



# **User Manual**

## **IP Encoder**

O5E1

# Important Safeguards and Warnings

## 1. Electrical safety

All installation and operation here should conform to local electrical safety codes.  
Use a certified/listed 12VDC Class2 or adequate PoE switch.  
Improper handling and/or installation could run the risk of fire or electrical shock.

## 2. Environment

Do not expose the unit to heavy stress, violent vibration or long-term exposure to water and humidity during transportation, storage, and/or installation.  
Do not install near sources of heat.  
Only install the product in environments inside the specification operating temperature and humidity range.  
Do not install the device near power lines, radar equipment or other electromagnetic radiation.  
Do not block any ventilation openings if any.

## 3. Operation and Daily Maintenance

Please shut down the device and then unplug the power cable before you begin any maintenance work.  
Always use the dry soft cloth to clean the device. If there is too much dust, use a cloth dampened with a small quantity of neutral detergent. Finally use the dry cloth to clean the device.  
The grounding holes of the product are recommended to be grounded to further enhance the reliability of the device.

## Statement

This guide is for reference only.  
Product, manuals, and specifications may be modified without prior notice. Speco Technologies reserves the right to modify these without notice and without incurring any obligation.  
Speco Technologies is not liable for any loss caused by improper operation.

## Regulatory Information

### FCC conditions:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

### FCC compliance:

This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. 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. 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.

**Note:**

Before installation, check the package and make sure that all components are included.

Contact your rep or Speco customer service department immediately if something is broken or missing in the package.

Accessory name	Amount
IP Encoder	1
Quick Start Guide	1
Installation Accessories Bag	1
CD	1

# Table of Contents

<b>1</b>	<b>Web Access and Login</b> .....	<b>3</b>
<b>2</b>	<b>Live View</b> .....	<b>5</b>
<b>3</b>	<b>Configuration</b> .....	<b>7</b>
3.1	System Configuration.....	7
3.1.1	System Information .....	7
3.1.2	Date and Time.....	7
3.1.3	Local Recording.....	8
3.1.4	Storage.....	8
3.2	Video Configuration.....	10
3.2.1	Image Configuration .....	10
3.2.2	Video / Audio Configuration .....	12
3.2.3	OSD Configuration .....	13
3.2.4	Video Mask .....	13
3.2.5	ROI Configuration .....	14
3.3	Alarm Setup .....	15
3.3.1	Motion Detection .....	15
3.3.2	Exception Alarm.....	16
3.3.3	Alarm In (Sensor Input).....	18
3.3.4	Alarm Out .....	18
3.3.5	Alarm Server .....	19
4.4	Analytics Configuration.....	19
4.4.1	Abandoned/Missing Object Detection .....	20
4.4.2	Video Exception .....	21
4.4.3	Line Crossing .....	22
4.4.4	Region Intrusion.....	24
4.4.5	Face Detection .....	25
4.4.6	Region Entrance.....	27
4.4.7	Region Exiting .....	27
4.4.8	Target Counting by Line .....	28
4.4.9	Target Counting by Area .....	30
4.4.10	Heat Map.....	31
4.5	Network Configuration .....	32
4.5.1	TCP/IP.....	32
4.5.2	Port .....	33
4.5.3	Server Configuration .....	34
4.5.4	Onvif.....	34
4.5.5	DDNS.....	35
4.5.6	SNMP .....	35
4.5.7	802.1x .....	36
4.5.8	RTSP .....	37
4.5.9	RTMP.....	37
4.5.10	UPNP.....	38
4.5.11	Email .....	38
4.5.12	FTP .....	38
4.5.13	HTTPS.....	39
4.5.14	HTTP POST .....	40
4.5.15	QoS.....	40
4.6	Security Configuration .....	41
4.6.1	User Admin .....	41

4.6.2	Online User .....	42
4.6.3	Block and Allow Lists.....	43
4.6.4	Security Management.....	43
4.7	Maintenance Configuration .....	44
4.7.1	Backup and Restore .....	44
4.7.2	Reboot .....	44
4.7.3	Upgrade .....	44
4.7.4	Operation Log .....	45
5	Search .....	46
5.4	Image Search .....	46
5.5	Video Search .....	48
5.5.1	Local Video Search .....	48
5.5.2	SD Card Video Search.....	49
<b>Appendix .....</b>		<b>52</b>
<b>Appendix 1 Troubleshooting .....</b>		<b>52</b>



---

## Welcome

Thank you for purchasing this device!

Please read this manual carefully before operating the unit and retain it for further reference.

Should you require any technical assistance, please contact Speco Technologies Technical Support at 1-800-645-5516.

# 1 Web Access and Login

The IP camera settings can be accessed via a web browser through the LAN.

Available web browser: IE (plug-in required)/ Firefox/Edge/Safari/Google Chrome

It is recommended to use the latest version of these web browsers.

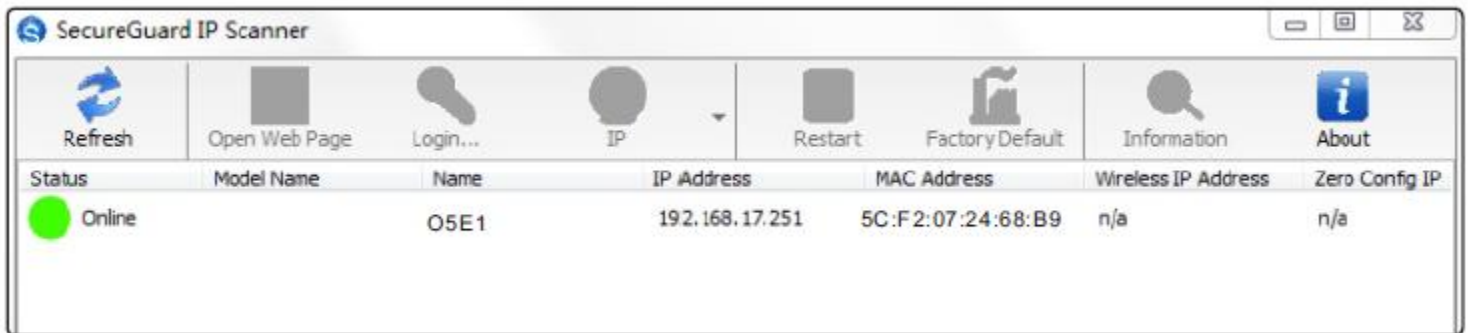
The menu display and operation of the camera may be slightly different by using the browser with plug-in or without plug-in. Installing plug-in will display more functions of the camera.

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

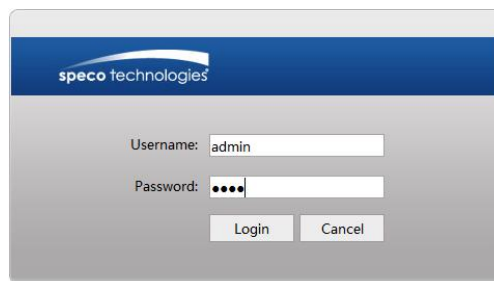
- Access through IP Scanner

① Make sure the PC and device are connected on the same local network. The device is set to DHCP by default and will be assigned an IP address by the DHCP server. Make sure that the local network has a DHCP server. Routers typically have a DHCP server built in.

② Install IP Scanner from the CD and run it after installation. IP Scanner is the tool for discovering the IP cameras on the local network.



③ In the device list, the IP address, model number, and MAC address of each device will be listed. Select the applicable device and double click to open up the web viewer. You can also manually enter the IP address in the address bar of the web browser. Read the privacy statement and then check and click "Already Read" to enter the login interface.



The login interface is shown above. Default username is **admin** and the password is **1234**. After logging in, follow directions to install applicable plug-ins for viewing video if prompted.

**Please change the default password** ✕

Modify Password     Match Onvif Password

Old Password

New Password

Confirm Password

Do not show again OK    Cancel

If this is the first time for you to log in, the password prompt may only change the admin password. By default, the ONVIF password will match the admin password that you set. Should you wish to change the ONVIF password to a different password than your admin password, go to the ONVIF section to change the password. (Config→Network→Ports/Connections→Onvif)

Port Server Onvif DDNS SNMP 802.1X RTSP RTMP UPnP Email FTP HTTPS QoS

---

Add Modify Delete

Index	User Name	User Type
1	admin	Administrator

**Edit User** ✕

User Name

New Password

Level

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

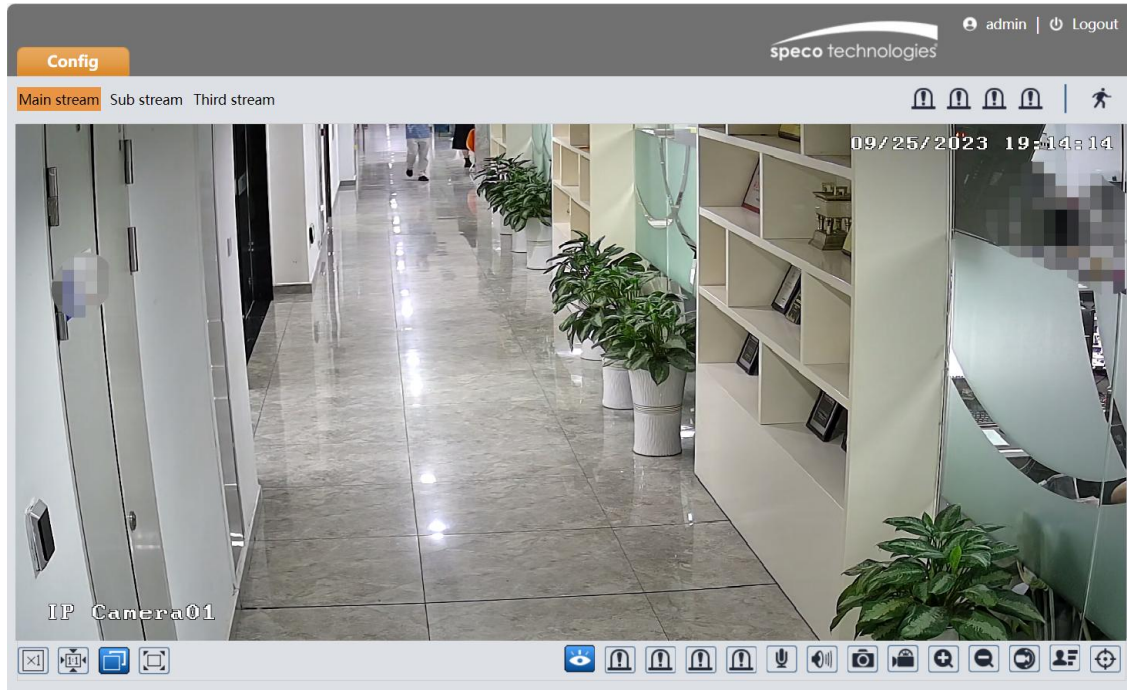
Confirm Password

OK    Cancel



## 2 Live View

The window below will be shown after logging in.



The following table describes the icons on the live view interface

Icon	Description	Icon	Description
	Original size of resolution		SD card recording indicator
	Fit (correct scale)		Abnormal color indicator
	Auto (fill the window)		Abnormal clarity indicator
	Full screen (show video only)		Scene change indicator
	Start/stop live view		Alarm output indicator
	Enable/disable alarm output		Sensor alarm indicator
	Start/stop two-way audio		Motion alarm indicator
	Enable/disable audio		Line crossing indicator
	Snapshot		Region Intrusion indicator
	Start/stop local recording		Object detection indicator (object abandoned/missing)
	Zoom in		Heat map indicator
	Zoom out		Face detection indicator
	COC (UTC) control		Line crossing target counting indicator
	Face detection		Region Intrusion target counting indicator
	Rule information display		


\*Plug-in free live view: two-way audio and local recording are not supported.

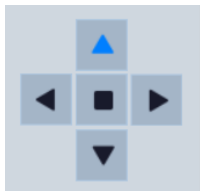
All indicator icons above will flash in live view interface only when the corresponding events are enabled.


