User Manual
4MP Dual Illumination IP Camera

O4LB1M / O4LT1M

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

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 camera near power lines, radar equipment or other electromagnetic radiation.
Do not block any ventilation openings if any.
Use all the weatherproofing hardware requirement to minimize weather intrusion.

3. Operation and Daily Maintenance

Please shut down the device and then unplug the power cable before you begin any maintenance work.
Do not touch the CMOS sensor optic component. You can use a blower to clean the dust on the lens surface.
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.
Please use a professional optical cleaning method to clean the enclosure. Improper enclosure cleaning (such as using cloth) may result in poor IR functionality and/or IR reflection.
The grounding holes of the product are recommended to be grounded to further enhance the reliability of the camera.
Dome cover is an optical device, please do not touch or wipe cover surface directly during installation and use, please refer to the following methods if dirt is found.
Stained with dirt:
Use oil-free soft brush or hair dryer to remove it gently.
Stained with grease or fingerprint.
Use oil-free cotton cloth or paper soaked with alcohol or detergent to wipe from the lens center outward. Change the cloth and wipe several times if it is not clean enough.

Warning

This camera should be installed by qualified personnel only.
All the examination and repair work should be done by qualified personnel.
Any unauthorized changes or modifications could void the warranty.

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
Network Camera Unit	1
Junction box	1
Quick Start Guide	1
Installation Accessories Bag	1
CD	1

Table of Contents

1 Introduction 2
2 Web Access and Login 3
3 Live View 5
4 Camera Configuration 7
4.1 System Configuration 7
4.1.1 System Information 7
4.1.2 Date and Time 7
4.1.3 Local Recording 7
4.1.4 Storage 8
4.2 Video Configuration 10
4.2.1 Image Configuration 10
4.2.2 Video / Audio Configuration 12
4.2.3 OSD Configuration 13
4.2.4 Video Mask 13
4.2.5 ROI Configuration 14
4.2.6 Zoom/Focus 14
4.3 Alarm Setup 15
4.3.1 Motion Detection 15
4.3.2 Exception Alarm 16
4.3.3 Alarm Server 17
4.4 Analytics Configuration 17
4.4.1 Abandoned/Missing Object Detection 17
4.4.2 Video Exception 19
4.4.3 Line Crossing 20
4.4.4 Region Intrusion 21
4.5 Network Configuration 23
4.5.1 TCP/IP 23
4.5.2 Port 24
4.5.3 Server Configuration 24
4.5.4 Onvif 25
4.5.5 DDNS 25
4.5.6 SNMP 26
4.5.7 802.1x 27
4.5.8 RTSP 27
4.5.9 UPNP 28
4.5.10 RTMP 28
4.5.11 Email 28
4.5.12 FTP 29
4.5.13 HTTPS 29
4.5.14 HTTP POST 30
4.5.15 QoS 31
4.6 Security Configuration 31
4.6.1 User Admin 31
4.6.2 Online User 33
4.6.3 Block and Allow Lists 33
4.6.4 Security Management 33
4.7 Maintenance Configuration 34
4.7.1 Backup and Restore 34
4.7.2 Reboot 35

4.7.3 Upgrade 35
4.7.4 Operation Log 35
5 Search 36
5.1 Image Search 36
5.2 Video Search 38
5.2.1 Local Video Search 38
5.2.2 SD Card Video Search 39
Appendix 42
Appendix 1 Troubleshooting 42

1 Introduction

Welcome

Thank you for purchasing this network camera!
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.

Main Features

- Built-in PoE (Power over Ethernet)
- IP67 rated for outdoor installations
- Remote viewing support via web browser, mobile APP, and CMS/VMS

Applications

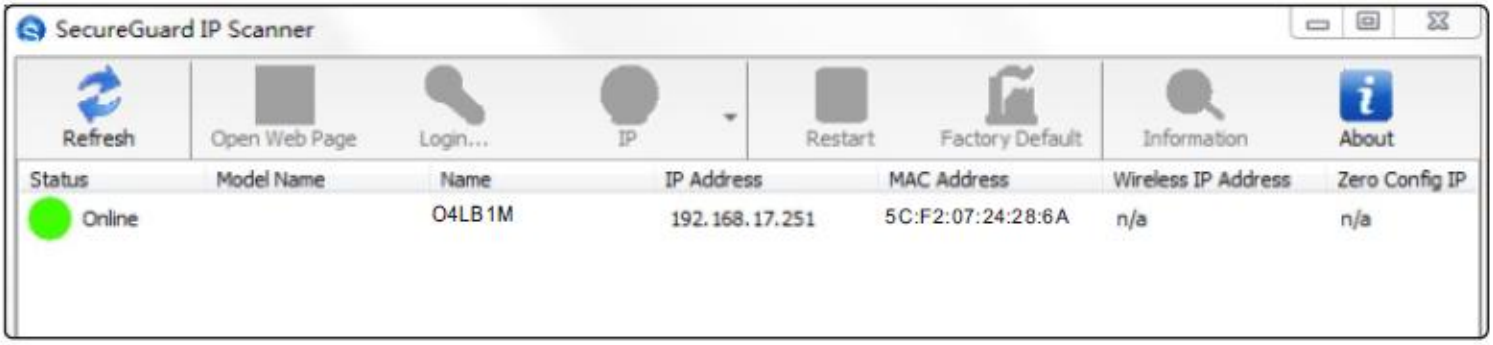
2 Web Access and Login

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:

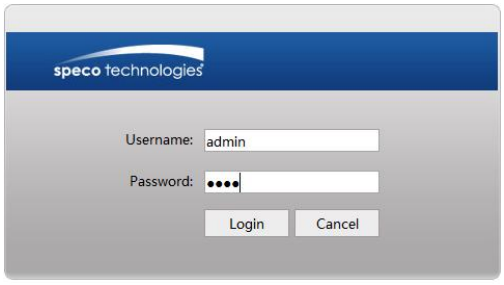
- Access through IP Scanner

Network connection:

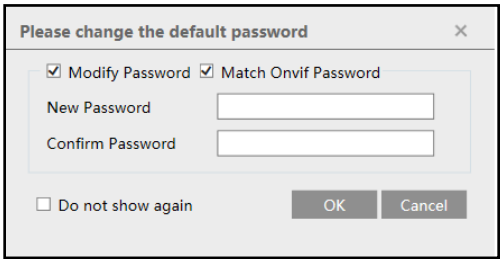
①Make sure the PC and IP-Cam are connected on the same local network. The camera is set to DHCP by default and will be assigned an IP address by the DHCP server. Make sure that the local network has a DHCP server. Routers typically have a DHCP server built in.
② Install IP Scanner from the CD and run it after installation. IP Scanner is the tool for discovering the IP cameras on the local network.



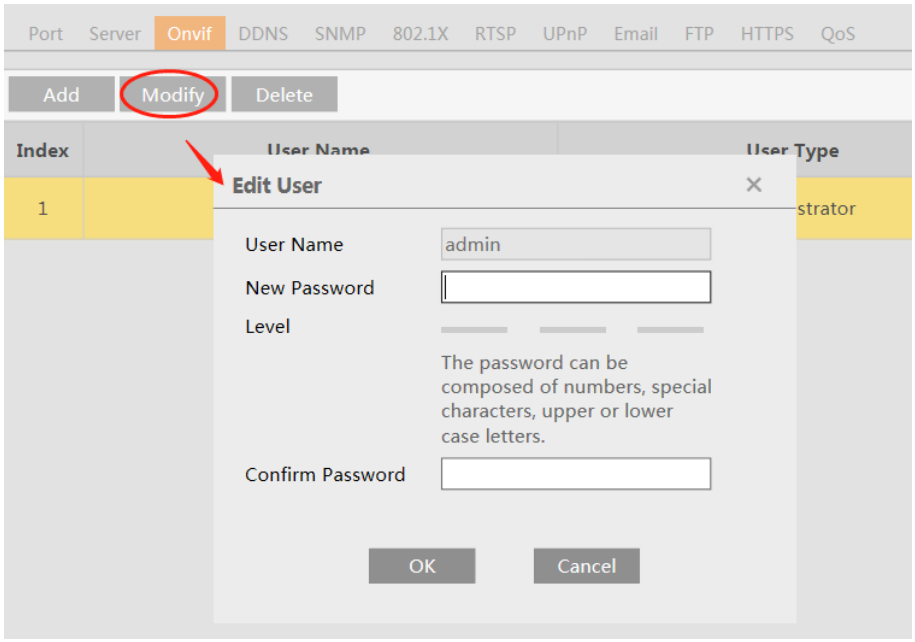
③ In the device list, the IP address, model number, and MAC address of each device will be listed. Select the applicable device and double click to open up the web viewer. You can also manually enter the IP address in the address bar of the web browser. Read the privacy statement and then check and click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



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

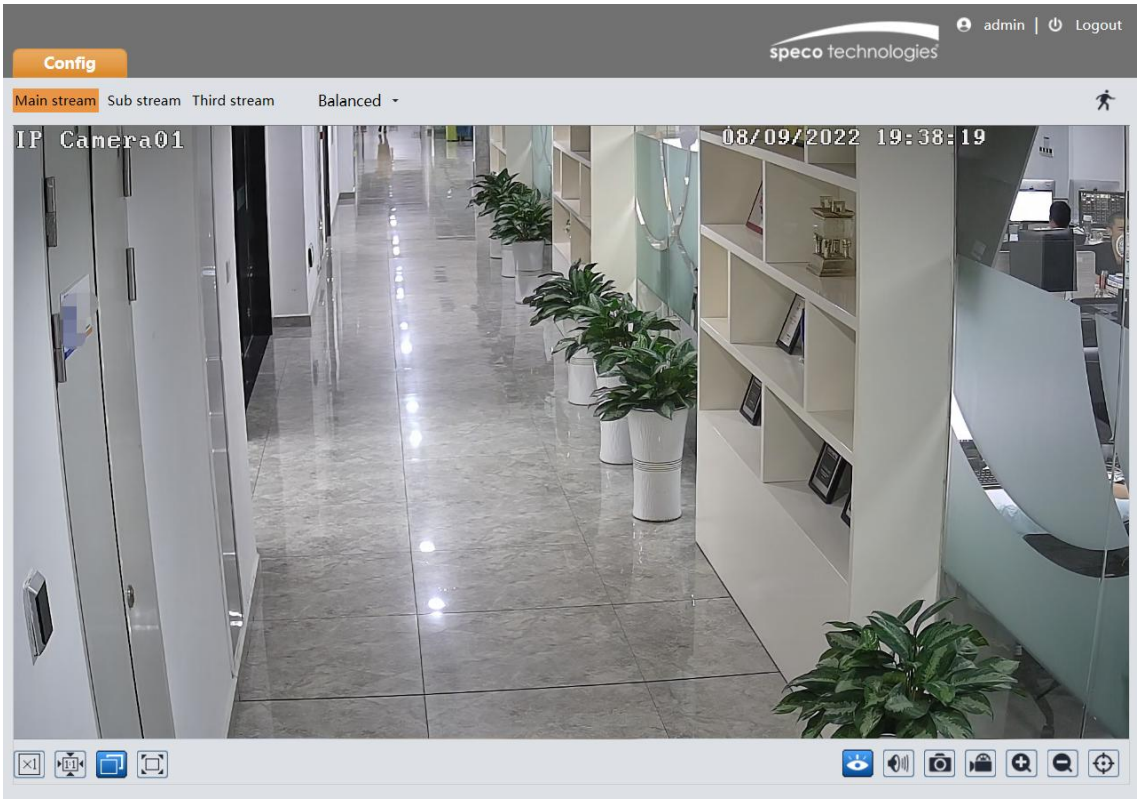


If this is the first time for you to log in, the password prompt may only change the admin password. To change ONVIF password, you either have to check the “Match Onvif Password” box (if available) or go to the the ONVIF section to change the password. (Config→Network→Ports/Connections→Onvif)



3 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		Zoom/Focus control (for motorized models)
	Fit (correct scale)		Rule information display
	Auto (fill the window)		SD card recording indicator
	Full screen (show video only)		Abnormal color indicator
	Start/stop live view		Abnormal clarity indicator
	Enable/disable audio		Scene change indicator
	Snapshot		Line crossing indicator
	Start/stop local recording		Region Intrusion indicator
	Zoom in (for motorized models)		Motion alarm indicator
	Zoom out (for motorized models)		

*Plug-in free live view: local recording is 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.

Click the zoom/focus control button to show the 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 Camera Configuration

Press the “Setup” button to go to the configuration interface.
Note: Wherever applicable, click the “Save” button to save the settings.

