be set here. If MIC is selected, MIC IN volume can be set. (Only some models support MIC)

### 4.2.3 OSD Configuration

Go to Image→OSD interface as shown below.



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

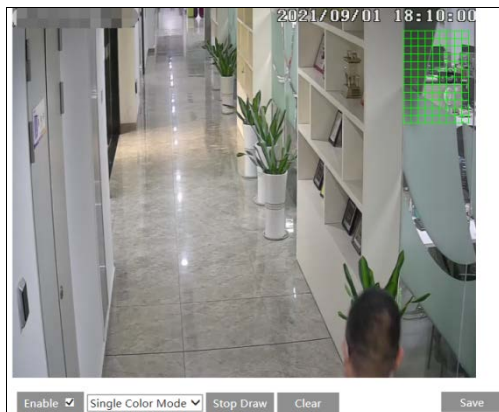


#### Picture Overlay Settings:

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

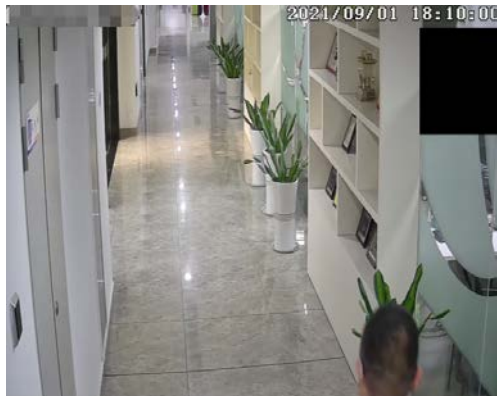
### 4.2.4 Video Mask

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



To set up video mask:

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

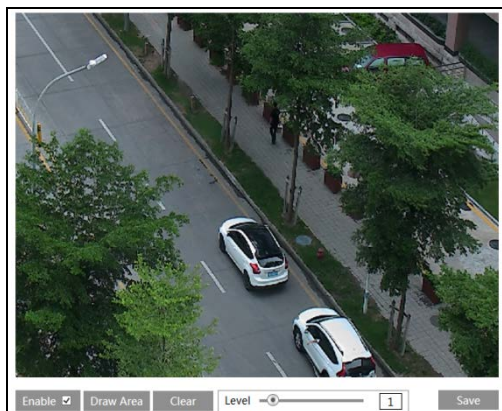


To clear the video mask:

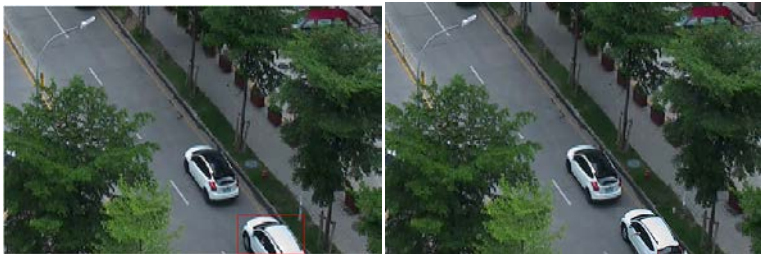
Click the “Clear” button to delete the current video mask area.

#### 4.2.5 ROI Configuration

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

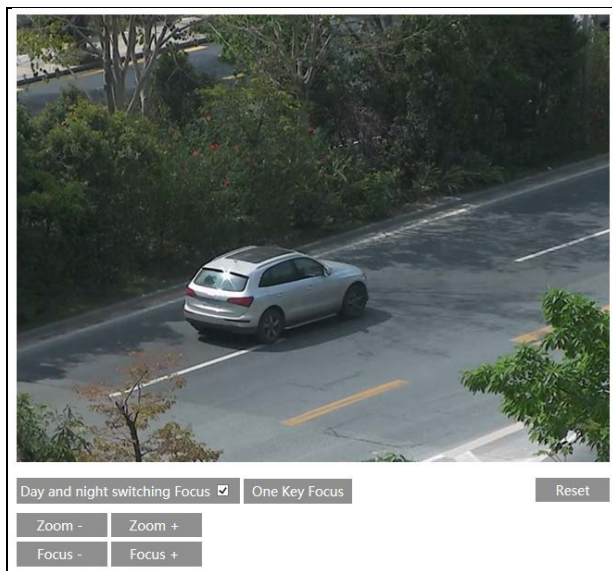


1. Check “Enable” and then click the “Draw Area” button.
2. Drag the mouse to set the ROI area.
3. Set the level.
4. Click the “Save” button to save the settings.