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

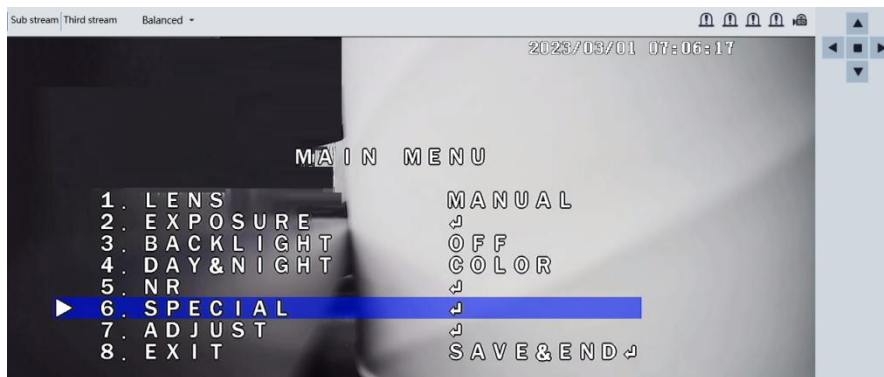
### COC (UTC) control:

COC control (or Up-The-Coax control) allows the user to remotely set the OSD menu for analog cameras over coaxial cable.




Click  to enter UTC control mode. The following buttons will display on the right panel of the live interface.







Click  in the middle to call the OSD menu of the analog camera.



Different analog cameras may have different main menus. The picture above is for reference only.

Move up or down to select the left menu by clicking  or . After selecting the desired menu, click  to enter the sub-menu or confirm the selection.

Select the right menu by clicking  or .

 means that there are sub-menus. After it is selected, click  to view the detailed menus.

**Note:** It is recommended to use the default settings for analog camera.

## 3 Configuration

Press the “Setup” button to go to the configuration interface.

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

### 3.1 System Configuration

#### 3.1.1 System Information

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

Device Name	<input type="text" value="O5E1"/>
Product Model	<input type="text" value="O5E1"/>
Brand	<input type="text" value="Speco"/>
Software Version	<input type="text" value="5.1.2.0(49806)"/>
Software Build Date	<input type="text" value="2023-08-18"/>
Onvif Version	<input type="text" value="22.12"/>
OCX Version	<input type="text" value="2.2.7.15"/>
MAC	<input type="text" value="5c:f2:07:40:1e:ef"/>
About this machine	<a href="#">View</a>

#### 3.1.2 Date and Time

To set the time and date, go to System → Date and Time. Please refer to the following interface.

**Zone** Date and Time

Zone

DST

Auto DST

Manual DST

Start Time

End Time

Time Offset

[Save](#)

Select the applicable time zone and enable / disable DST as needed.

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

### 3.1.3 Local Recording

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

Additionally, the snapshots triggered by smart events (like line crossing detection, intrusion detection, etc.) can be selected to save to the local PC.

### 3.1.4 Storage

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

- **SD Card Management**

When the card is used for the first time, click the “Format” button to format the SD card. **All data on the card will be cleared by clicking this button.**

Click the “Eject” button to stop writing data to the 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 Storage→Record to go to the interface as shown below.

Management **Record** Snapshot USB disk

**Record Parameters**

Record Stream Main stream

Pre Record Time No Pre Record ( H264,H265,MJPEG )

Cycle Write Yes

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.

**Timing**

Enable Schedule Record

Erase  Add

**Week Schedule**

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 04-19 + -

00:00-24:00 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 System→Storage→Snapshot to go to the interface as shown below.

Management	Record	Snapshot	USB disk
<b>Snapshot Parameters</b>			
Image Format	JPEG		
Resolution	1280x720		
Image Quality	Low		
<b>Event Trigger</b>			
Snapshot Interval	1	Second	
Snapshot Quantity	5		

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](#)).

- **USB Disk**

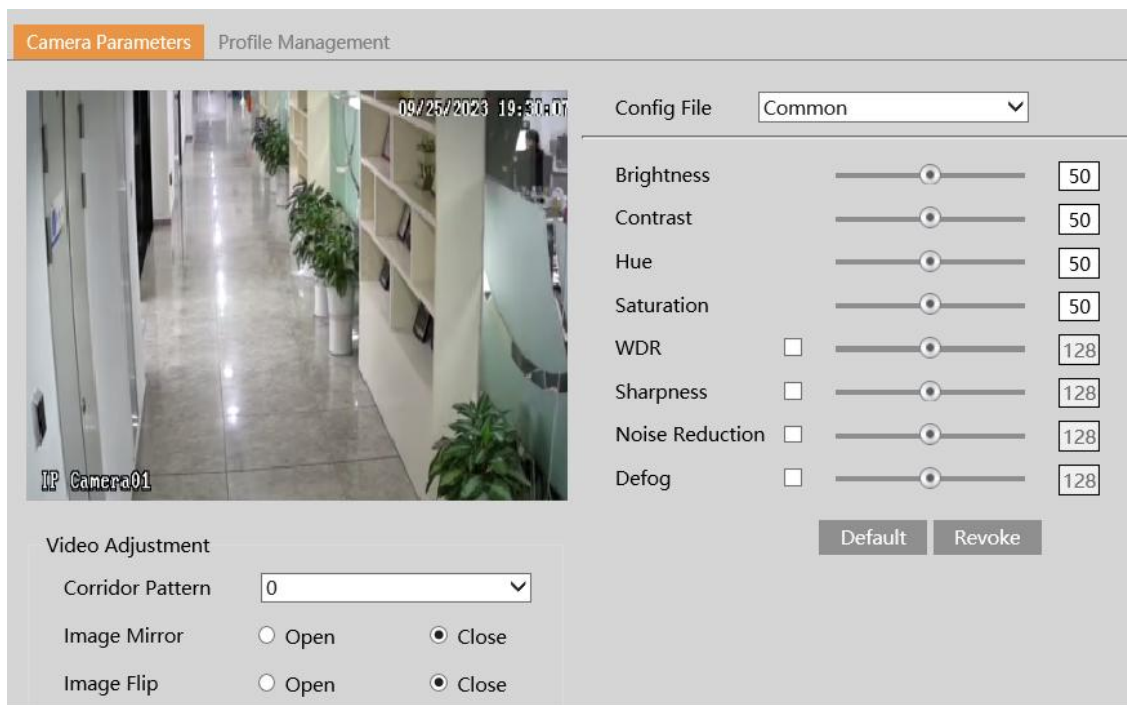
You can only view the capacity of the USB storage device, such as total capacity, used capacity and available capacity.

## 3.2 Video Configuration

Video Configuration includes Display Settings, Video/Audio Setup, OSD, Privacy Mask and Region of Interest.

### 3.2.1 Image Configuration

In the Display Settings interface as shown below, various settings can be adjusted, such as brightness, contrast, hue, and saturation and so on. The common mode and day and night mode can be set up separately. The image effect can be quickly viewed by switching the configuration file.



**Brightness:** Set the brightness level of the camera’s image.

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

**Hue:** Set the total color degree of the image.

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

**WDR:** WDR can adjust the camera to provide a better image when there are both very bright and very dark areas simultaneously in the field of the view by lowering the brightness of the bright area and increasing the brightness of the dark area. Recording will be stopped for a few seconds while the mode is changing from non-WDR to WDR mode.

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

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

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

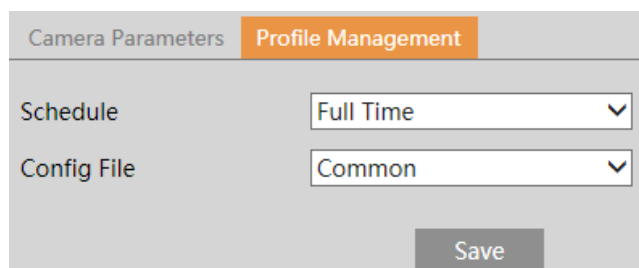
**Corridor Pattern:** Corridor viewing modes can be used for situations such as long hallways. 0, 90, 180 and 270 are available. The default value is 0. The video resolution should be 1080P or below if this function is used.

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

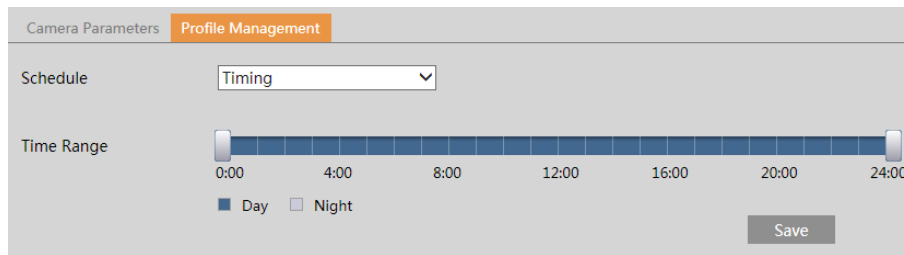
**Image Flip:** Turn the current video image vertically.

Schedule Settings of Image Parameters:

Click the “Profile Management” tab as shown below.



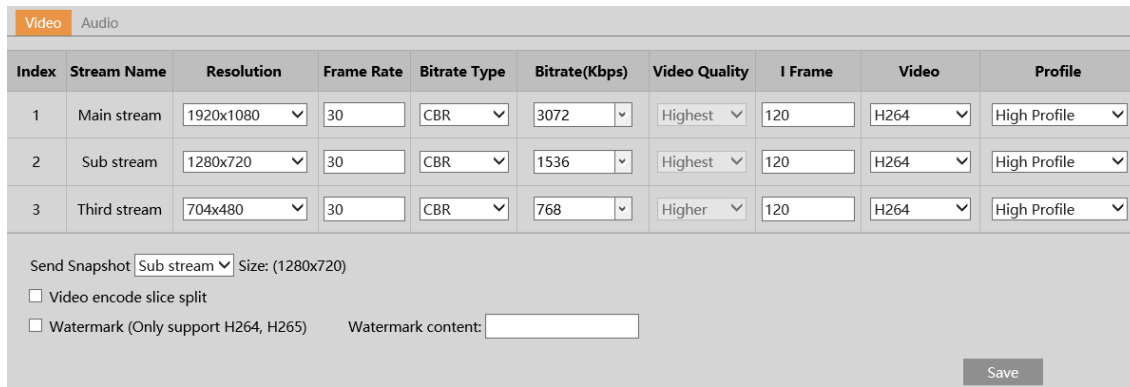
Set full time schedule for common mode and specified time schedule for day and night. Choose “Timing” in the drop-down box of schedule as shown below.



Drag “🕒” icons to set the time of day and night. Blue means daytime 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.

### 3.2.2 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.



Three video streams can be adjustable.

**Resolution:** The size of image.

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

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

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

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

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

**Video Compression:** MJPEG, H264+, H264, H265or 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.

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

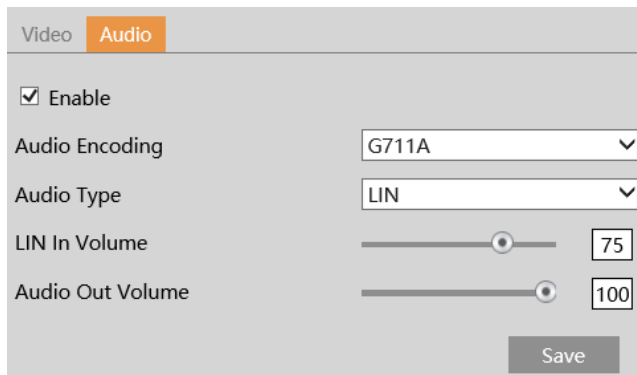
**Send Snapshot:** Set the snapshot stream.