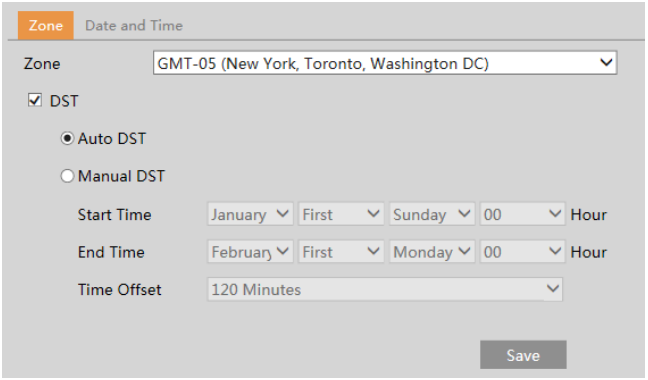
4.1 System Configuration

4.1.1 System Information

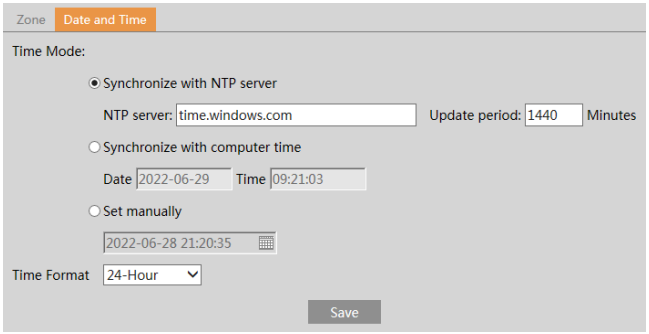
In the “System Information” interface, the system information of the device is listed.

4.1.2 Date and Time

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

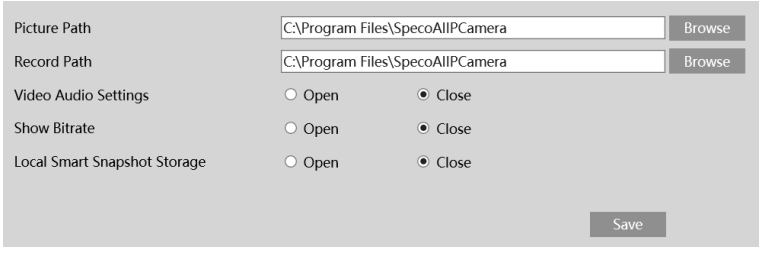


Select the applicable time zone and enable / disable DST as needed.
Click the “Date and Time” tab to set the time, date and time format.



4.1.3 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.

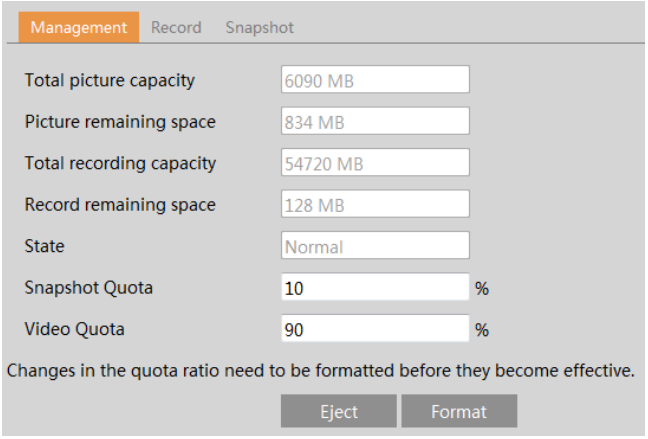


Additionally, the snapshots triggered by smart events (including line crossing detection and region intrusion detection) can be

selected to save to the local PC.

4.1.4 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.**

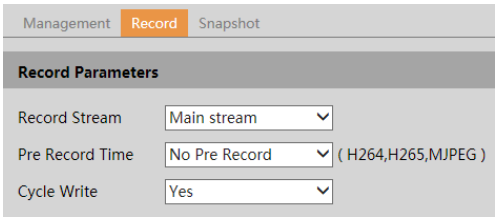
Click the "Eject" button to stop writing data to the SD card. Then the SD card can be ejected safely.

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**

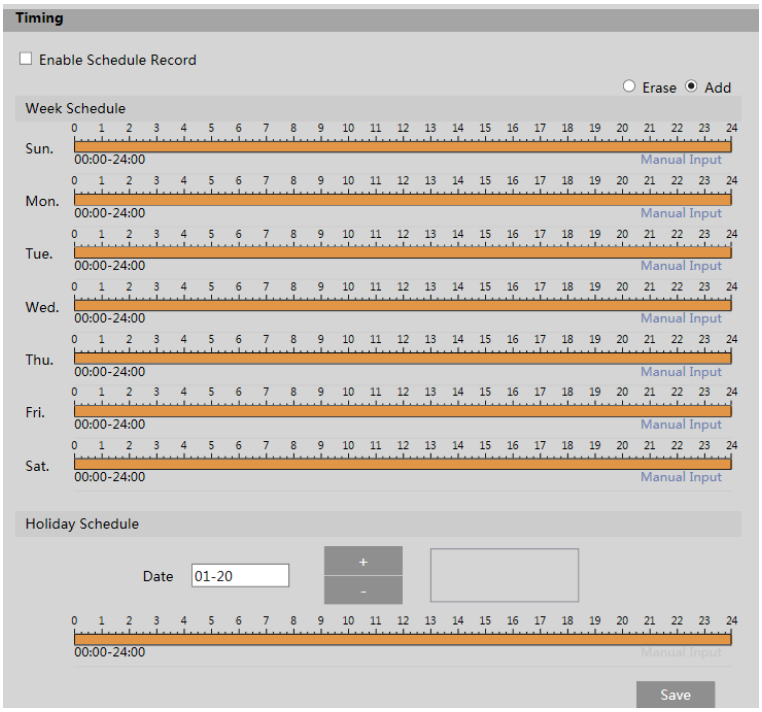
1. Go to Storage→Record to go to the interface as shown below.



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.



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).

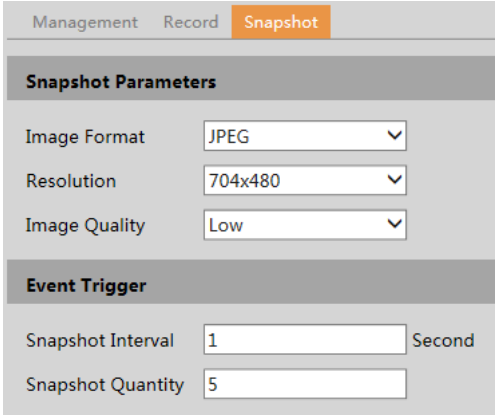
Day schedule

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.



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

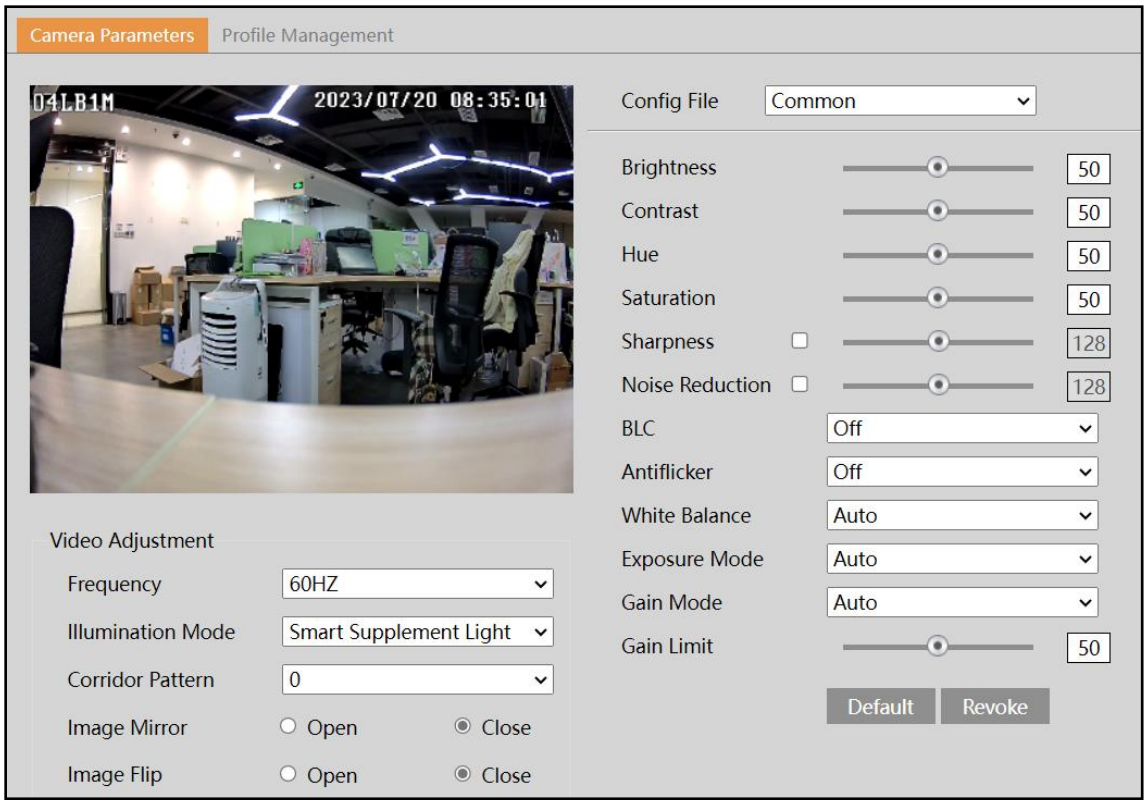
same as the schedule recording (See Schedule Recording).

4.2 Video Configuration

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

4.2.1 Image Configuration

In the Image 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.
Different models may have different menus.



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

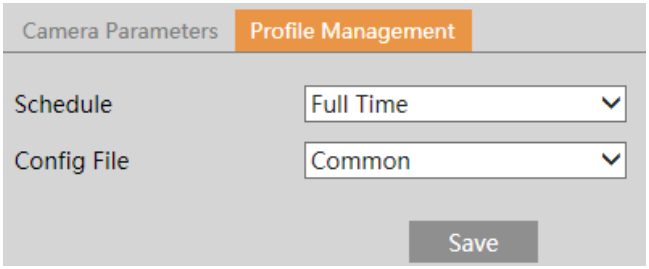
Antiflicker:

- Off: disables the anti-flicker function. This is used mostly in outdoor installations.

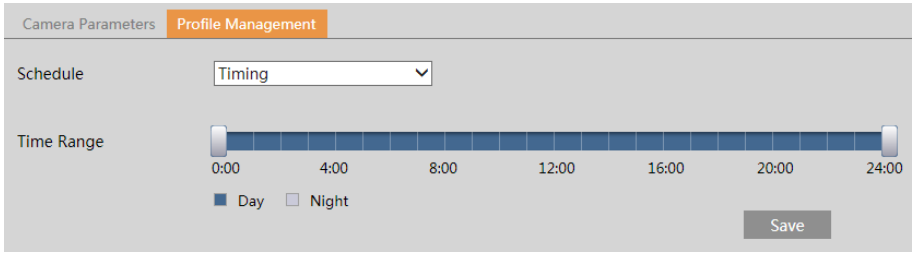
- 50Hz: reduces flicker in 50Hz lighting conditions.
- 60Hz: reduces flicker in 60Hz lighting conditions.

White Balance: Adjust the color temperature according to the environment automatically.
Exposure Mode: Choose “Auto” or “Manual”. If manual is chosen, the digital shutter speed can be adjusted.
Gain Mode: Choose “Auto” or “Manual”. If “Auto” is selected, the gain value will be automatically adjusted (within the set gain limit value) according to the actual situation. If “Manual” is selected, the gain value shall be set manually. The higher the value is, the brighter the image is.
Frequency: 50Hz and 60Hz can be optional.
Corridor Pattern: Corridor viewing modes can be used for situations such as long hallways. 0, 90, 180 and 270 are available. The default value is 0.
Image Mirror: Turn the current video image horizontally.
Image Flip: Turn the current video image vertically.

Illumination Mode: choose “White light”, “Infrared light” or “Smart supplement light” as needed.
If “White light” is selected, “White Light Mode” and “Overexposure Control” can be configured.
White Light Mode: Choose “Off”, “Auto” or “Manual”. Please select it as needed.
Overexposure Control: Choose “OFF”, “Low”, “Mid” or “High”. This function can automatically adjust the exposure parameter according to the actual effect of the image, effectively avoiding detail missing caused by image overexposure, so that the image will be more vivid. Please set it as needed.
If “Infrared light” is selected, “Smart IR” and “Day/Night Mode” can be configured.
Smart IR: Choose “ON” or “OFF”. This function can effectively avoid image overexposure so as to make the image more realistic. The higher the level is, the more overexposure compensation will be given.
Day/Night Mode: Choose “Auto”, “Day”, “Night” or “Timing”.
Smart supplement light: If selected, in low ambient light, the system will automatically turn on the invisible infrared light. Once there are people appearing in the detection area, it will automatically switch to full-brightness visible white light. When people are no longer detected, it will resume to Infrared light.
Schedule Settings of Image Parameters:
Click the “Profile Management” tab as shown below.



