



User Manual

6MP Fisheye Network Camera

O6MDP4

Please read this instruction 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 power supply 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.
Caution: Be mindful when positioning the camera as its built-in illumination may cause temporary glare to approaching drivers.

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 don't 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	9
4.1	System Configuration	9
4.1.1	System Information	9
4.1.2	Date and Time	9
4.1.3	Local Recording	10
4.1.4	Storage	10
4.1.5	Configuring Fisheye Parameters	12
4.2	Video Configuration	12
4.2.1	Image Configuration	12
4.2.2	Video / Audio Configuration	14
4.2.3	OSD Configuration	15
4.2.4	Video Mask	16
4.2.5	ROI Configuration	17
4.3	Alarm Setup	17
4.3.1	Motion Detection	17
4.3.2	Exception Alarm	18
4.3.3	Alarm In (Sensor Input)	20
4.3.4	Alarm Out	21
4.3.5	Alarm Server	22
4.4	Analytics Configuration	22
4.4.1	Line Crossing	23
4.4.2	Region Intrusion	25
4.4.3	Region Entrance	26
4.4.4	Region Exiting	27
4.4.5	Target Counting by Line	27
4.4.6	Crowd Density Detection	28
4.4.7	Heat Map	30
4.4	Network Configuration	31
4.4.1	TCP/IP	31
4.4.2	Port	32
4.4.3	Server Configuration	32
4.4.4	Onvif	33
4.4.5	DDNS	33
4.4.6	SNMP	34
4.4.7	802.1x	35
4.4.8	RTSP	35
4.4.9	RTMP	36
4.4.10	UPNP	36
4.4.11	Email	36
4.4.12	FTP	37
4.4.13	HTTP POST	38
4.4.14	HTTPS	38
4.4.15	QoS	39
4.5	Security Configuration	40
4.5.1	User Admin	40
4.5.2	Online User	41

4.5.3	Block and Allow Lists.....	41
4.5.4	Security Management.....	42
4.6	Maintenance Configuration.....	43
4.6.1	Backup and Restore	43
4.6.2	Reboot	44
4.6.3	Upgrade	44
4.6.4	Operation Log	44
4.6.5	Debug Mode	45
5	Search.....	46
5.1	Image Search	46
5.2	Video Search.....	47
Appendix		49
Appendix 1 Troubleshooting		49

1 Introduction

Welcome

Thank you for purchasing this network camera!

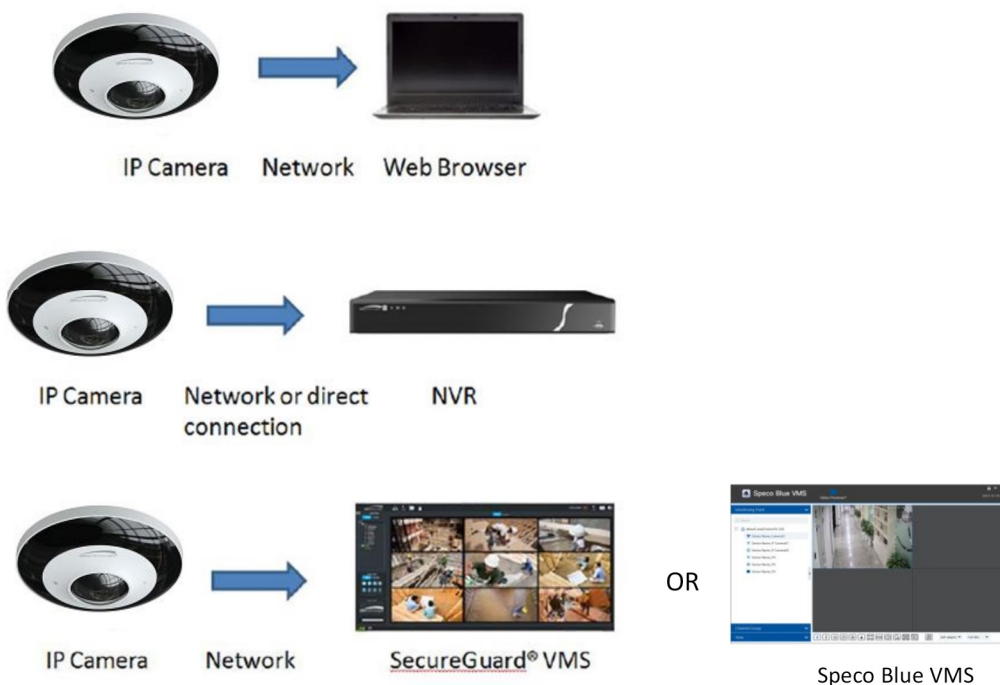
Please read this manual carefully before operating the unit and retain it for further reference.

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)
- 1/2.5" 6MP progressive scan CMOS, 360° panoramic image
- Remote viewing support via web browser, mobile APP, and VMS

Applications



DORI Distance

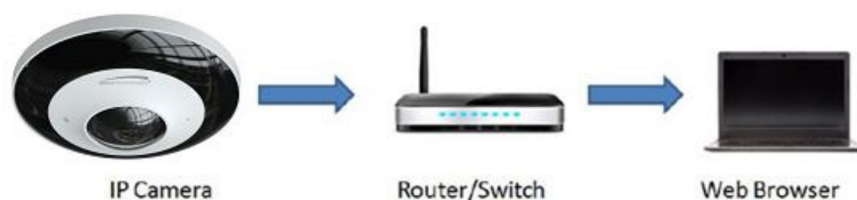
Level	Detect (25px/m)	Observe (63px/m)	Recognize (125px/m)	Identify (250px/m)
Object Distance	33m(108ft)	13m(42ft)	6m(210ft)	3m(10ft)
Recommended Installation Height	2.5m (8.2ft)			

2 Web Access and Login

The IP camera settings can be accessed via a web browser (Internet Explorer 8 and up) through the LAN.

- Access through Speco Blue Scanner

Network connection:



- ① Make 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 Speco Blue Scanner and run it after installation. Speco Blue Scanner is the tool for discovering the IP cameras on the local network. It can be downloaded from www.specotech.com.
- 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.

The screenshot shows the login interface for Speco Technologies. It features a blue header with the 'speco technologies' logo. Below the header, there are two input fields: 'Username:' with the text 'admin' and 'Password:' with four dots. At the bottom, there are two buttons: 'Login' and 'Cancel'.

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.

The screenshot shows a dialog box titled 'Please change the default password'. It has a close button (X) in the top right corner. Inside the dialog, there is a section for 'Modify Password' with a checkbox labeled 'Match Onvif Password' which is checked. Below this are three input fields: 'Old Password', 'New Password', and 'Confirm Password'. A note below the fields states: 'The password can be composed of numbers, special characters, upper or lower case letters.' At the bottom right, there are 'OK' and 'Cancel' buttons.

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)

PortServerOnvifDDNSSNMP802.1XRTSPRTMPUPnPEmailFTPHTTPSQoS

AddModifyDelete

Index	User Name	User Type
1	admin	Administrator

Edit User

User Name

admin

New Password

Level

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

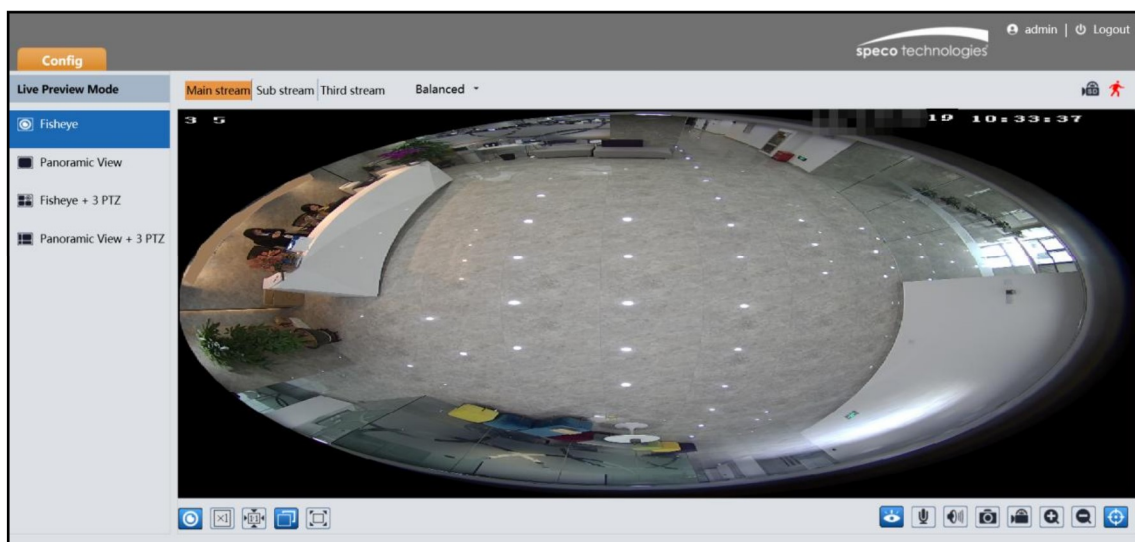
Confirm Password

OK

Cancel

3 Live View

The window below will be shown after logging in. Before you view the live image, please set the stream mode and installation method as needed (see [Configuring Fisheye Parameters](#) for details).