**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.

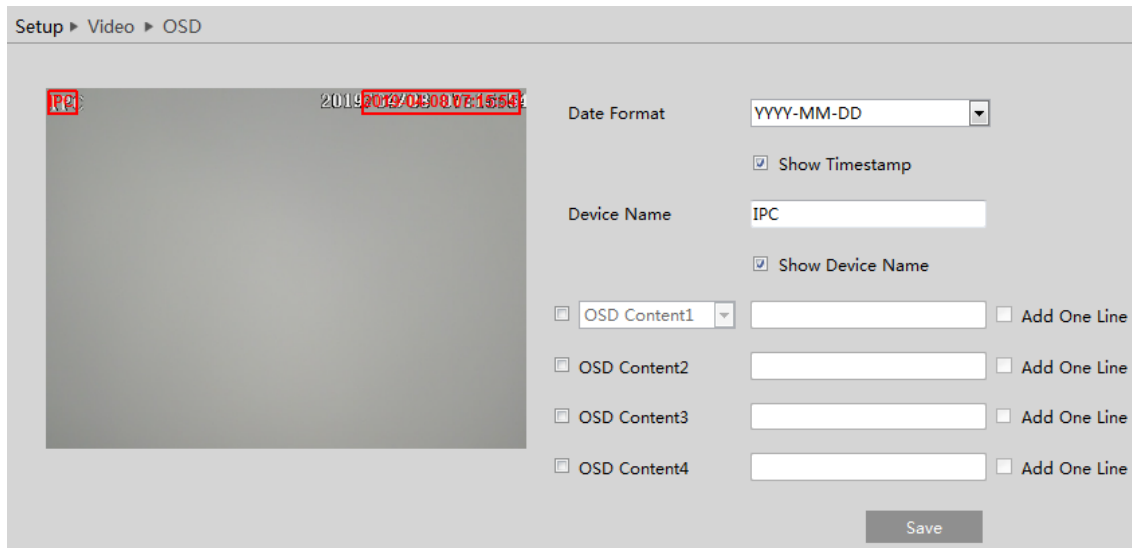




Audio Encoding: G711A and G711U are selectable.  
 Audio Type: LIN.  
 Please set LIN In Volume and audio out volume as needed.

### 3.2.3 OSD Configuration

Go to Video→OSD interface as shown below.



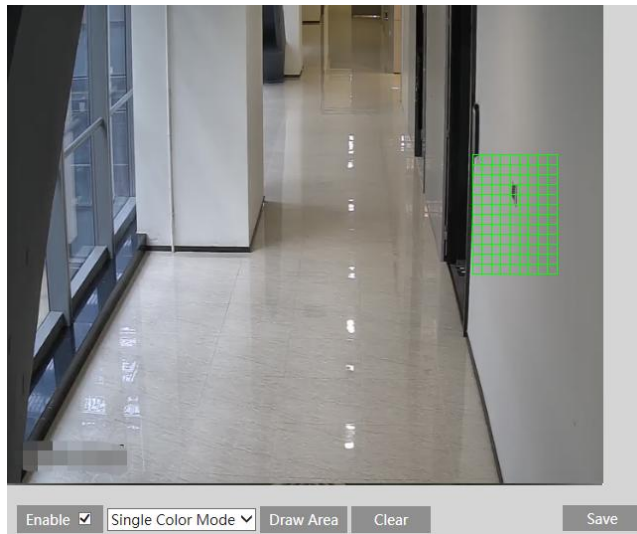
Set time stamp, device name, OSD content and picture overlap here. After enabling the corresponding display and entering the content, drag them to change their position. Then click the “Save” button to save the settings.

#### Picture Overlap 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.

### 3.2.4 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.

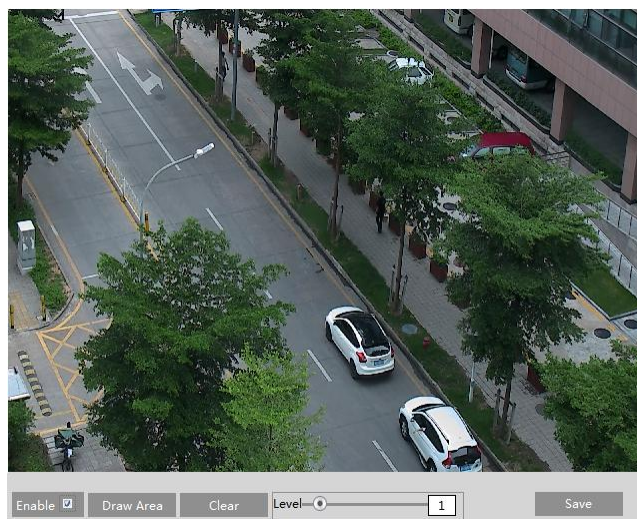


To clear the video mask:

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

### 3.2.5 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.



## 3.3 Alarm Setup

### 3.3.1 Motion Detection

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

Detection Config
Area and Sensitivity
Schedule

Enable

Alarm Holding Time  ▾

Trigger Alarm Out

Alarm Out 0  Alarm Out 1  Alarm Out 2  Alarm Out 3

Trigger SD Card Snapshot

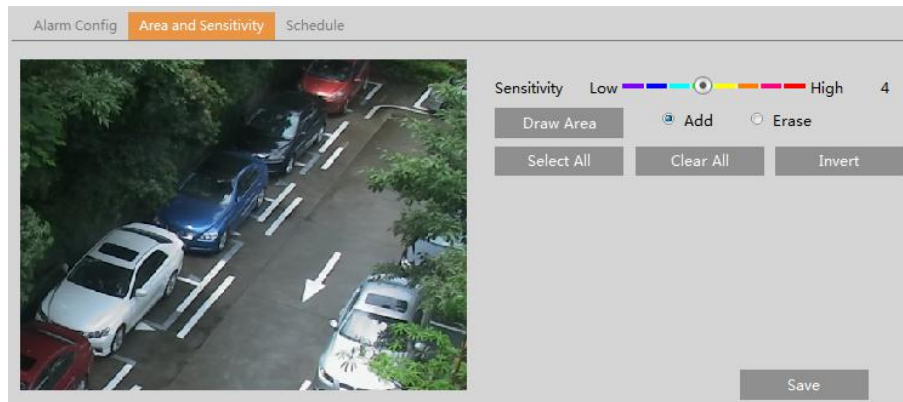
Trigger SD Card Recording

Trigger Email

Trigger FTP

1. Check “Enable” check box to activate motion-based alarms. If unchecked, the device will not send out any signals to trigger motion-based recording to the NVR or CMS, even if there is motion in the video.
- Trigger Alarm Out:** If selected, this would trigger external relay outputs that are connected to the device on detecting a motion-based alarm.
- Trigger SD Card Snapshot:** If selected, the system will capture images on motion detection and save the images on an SD card.
- Trigger SD Card Recording:** If selected, video will be recorded on an SD card on motion detection.
- Trigger Email:** If “Trigger Email” and “Attach Picture” are checked (email address must be set first in the Email configuration interface), the captured pictures and triggered event will be sent into those addresses.
- Trigger FTP:** If “Trigger FTP” and “Attach Picture” are checked, the captured pictures will be sent into FTP server address. Please refer to FTP configuration chapter for more details.

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



Move the “Sensitivity” scroll bar to set the sensitivity. Higher sensitivity value means that motion will be triggered more easily. Select “Add” and click “Draw”. Drag the mouse to draw the motion detection area; Select “Erase” and drag the mouse to clear motion detection area.

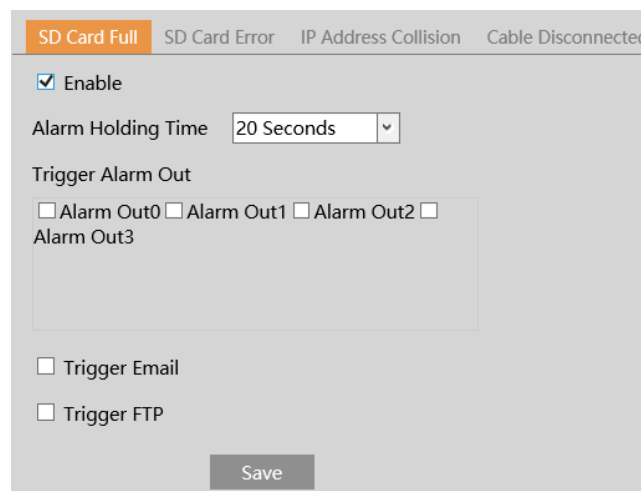
After that, click the “Save” to save the settings. “Clear All” can be used to clear out the entire motion zone.

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](#)).

### 3.3.2 Exception Alarm

#### ● SD Card Full

1. Go to Alarm→Exception Alarm→SD Card Full.



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

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

#### ● SD Card Error

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

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

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

3. Set alarm trigger options. Trigger alarm out, Email and FTP. The setup steps are the same as motion detection. Please refer to [motion detection](#) section for details.

### ● IP Address Conflict

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

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

3. Trigger alarm out. When the IP address of this device conflicts with the IP address of other devices, the system will trigger the alarm out.

### ● Cable Disconnection

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

1. Go to Alarm → Exception Alarm → Cable Disconnected as shown below.

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

### 3.3.3 Alarm In (Sensor Input)

This function is only available for some models. To set sensor alarm (alarm in):  
Go to Alarm→Alarm In interface as shown below.

1. Click “Enable” and set the alarm type, alarm holding time and sensor name.
  2. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to [motion detection](#) section for details.
  4. Set the schedule of the sensor alarm. The setup steps of the schedule are the same as the schedule recording setup. (See [Schedule Recording](#)).
- Select the sensor ID and click “Apply settings to” to quickly apply the settings to the other alarm input.

### 3.3.4 Alarm Out

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

**Alarm Out ID:** The alarm out can be set respectively by selecting alarm out ID.

**Alarm Out Mode:** Alarm linkage, manual operation and schedule are optional.

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

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

Alarm Out ID	Alarm Out0
Alarm Out Mode	Manual Operation
Alarm Type	NC
Manual Operation	<input type="button" value="Open"/> <input type="button" value="Close"/>
<input type="button" value="Save"/>	

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

Alarm Out ID	Alarm Out0
Alarm Out Mode	Timing
Alarm Type	NC
<input type="radio"/> Erase <input checked="" type="radio"/> Add	
Time Range	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 07:00-16:00 <span style="float: right;">Manual Input</span>
<input type="button" value="Save"/>	

### 3.3.5 Alarm Server

Go to Alarm→Alarm Server interface as shown below.

Set the server address, port, heartbeat, and heartbeat interval. When an alarm occurs, the device 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
<input type="button" value="OK"/>	

## 4.4 Analytics Configuration

This device supports certain smart functions, such as line crossing detection, region intrusion detection, etc. These events can be triggered as alarm events.

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 Abandoned/Missing Object Detection

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

To set abandoned/missing object detection:

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

The screenshot shows the 'Detection Config' interface with three tabs: 'Detection Config' (selected), 'Area', and 'Schedule'. Under 'Detection Config', there is a checked 'Enable' checkbox. Below it are two radio buttons: 'Enable Abandoned Object Detection' (selected) and 'Enable Missing Object Detection'. There are two input fields: 'Duration of Delay' set to '10' with the unit 'Second', and 'Alarm Holding Time' set to '20 Seconds' with a dropdown arrow. A section titled 'Trigger Alarm Out' contains four checkboxes: 'Alarm Out 0', 'Alarm Out 1', 'Alarm Out 2', and 'Alarm Out 3', all of which are unchecked. Below this are four more checkboxes: 'Trigger SD Card Snapshot', 'Trigger SD Card Recording', 'Trigger Email', and 'Trigger FTP', all unchecked. A 'Save' button is located at the bottom right of the configuration panel.

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

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

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

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

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

4. Set an alarm area for abandoned/ missing object detection. Click the “Area” tab to go to the interface as shown below.

The screenshot shows the 'Area' configuration interface. It has three tabs: 'Detection Config', 'Area' (selected), and 'Schedule'. The main area displays a live video feed of a museum exhibit with a yellow bounding box drawn around a vase on a display case. To the right of the video feed is an 'Alarm Area' dropdown menu set to '1'. At the bottom of the interface are three buttons: 'Stop Draw', 'Clear', and 'Save'.



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 missing object detection that the drawn frame must be very close to the margin of the object in enhancing the sensitivity and accuracy of the detection.
5. Abandoned/missing object detection cannot determine the objects’ ownership. For instance, there is an unattended package in the station. Abandoned object detection can detect the package itself but it cannot determine to whom it belongs to.
6. Try not to enable abandoned/missing object detection when light changes greatly in the scene.
7. Try not to enable abandoned/missing object if there are complex and dynamic environments in the scene.
8. Adequate light and clear scenery are very important to abandoned/missing object detection.