## 4.2.6 Lens Control

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



## 4.3 Alarm Configuration

### 4.3.1 Motion Detection

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

Detection Config    Area and Sensitivity    Schedule

☒ Enable

Alarm Holding Time    20 Seconds    ▼

☐ Trigger SD Snapshot

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

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

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

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

**Trigger FTP:** If “Trigger FTP” 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.

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 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.

2. Click “Enable”.

3. 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.

#### ● 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**

☒ Enable

Alarm Holding Time   20 Seconds   ▾

☐ Trigger Email

☐ Trigger FTP

Save

2. Click “Enable”.

3. Set the alarm holding time and 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   0.0.0.0

Port   8010

Heartbeat   Disable   ▾

Heartbeat interval   30   Second

OK

## 4.4 Network Configuration

### 4.4.1 TCP/IP

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



IPv4 IPv6 PPPoE Config IP Change Notification Config

☐ Obtain an IP address automatically

☒ Use the following IP address

IP Address

Subnet Mask

Gateway

Preferred DNS Server

Alternate DNS Server

**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

☒ Enable

User Name

Password

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

☐ Trigger Email

☐ Trigger FTP

**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.

### 4.4.2 Port

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

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

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

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

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

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

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

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

### 4.4.3 Server Configuration

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

☒ Enable

Server Port	<input type="text" value="2009"/>
Server Address	<input type="text"/>
Device ID	<input type="text" value="1"/>

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.

#### 4.4.4 Onvif

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

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

You can also add new users in the Onvif interface.

The screenshot shows the 'Onvif' tab in a configuration interface. At the top, there are tabs for 'Port', 'Server', 'Onvif', and 'DDNS'. Below these are buttons for 'Add', 'Modify', and 'Delete'. The 'Add' button is circled in red. Below the buttons is a table with columns 'Index', 'User Name', and 'User Type'. The first row shows '1', 'admin', and 'Administrator'. A red arrow points from the 'Add' button to a 'Add User' dialog box. The dialog box has a close button (X) in the top right corner. It contains the following fields: 'User Name' (text input), 'Password' (text input), 'Level' (text input), 'Confirm Password' (text input), and 'User Type' (dropdown menu). Below these fields is a note: 'The password can be composed of numbers, special characters, upper or lower case letters.' At the bottom of the dialog box are 'OK' and 'Cancel' buttons.

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

#### 4.4.5 DDNS

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

1. Go to Config→Network→ DDNS.

The screenshot shows the 'DDNS' configuration interface. It has a checkbox labeled 'Enable' which is checked. Below this are four fields: 'Server Type' (a dropdown menu showing 'www.dyndns.com'), 'User Name' (a text input field), 'Password' (a text input field), and 'Domain' (a text input field). At the bottom right is a 'Save' button.

2. Apply for a domain name. Take www.dvrdyndns.com for example.  
Enter www.dvrdyndns.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.

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.dvrdyndns.com

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

[Please add different domain names](#)

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

#### 4.4.6 SNMP

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

1. Go to Config→Network→SNMP.

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

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

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

#### 4.4.7 802.1x

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

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

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.

## 4.4.8 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"/>
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
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.

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.

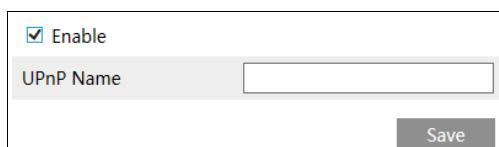
3. Avoid the use of the same multicast address in the same local network.

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.

#### 4.4.9 UPnP

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

Go to Config→Network→UPnP. Enable UPnP and then enter UPnP name.

The image shows a web-based configuration interface for UPnP. It features a checkbox labeled "Enable" which is checked. Below this is a text input field labeled "UPnP Name". At the bottom right of the form is a "Save" button.