The following table describes the icons on the live view interface.

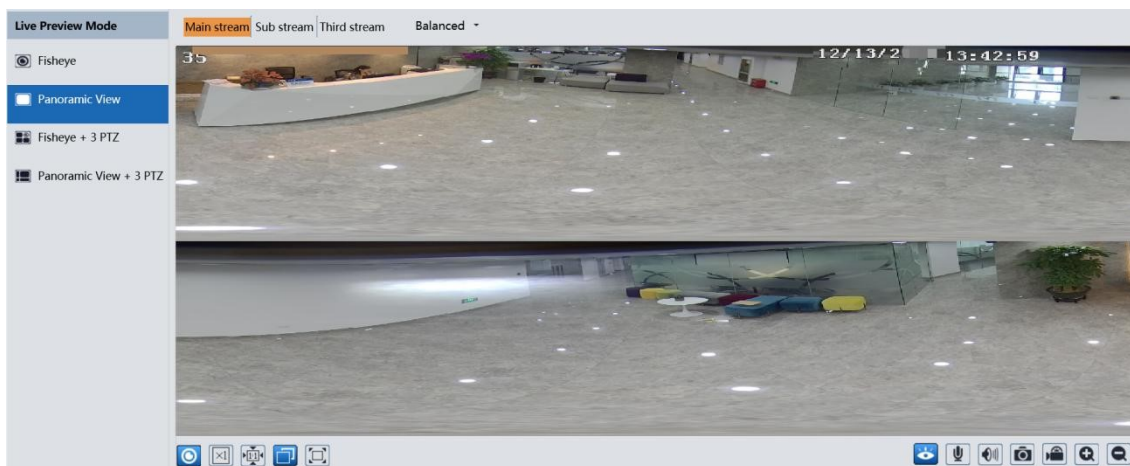
Icon	Description	Icon	Description
	Select live preview mode		Zoom out
	Original size		Rule information display
	Appropriate size		Sensor alarm indicator icon
	Auto		Motion alarm indicator icon
	Full screen		SD card recording indicator
	Start/stop live view		Line crossing indicator
	Start/stop two-way audio		Intrusion indicator
	Enable/disable audio		Region entrance indicator
	Snap		Region exiting indicator
	Start/stop recording		Target counting (by line) indicator
	Zoom in		Crowd density detection indicator

- 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.

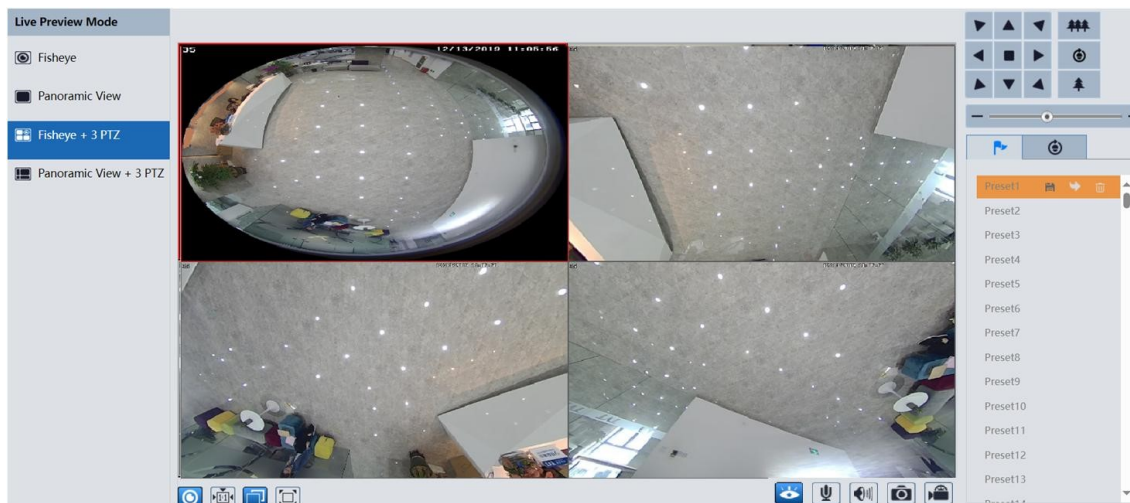
Click to select the live view mode.

Fisheye view mode: See the picture as shown above.

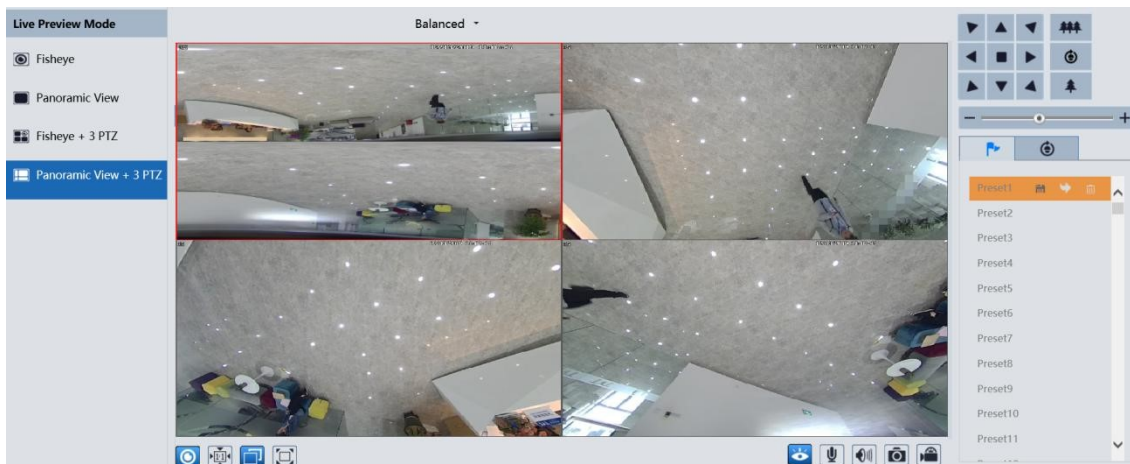
Panoramic view mode



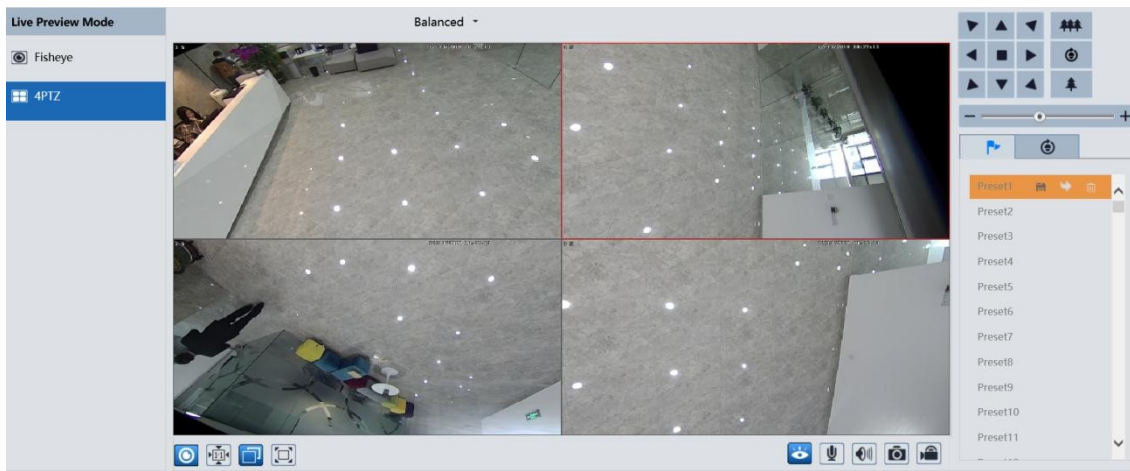
Fisheye+ 3PTZ view mode



Panoramic + 3PTZ view mode



4PTZ view mode (you need to switch the stream mode in the fisheye parameter interface)



4PTZ fusion view mode: you can view an entire picture formed by 4 small windows. Each small window cannot be controlled by PTZ panel.