### 4.4.2 Video Exception

This function can detect changes in the surveillance environment affected by the external factors. Go to Event→Video Exception interface as shown below.

Detection Config Sensitivity

Scene Change Detection

Video Blur Detection

Abnormal Color Detection

Alarm Holding Time 20 Seconds

Trigger Alarm Out

Alarm Out 0  Alarm Out 1  Alarm Out 2  Alarm Out 3

Trigger SD Card Snapshot

Trigger SD Card Recording

Trigger Email

Trigger FTP

Save

1. Enable the applicable detection that is desired.

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

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

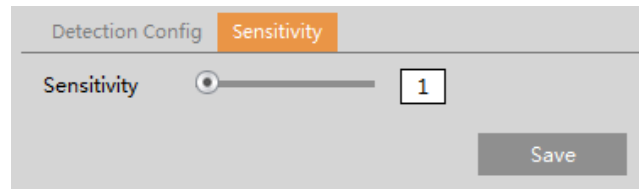
**Abnormal Color Detection:** Alarms will be triggered if the image is abnormal caused by color deviation.

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

[detection](#) section for details.

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

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



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

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

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

**The sensitivity value of Abnormal Color Detection:** The higher the value is, the more sensitive the system responds to the color shift of the image.

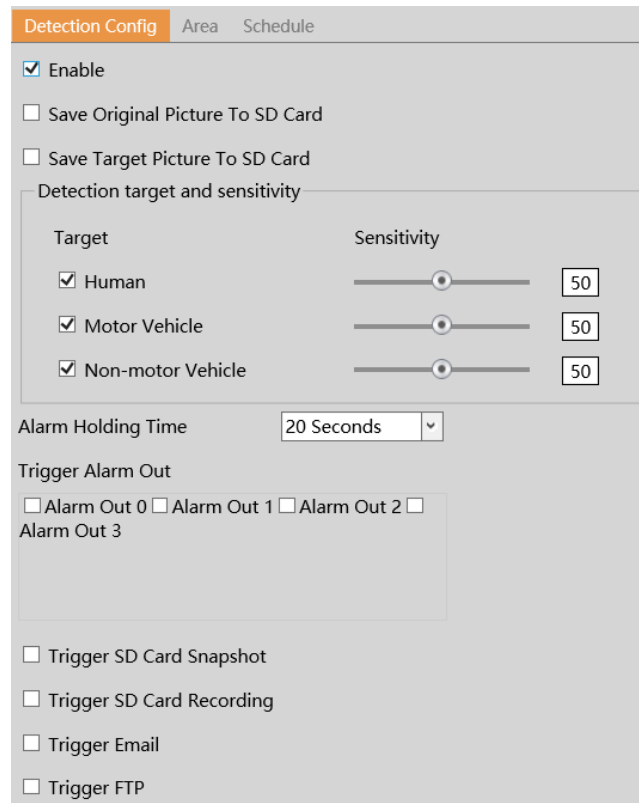
#### ※ The requirements of camera and surrounding area

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.

### 4.4.3 Line Crossing

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

Go to Event→Line Crossing interface as shown below.



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

**Save Original Picture To SD Card:** If it is enabled, the detected original pictures will be captured and saved to the SD card when

there are targets detected.

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

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

**Detection Target:**

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

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

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

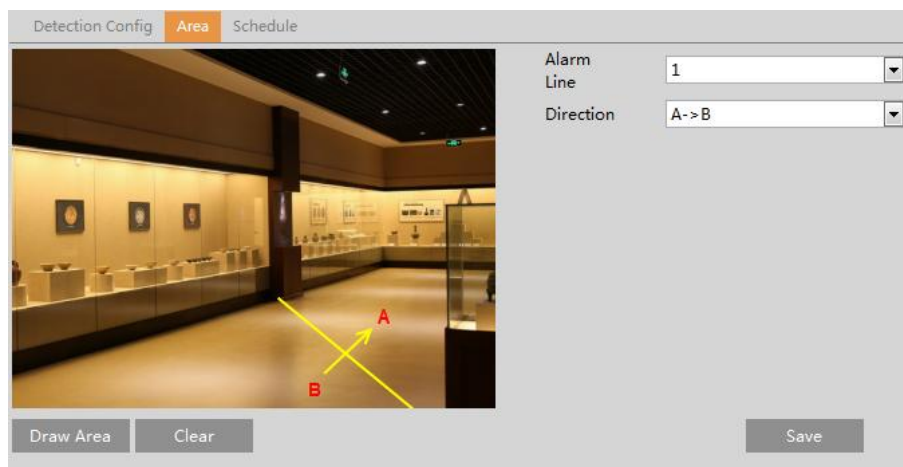
All of the three types of objects can be selected simultaneously. Please select the detection objects as needed. If no object/target is selected, alarms will not be triggered even if line crossing detection is enabled.

2. Set the alarm holding time.

3. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to [motion detection](#) section for details.

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

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



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

**Direction:** A<->B, A->B and A<-B optional. This indicates the direction of the intruder 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 the “Draw Area” button and then drag the mouse to draw a line in the image. Click the “Stop Draw” button to stop drawing. Click the “Clear” button to delete the lines. Click the “Save” button to save the settings.

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

※ **Configuration of camera and surrounding area**

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

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

3. Cameras should be mounted at a height of 10ft or above.

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

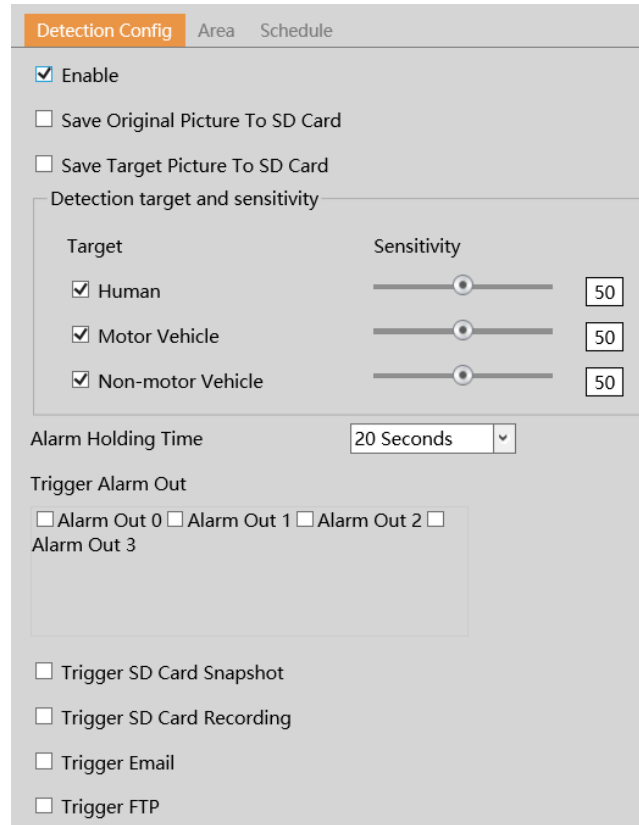
5. The detected objects should not be less than 1% of the entire image and the largest sizes of the detected objects should not be more than 1/8 of the entire image.

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

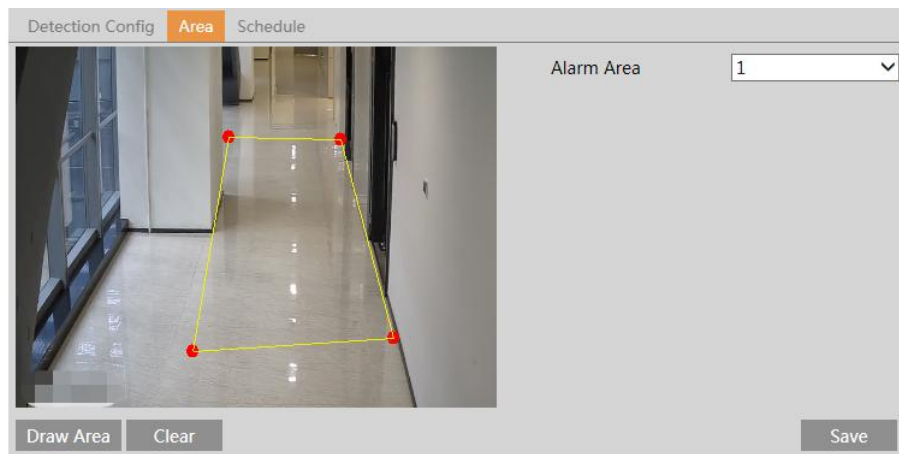
7. Adequate light and clear scenery are crucial for line crossing detection.

#### 4.4.4 Region Intrusion

**Region Intrusion:** Alarms will be triggered if the target intrudes into the defined areas.  
Go to Event→Region Intrusion interface as shown below.



1. Enable intrusion alarm and select the snapshot type and the detection target.
2. Set the alarm holding time.
3. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to [motion detection](#) section for details.
4. Click the “Save” button to save the settings.
5. Set alarm areas for the intrusion detection. Click the “Area” tab to go to the interface as shown below.



- Set the alarm area number on the right side. Up to 4 alarm areas can be added.  
Click the “Draw Area” button and then click around the area where you want to set as the alarm area in the image on the left side (the alarm area should be a closed area). Click the “Stop Draw” button to stop drawing. Click the “Clear” button to delete the alarm area. Click the “Save” button to save the settings.
6. Set the schedule of the intrusion detection. The setup steps of the schedule are the same as schedule recording setup (See

[Schedule Recording](#)).

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

1. Auto-focusing function should not be enabled for intrusion detection.
2. Avoid the scenes with many trees or the scenes with various light changes (like many flashing headlights). The ambient brightness of the scenes shouldn't be too low.
3. Cameras should be mounted at a height of 10ft or above.
4. Keep the mounting angle of the camera at about 45°.
5. The detected objects should not be less than 1% of the entire image and the largest sizes of the detected objects should not be more than 1/8 of the entire image.
6. Make sure cameras can view objects for at least 2 seconds in the detected area for accurate detection.
7. Adequate light and clear scenery are crucial to line crossing detection.

#### 4.4.5 Face Detection

Face detection function is to detect the face appearing in the surveillance scene. Alarms will be triggered when a face is detected. The setting steps are as follows:

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

Detection Config Area Advanced Schedule

State Working

Enable

Save Source Information To SD Card

Save Face Information To SD Card

Trigger alarm condition All

Alarm Holding Time 20 Seconds

Trigger Alarm Out

Alarm Out 0  Alarm Out 1  Alarm Out 2  Alarm Out 3

Trigger SD Card Snapshot

Trigger SD Card Recording

Trigger Email

Trigger FTP

Save

2. Enable the face detection function.

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

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

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

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

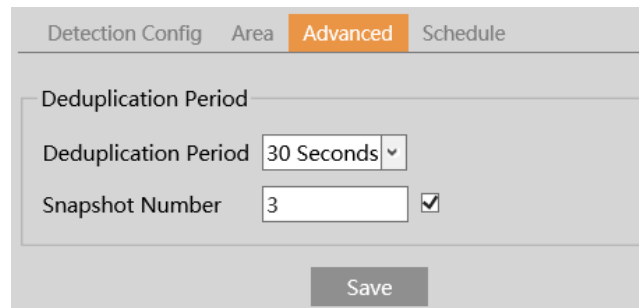
4. Set alarm detection area.



Use this to draw the approximate size of the face that you want the camera to capture. This is useful when there are multiple faces in the background or foreground that are not needed to be captured. To enable, Click “Draw Area” and drag the border lines of the rectangle to modify its size. Move the rectangle to change its position. Click “Stop Draw” to stop drawing the area. Click “Clear” to clear the area. Then set the detectable face size by defining the maximum value and the minimum value (The default size range of a single face image occupies from 3% to 50% of the entire image).

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

6. Advanced configuration. Choose the deduplication period and snapshot number as needed to avoid capturing multiple similar pictures in a very short period of time.