☒ Enable

UPnP Name

Save

#### 4.4.10 Email

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

Go to Config→Network →Email.

**Sender**

Sender Address   
User Name  ☒ Anonymous Login  
Password   
Server Address   
Secure Connection    
SMTP Port    
☐ Send Interval(S)  (10-3600)

**Recipient**

xxx@126.com

Recipient Address

**Sender Address:** sender's e-mail address.

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

**Server Address:** The SMTP IP address or host name.

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

**SMTP Port:** The SMTP port.

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

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

**Recipient Address:** receiver's e-mail address.

#### 4.4.11 FTP

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

1. Go to Config→Network →FTP.



Server Name	Server Address	Port	User Name	Upload Path
<div style="border: 1px solid gray; padding: 10px; margin: 10px auto; width: 80%;"> <div style="border-bottom: 1px solid gray; margin-bottom: 5px;">Add FTP</div> <div style="display: flex; justify-content: space-between;"> <div> <p>Server Name: <input type="text" value="test"/></p> <p>Server Address: <input type="text" value="192.168.1.3"/></p> <p>Upload Path: <input type="text" value="Example/Dir/folder"/></p> <p>Port: <input type="text" value="21"/></p> <p>User Name: <input type="text" value="admin"/></p> <p>Password: <input type="password" value="*****"/></p> </div> <div> <p><input type="checkbox"/> Anonymous</p> </div> </div> <div style="display: flex; justify-content: flex-end; margin-top: 10px;"> <span>OK</span> <span>Cancel</span> </div> </div>				
<span>Add</span> <span>Modify</span> <span>Delete</span> <span>Test</span> <span>Save</span>				

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

**Server Name:** The name of the FTP server.

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

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

**Port:** The port of the FTP server.

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

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

☒ Trigger FTP

Server Address

☒ 192.168.1.3

☒ Attach Picture

Save

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

For example: a motion alarm occurs

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

Event name table:

File Name	Event Type
IP	IP address change
MOTION	Motion Detection
SDFULL	SD Full
SDERROR	SD Error

TXT file content:

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

For example:

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

## 4.4.12 HTTPS

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

Go to Config → Network → HTTPS as shown below.

The screenshot shows the HTTPS configuration page with the "Enable" checkbox checked. Under "Certificate installed", a default certificate is listed with details: C=CN, ST=GD, L=SZ, O=IPC, OU=embeddec. A "Delete" button is next to it. The "Attribute" section shows the certificate's details: Issued to: C=CN, ST=GD, L=SZ, O=IPC, OU=embeddec, H=localhost; Issuer: C=CN, ST=GD, L=SZ, O=IPC, OU=embeddec, H=localhost; Validity date: 2020-03-14 08:12:45 - 2033-11-21 08:12:45. A "Save" button is at the bottom right.

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.

The screenshot shows the HTTPS configuration page with the "Enable" checkbox checked. Under "Installation type", three options are available: "Have signed certificate, install directly" (selected), "Create a private certificate", and "Create a certificate request". Below this, the "Install certificate" section has a "Browse" button and an "Install" button. A "Save" button is at the bottom right.

\* 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

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.

#### 4.4.13 QoS

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

Go to Config→Network→QoS.

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

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

Alarm DSCP: The range is from 0 to 63.

Manager DSCP: The range is from 0 to 63.

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

## 4.5 Security Configuration

### 4.5.1 User Configuration

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

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

#### Add user:

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

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

#### Modify user:

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

**Edit User**

User Name: admin

Old Password:

New Password:

Level:

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

Confirm Password:

User Type: Administrator

☐ Select All

- ☒ Remote storage settings
- ☒ Remote image settings
- ☒ Remote PTZ control
- ☒ Remote alarm server configuration
- ☒ Remote intelligent event configuration
- ☒ Remote network advanced configuration
- ☒ Remote security management

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. Select the user permissions for advanced or normal user.
6. Click the “OK” button to save the settings.

#### Delete user:

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

**Note:** The default administrator account cannot be deleted.

**Safety Question Settings:** set the questions and answers for admin so as to reset the password after you forget the password.

## 4.5.2 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).

### 4.5.3 Block and Allow Lists

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

The setup steps are as follows:

Check the “Enable address filtering” check box.