In panoramic + 3PTZ view mode or fisheye + 3PTZ view mode or 4PTZ view mode, select a PTZ window and view the image from every direction by controlling PTZ panel.

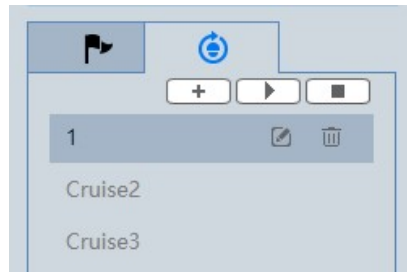
The descriptions of the PTZ control panel are as follows:

Icon	Description	Icon	Description
	Move upper left direction		Move upper right direction
	Move up		Stop movement
	Move left		Move right
	Move lower left direction		Move lower right direction
	Move down		Speed adjustment
	Zoom out		Zoom in
	Focus -		Focus +
	Iris -		Iris +
	Auto scan		Wiper
	Light		Radom scan
	Group scan		Preset

Select and set the preset and then click to save the position of the preset. After the preset is set, select it and click to call the preset. Select the set preset and click to delete it.

To create a cruise:

1. Click as shown below.



2. Click  to create a cruise. In the cruise creation window, enter the cruise name and then click “Add preset”.

3. In the preset adding window, select the preset name and time. Click “OK” to add this preset. After the presets are added to the cruise, click “OK” to save the settings.

Select the cruise and then click  to start cruise. Click  to stop cruise.

The added cruise also can be modified and deleted by clicking  or .

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.

Device Name	O6MDP4
Product Model	O6MDP4
Brand	Speco
Software Version	5.2.0.57222B240509.IF3.U3(13A11)
Software Build Date	2024-05-09
Onvif Version	23.12
OCX Version	5.2.0.56918
MAC	5C:F2:07:24:68:59
About this machine	View
Open Source Software Licenses View	View

4.1.2 Date and Time

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

Date and Time

Summer Time

Zone: GMT-05 (New York, Toronto, Washington DC)

The device time zone is different from the computer time zone, please select the correct time zone

Time Mode:

☒ Synchronize with NTP server

NTP server: time.windows.com

Update period: 1440 Minutes

☐ Set manually

Set Time: 2024-05-10 04:50:44

☐ Sync with computer local time

Save

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

Date and Time

Summer Time

☒ DST

☒ Auto DST

☐ Manual DST

Start Time

January

First

Sunday

00

Hour

End Time

February

First

Monday

00

Hour

Time Offset

120 Minutes

Save

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 audio in the recorded files.

The screenshot shows the 'Local Recording' settings window. It has two text input fields for 'Picture Path' and 'Record Path', both containing 'C:\Program Files\NetIPCamera\Picture' and 'C:\Program Files\NetIPCamera\Record' respectively, with 'Browse' buttons to the right. Below these are three radio button groups: 'Video Audio Settings' (Open, Close), 'Show Bitrate' (Open, Close), and 'Local Smart Snapshot Storage' (Open, Close). The 'Close' option is selected in all three groups. A 'Save' button is at the bottom.

Show Bitrate: enable or disable the bitrate display on the live video.

Additionally, the snapshots triggered by smart events 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.

The screenshot shows the 'Storage Management' interface with tabs for 'Management', 'Record', 'Snapshot', and 'FTP Snapshot'. The 'Management' tab is active. It displays several storage metrics: 'Total picture capacity' (3043 MB), 'Picture remaining space' (3042 MB), 'Total recording capacity' (27328 MB), and 'Record remaining space' (25280 MB). There are also dropdowns for 'State' (Normal), 'Snapshot Quota' (10%), and 'Video Quota' (90%). A note states: 'Changes in the quota ratio need to be formatted before they become effective.' At the bottom are 'Eject' and 'Format' buttons.

● 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.

The screenshot shows the 'Record Parameters' interface with tabs for 'Management', 'Record', 'Snapshot', and 'FTP Snapshot'. The 'Record' tab is active. It displays three dropdown menus: 'Record Stream' (Main stream), 'Pre Record Time' (No Pre Record), and 'Cycle Write' (Yes). To the right of the 'Pre Record Time' dropdown is the text '(H264,H265,MJPEG)'.

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 Manual Input Select All Invert Clear

Week Schedule

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Sun.	00:00-24:00 Apply settings to Manual Input Select All Invert Clear																								
Mon.	00:00-24:00 Apply settings to Manual Input Select All Invert Clear																								
Tue.	00:00-24:00 Apply settings to Manual Input Select All Invert Clear																								
Wed.	00:00-24:00 Apply settings to Manual Input Select All Invert Clear																								
Thu.	00:00-24:00 Apply settings to Manual Input Select All Invert Clear																								
Fri.	00:00-24:00 Apply settings to Manual Input Select All Invert Clear																								
Sat.	00:00-24:00 Apply settings to Manual Input Select All Invert Clear																								

Holiday Schedule

Date(MM-DD) + -

	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
	00:00-24:00 Apply settings to Manual Input Select All Invert Clear																								

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** FTP Snapshot

Snapshot Parameters

Image Format

Resolution

Image Quality

Event Trigger

Snapshot Interval Second

Snapshot Quantity

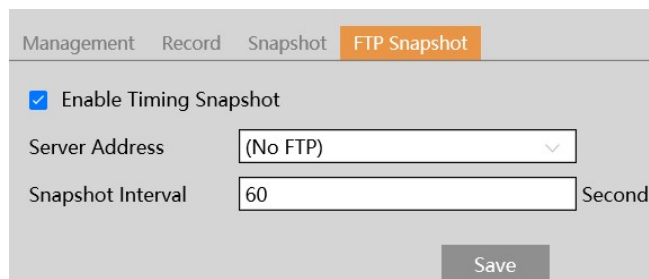
Set the format, resolution and quality of the image saved on the SD card and the snapshot interval and quantity and the timing snapshot here.

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](#)).

● FTP Snapshot Settings

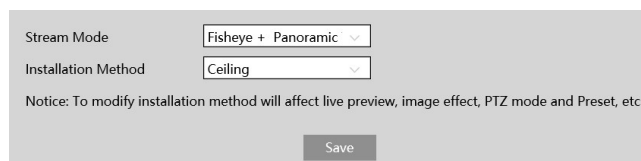
If enabled, the system will upload snapshots to the FTP server according to the time interval.



Server Address: select the set FTP server. See [FTP section](#) for the FTP server setting.

4.1.5 Configuring Fisheye Parameters

Before viewing the live image, please go to Config→System→Fisheye Parameters menu to set the stream mode and installation method.



Stream mode: “Fisheye”, “Panoramic View”, “Fisheye + Panoramic view + 3PTZ”, “Fisheye + 4PTZ” or “Fisheye + 4PTZ Fusion” mode are optional.

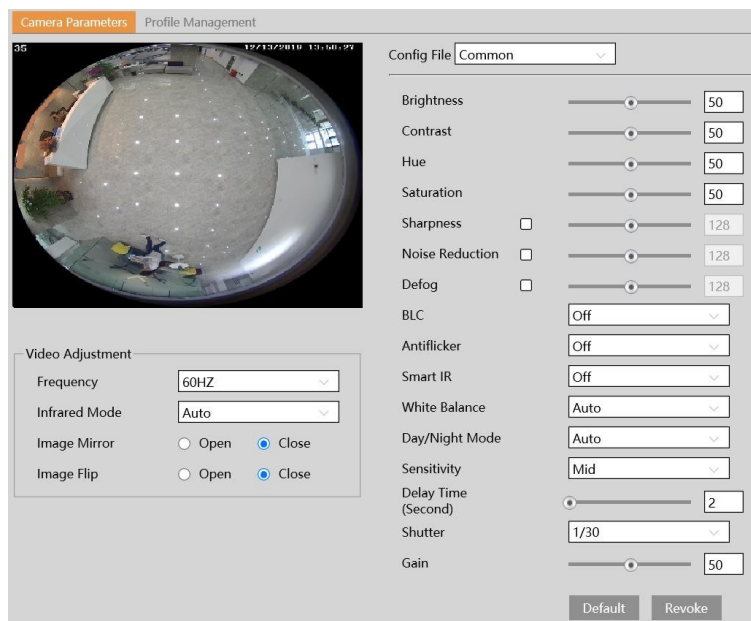
Installation method: wall, ceiling and desktop are optional. Please select the installation mode according to the actual way of installation.