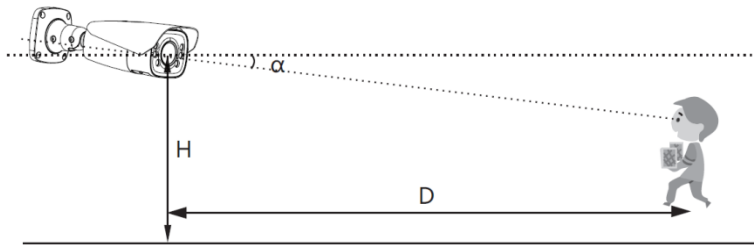


**Deduplication Period:** If 5 seconds is selected, the camera will capture the same target once every 5 seconds during its continuous tracking period.

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

#### ※ Configuration requirements of camera and surrounding area

1. Cameras must be installed in the area with stable and adequate light sources.
2. The installation height ranges from 1.9m (6.2ft) to 2.5m (8.2ft), adjustable according to the focal-length of different lenses and object distances.
3. The depression angle (a) of the camera shall be less than or equal to 15°.



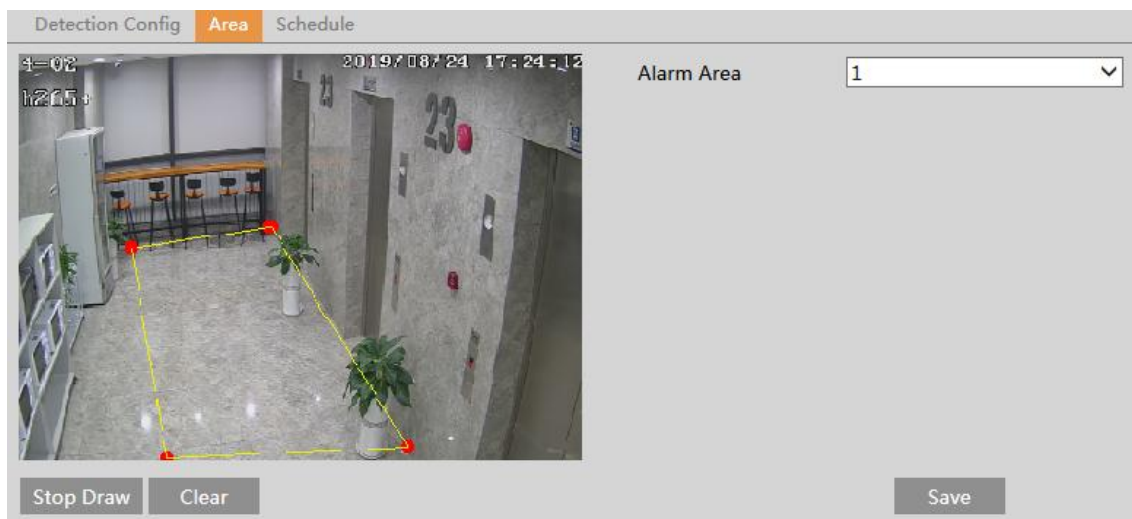
4. The object distance depends on the focal-length of the lens mounted in the camera.
5. In order to guarantee the captured face recognition rate, the requirement for face capture are: left or right face turn angle is less than about 30°; pitching angle is less than 20°.
6. Face illumination must be uniform, if the brightness is low or there is a large area of shadow, need to do the light filling.
7. When the capture scenario is backlight, the camera's BLC/HLC/WDR need to be turned on, or fill the light.
8. The face recognition do not support black & white mode for now.

#### 4.4.6 Region Entrance

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

Go to Config→Event→Region Entrance interface.

1. Enable region entrance detection and select the snapshot type and the detection target.
2. Set the alarm holding time.
3. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to [motion detection](#) section for details.
4. Click the “Save” button to save the settings.
5. Set the alarm area of the region entrance detection. Click the “Area” tab to go to the interface as shown below.



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

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

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

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

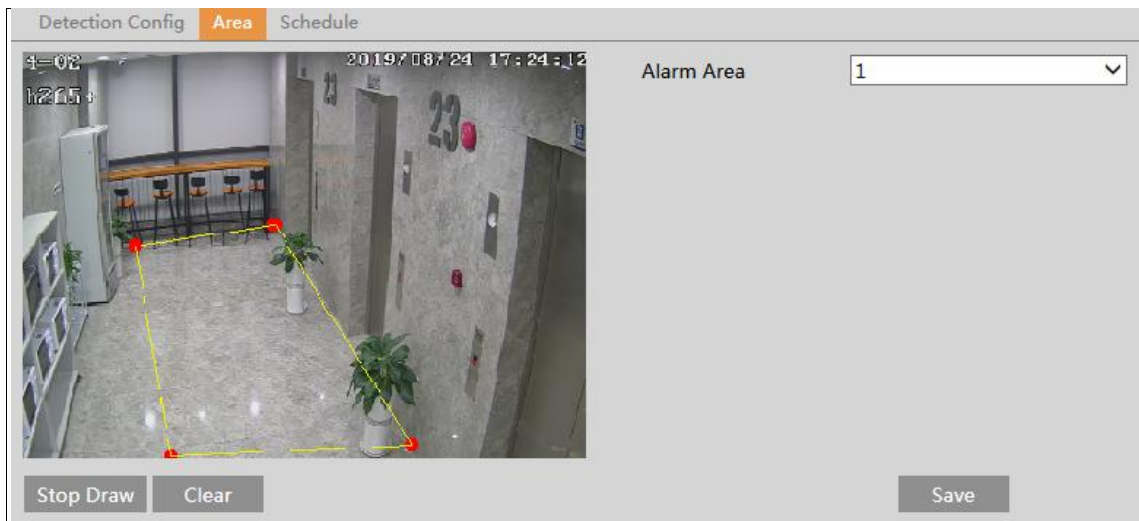
#### 4.4.7 Region Exiting

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

Go to Config→Event→Region Exiting interface.

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

2. Set the alarm holding time.
3. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to [motion detection](#) section for details.
4. Click the “Save” button to save the settings.
5. Set the alarm area of the region exiting detection. Click the “Area” tab to go to the interface as shown below.



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

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

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

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

#### 4.4.8 Target Counting by Line

This function is used to detect, track and count the number of people or vehicles crossing the set alarm line.

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



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

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

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

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

3. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to [motion detection](#) section for details.

4. Set the area of the target counting. Click the “Area” tab to go to the interface as shown below.

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

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

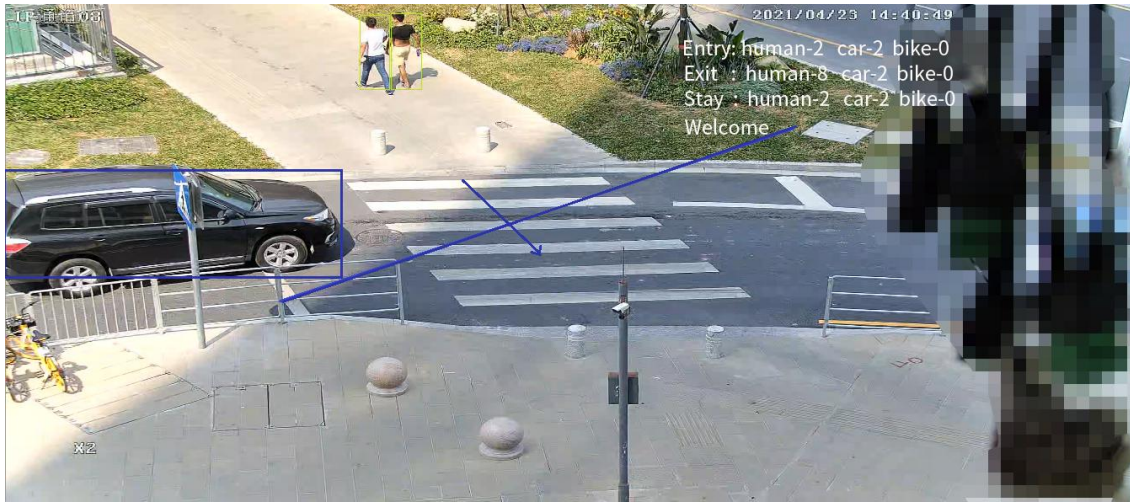
**Statistics:** If enabled, you can see the statistical information in the live view interface. If disabled, the statistical information will not be displayed in the live view interface.

The statistical OSD information can be customized as needed.

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

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

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



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

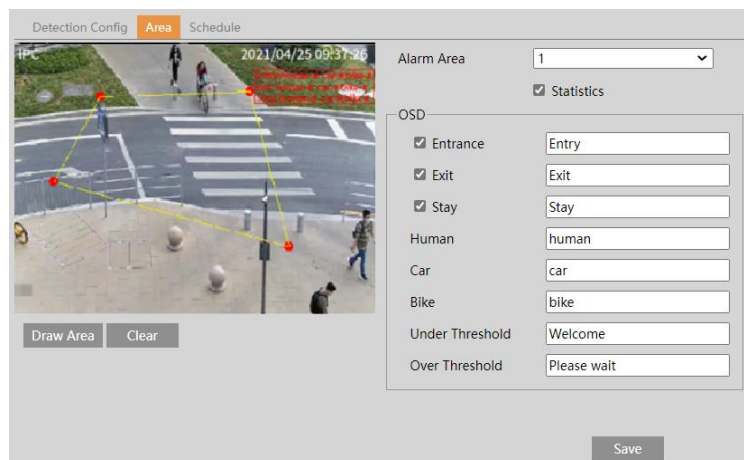
Target Counting by Line				
Report Type		Count Type	Count Time	
Daily Report		Enter	2023	Year 5
			Month 11	Day
			Count	
			Table	
			Statistics	
Index	Count Time	Human	Motor Vehicle	Non-motor Vehicle
1	2023-05-11 00:00:00 ~ 2023-05-11 00:59:59	0	0	0
2	2023-05-11 01:00:00 ~ 2023-05-11 01:59:59	0	0	0

Please select report type, count type and start time as needed. Then click “Count” to search the statistic result. Click “Statistics” to view the statistic result intuitively.

#### 4.4.9 Target Counting by Area

This function is used to detect, track and count the number of people or vehicles intruding into a pre-defined area.

1. Go to Config→Event→Target Counting by Area.
2. Enable target counting by area, select the snapshot type, the detection target, counting reset and alarm linkages. The setup steps are the same as the target counting by line.
3. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to [motion detection](#) section for details.
4. Set the statistic area. Click the “Area” tab to go to the interface as shown below.

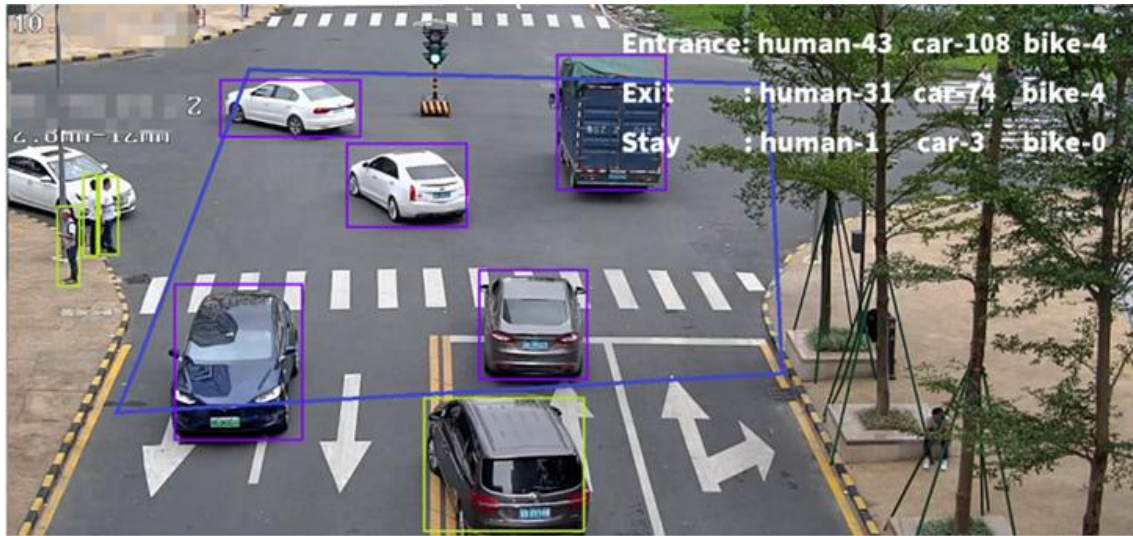


Select the alarm area number on the right side. Only one alarm area can be added.