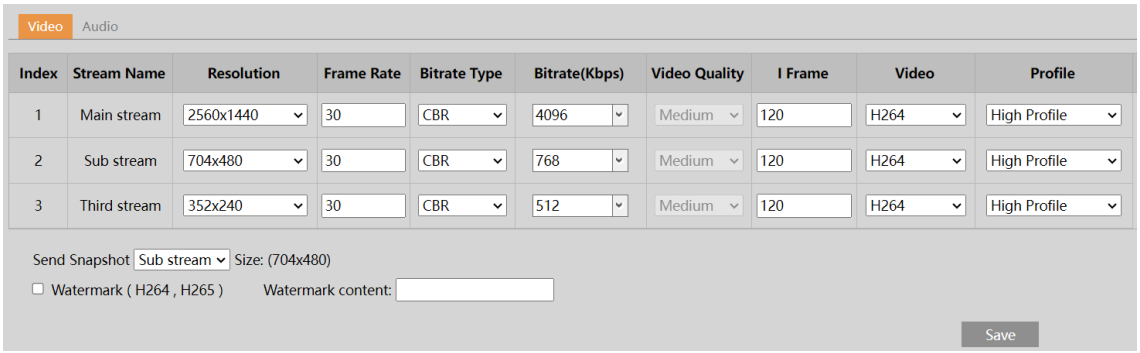
Set full time schedule for common, day or night mode and specified time schedule for day and night. Choose “Timing” in the drop-down box of schedule as shown below.



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.

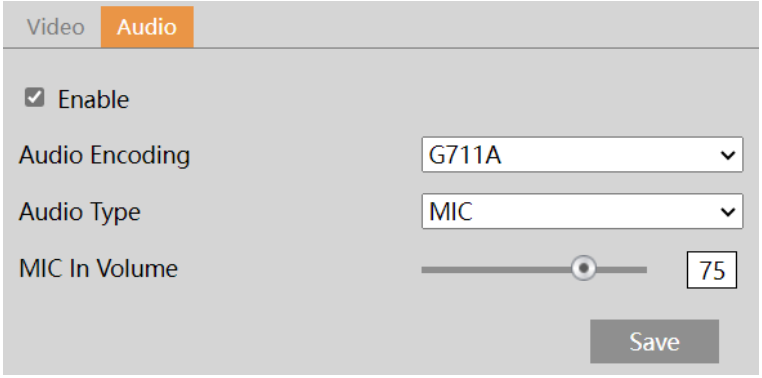
4.2.2 Video / Audio Configuration

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.



Three video streams can be adjustable.
Resolution: The size of image.
Frame rate: The higher the frame rate, the video is smoother.
Bitrate type: CBR and VBR are optional. Bitrate is related to image quality. CBR means that no matter how much change is seen in the video scene, the compression bitrate will be kept constant. VBR means that the compression bitrate will be adjusted according to scene changes. For example, for scenes that do not have much movement, the bitrate will be kept at a lower value. This can help optimize the network bandwidth usage.
Bitrate: it can be adjusted when the mode is set to CBR. The higher the bitrate, the better the image quality will be.
Video Quality: It can be adjusted when the mode is set to VBR. The higher the image quality, the more bitrate will be required.
I Frame interval: It determines how many frames are allowed between a "group of pictures". When a new scene begins in a video, until that scene ends, the entire group of frames (or pictures) can be considered as a group of pictures. If there is not much movement in the scene, setting the value higher than the frame rate is fine, potentially resulting in less bandwidth usage. However, if the value is set too high, and there is a high frequency of movement in the video, there is a risk of frame skipping.
Video Compression: H264 or H265 can be optional. MJPEG is not available for main stream. If H.265 is chosen, make sure the client system is able to decode H.265. 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. Some models may support MIC type.

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)

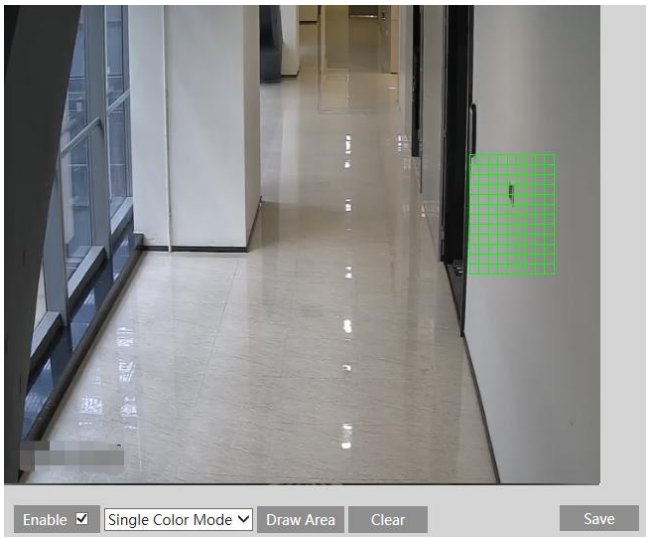
4.2.3 OSD Configuration

Go to 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.

4.2.4 Video Mask

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

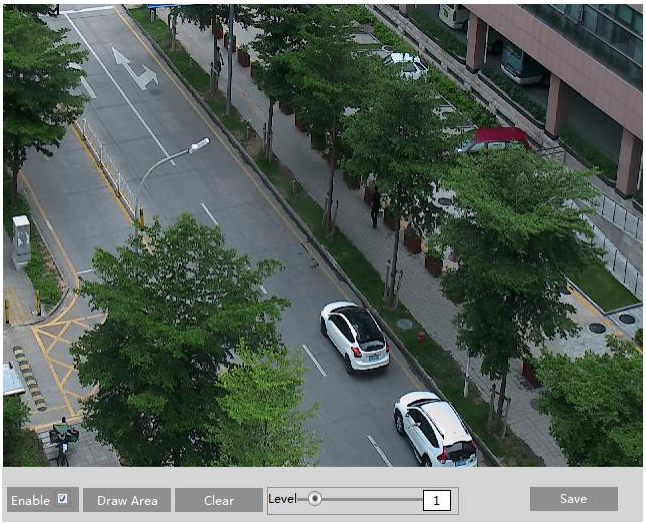


To set up video mask:
1. Enable video mask.
2. Click the “Draw Area” button and then drag the mouse to draw the video mask area.
3. Click the “Save” button to save the settings.
4. Return to the live to verify that the area have been drawn as shown as blocked out in the image.

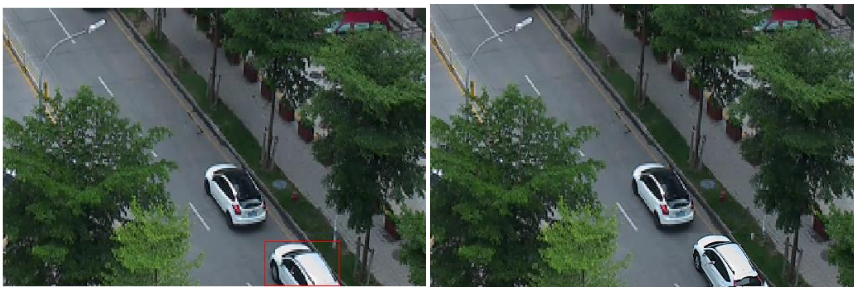
To clear the video mask:
Click the “Clear” button to delete the current video mask area.

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.

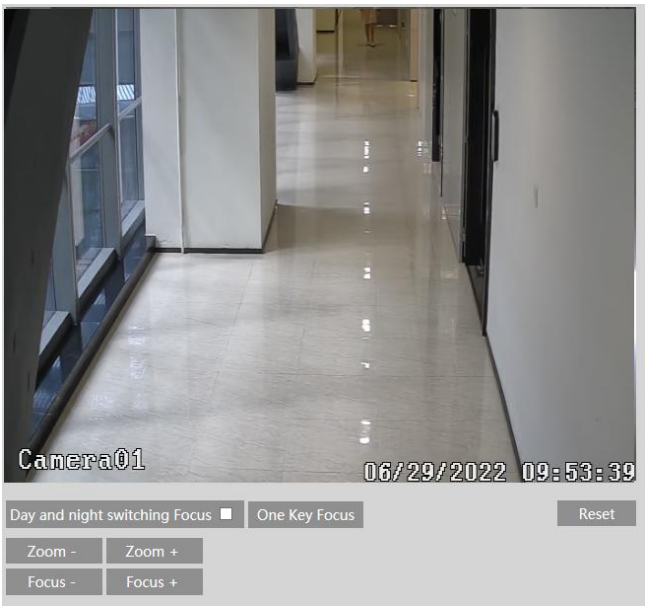


1. Check “Enable” and then click the “Draw Area” button.
2. Drag the mouse to set the ROI area.
3. Set the level.
4. Click the “Save” button to save the settings.



4.2.6 Zoom/Focus

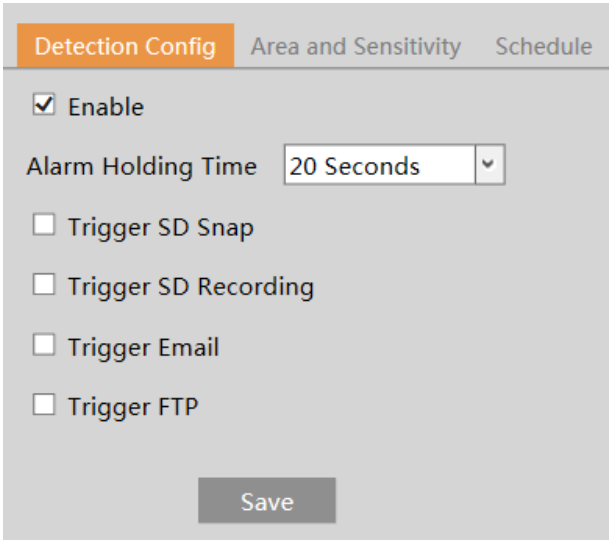
This function is only available for the model with motorized zoom lens. Within this section, zoom and focus can be controlled. If the image is out of focus after a manual adjustment, one key focus can be used to set the focus automatically.



4.3 Alarm Setup

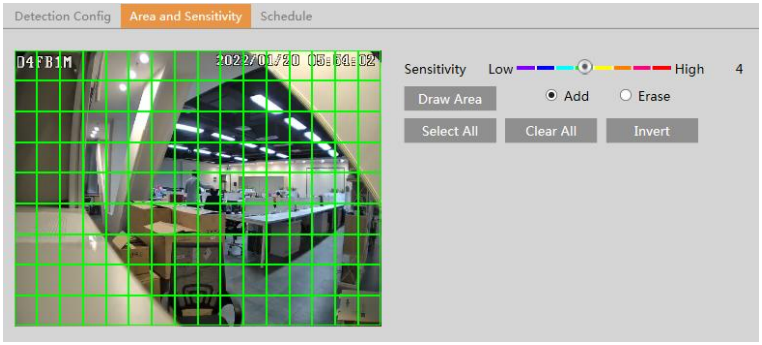
4.3.1 Motion Detection

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



1. Check “Enable” check box to activate motion-based alarms. If unchecked, the camera will not send out any signals to trigger motion-based recording to the NVR or CMS, even if there is motion in the video.
Alarm Holding Time: it refers to the interval time between the adjacent motion detections. For instance, if the alarm holding time is set to 20 seconds, once the camera detects a motion, it will go to alarm and would not detect any other motion in 20 seconds. If there is another motion detected during this period, it will be considered as continuous movement; otherwise it will be considered as a single motion.
Trigger SD Snap: If selected, the system will capture images on motion detection and save the images on an SD card.
Trigger SD Recording: If selected, video will be recorded on an SD card on motion detection.
Trigger Email: If “Trigger Email” and “Attach Picture” are checked (email address must be set first in the Email configuration interface), the captured pictures and triggered event will be sent into those addresses.
Trigger FTP: If “Trigger FTP” and “Attach Picture” are checked, the captured pictures will be sent into FTP server address. Please refer to FTP configuration chapter for more details.