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.



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

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

Hue: Set the total color degree of the image.

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

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

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

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

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

Backlight Compensation (BLC):

- Off: disables the backlight compensation function. It is the default mode.
- HWDR: WDR can adjust the camera to provide a better image when there are both very bright and very dark areas simultaneously in the field of the view by lowering the brightness of the bright area and increasing the brightness of the dark area. Recording will be stopped for a few seconds while the mode is changing from non-WDR to WDR mode.
- HLC: lowers the brightness of the entire image by suppressing the brightness of the image's bright area and reducing the size of the halo area.
- BLC: If enabled, the auto exposure will activate according to the scene so that the object of the image in the darkest area will be seen clearly.

Antiflicker:

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

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

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

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

Shutter: Set the upper limit of the effective exposure time. The exposure time will be automatically adjusted (within the set shutter limit value) according to the actual situation.

Gain: Set the upper limit of the gain. The gain value will be automatically adjusted (within the set gain limit value) according to the actual situation.

Frequency: 50Hz and 60Hz can be optional.

Infra-red Mode: Choose "Auto", "ON" or "OFF".

Image Mirror: Turn the current video image horizontally.

Image Flip: Turn the current video image vertically.

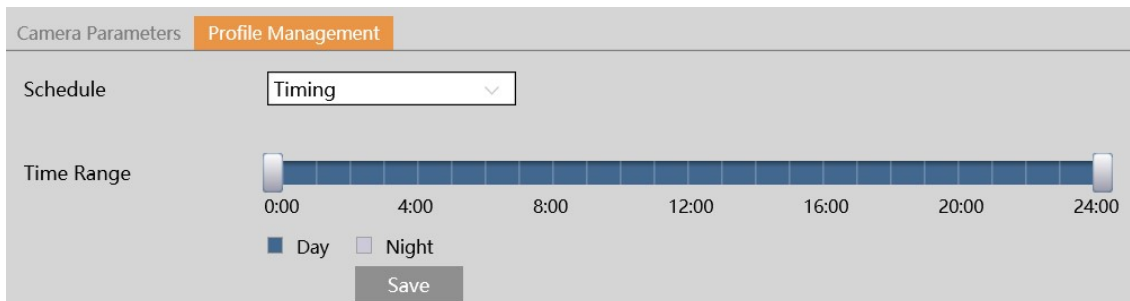
Note: For some items, if selected/enabled, the camera will reboot automatically. After that, clicking “Default” button will not take effect.

Schedule Settings of Image Parameters:

Click the “Profile Management” tab as shown below.



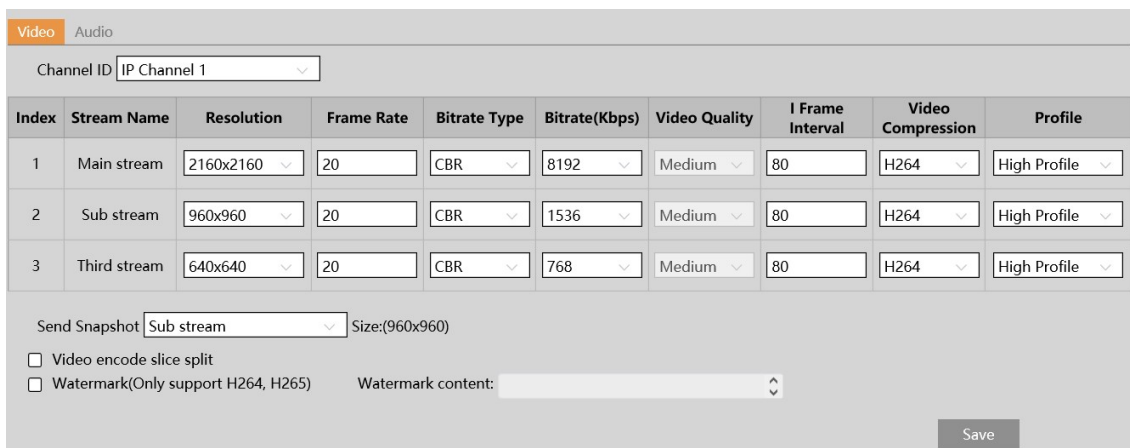
Set full time schedule for common, auto mode and specified time schedule for day and night. Choose “Timing” in the drop-down box of schedule as shown below.



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

4.2.2 Video / Audio 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.



Index	Stream Name	Resolution	Frame Rate	Bitrate Type	Bitrate(Kbps)	Video Quality	I Frame Interval	Video Compression	Profile
1	Main stream	2160x2160	20	CBR	8192	Medium	80	H264	High Profile
2	Sub stream	960x960	20	CBR	1536	Medium	80	H264	High Profile
3	Third stream	640x640	20	CBR	768	Medium	80	H264	High Profile

Send Snapshot: ☐ Sub stream Size:(960x960)

☐ Video encode slice split

☐ Watermark(Only support H264, H265) Watermark content:

Save

You can select streams for different channels.

For instance, “Fisheye + Panoramic View +3PTZ” mode:

IP Channel 1: Fisheye view channel, 3 streams can be set. Please set them according to the actual network condition.

IP Channel 2: Panoramic view channel, 3 streams can be set. Please set them according to the actual network condition.

IP Channel 3/4/5: PTZ view channel, main stream can be set for each channel. Please set them according to the actual network condition.

Resolution: The size of image.

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

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

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

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

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

Video Compression: MJPEG, H264+, H264, H265 or H265+ can be optional. If H.265/H.265+ is chosen, make sure the client system is able to decode H.265/H.265+. Compared to H.265, H.265+ saves more storage space with the same maximum bitrate in most scenes. Compared to H.264, H.265 reduces the transmission bitrate under the same resolution, frame rate and image quality.

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

Send Snapshot: Set the snapshot stream.

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

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

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

The screenshot shows the 'Audio' configuration tab. It includes an 'Enable' checkbox which is checked. Below it are two dropdown menus: 'Audio Encoding' set to 'G711A' and 'Audio Type' set to 'MIC'. At the bottom, there are two volume sliders, both set to 75: 'MIC In Volume' and 'Audio Out Volume'.

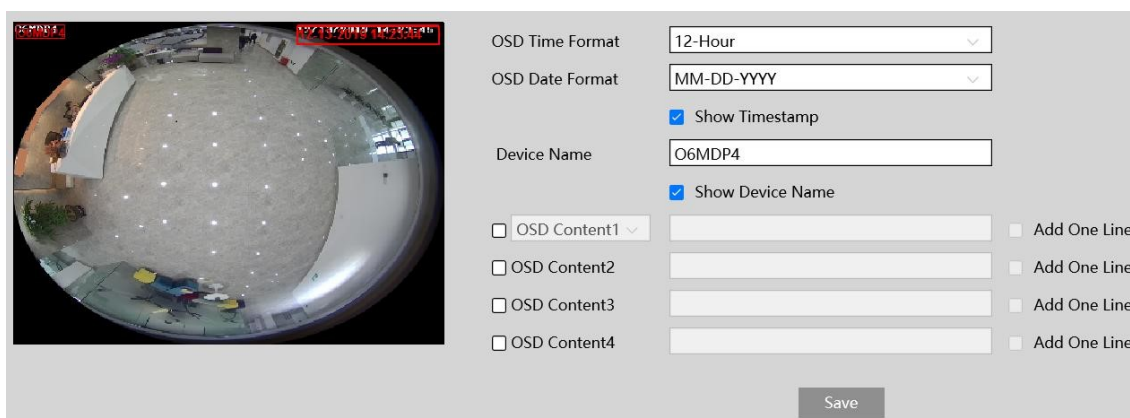
Audio Encoding: G711A and G711U are selectable.

Audio Type: MIC or LIN. (If the internal MIC is used, choose “MIC”. If you want to use external line-level audio input device, choose “LIN”.)

LIN/MIC IN Volume: Set it as needed.

4.2.3 OSD Configuration

Go to Video→OSD interface as shown below.



OSD Time Format: 12-Hour

OSD Date Format: MM-DD-YYYY

☒ Show Timestamp

Device Name: O6MDP4

☒ Show Device Name

☐ OSD Content1

☐ OSD Content2

☐ OSD Content3

☐ OSD Content4

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  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.

Note: The OSD information only can be overlaid on fisheye channel.

4.2.4 Video Mask

Go to Image→Privacy 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→Region of Interest 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.