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

### 4.5.4 Security Management

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

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

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

#### ● Password Security

Please set the password level and expiration time as needed.

Password Level: Weak, Medium or Strong.

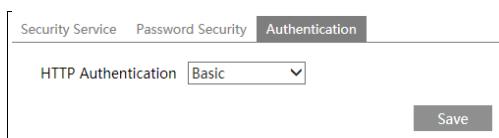
Weak level: Numbers, special characters, upper or lower case letters can be used. You can choose one of them or any combination of them when setting the password.

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

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

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

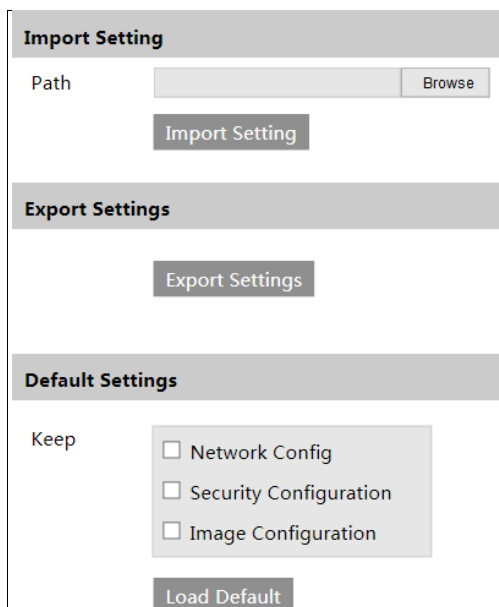
HTTP Authentication: Basic or Token is selectable.



## 4.6 Maintenance Configuration

### 4.6.1 Backup and Restore

Go to Config→Maintenance→Backup & Restore.



- **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.

## 4.6.2 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.

## 4.6.3 Upgrade

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

Local upgrade

Path

Browse

Upgrade

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

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

## 4.6.4 Operation Log

To query and export log:

1. Go to Config→Maintenance→Operation Log.

Main Type	Operation	Sub Type	Log in			
Start Time	2021-09-06 00:00:00	End Time	2021-09-06 23:59:59	Search	Export	
Index	Time	Main Type	Sub Type	User Name	Login IP	Hostname
1	2021-09-06 03:1...	Operation	Log in	admin	10.20.52.7	
2	2021-09-06 03:1...	Operation	Log in	admin	10.20.52.7	

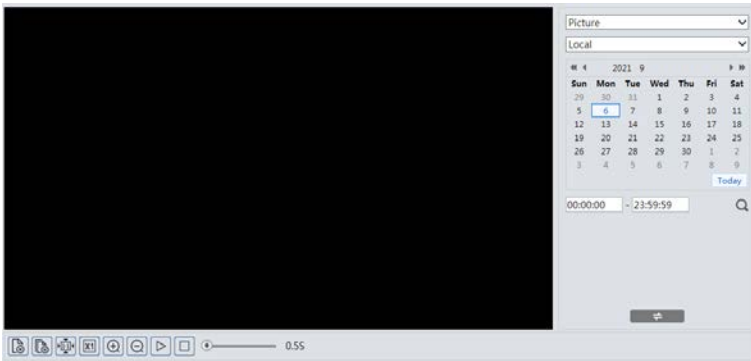
2. Select the main type, sub type, start and end time.
3. Click “Search” to view the operation log.
4. Click “Export” to export the operation log.




## 5.1 Image Search

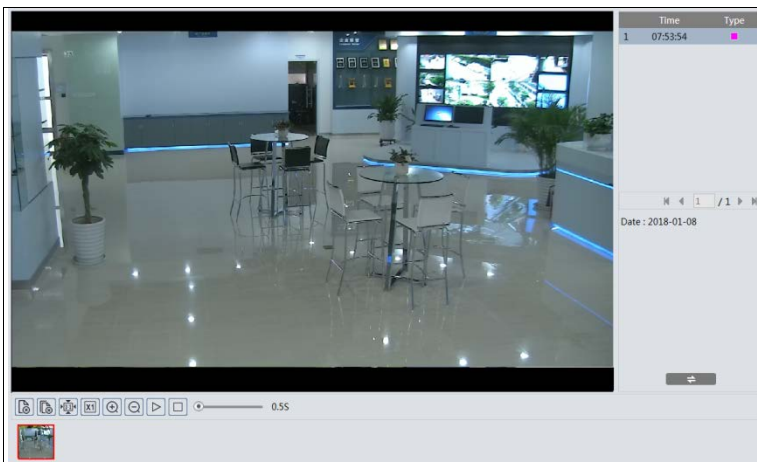
Click **Search** to go to the interface as shown below. Images that are saved on the SD card can be found here.