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

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

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



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

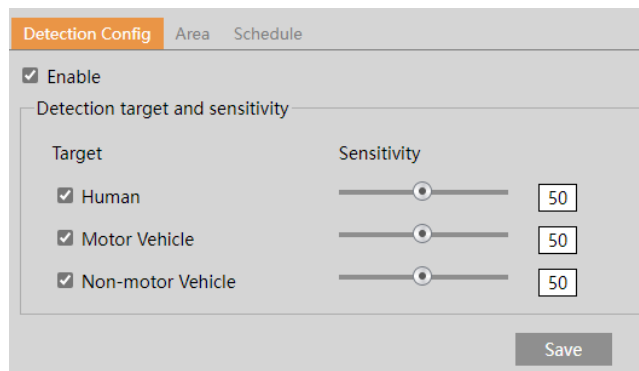
Index	Count Time	Human	Motor Vehicle	Non-motor Vehicle
1	2023-05-11 00:00:00 ~ 2023-05-11 00:59:59	0	0	0
2	2023-05-11 01:00:00 ~ 2023-05-11 01:59:59	0	0	0

Please select report type, count type and start time as needed. Then click “Count” to search the statistic result. Click “Statistics” to view the statistic result intuitively.

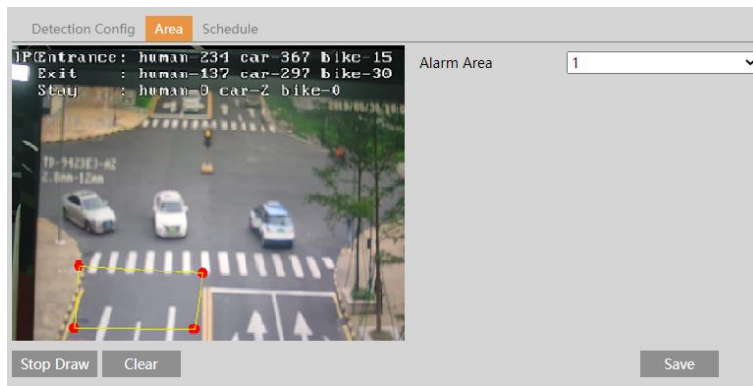
#### 4.4.10 Heat Map

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

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



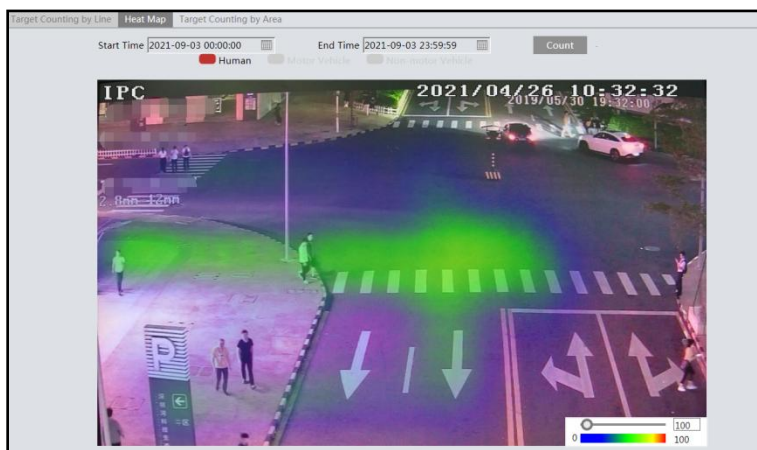
2. Set heat map display area. Up to 4 areas can be set.



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

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

4. View the heat map data (click Statistics→Heat Map). Set the start time and the end time. Click “Count” to view the heat map as shown below. The default heat map is people flow data display. Click “Motor Vehicle” or “Non-motor Vehicle” to view the corresponding data.



## 4.5 Network Configuration

### 4.5.1 TCP/IP

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

**Use IP address (take IPv4 for example)**-obtain a local IP address automatically through DHCP. A typical router has a DHCP server built in, and therefore is able to assign an IP address to the device.

**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 device will get a dynamic WAN IP address. This IP address will change frequently. To be notified, the IP change notification function can be used.

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

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

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

#### 4.5.2 Port

Go to Network→Ports/Connection 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="554"/>
RTSP Port	<input type="text" value="9008"/>
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.

### 4.5.3 Server Configuration

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

<input checked="" type="checkbox"/> 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 VMS. Then enable the auto report in the VMS when adding a new device. Next, enter the remaining information of the device in the VMS. After that, the system will automatically allot a device ID. Please check it in the VMS.

3. Enter the above-mentioned server address, server port and device ID in the corresponding boxes. Click the “Save” button to save the settings.

### 4.5.4 Onvif

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

Index	User Name	User Type
1	admin	Administrator

**Add User** [X]

User Name

Password

Level

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

Confirm Password

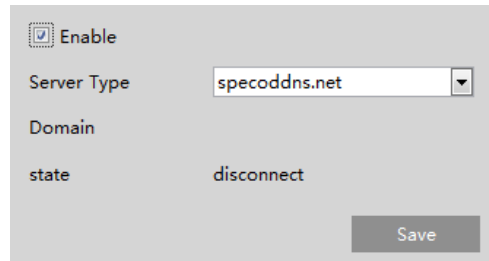
User Type

**Note:** when adding the device to the third-party platform with ONVIF/RTSP protocol, please enter the username and password created in the above interface.

#### 4.5.5 DDNS

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

1. Go to Network → Ports/Connections → DDNS.



Enable

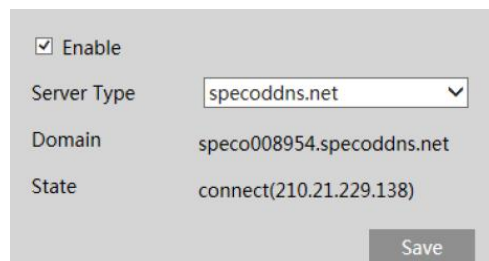
Server Type specoddns.net

Domain

state disconnect

Save

2. Enable, save and use DDNS to log in.



Enable

Server Type specoddns.net

Domain speco008954.specoddns.net

State connect(210.21.229.138)

Save

#### 4.5.6 SNMP

To get device status, parameters and alarm information and remotely manage the device, 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 Network → Ports/Connections → SNMP.

**SNMP v1/v2**

Enable SNMPv1

Enable SNMPv2

Read SNMP Community:

Write SNMP Community:

Trap Address:

Trap Port:

Trap community:

---

**SNMP v3**

Enable SNMPv3

Read User Name:

Security Level:

Authentication Algorithm:  MDS  SHA

Authentication Password:

Private-key Algorithm:  DES  AES

Private-key Algorithm:

Write User Name:

Security Level:

Authentication Algorithm:  MDS  SHA

Authentication Password:

Private-key Algorithm:  DES  AES

Private-key Algorithm:

---

**Other Settings**

SNMP Port:

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.

#### 4.5.7 802.1x

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

Enable

Protocol Type:

EAPOL Version:

User Name:

Password:

Confirm Password:

To use this function, the device 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 device 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.

#### 4.5.8 RTSP

Go to Network→ Ports/Connections→RTSP.

Enable

Port: 9008

Address: rtsp://IP or domain name:port/profile1  
rtsp://IP or domain name:port/profile2  
rtsp://IP or domain name:port/profile3

Multicast address

Main stream: 239.0.0.0 50554  Automatic start

Sub stream: 239.0.0.1 51554  Automatic start

Third stream: 239.0.0.2 52554  Automatic start

Audio: 239.0.0.3 53554  Automatic start

Allow anonymous login (No username or password required)

Save

Select “Enable” to enable the RTSP function.

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

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

#### Multicast Address

**Main stream:** The address format is

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

**Sub stream:** The address format is

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

**Third stream:** The address format is

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

**Audio:** Having entered the main/sub stream in a media player (like VLC), 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.

#### 4.5.9 RTMP

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

Go to Config→Network→ Ports/Connections→RTMP.

Port Server Onvif DDNS SNMP 802.1X RTSP **RTMP** UPnP Email

Enable (Only supports H264)

Stream Type:  Main stream  Sub stream  Third stream

Reconnect After Timeout: 30 Second

Server Address: example : rtmp://127.0.0.1:1935/live/liv

Connection Status: Not Connected Refresh

Save

Check “Enable”, select stream type, set the reconnection time after timeout and server address as needed.  
Server address: Enter the server address allocated by the third party server.  
After that, click “Save” to save the settings. Then click “Refresh” to view the connection status.

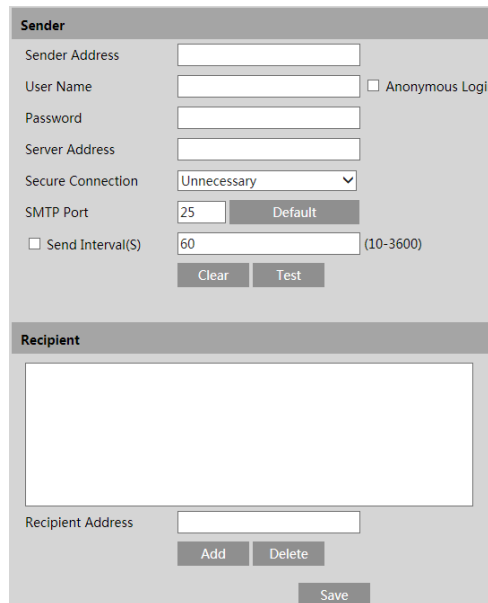
#### 4.5.10 UPNP

If this function is enabled, the device can be quickly accessed through the LAN.  
Go to Network→ Ports/Connections→UPnP. Enable UPnP and then enter UPnP name.



#### 4.5.11 Email

If you need to trigger Email when an alarm happens or IP address is changed, please set the Email here first.  
Go to Network→ Ports/Connections→Email.



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

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

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

Select the secure connection type at the “Secure Connection” pull-down list according to what’s required.

**SMTP Port:** The SMTP port.

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

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

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

#### 4.5.12 FTP

After an FTP server is set up, captured pictures from events will be uploaded to the FTP server.  
Go to Network→ Ports/Connections→FTP.

Server Name	Server Address	Port	User Name	Upload Path
<div style="border: 1px solid gray; padding: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span>Add FTP</span> <span>×</span> </div> <div style="margin-top: 10px;"> <p>Server Name <input type="text"/></p> <p>Server Address <input type="text"/></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"/> <input type="checkbox"/> Anonymous</p> <p>Password <input type="password"/></p> </div> <div style="margin-top: 10px; text-align: center;"> <input type="button" value="OK"/> <input type="button" value="Cancel"/> </div> </div>				
<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Test"/> <input type="button" value="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.

#### 4.5.13 HTTPS

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

Go to Network → Ports/Connections → HTTPS as shown below.

Enable  
 Disable HTTP (Checking this option may cause no video image in Google and Firefox!)

Certificate installed: C=CN, ST=GD, L=SZ, O=embeddedsoftewar

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

There is a certificate installed by default as shown above. Enable this function and save it. Then the device 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:

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

\* Click "Create a private certificate" to enter the following creation interface.

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

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

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

#### 4.5.14 HTTP POST

Go to Config→Network →Ports/Connections→HTTP POST interface.

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

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

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

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

#### 4.5.15 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 Network→ Ports/Connections→QoS.

Video/Audio DSCP	0
Alarm DSCP	0
Manager DSCP	0

Save

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 Admin

Go to Security→User Admin interface as shown below.

Index	User Name	User Type
1	admin	Administrator

#### Add user:

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

**Add User**

User Name:

Password:

Level:

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

Confirm Password:

User Type:

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

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

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

4. Choose the user type and select the permission.

6. Click the “OK” button and then the newly added user will be displayed in the user list.

#### Modify user:

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

3. Enter the old password of the user in the “Old Password” text box.
4. Enter the new password in the “New password” and “Confirm Password” text box.
5. Modify the permission as necessary.
6. Click the “OK” button to save the settings.