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



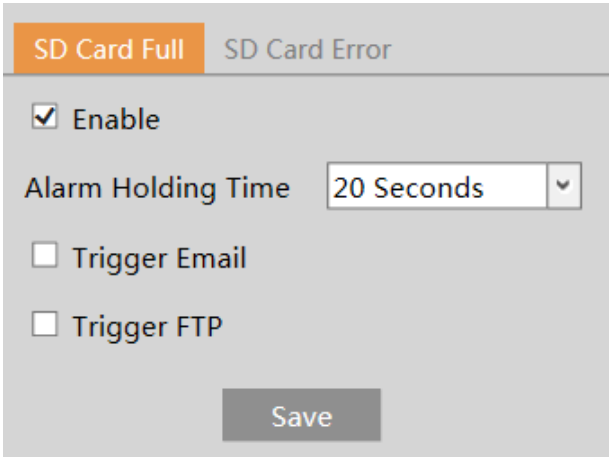
Move the “Sensitivity” scroll bar to set the sensitivity. Higher sensitivity value means that motion will be triggered more easily. Select “Add” and click “Draw”. Drag the mouse to draw the motion detection area; Select “Erase” and drag the mouse to clear motion detection area.
After that, click the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

4.3.2 Exception Alarm

- **SD Card Full**

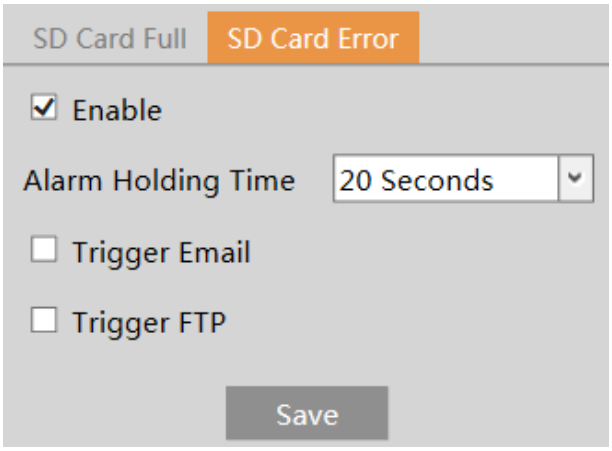
1. Go to Alarm→Exception Alarm→SD Card Full.



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**

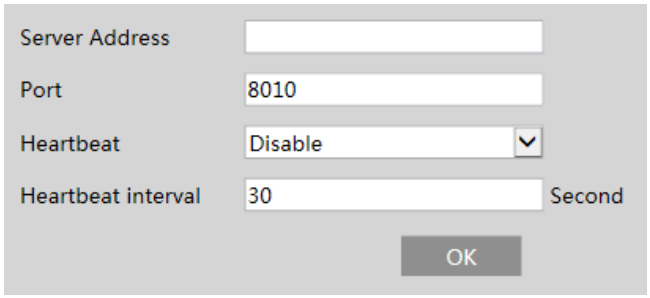
When there are some errors in writing SD card, the corresponding alarms will be triggered.
1. Go to Alarm→Anomaly→SD Card Error as shown below.



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 detectionchapter 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.



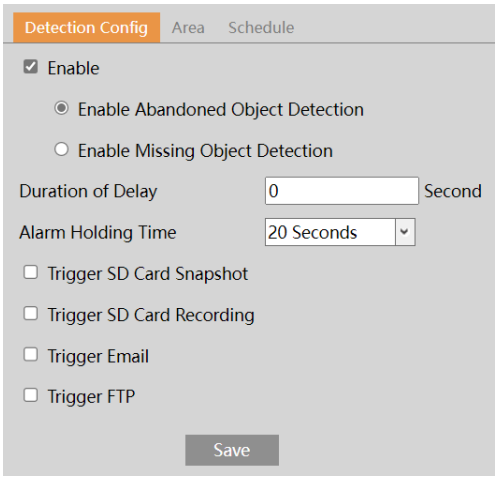
4.4 Analytics Configuration

This series of IP cameras 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.

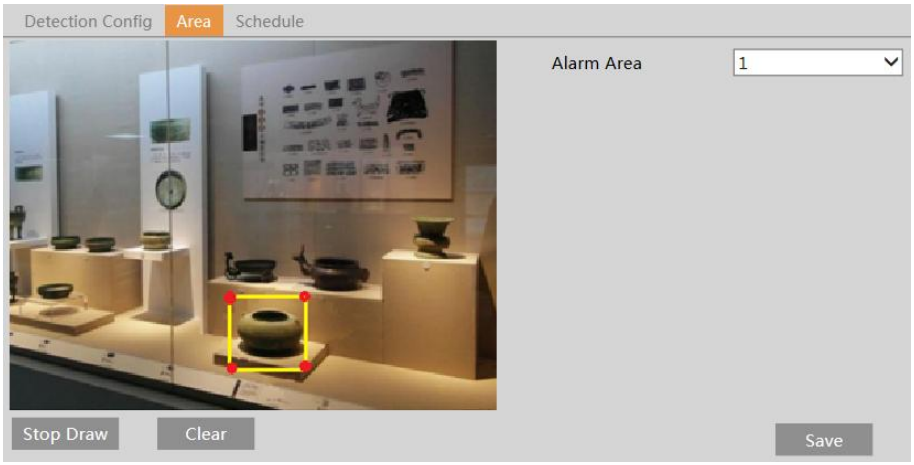
4.4.1 Abandoned/Missing Object Detection

Alarms will be triggered when the objects are removed from or left at the pre-defined area.
To set object removal detection:
Go to Config→Event→Object Abandoned/Missing interface as shown below.



1. Enable object removal 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.
Duration of Delay: it is the alarm delay time of the object left in the region (ranging from 10~3600s) or the alarm delay time of the object removed from the region (ranging from 3~3600s). For example, if "Enable Abandoned Object Detection" is selected and the duration of delay is set as 10, alarms will be triggered after the object is left and stay in the region for 10s, but when someone takes away the object within 10s, alarms will not be triggered.

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 alarm area of the object removal detection. Click the "Area" tab to go to the interface as shown below.



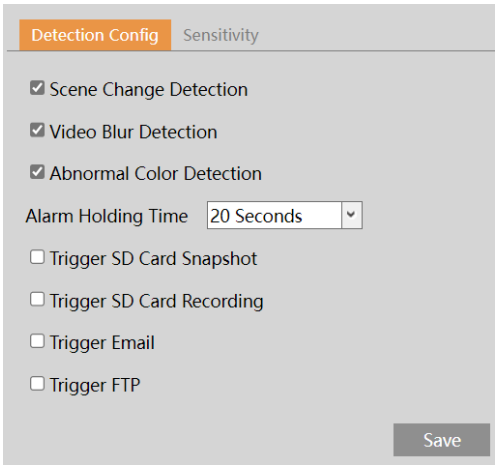
Set the alarm area number and then enter the desired alarm area name. Only one alarm area can be added. Click the "Draw Area" button and then click around the area where you want to set as the alarm area in the image (the alarm area should be a closed area). Click the "Stop Draw" button to stop drawing. Click the "Clear" button to delete the alarm area. Click the "Save" button to save the settings.
5. Set the schedule. 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.

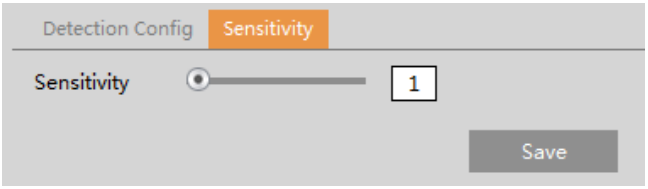
5. Abandoned/missing object detection cannot determine the objects' ownership. For instance, there is an unattended package in the station. Abandoned object detection can detect the package itself but it cannot determine to whom it belongs to.
6. Try not to enable object removal detection when light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

4.4.2 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.



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.

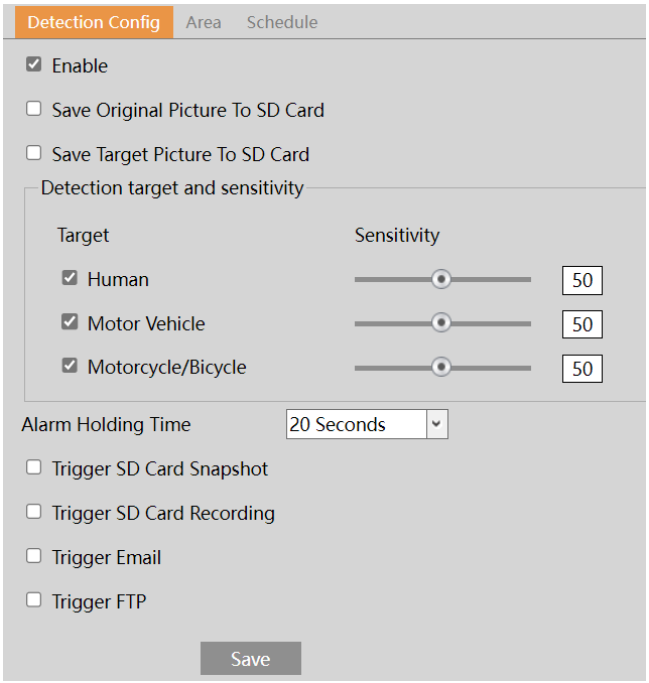


Drag the slider to set the sensitivity value or directly enter the sensitivity value in the textbox. Click "Save" button to save the settings.
The sensitivity value of Scene Change Detection: The higher the value is, the more sensitive the system responds to the amplitude of the scene change.
The sensitivity 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.

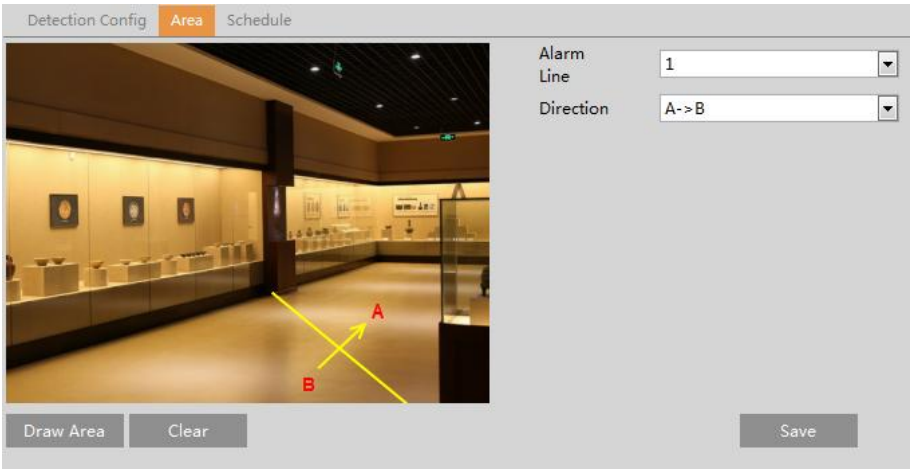
※**The requirements of camera and surrounding area**
1. Auto-focusing function should not be enabled for exception detection.
2. Try not to enable exception detection when light changes greatly in the scene.

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 the targets cross the alarm line.
Save Target Picture to SD Card: If it is enabled, the detected target cutout pictures will be captured and saved to the SD card when the targets cross the alarm line.
Note: To save snapshots to the local PC, please enable "Local Smart Snapshot Storage" in the local config interface first. To save snapshots to the SD card, please install an SD card first.
Detection Target:
Human: Select it and then alarms will be triggered if someone crosses the pre-defined alarm lines.
Motor Vehicle: Select it and then alarms will be triggered if a vehicle with four or more wheels (eg. a car, bus or truck) crosses the pre-defined alarm lines.
Motorcycle/Bicycle: Select it and then alarms will be triggered if a vehicle with two wheels (eg. a motorcycle or bicycle) crosses the pre-defined alarm lines.
All of the three types of objects can be selected simultaneously. Please select the detection objects as needed. If no object/target is selected, alarms will not be triggered even if line crossing detection is enabled.
2. Set the alarm holding time.
3. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection section for details.
4. Click "Save" button to save the settings.
5. Set area and sensitivity of the line crossing alarm. Click the "Area" tab to go to the interface as shown below.