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



### ● Local Image Search

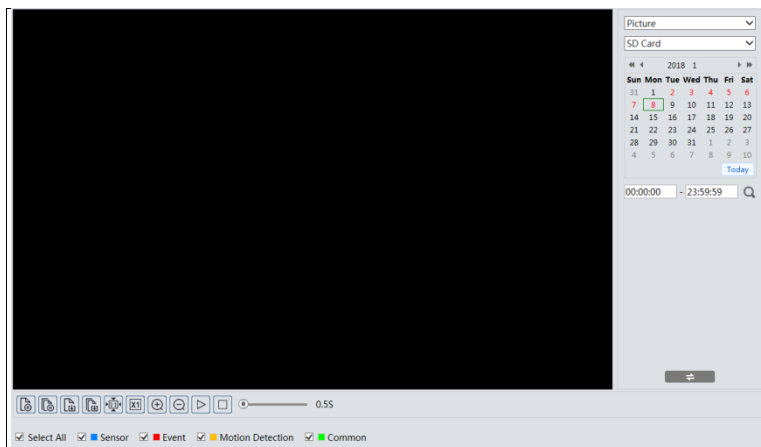
1. Choose “Picture”—“Local”.
2. Set time: Select date and choose the start and end time.
3. Click  to search the images.
4. Double click a file name in the list to view the captured photos as shown above.





Click  to return to the previous interface.












## ● SD Card Image Search

1. Choose “Picture”—“SD Card”.



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

The descriptions of the buttons are shown as follows.

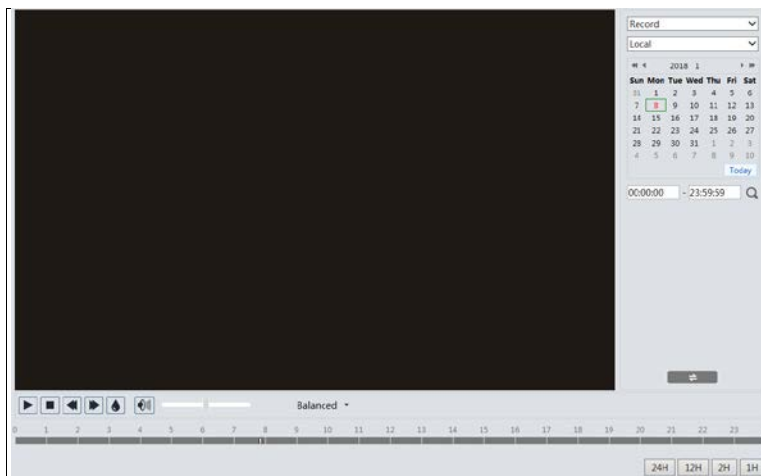
Icon	Description	Icon	Description
	Close: Select an image and click this button to close the image.		Close all: Click this button to close all images.
	Save: Click this button to select the path for saving the image on the PC.		Save all: Click this button to select the path for saving all pictures on the PC.
	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.