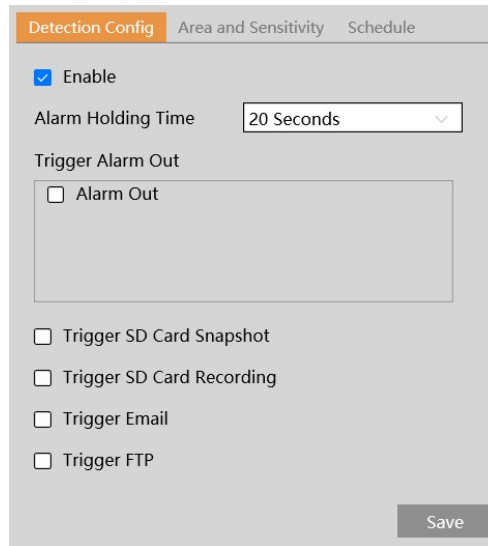


1. Check “Enable” and then click the “Draw Area” button.
2. Drag the mouse to set the ROI area.
3. Set the level.
4. Click the “Save” button to save the settings.

4.3 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 Out: If selected, this would trigger an external relay output that is connected to the camera on detecting a motion based alarm.

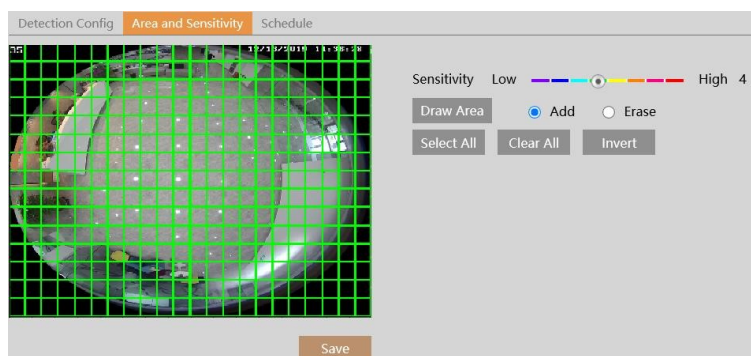
Trigger SD Card Snapshot: If selected, the system will capture images on motion detection and save the images on an SD card.

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](#)).

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→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](#) chapter for details.

● IP Address Conflict

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

The screenshot shows a configuration window with four tabs at the top: "SD Card Full", "SD Card Error", "IP Address Collision" (which is selected and highlighted in orange), and "Cable Disconnected". Inside the window, there is a section with a checked checkbox labeled "Enable". Below this is a label "Alarm Holding Time" followed by a dropdown menu currently showing "20 Seconds". Underneath is a label "Trigger Alarm Out" followed by a large rectangular box containing a single unchecked checkbox labeled "Alarm Out". At the bottom right of the window is a grey button labeled "Save".

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

3. Trigger alarm out. When the IP address of the camera is in conflict with the IP address of other devices, the system will trigger the alarm out.

● Cable Disconnection

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

The screenshot shows a configuration window with four tabs at the top: "SD Card Full", "SD Card Error", "IP Address Collision", and "Cable Disconnected" (which is selected and highlighted in orange). The interface is identical to the previous one, with a checked "Enable" checkbox, an "Alarm Holding Time" dropdown set to "20 Seconds", a "Trigger Alarm Out" section with an unchecked "Alarm Out" checkbox, and a "Save" button at the bottom right.

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

3. Trigger alarm out. When the camera is disconnected, the system will trigger the alarm out.

4.3.3 Alarm In (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](#) chapter for details.
3. Click “Save” button to save the settings.
4. Set the schedule of the sensor alarm. The setup steps of the schedule are the same as the schedule recording setup. (See [Schedule Recording](#)).

4.3.4 Alarm Out

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

Alarm Out Mode: Alarm linkage, manual operation, day/night switch linkage 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.

Day/Night Switch Linkage: Having selected this mode, select the alarm type and choose to open or close alarm out when the camera switches to day mode or night mode.

Alarm Out Mode

ight switch linkage

Alarm Type

NC

Day

Close

Night

Close

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 Mode

Timing

Alarm Type

NC

Time Range

07:15-14:30

0

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

Manual Input

Save

4.3.5 Alarm Server

Go to Alarm→Alarm Server interface as shown below.

Server Address

0.0.0.0

Port

8010

Heartbeat

Disable

Heartbeat interval

30

Second

Edit

Click “Edit” to set the alarm server.
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.
Click  to view the entire server address; click  to hide a part of sensitive data.

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.

Note: Events may vary by different installation methods and stream modes. Go to Config→System→Fisheye Parameters to set the stream mode and installation method.

* When the installation method is set to “Wall” or “Desktop” and the stream mode is set to “Panoramic View” or “Fisheye + Panoramic view +3 PTZ”, line crossing/region intrusion/region entrance/region exiting/target counting by line (human/motor vehicle/ non-motor vehicle classification) or crowd density detection is supported.

* When the installation method is set to “Ceiling” and the stream mode is set to any one of the stream modes except “Panoramic view”, line crossing/region intrusion/region entrance/region exiting/target counting by line (only human), heat map or crowd density detection is supported.

4.4.1 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.

Note: When the installation method is set to “Ceiling”, only “Human” can be selected.

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.

Push target trajectory with a persistent connection: Push target trajectory (moving coordinate) to API test tool with a persistent connection. If enabled, the system will push the target trajectory upon detecting a target. If disabled, the system will push the target trajectory only when triggering line crossing alarm.

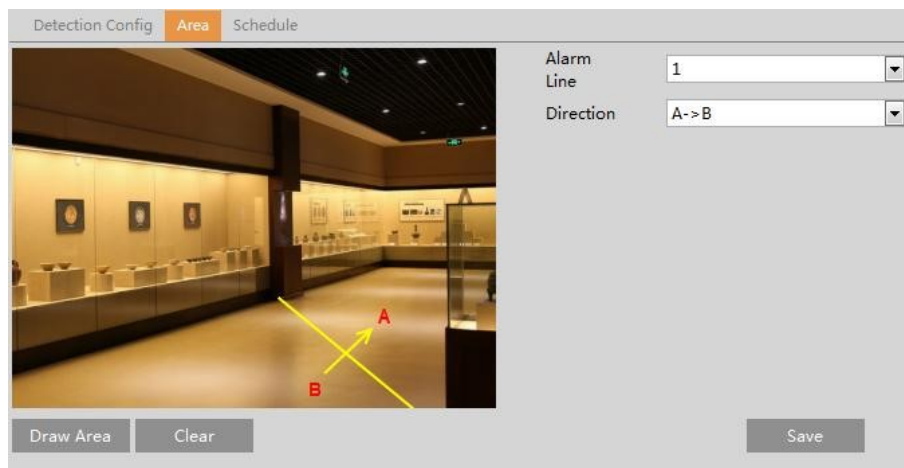
2. Set the alarm holding time.

3. Set alarm trigger options. The setup steps are the same as motion detection alarm. 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” tab to go to the interface as shown below.

Note: The image display may be different due to different installation modes. The following picture is for reference only.



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](#)).

In the live view interface, click “Panoramic view” (desktop or wall mounting mode) or “Fisheye” (ceiling mounting mode) to view line crossing detection.

※ **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.

4.4.2 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.

Detection ConfigAreaSchedule

☒ Enable

☐ Save Original Picture To SD Card

☐ Save Target Picture To SD Card

Detection target and sensitivity

Target

☒ Human

Sensitivity

50

☐ Push target trajectory with a persistent connection

Alarm Holding Time

20 Seconds

Trigger Alarm Out

☐ Alarm Out

☐ Trigger SD Card Snapshot

☐ Trigger SD Card Recording

☐ Trigger Email

☐ Trigger FTP

Save

1. Enable intrusion alarm and select the snapshot type and the detection target.
- Save Original Picture:** If it is enabled, the detected original pictures will be captured and saved to the SD card when the target intrudes into the pre-defined areas.
- Save Target Picture:** If it is enabled, the detected target cutout pictures will be captured and saved to the SD card when the target intrudes 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.

Non-motor Vehicle: 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.

Note: When the installation method is set to “Ceiling”, only “Human” can be selected.

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.

Push target trajectory with a persistent connection: Push target trajectory (moving coordinate) to API test tool with a persistent connection. If enabled, the system will push the target trajectory upon detecting a target. If disabled, the system will push the target trajectory only when triggering region intrusion alarm.