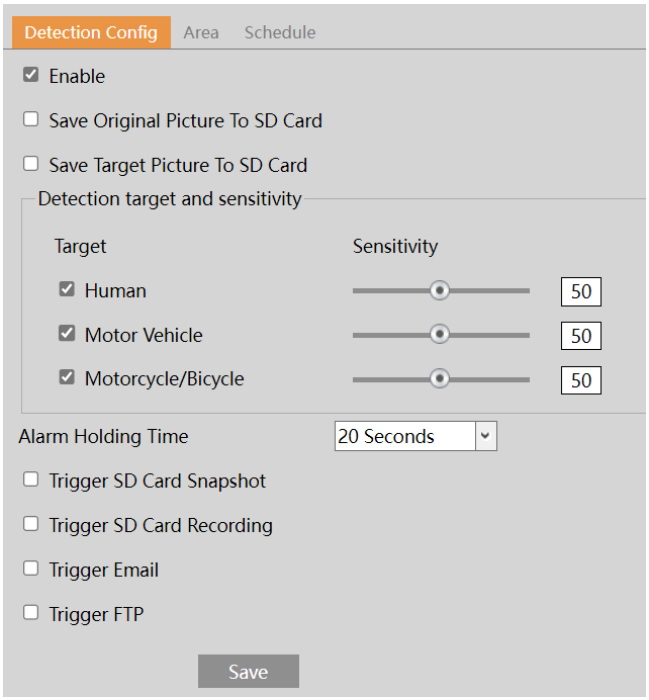


Set the alarm line number and direction. Up to 4 lines can be added. Multiple lines cannot be added simultaneously.
Direction： A<->B, A->B and A<-B optional. This indicates the direction of the intruder who crosses over the alarm line that would trigger the alarm.
A<->B: The alarm will be triggered when 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).

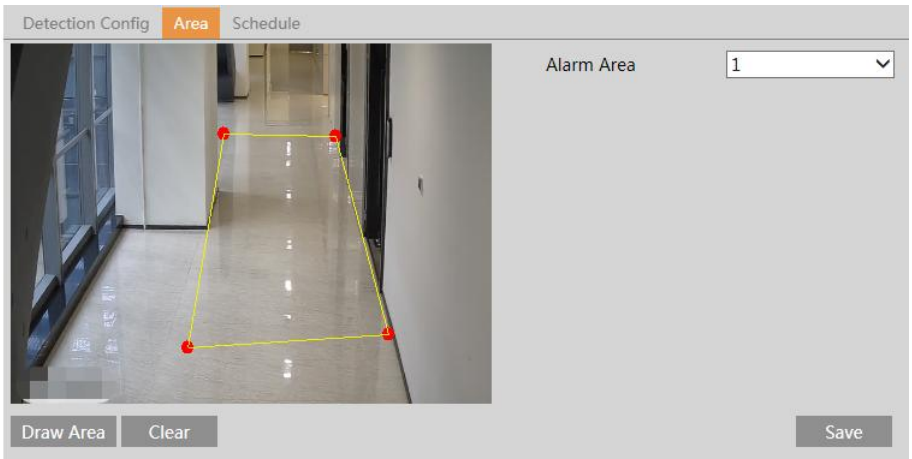
※**Configuration of camera and surrounding area**
1. Auto-focusing function should not be enabled for line crossing detection.
2. Avoid the scenes with many trees or the scenes with various light changes (like many flashing headlights). The ambient brightness of the scenes shouldn't be too low.
3. Cameras 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 region intrusion detection and select the snapshot type and the detection target.
Save Original Picture to SD Card: If it is enabled, the detected original pictures will be captured and saved to the SD card when targets intrude into the pre-defined areas.
Save Target Picture to SD Card: If it is enabled, the detected target cutout pictures will be captured and saved to the SD card when targets intrude into the pre-defined areas.
Note: To save snapshots to the local PC, please enable "Local Smart Snapshot Storage" in the local config interface first. To save snapshots to the SD card, please install an SD card first.
Detection Target:
Human: Select it and then alarms will be triggered if someone intrudes into the pre-defined area.
Motor Vehicle: Select it and then alarms will be triggered if a vehicle with four or more wheels (eg. a car, bus or truck) intrudes into the pre-defined area.
Motorcycle/Bicycle: Select it and then alarms will be triggered if a vehicle with two wheels (eg. a motorcycle or bicycle) intrudes into the pre-defined area.
All of the three types of objects can be selected simultaneously. Please select the detection objects as needed. If no object/target is selected, alarms will not be triggered even if intrusion detection is enabled.
2. Set the alarm holding time.
3. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection chapter for details.
4. Click "Save" button to save the settings.
5. Set the alarm area of the intrusion detection. Click the "Area" tab to go to the interface as shown below.



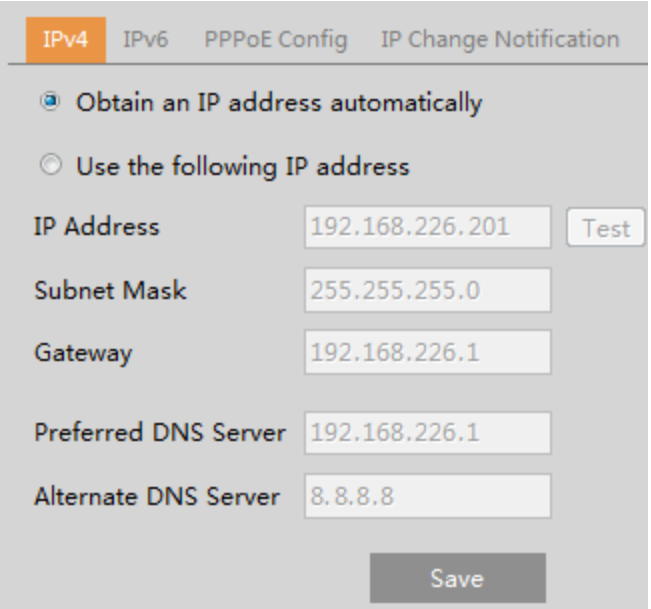
Set the alarm area number on the right side. Up to 4 alarm areas can be added.
Click the “Draw Area” button and then click around the area where you want to set as the alarm area in the image on the left side (the alarm area should be a closed area). Click the “Stop Draw” button to stop drawing. Click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

※**Configuration requirements of camera and surrounding area**
1. Auto-focusing function should not be enabled for region intrusion detection.
2. Avoid the scenes with many trees or the scenes with various light changes (like many flashing headlights). The ambient brightness of the scenes shouldn’t be too low.
3. Cameras should be mounted at a height of 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.

4.5 Network Configuration

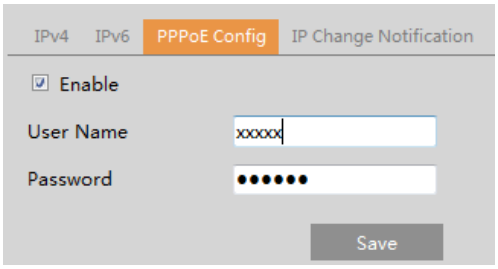
4.5.1 TCP/IP

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

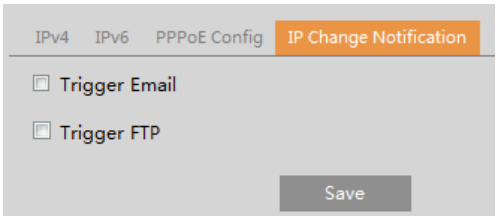


Use IP address (take IPv4 for example)-obtain a local IP address automatically through DHCP. A typical router has a DHCP server built in, and therefore is able to assign an IP address to the camera.

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



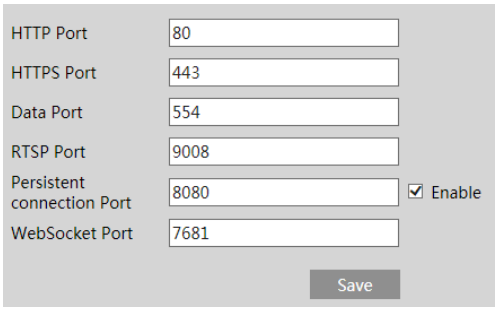
Either method of network connection can be used. If PPPoE is used to connect internet, the camera will get a dynamic WAN IP address. This IP address will change frequently. To be notified, the IP change notification function can be used.
Click “IP Change Notification Config” to go to the interface as shown below.



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

4.5.2 Port

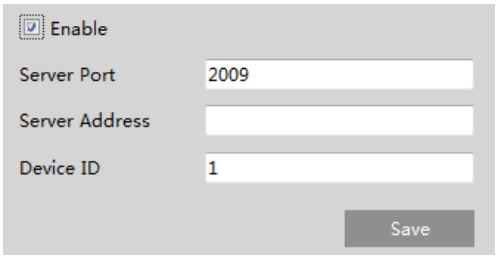
Go to Network→Ports/Connections as shown below. HTTP port, Data port and RTSP port can be set.



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

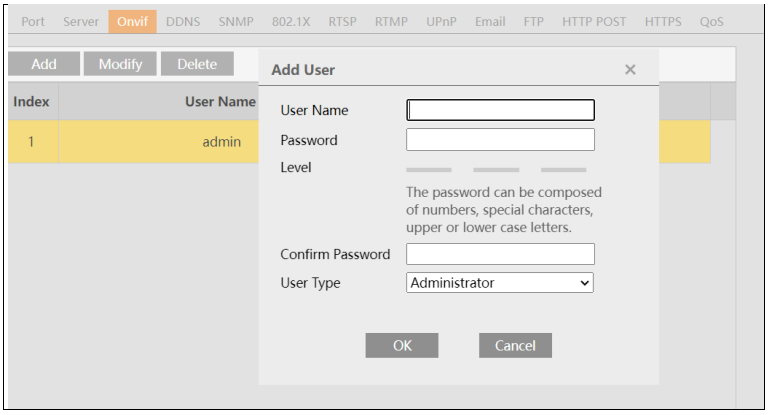
This function is mainly used for connecting network video management system.



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

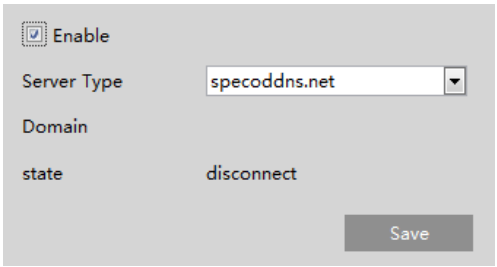
The camera can be searched and connected to the third-party platform via ONVIF/RTSP protocol.



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 camera is set up with a DHCP connection, DDNS should be set for accessing the camera from the internet.
1. Go to Network→ Ports/Connections→DDNS.

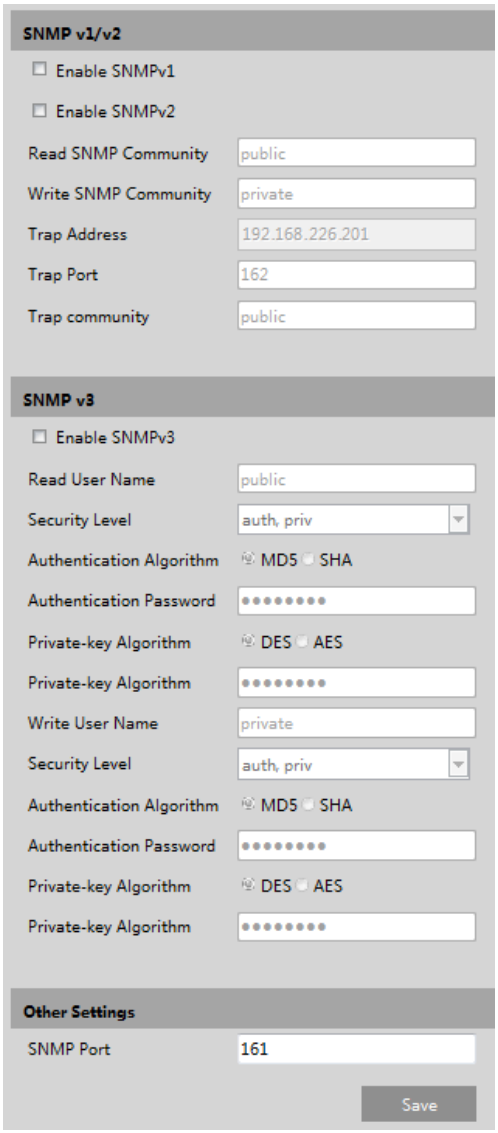


2. Enable, save and use DDNS to log in.

4.5.6 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 Network→ Ports/Connections→SNMP.

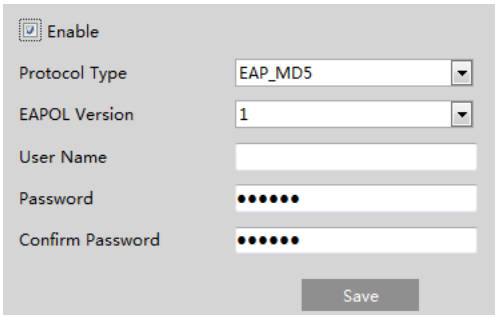


2. Check the corresponding version checkbox (Enable SNMPv1, Enable SNMPv2, Enable SNMPv3) according to the version of the SNMP software that will be used.