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

**Delete user:**

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

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

**4.6.2 Online User**

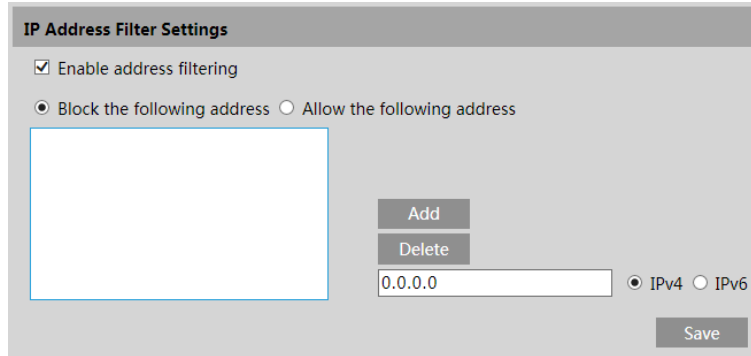
Go to Security→Online User to view the user who is viewing the live video.

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

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

### 4.6.3 Block and Allow Lists

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



The screenshot shows the 'IP Address Filter Settings' configuration page. It features a checked box for 'Enable address filtering'. Below this, there are two radio buttons: 'Block the following address' (selected) and 'Allow the following address'. A large empty text box is provided for entering IP addresses. To the right of this box are 'Add' and 'Delete' buttons. Below these buttons is a text input field containing '0.0.0.0'. To the right of this field are two radio buttons: 'IPv4' (selected) and 'IPv6'. At the bottom right of the configuration area is a 'Save' button.

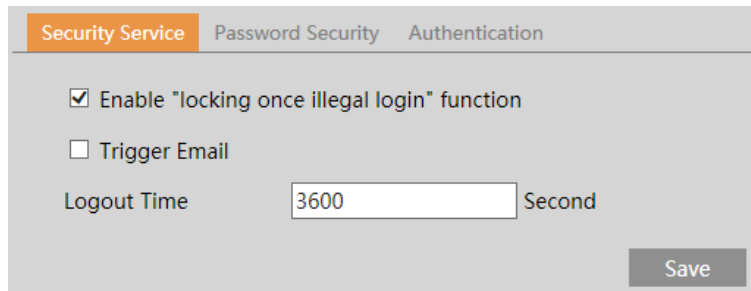
The setup steps are as follows:

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.

### 4.6.4 Security Management

Go to Security→Security Management as shown below.



The screenshot shows the 'Security Management' configuration page with three tabs: 'Security Service' (selected), 'Password Security', and 'Authentication'. Under the 'Security Service' tab, there is a checked box for 'Enable “locking once illegal login” function'. Below this is an unchecked box for 'Trigger Email'. The 'Logout Time' is set to '3600' in a text input field, followed by the unit 'Second'. A 'Save' button is located at the bottom right.

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 five times will make the login interface locked. The device can be logged in again after a half hour or after the device reboots.

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

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

#### ● Password Security



The screenshot shows the 'Password Security' configuration page with three tabs: 'Security Service', 'Password Security' (selected), and 'Authentication'. Under the 'Password Security' tab, there are two dropdown menus: 'Password Level' set to 'weak' and 'Expiration Time' set to 'Never'. A 'Save' button is located at the bottom right.

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,

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.

## 4.7 Maintenance Configuration

### 4.7.1 Backup and Restore

Go to Maintenance→Backup & Restore.

The screenshot displays a web interface for maintenance configuration. It is divided into three main sections: 'Import Setting', 'Export Settings', and 'Default Settings'. The 'Import Setting' section includes a 'Path' input field with a 'Browse' button and an 'Import Setting' button. The 'Export Settings' section features an 'Export Settings' button. The 'Default Settings' section has a 'Keep' section with three checkboxes: 'Network Config', 'Security Configuration', and 'Image Configuration', and a 'Factory Default' button at the bottom.

- **Import & Export Settings**

Configuration settings of the device can be exported from a device into another device.

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.

**Note:** The login password needs to be entered after clicking the “Import Setting” button.

- **Default Settings**

Click the “Load Default” button and then verify the password to restore all system settings to the default factory settings except those you want to keep.

### 4.7.2 Reboot

Go to Maintenance→Reboot.

Click the “Reboot” button and then enter the password to reboot the device.

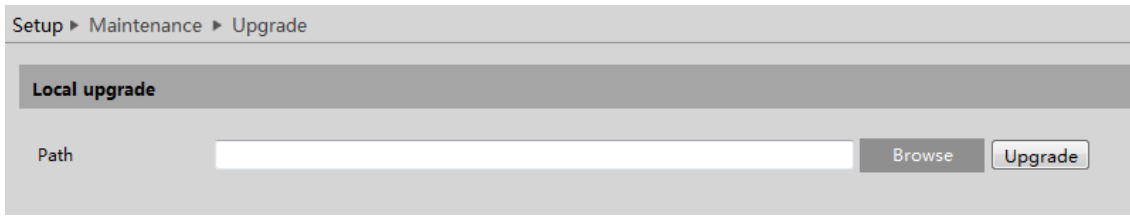
**Timed Reboot Setting:**

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

### 4.7.3 Upgrade

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





1. Click the “Browse” button to select the save path of the upgrade file
  2. Click the “Upgrade” button to start upgrading the firmware.
  3. Enter the correct password and then the device will restart automatically
- Caution!** Do not close the browser or disconnect the device from the network during the upgrade.

#### 4.7.4 Operation Log

To query and export log:

1. Go to Maintenance→Operation Log.

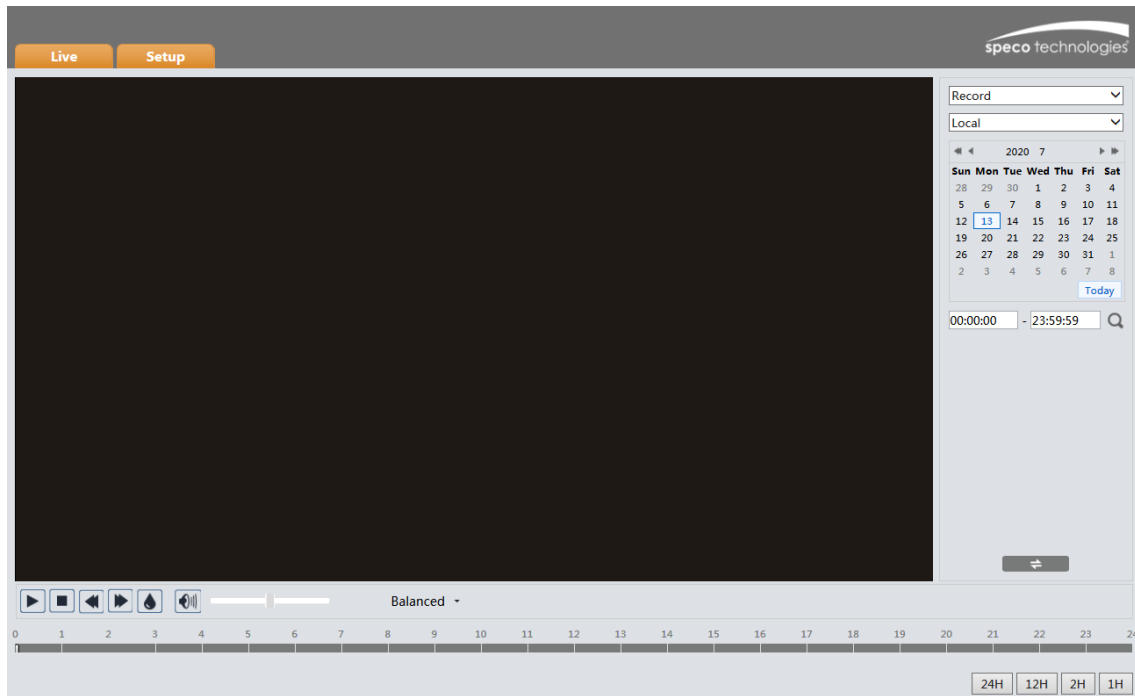
Index	Time	Main Type	Sub Type	User Name	Login IP
1	2019-04-08 08:43:43	Alarm	Motion start		
2	2019-04-08 08:43:24	Alarm	Vfd Alarm		
3	2019-04-08 08:43:14	Alarm	Motion stop		
4	2019-04-08 08:41:20	Alarm	Motion start		
5	2019-04-08 08:40:26	Alarm	Motion stop		
6	2019-04-08 08:40:06	Alarm	Motion start		
7	2019-04-08 08:37:18	Alarm	Motion stop		
8	2019-04-08 08:34:43	Alarm	Motion start		

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 Search

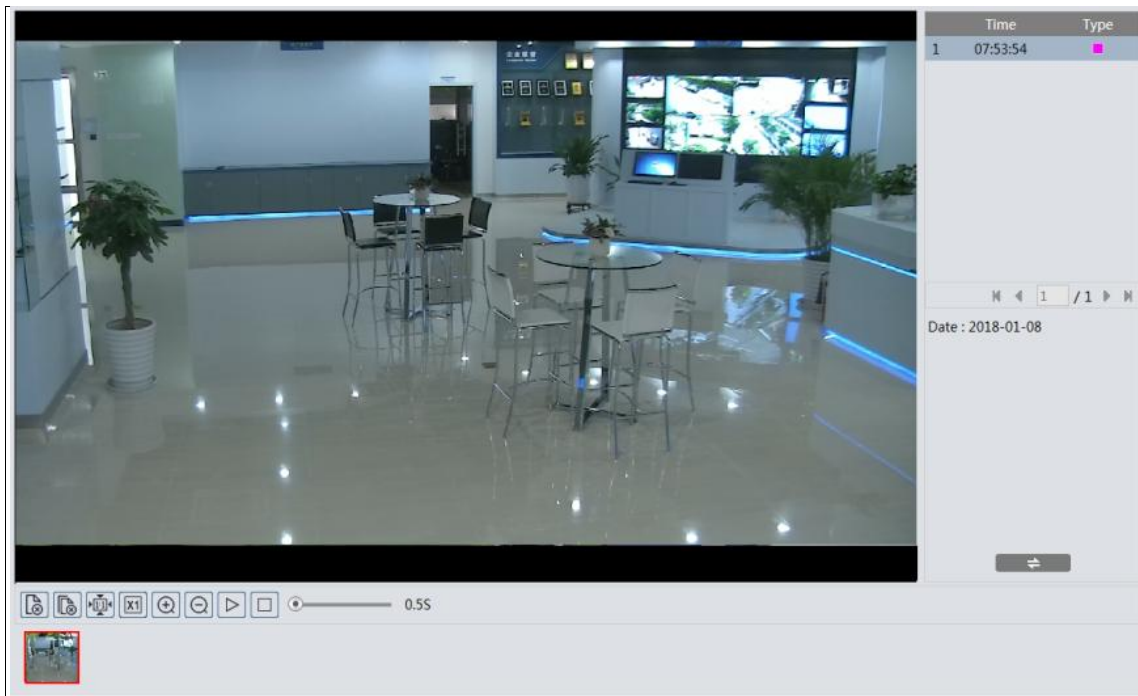
### 5.4 Image Search


In the Setup interface, click Search to go to the interface as shown below. Images that are saved on the PC or SD card can be found here.