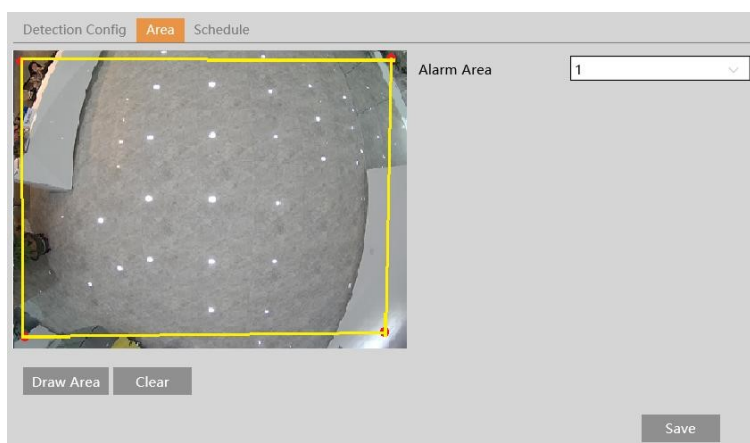
2. Set the alarm holding time.

3. Set alarm trigger options. The setup steps are the same as motion detection alarm. 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.

Note: The image display may be different due to different installation modes. The following picture is for reference only.



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](#)).

In the live view interface, click “Panoramic view” (desktop or wall mounting mode) or “Fisheye” (ceiling mounting mode) to view region intrusion detection.

※ 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.

4.4.3 Region Entrance

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

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

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

2. Set the alarm holding time and alarm trigger options.

3. Set the alarm area of the region entrance detection.
4. Set the schedule of the region entrance detection.

The setup steps of the region entrance detection are the same as the region intrusion detection setup (See [Region Intrusion](#) for details).

4.4.4 Region Exiting

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

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

1. Enable region exiting detection and select the snapshot type and the detection target.
2. Set the alarm holding time and alarm trigger options.
3. Set the alarm area of the region exiting detection.
4. Set the schedule of the region exiting detection.

The setup steps of the region exiting detection are the same as the region intrusion detection setup (See [Region Intrusion](#) for details).

4.4.5 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 and select the snapshot type and the detection target.

Detection Target: Select the target to calculate. Human, motor vehicle and motorcycle/bicycle can be selected.

Note: When the installation method is set to “Ceiling”, only “Human” can be selected.

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

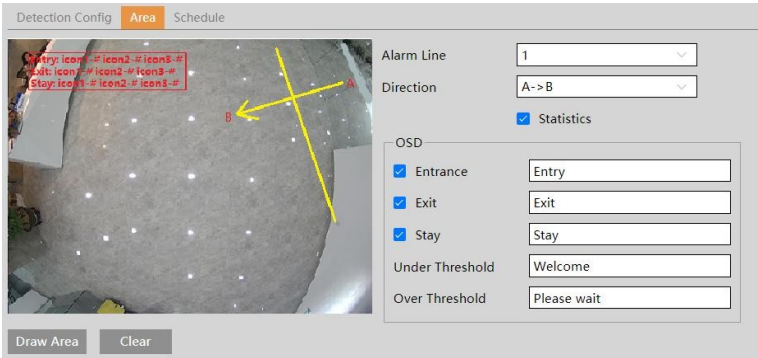
Push target trajectory with a persistent connection: Push target trajectory (moving coordinate) to API test tool with a persistent connection. If enabled, the system will push the target trajectory upon detecting a target. If disabled, the system will push the target trajectory only when triggering target counting by line.

Close Event Snapshot: if enabled, the pictures that are captured when counting targets will be neither saved to an SD card/local PC nor pushed to the NVR/APP/VMS platform/....

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 people/motor vehicle/non-motor vehicle 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.

Note: The image display may be different due to different installation modes. The following picture is for reference only.



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.

Click the “Save” button to save the settings.

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 by clicking “Panoramic view” (desktop or wall mounting mode) or “Fisheye” (ceiling mounting mode) .

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

Heat Map

Report Type

Daily Report

Count Type

Enter

Count Time

2024

Year

5

Month

10

Day

Count

Table

Chart

Export

Index	Count Time	Human	Motor Vehicle	Non-motor Vehicle
1	2024/05/10 00:00:00 ~ 2024/05/10 00:59:59	0	0	0
2	2024/05/10 01:00:00 ~ 2024/05/10 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 “Chart” to view the statistic result intuitively.

4.3.6 Crowd Density Detection

This function can detect the density of the people in a specified area (like square, supermarket). Go to Config→Event→Crowd Density as shown below.

1. Enable the crowd density detection.
2. Set “Refresh Frequency”, “Density Alarm Threshold” and “Alarm Holding Time”.

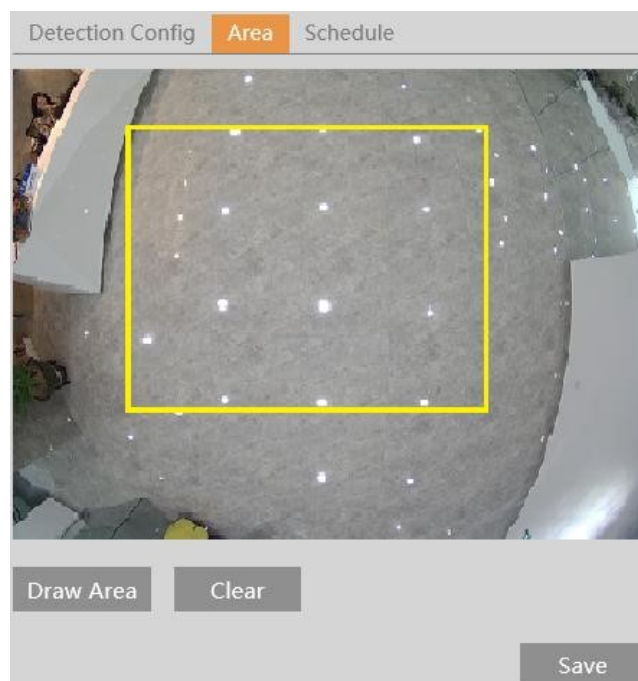
Refresh Frequency: The refresh frequency of the detection result.

Density Alarm Threshold: Alarms will be triggered once the percentage of the crowd density in a specified area exceeds the pre-defined threshold value.

3. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection section for details.
4. Set an alarm area for the crowd density detection. Click the “Area” tab as shown below.

Click “Draw Area” and drag the mouse to draw a rectangle area. Drag the border lines of the rectangle to modify its size and move the rectangle to change its position. Click “Stop Draw” to stop drawing the area. Click “Clear” to clear the area.

Note: The image display may be different due to different installation modes. The following picture is for reference only.



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

Note: The camera only can roughly calculate the crowd density through detecting the human faces. The head or back of the person detected is not counted.

※Configuration of camera and surrounding area

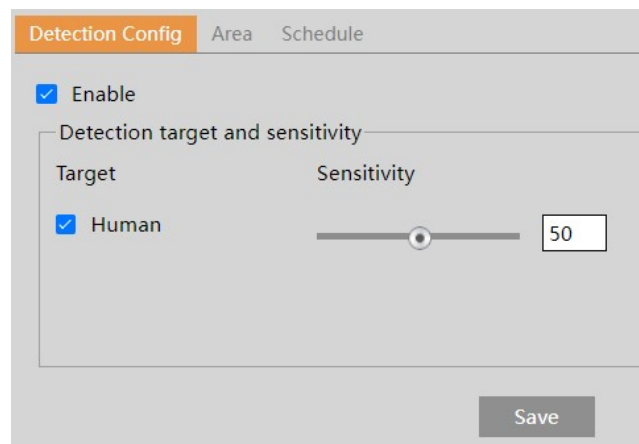
1. The camera lens should face to the people flow.
2. The size range of a single person image should take up from 1% to 5% of the entire image and the height range of a single person image should occupy from 1/5 to 1/2 of the entire image.
3. This function is inapplicable to the scene where there are many moving objects except human shape. (eg. moving cars)
4. A lot of trees and billboards will affect the detection results in the detected area.

4.4.6 Heat Map

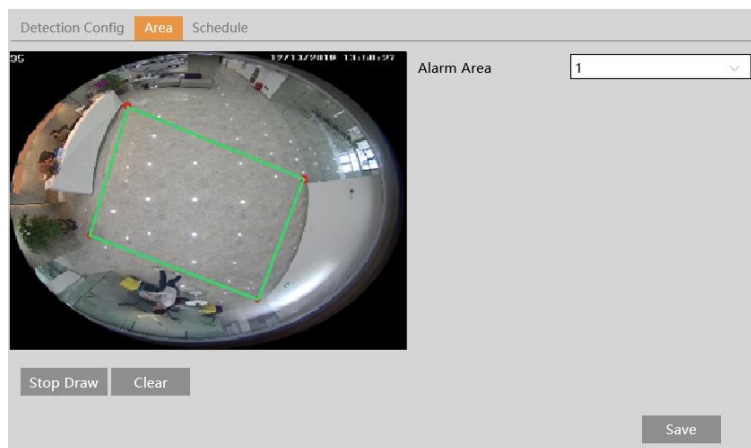
Note: Only when the installation method is set to “Ceiling”, can heat map be available.