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

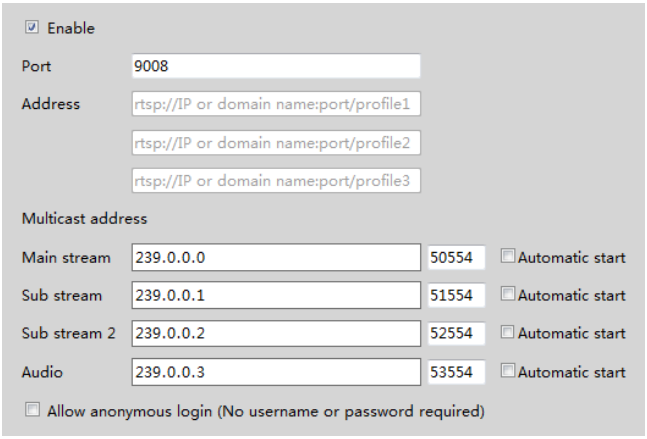
If it is enabled, the camera's data can be protected. When the camera is connected to the network protected by the IEE802.1x, user authentication is needed.



To use this function, the camera shall be connected to a switch supporting 802.1x protocol. The switch can be reckoned as an authentication system to identify the device in a local network. If the camera connected to the network interface of the switch has passed the authentication of the switch, it can be accessed via the local network.
Protocol type and EAPOL version: Please use the default settings.
User name and password: The user name and password must be the same with the user name and password applied for and registered in the authentication server.

4.5.8 RTSP

Go to Network→ Ports/Connections→RTSP.



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.

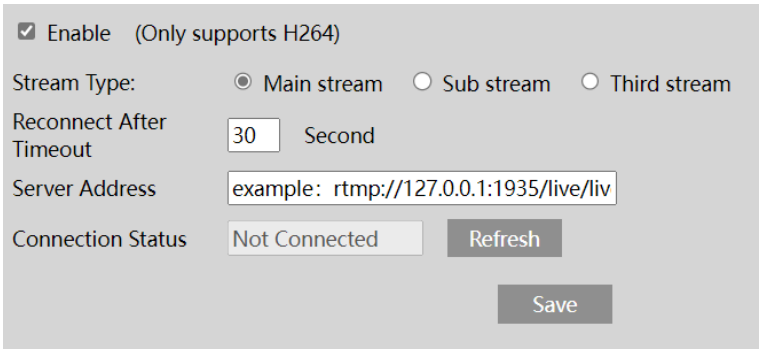
Multicast Address
Main stream: The address format is
"rtsp://IP address: rtsp port/profile1?transportmode=mcast".
Sub stream: The address format is
"rtsp://IP address: rtsp port/profile2?transportmode=mcast".
Third stream: The address format is
"rtsp://IP address: rtsp port/profile3?transportmode=mcast".
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 UPNP

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

4.5.10 RTMP

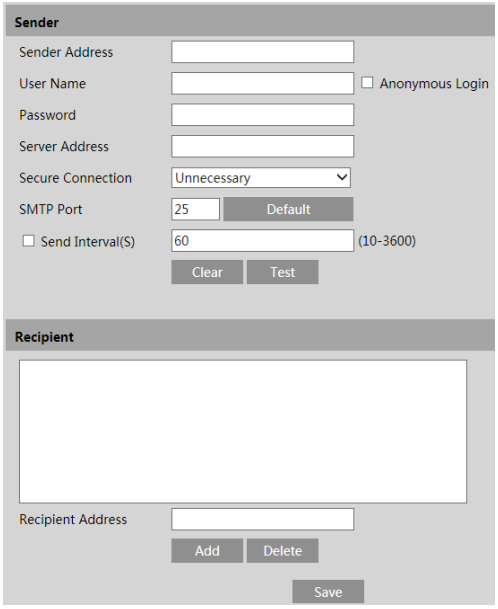
You can access the third-party (like YouTube) to realize video live view through RTMP protocol.
Go to Config→ Network→ Ports/Connections→RTMP.



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.

4.5.11 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.

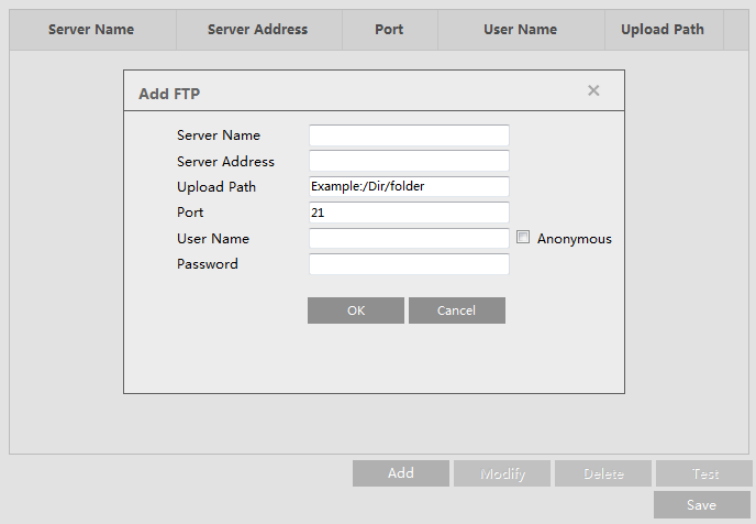


Sender Address: sender's e-mail address.
User name and password: sender's user name and password (you don't have to enter the username and password if "Anonymous

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

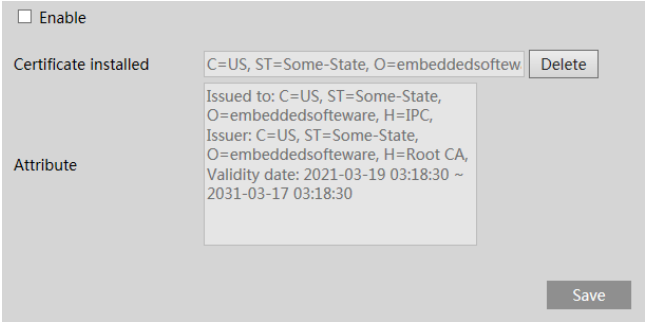
After an FTP server is set up, captured pictures from events will be uploaded to the FTP server.
Go to Network→ Ports/Connections→FTP.



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

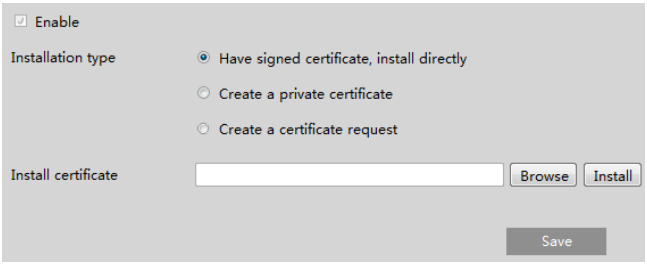
4.5.13 HTTPS

HTTPs provides authentication of the web site and protects user privacy.
Go to Network→ Ports/Connections→HTTPS as shown below.

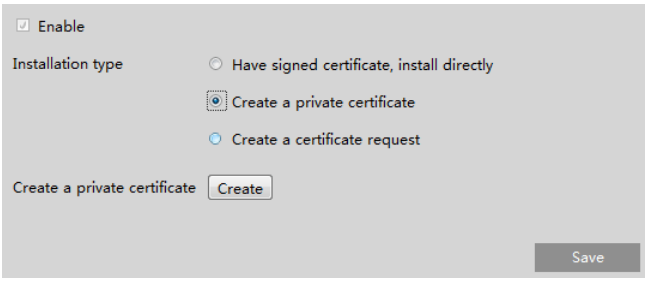


There is a certificate installed by default as shown above. Enable this function and save it. Then the camera can be accessed by

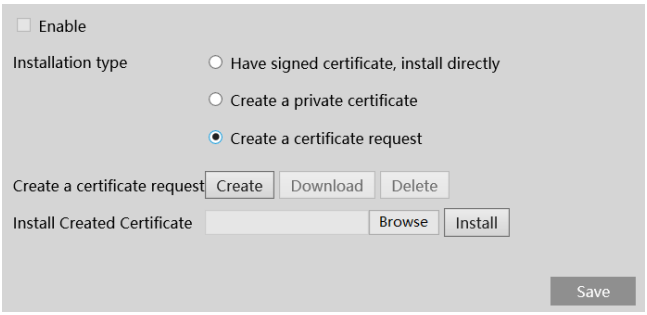
entering https://IP: https port via the web browser (eg. https://192.168.226.201:443).
A private certificate can be created if users don't want to use the default one. Click "Delete" to cancel the default certificate. Then the following interface will be displayed.



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



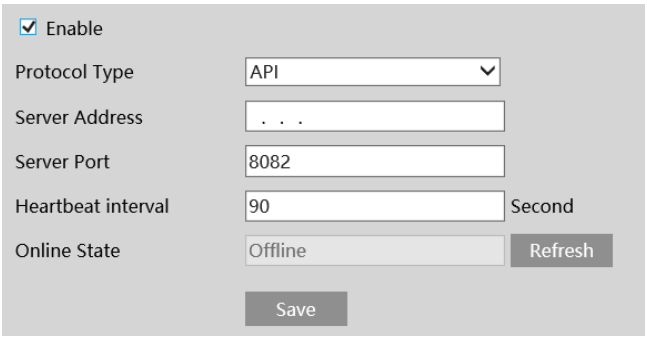
Click the "Create" button to create a private certificate. Enter the country (only two letters available), domain (camera's IP address/domain), validity date, password, province/state, region and so on. Then click "OK" to save the settings.
* Click "Create a certificate request" to enter the following interface.



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

4.5.14 HTTP POST

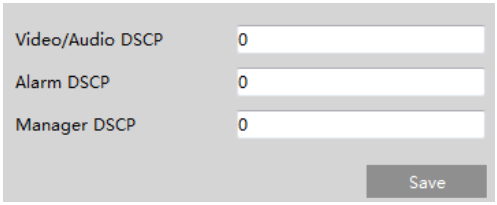
Go to Config→Network→Ports/Connections→HTTP POST interface.
Check "Enable", select protocol type and then set the server address (IP address/domain name), server port and heartbeat interval.



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

4.5.15 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.

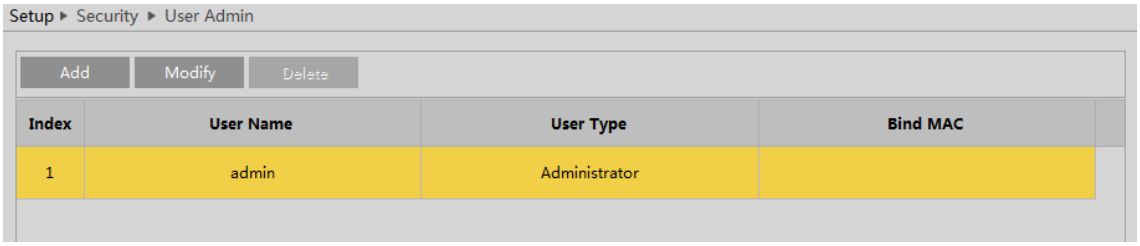


Video/Audio DSCP: The range is from 0 to 63.
Alarm DSCP: The range is from 0 to 63.
Manager DSCP: The range is from 0 to 63.
Generally speaking, the larger the number is, the higher the priority is.

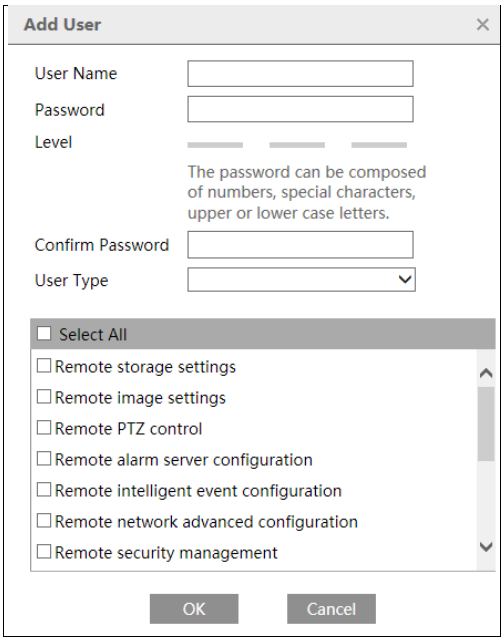
4.6 Security Configuration

4.6.1 User Admin

Go to Security→User Admin interface as shown below.