#### ● Local Image Search

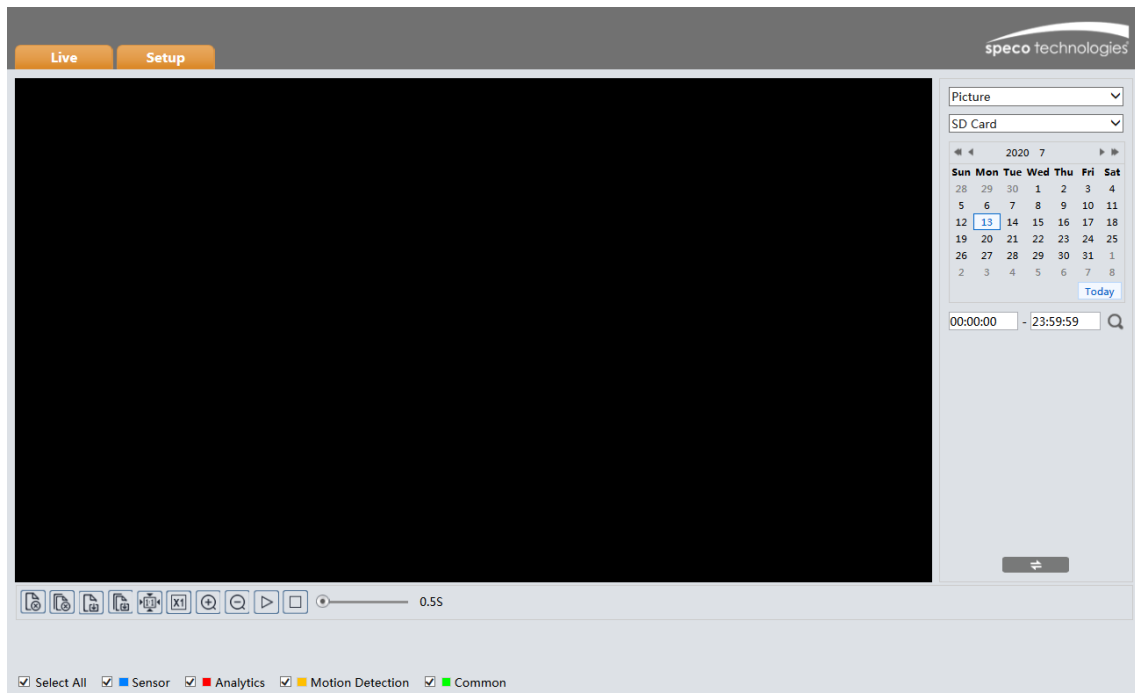
1. Choose "Picture"—"Local".
2. Set time: Select date and choose the start and end time.
3. Click  to search the images.
4. Double click a file name in the list to view the captured photos as shown above.





Click  to return to the previous interface.












● **SD Card Image Search**

1. Choose “Picture”—“SD Card”.



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

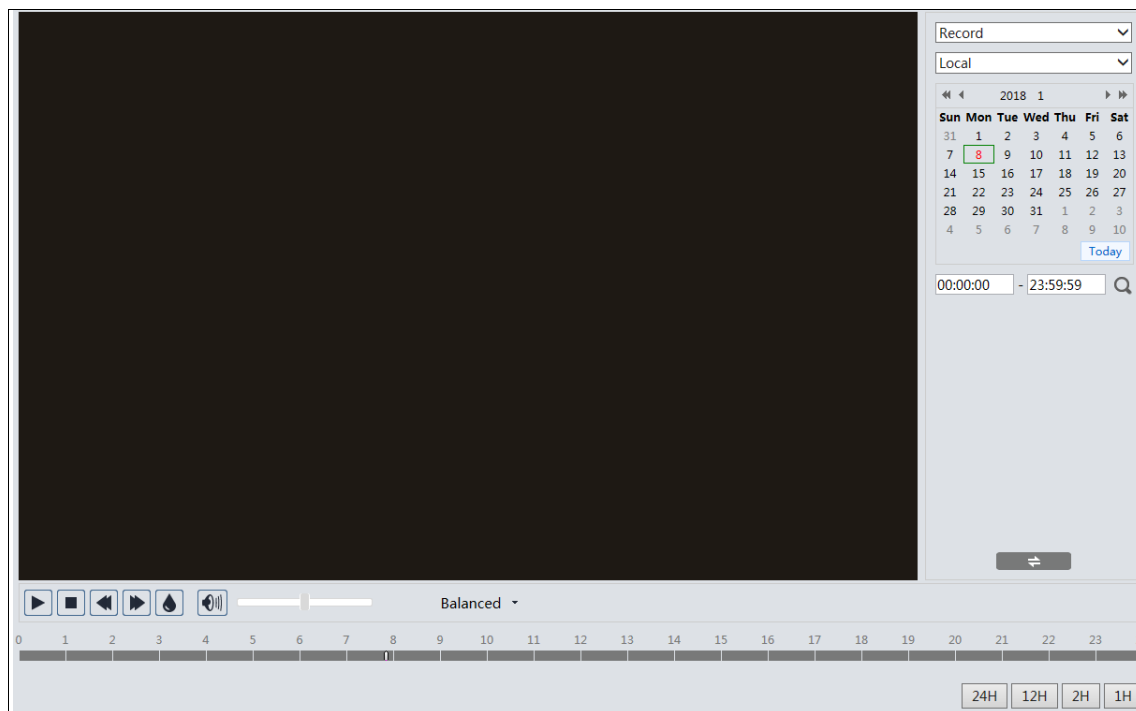
The descriptions of the buttons are shown as follows.


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

## 5.5 Video Search








### 5.5.1 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.

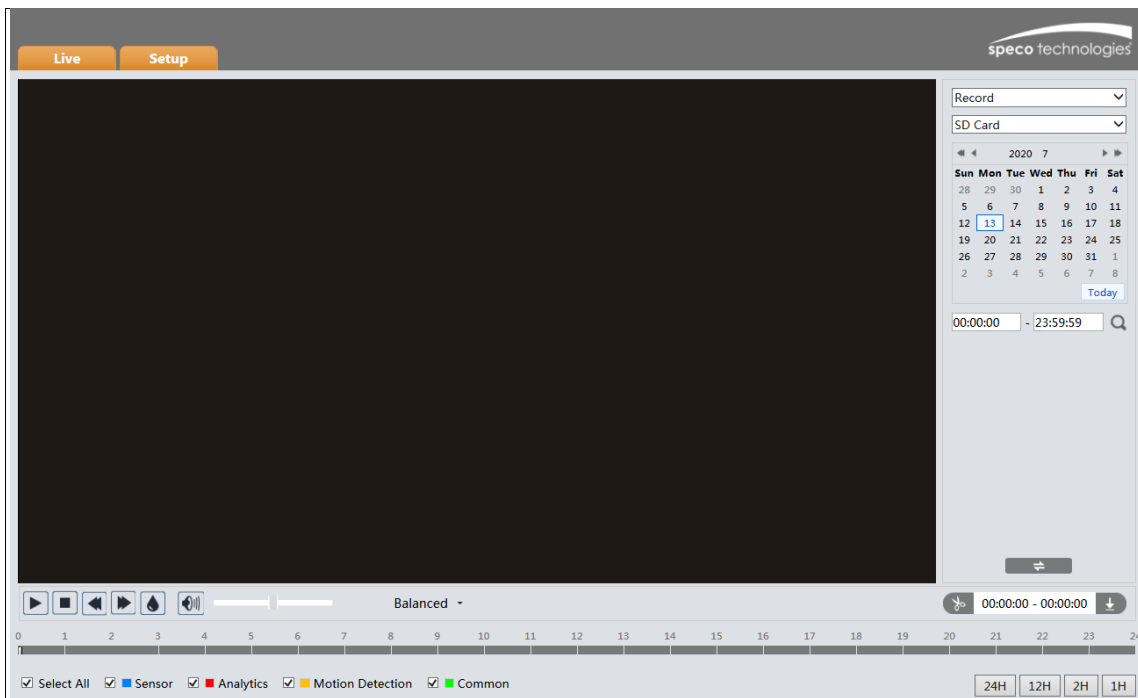


Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button
	Stop button		Speed down
	Speed up		Watermark display
	Enable / disable audio; drag the slider to adjust the volume after enabling audio.		

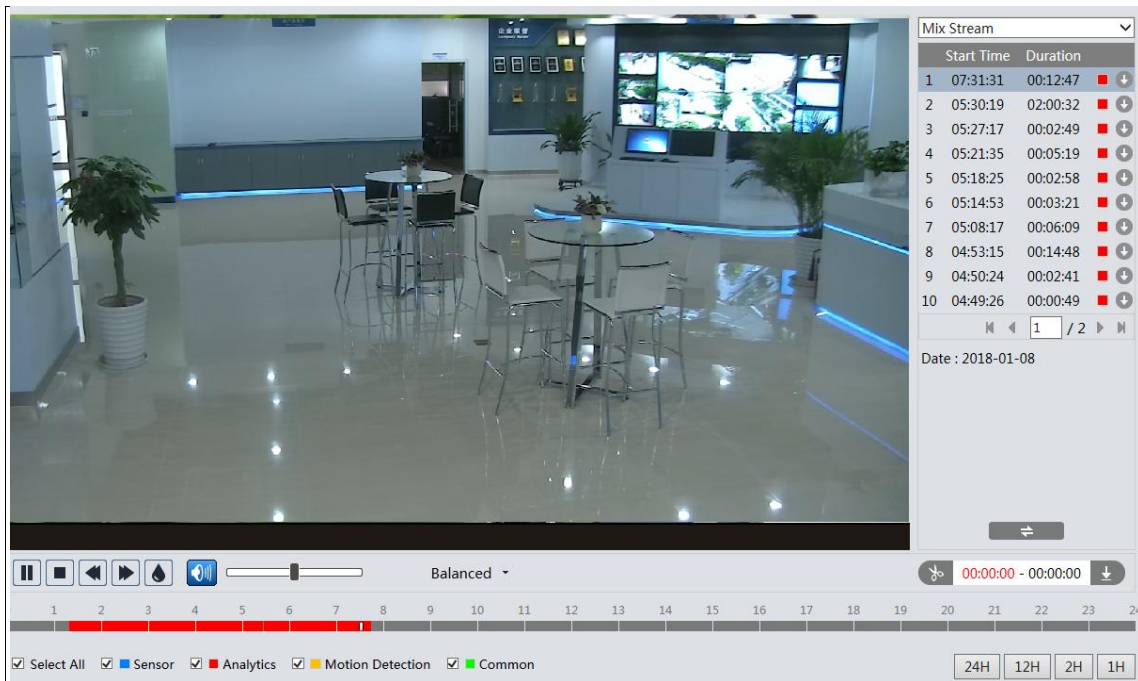
### 5.5.2 SD Card Video Search

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

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







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



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

Video clip and downloading

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

Index	Process	Record	Start Time	End Time	Path	Operate
1	100%	Cut	2018-01-16 01:1...	2018-01-16 01:1...	<a href="#">Favorites</a>	Open

Set up D:\Favorites Clear List Close

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

Click "Open" to play the video.

Click "Clear List" to clear the downloading list.

Click "Close" to close the downloading window.

# Appendix

## Appendix 1 Troubleshooting

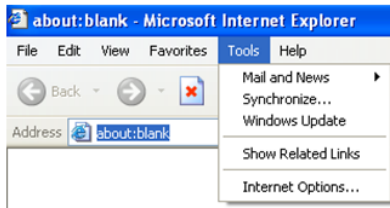
### IP Scanner does not show any device.

Make sure that the PC that's running IP Scanner is on the same local network as the devices.

### Internet Explorer cannot download ActiveX control.

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

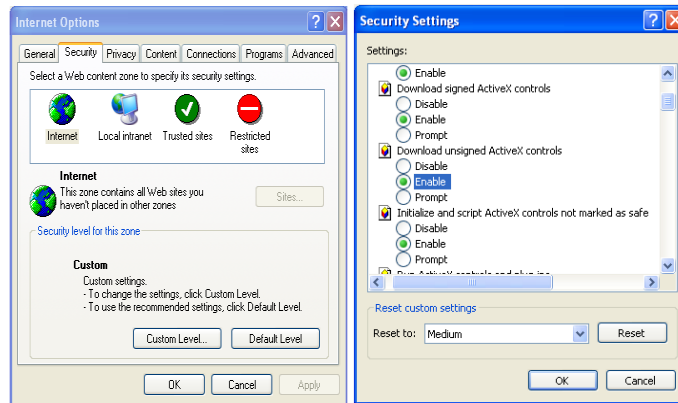
1. Open IE browser and then click Tools→Internet Options.



2. Select Security→Custom Level.

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

4. Click OK to finish setup.



### No sound can be heard.

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

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





---

**Models: O5E1**

**Federal Communications Commission (FCC) Statements**

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

**FCC Responsible Party:**

Speco Technologies  
200 New Highway  
Amityville, NY11701  
[www.specotech.com](http://www.specotech.com)