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.



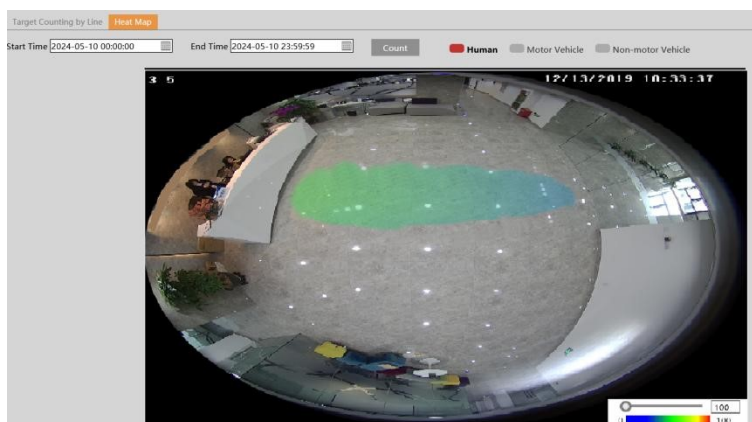
2. Set heat map display area. Up to 4 areas can be set.



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.



4.4 Network Configuration

4.4.1 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. Click “Edit”, 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.

4.4.2 Port

Go to Network→Advanced interface as shown below.

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

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

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

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

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

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

4.4.3 Server Configuration

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

1. Click “Edit” and then 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.

4.4.4 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.

4.4.5 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→ DDNS.

2. Click “Edit” to enable, save and use DDNS to log in.

4.4.6 SNMP

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

1. Go to Network→SNMP.

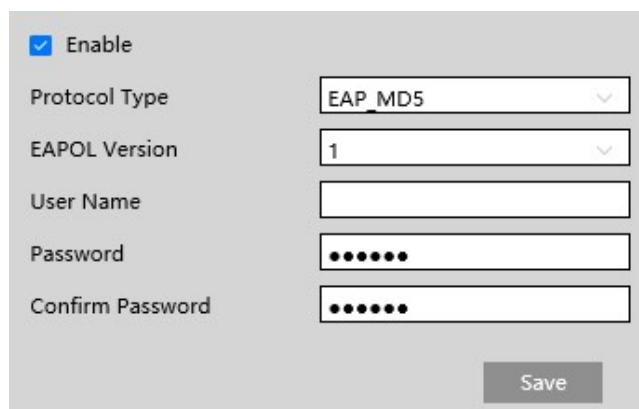
The image shows a web-based configuration interface for SNMP. It is divided into three main sections: 'SNMP v1/v2', 'SNMP v3', and 'Other Settings'.
SNMP v1/v2 section includes:
- 'Enable SNMPv1' and 'Enable SNMPv2' checkboxes, both currently unchecked.
- 'Read SNMP Community' text input field with 'public' entered.
- 'Write SNMP Community' text input field with 'private' entered.
- 'Trap Address' text input field with '192. ***. ***. 201' entered.
- 'Trap Port' text input field with '162' entered.
- 'Trap community' text input field with 'public' entered.
SNMP v3 section includes:
- 'Enable SNMPv3' checkbox, currently unchecked.
- 'Read User Name' text input field with 'public' entered.
- 'Security Level' dropdown menu with 'auth, priv' selected.
- 'Authentication Algorithm' radio buttons for 'MD5' (selected) and 'SHA'.
- 'Authentication Password' masked text input field with 8 dots.
- 'Private-key Algorithm' radio buttons for 'DES' (selected) and 'AES'.
- 'Private-key Password' masked text input field with 8 dots.
- 'Write User Name' text input field with 'private' entered.
- 'Security Level' dropdown menu with 'auth, priv' selected.
- 'Authentication Algorithm' radio buttons for 'MD5' (selected) and 'SHA'.
- 'Authentication Password' masked text input field with 8 dots.
- 'Private-key Algorithm' radio buttons for 'DES' (selected) and 'AES'.
- 'Private-key Password' masked text input field with 8 dots.
Other Settings section includes:
- 'SNMP Port' text input field with '161' entered.
At the bottom right of the form is an 'Edit' button with a pencil icon.

2. Click “Edit” and then 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.

4.4.7 802.1x

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



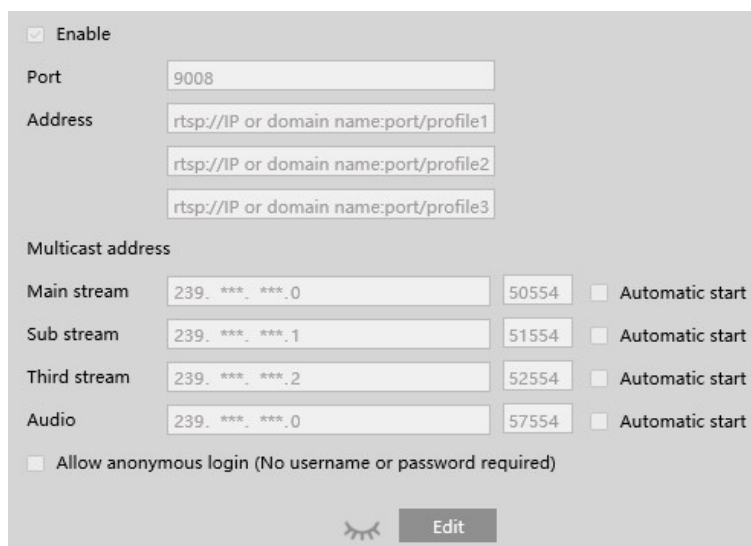
To use this function, the camera shall be connected to a switch supporting 802.1x protocol. The switch can be reckoned as an authentication system to identify the device in a local network. If the camera connected to the network interface of the switch has passed the authentication of the switch, it can be accessed via the local network.

Protocol type and EAPOL version: Please use the default settings.

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

4.4.8 RTSP

Go to Network→RTSP.



Click "Edit" and then 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".

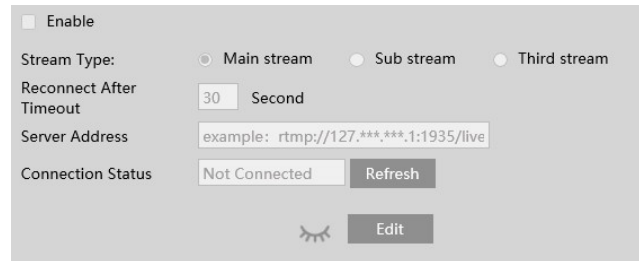
Third stream: The address format is

“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.

4.4.9 RTMP

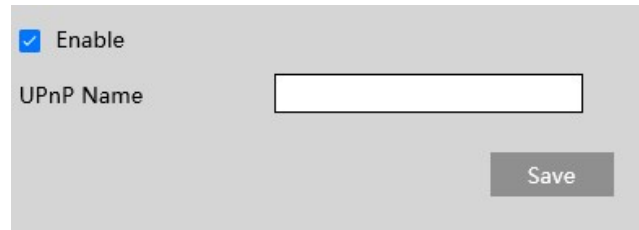
You can access the third-party (like YouTube) to realize video live view through RTMP protocol. Go to Config→Network→RTMP.

The image shows a configuration window for RTMP. At the top, there is a checkbox labeled "Enable". Below it, the "Stream Type:" section has three radio buttons: "Main stream", "Sub stream", and "Third stream". The "Reconnect After Timeout" section features a numeric input field with the value "30" and a label "Second". The "Server Address" section has a text input field containing the example "rtmp://127.***.***.1:1935/live". The "Connection Status" section shows a button labeled "Not Connected" and a "Refresh" button. At the bottom, there is a button with a camera icon and an "Edit" button.

Click “Edit” and then check “Enable”, select stream type and 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.

4.4.10 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.

The image shows a configuration window for UPnP. It starts with a checked checkbox labeled "Enable". Below this, the "UPnP Name" label is followed by a text input field. A "Save" button is located at the bottom right of the window.

4.4.11 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→Email.

Sender

Sender Address

User Name ☐ Anonymous Login

Password

Server Address

Secure Connection

SMTP Port

☐ Send Interval(S) (10-3600)

Recipient

Edit and Test

Click “Edit and Test” to set the sender and the recipient.