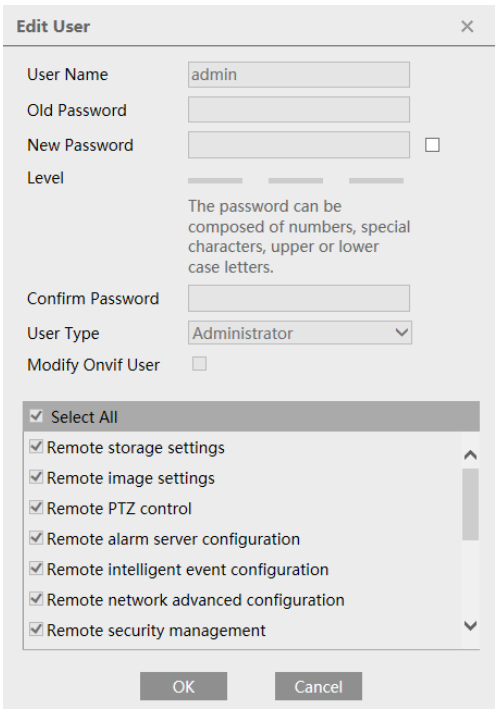
Add user:
1. Click “Add” to pop up the following textbox.



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.

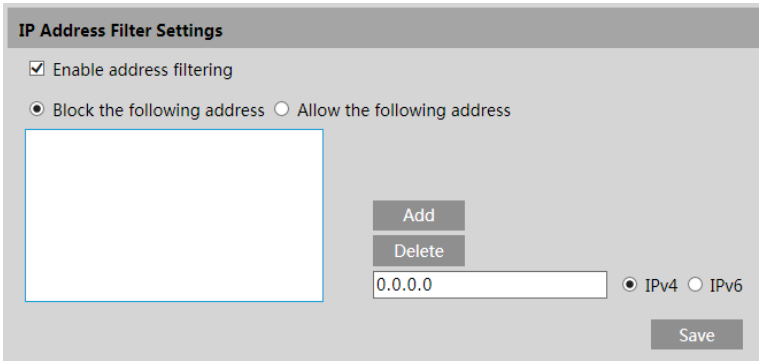
4.6.2 Online User

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

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

4.6.3 Block and Allow Lists

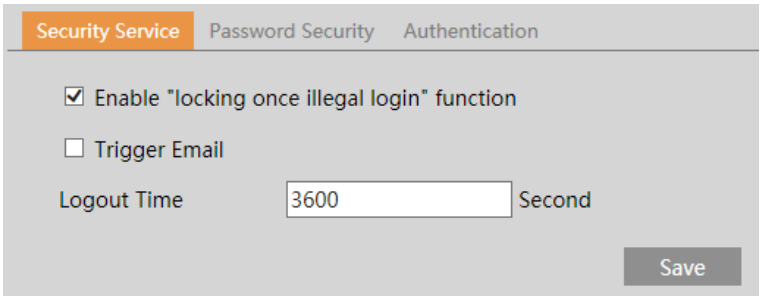
Go to Security→Block and Allow Lists as shown below.



The 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.



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 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.
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.

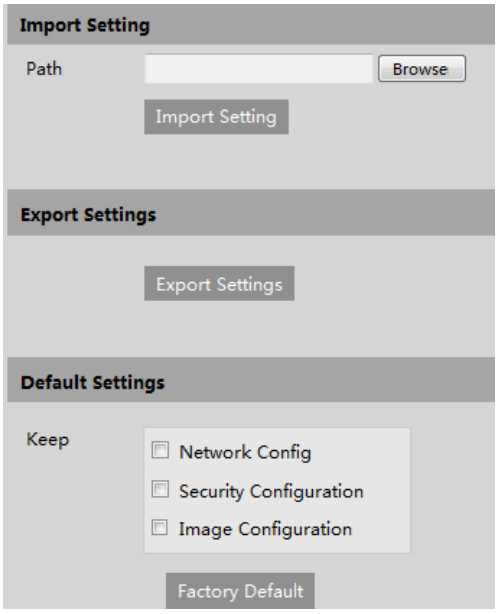
- **Password Security**

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.



- **Import & Export Settings**

Configuration settings of the camera can be exported form a camera into another camera.
1. Click “Browse” to select the save path for import or export information on the PC.
2. Click the “Import Setting” or “Export Setting” button.

- **Default Settings**

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

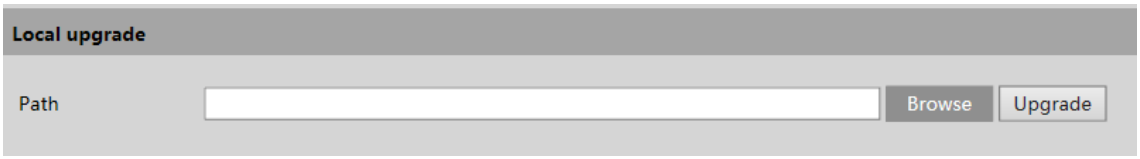
4.7.2 Reboot

Go to Maintenance→Reboot.
Click the “Reboot” button to reboot the device.

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

4.7.3 Upgrade

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

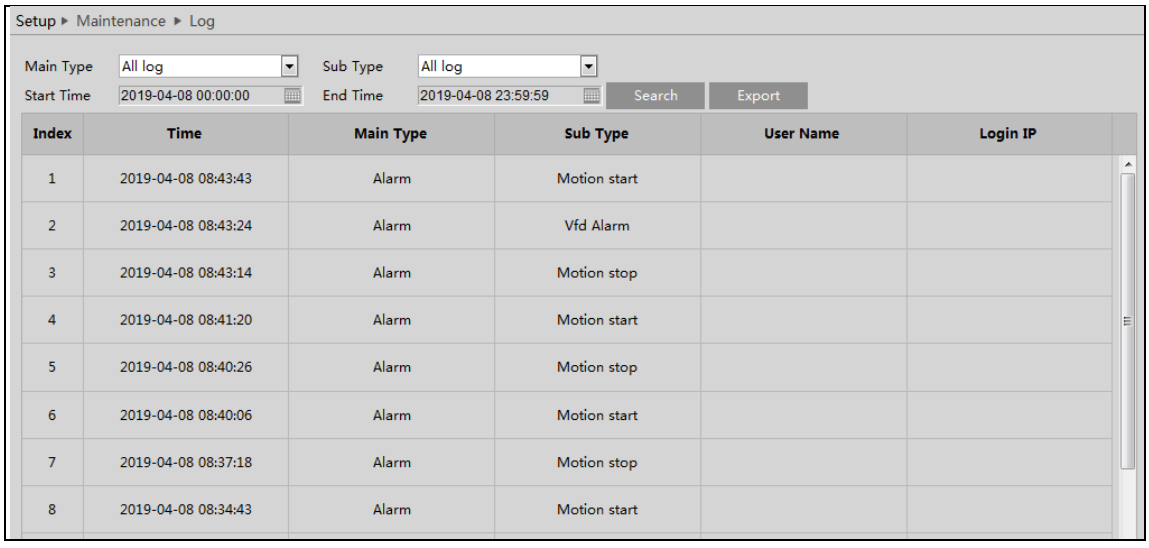


1. Click the “Browse” button to select the save path of the upgrade file
2. Click the “Upgrade” button to start upgrading the firmware.
3. The device will restart automatically

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

4.7.4 Operation Log

To query and export log:
1. Go to Maintenance→Operation Log.

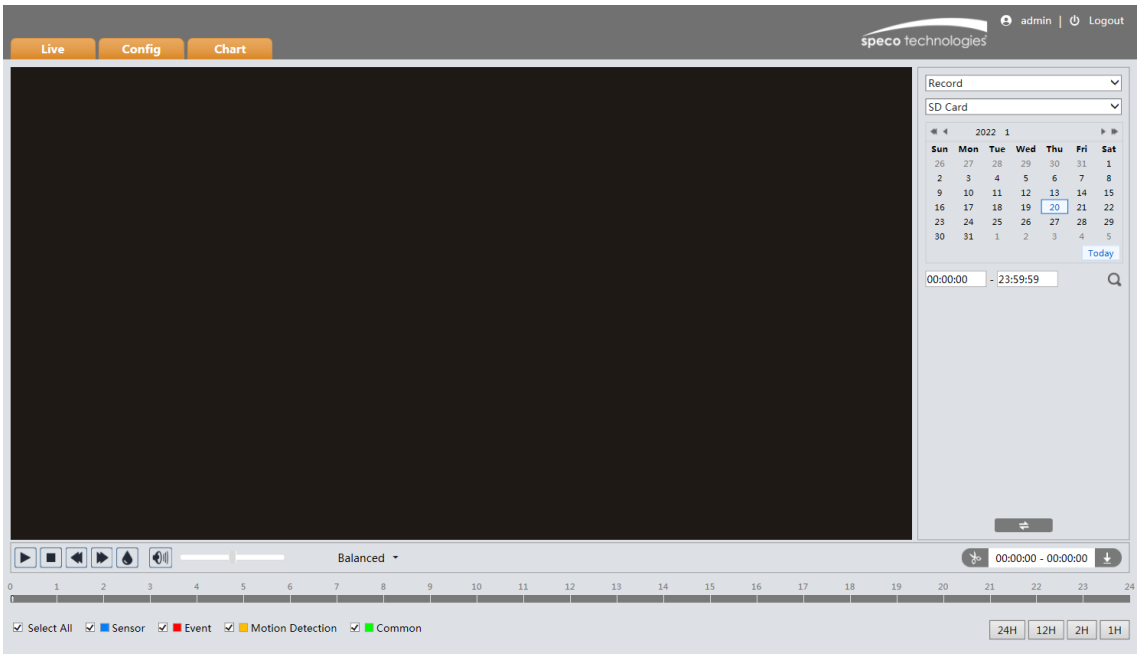


2. Select the main type, sub type, start and end time.
3. Click “Search” to view the operation log.
4. Click “Export” to export the operation log.

5 Search

5.1 Image Search

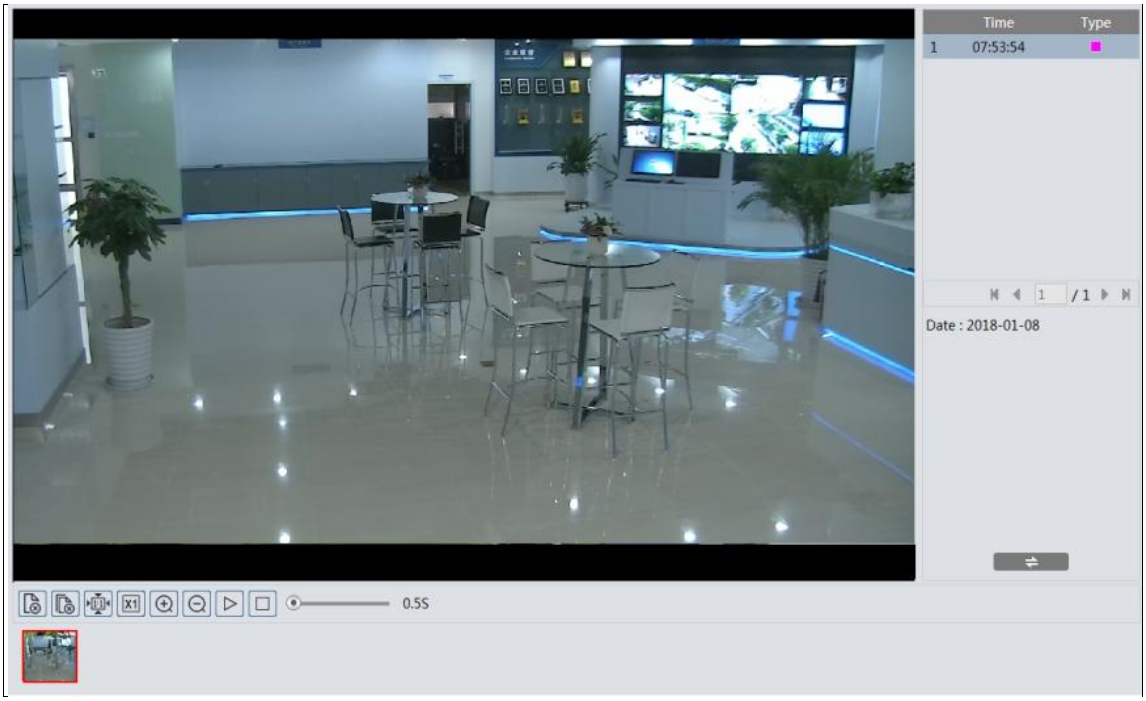
In the Setup interface, click Search to go to the interface as shown below. Images that are saved on the PC or SD card can be found here.