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




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

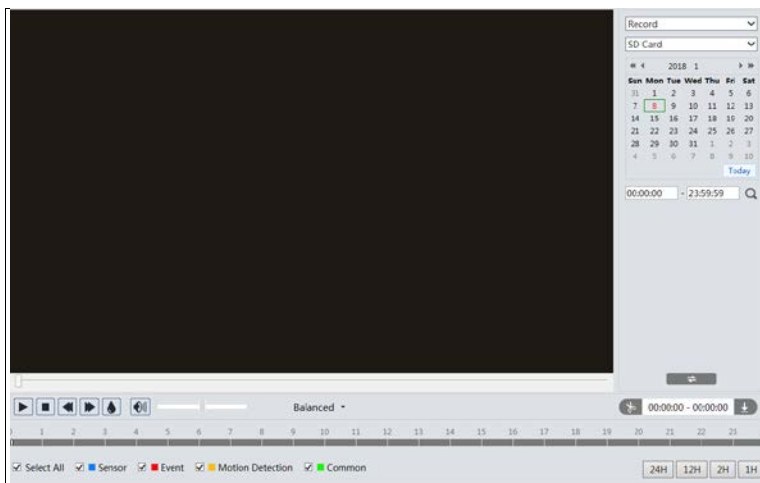


Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button
	Stop button		Speed down
	Speed up		Watermark display
	Enable / disable audio; drag the slider to adjust the volume after enabling audio.		

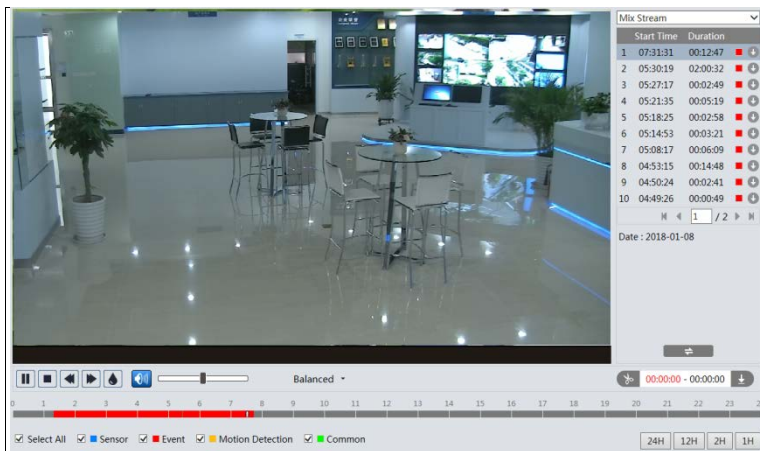
### 5.2.2 SD Card Video Search

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

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



4. Select the alarm events at the bottom of the interface.
5. Select mix stream (video and audio stream) or video stream as needed.
6. Double click on a file name in the list to start playback.



**Note:** ⏮ and ⏭ cannot be displayed in the above interface via the plug-in free browser. Additionally, for plug-in free playback, playback mode switch (balanced/real-time/fluent mode) and downloading functions are not supported too.

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

Video clip and downloading

1. Search the video files according to the above mentioned steps.
2. Select the start time by clicking on the time table.
3. Click 🗂 to set the start time and then this button turns blue (🗂).
4. Select the end time by clicking on the time table. Then click 🗂 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
<div> Set up D:\Favorites Clear List Close </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 Troubleshooting

### How to find the password?

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

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

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

### Fail to connect devices through IE browser.

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

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

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

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

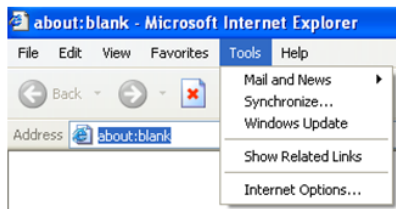
### IP tool cannot search devices.

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

### IE cannot download 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.

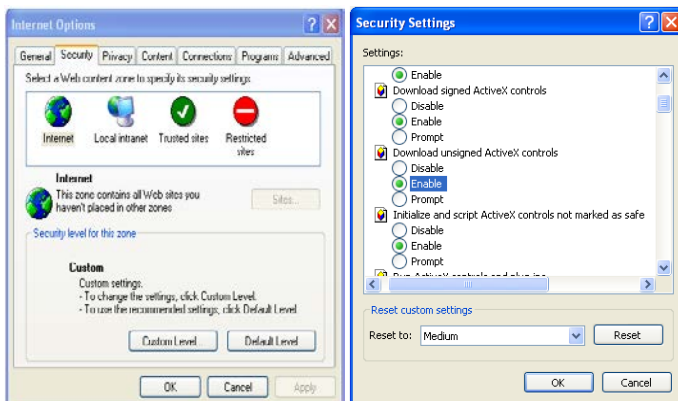


② Select Security-----Custom Level....

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.