- **Local Image Search**

1. Choose “Picture”—“Local”.

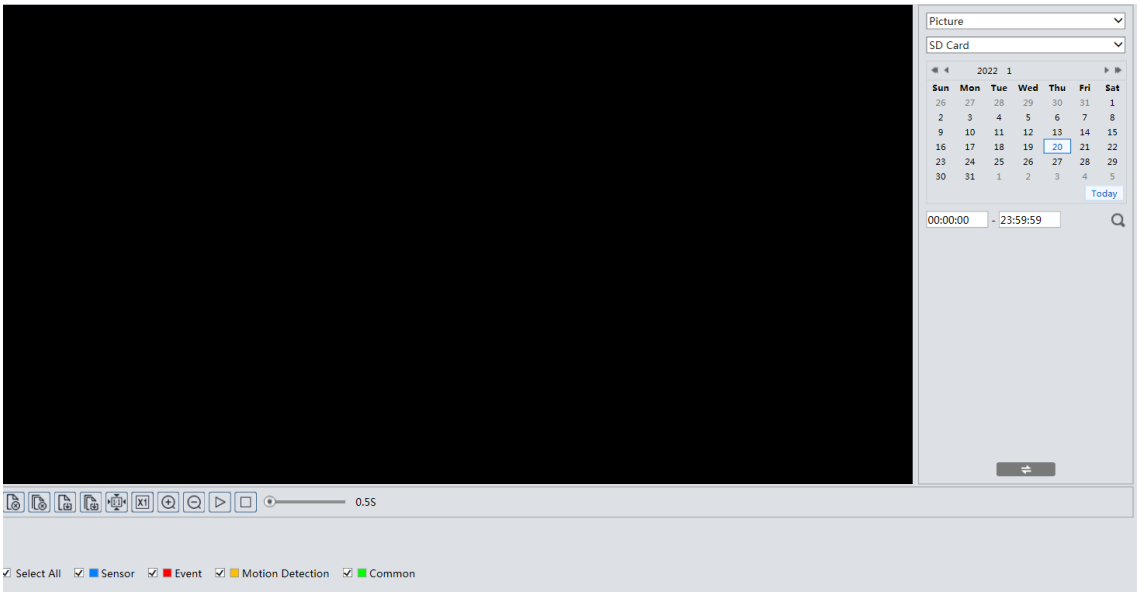
2. Set time: Select date and choose the start and end time.
3. Click to search the images.
4. Double click a filename in the list to view the captured photos as shown above.



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.

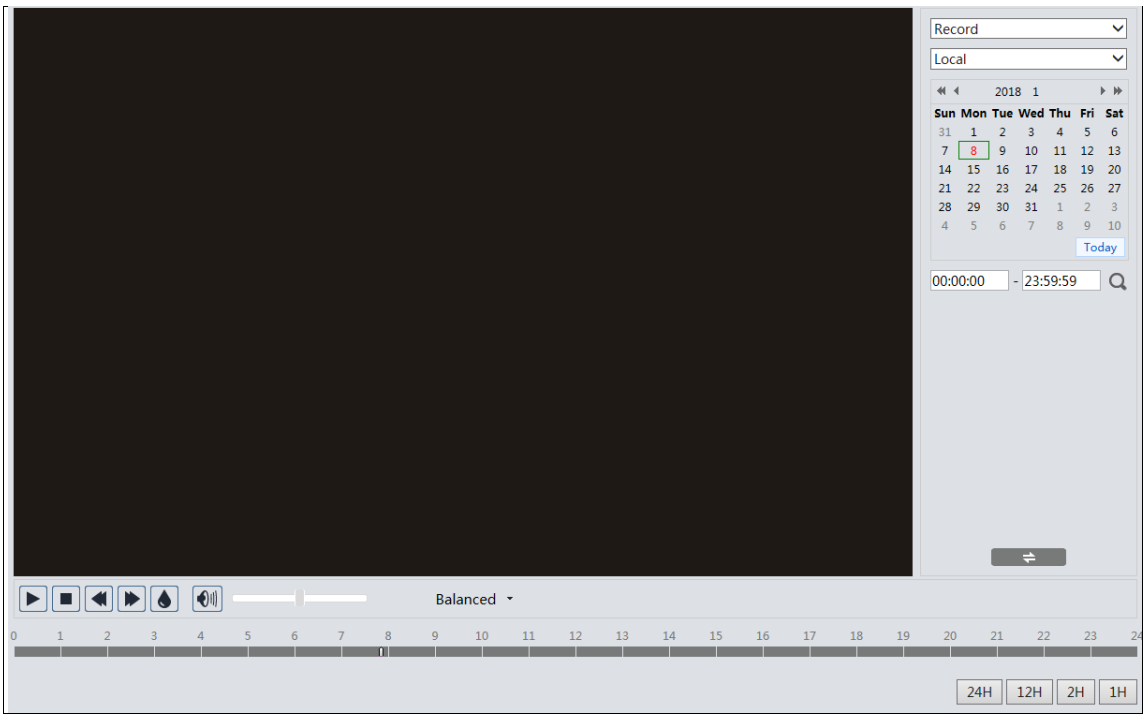
The descriptions of the buttons are shown as follows.

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.
5.5S	Play speed: Play speed of the slide show.		

5.2 Video Search

5.2.1 Local Video Search

Click Search to go to the interface as shown below. Videos were recorded locally to the PC can be played in this interface.



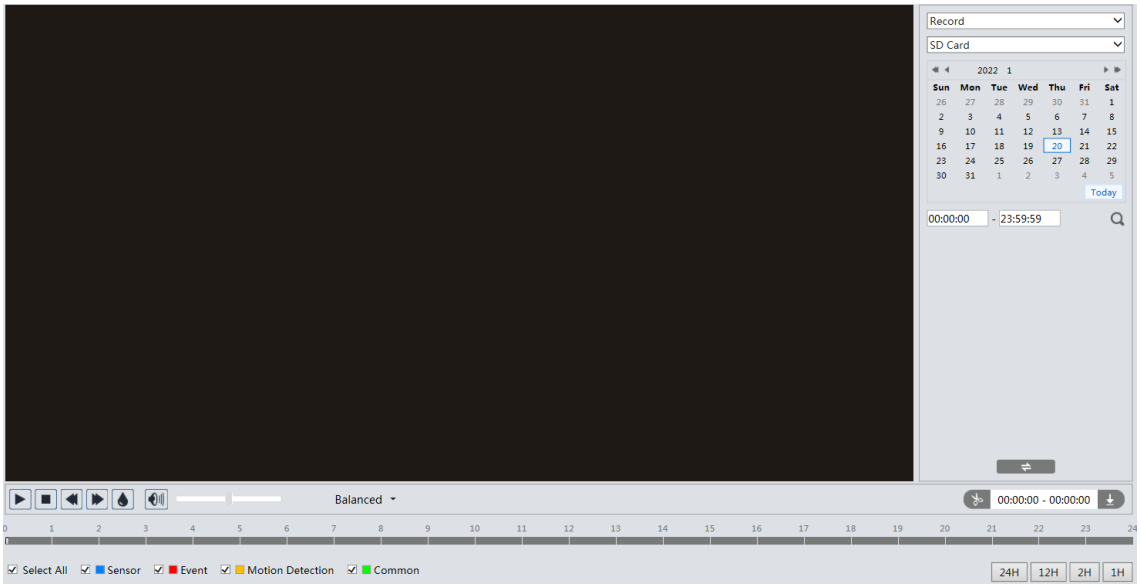
1. Choose “Record”—“Local”.
2. Set search time: Select the date and choose the start and end time.
3. Click to search the images.
4. Double click on a file name in the list to start playback.

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

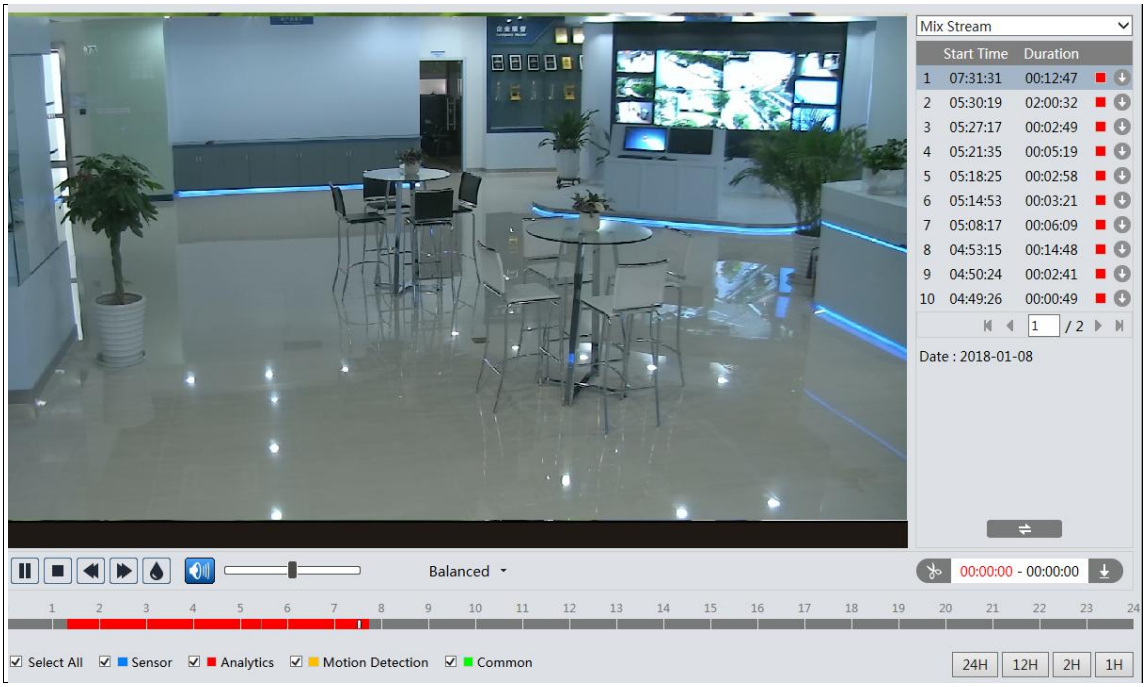
5.2.2 SD Card Video Search

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

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



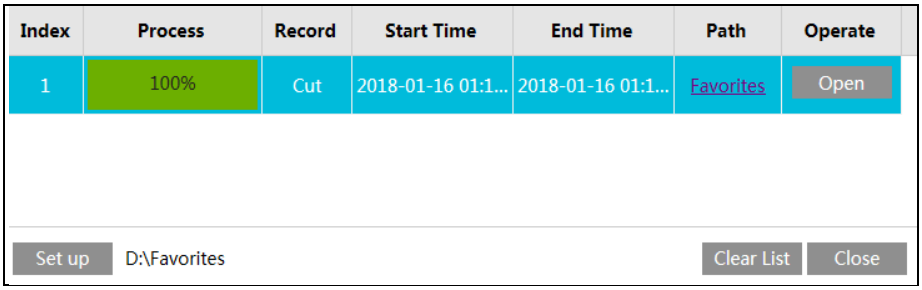
4. Select the alarm events at the bottom of the interface.
5. Select mix stream (video and audio stream) or video stream as needed.
6. Double click on a file name in the list to start playback.



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

Video clip and downloading

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



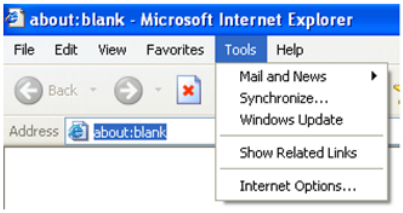
Click “Set up” to set the storage directory of the video files.
Click “Open” to play the video.
Click “Clear List” to clear the downloading list.
Click “Close” to close the downloading window.

Appendix

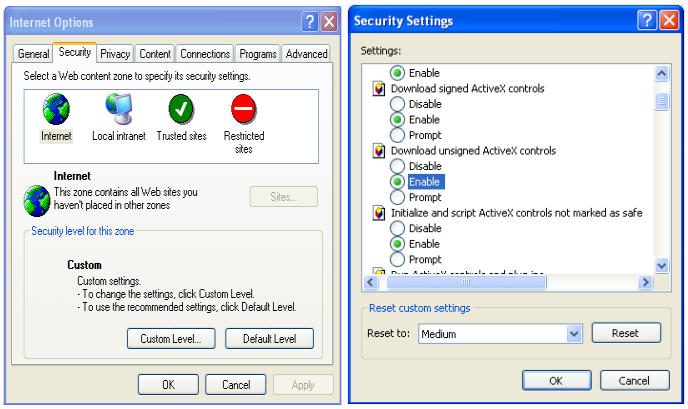
Appendix 1 Troubleshooting

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: O4LB1M / O4LT1M

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