Sender Address: sender’s e-mail address.

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

Server Address: The SMTP IP address or host name.

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

SMTP Port: The SMTP port.

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

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

Recipient Address: receiver’s e-mail address.

4.4.12 FTP

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

Go to Network→FTP.

Add FTP

Server Name

Server Address

Upload Path

Port

User Name ☐ Anonymous

Password

OK Cancel

Background Table:

Server Name	Server Address	Port	User Name	Upload Path
Add Modify Delete Test Save				

Click “Edit and Test” and then click “Add” to add the information of the FTP. After that, click “Save” to save the settings.

Server Name: The name of the FTP server.

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

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

Port: The port of the FTP server.

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

4.4.13 HTTP POST

Go to Config→Network→HTTP POST interface.

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

The screenshot shows the HTTP POST configuration interface. It includes a checkbox for "Enable", a "Protocol Type" dropdown menu set to "API", a "Server Address" text field with "0.0.0.0", a "Server Port" text field with "8082", a "Heartbeat interval" text field with "90" and a unit dropdown set to "Second", and an "Online State" dropdown menu set to "Offline". There is a "Refresh" button next to the "Online State" dropdown and an "Edit" button at the bottom right.

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 human picture, motor vehicle picture) and so on.

4.4.14 HTTPS

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

Go to Network→HTTPS as shown below.

The screenshot shows the HTTPS configuration interface. It includes a checkbox for "Enable", a "Certificate installed" section with a text field showing "C=US, ST=Some-State, O=embeddedsoftware" and a "Delete" button, and an "Attribute" section with a text area showing the certificate details: "Issued to: C=US, ST=Some-State, O=embeddedsoftware, H=IPC, Issuer: C=US, ST=Some-State, O=embeddedsoftware, H=Root CA, Validity date: 2021-03-19 03:18:30 ~ 2031-03-17 03:18:30". There is a "Save" button at the bottom right.

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

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

☐ 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.

☐ Enable

Installation type

☐ Have signed certificate, install directly

☒ Create a private certificate

☐ Create a certificate request

Create a private certificate

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

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

☐ Enable

Installation type

☐ Have signed certificate, install directly

☐ Create a private certificate

☒ Create a certificate request

Create a certificate request

Install Created Certificate

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

4.4.15 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→QoS.

Video/Audio DSCP

0

Alarm DSCP

0

Manager DSCP

0

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

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

4.5 Security Configuration

4.5.1 User Admin

Go to Security→User Admin interface as shown below.

Setup ▶ Security ▶ User Admin			
Add Modify Delete			
Index	User Name	User Type	Bind MAC
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

Advanced User

☐ 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

☐ Remote configuration backup and recovery

OK

Cancel

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

Modify user:

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

Delete user:

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

Note: The default administrator account cannot be deleted.

4.5.2 Online User

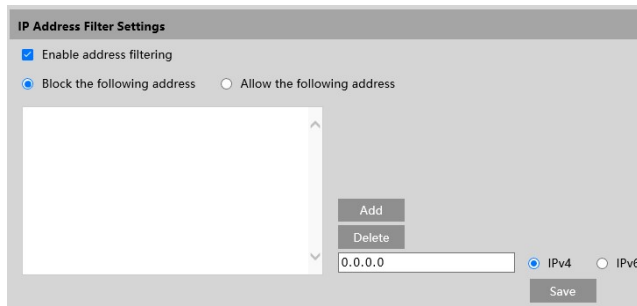
Go to Security→Online User to view the user who is viewing the live video.

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).

4.5.3 Block and Allow Lists

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



The screenshot shows the 'IP Address Filter Settings' window. It has a title bar and a main content area. At the top, there is a checked checkbox for 'Enable address filtering'. Below it, there are two radio buttons: 'Block the following address' (selected) and 'Allow the following address'. A large empty list box is in the center. To the right of the list box are 'Add' and 'Delete' buttons. Below the list box is an input field containing '0.0.0.0'. To the right of the input field are two radio buttons: 'IPv4' (selected) and 'IPv6'. At the bottom right is a 'Save' button.

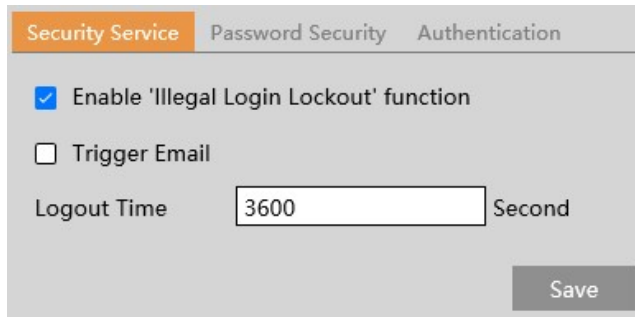
The setup steps are as follows:

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.

4.5.4 Security Management

Go to Security→Security Management as shown below.



The screenshot shows the 'Security Service' tab in the 'Security Management' section. It has a title bar with 'Security Service', 'Password Security', and 'Authentication' tabs. The 'Security Service' tab is active. It contains a checked checkbox for 'Enable 'Illegal Login Lockout' function'. Below it is an unchecked checkbox for 'Trigger Email'. There is a 'Logout Time' label followed by an input field containing '3600' and the word 'Second'. At the bottom right is a 'Save' button.

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.

● Password Security



The screenshot shows the 'Password Security' tab in the 'Security Management' section. It has a title bar with 'Security Service', 'Password Security', and 'Authentication' tabs. The 'Password Security' tab is active. It contains a 'Password Level' label followed by a dropdown menu showing 'Weak'. Below it is an 'Expiration Time' label followed by a dropdown menu showing 'Never'. At the bottom right is a 'Save' button.

Please set the password level and expiration time as needed.

Password Level: Weak, Medium or Strong.

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

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

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

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

HTTP Authentication: Basic or Token is selectable.

Security Service Password Security **Authentication**

HTTP Authentication Basic

Save

4.6 Maintenance Configuration

4.6.1 Backup and Restore

Go to Maintenance→Backup & Restore.

Import Setting

Path Browse

Import Setting

Export Settings

Export Settings

Restore Default Parameters

Keep

- ☐ Network Config
- ☐ Security Configuration
- ☐ Image Configuration

Restore Default Parameters

Restore Factory Settings

Restore Factory Settings

- **Import & Export Settings**

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

1. Click “Browse” to select the save path for import or export information on the PC.
2. Click the “Import Setting” or “Export Setting” button.

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

- **Restore Default Parameters**

Click the “Restore Default Parameters” button and then verify the password to restore all parameters to the default parameters except those you want to keep.

- **Restore Factory Settings**

Click the “Restore Factory Settings” button and then verify the password to restore all system settings to the default factory settings.

4.6.2 Reboot

Go to Config→Maintenance→Reboot.

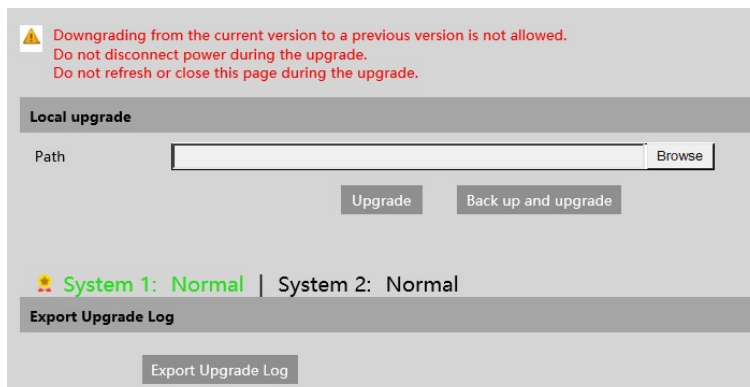
Click the “Reboot” button and then enter the password to reboot the device.

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, click the “Save” button and then enter the password to save the settings.

4.6.3 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” or “Back up and upgrade” button to start upgrading the firmware.
3. Enter the correct password and then the device will restart automatically.

Note: If “Back up and upgrade” is selected, the configuration file will be exported to your local PC before starting upgrading.

Caution:

1. Do not allow downgrading from the current version to the lower version.
2. Do not refresh/close the browser or disconnect the camera from the network during the upgrade, or it will cause system failure. After the device is successfully upgraded, there are ten minutes of observation. During this observation period, do not upgrade the device again.

Note: To decrease the upgrade risk, this series of cameras adopts two systems. After one system is successfully upgraded, the other system will be synchronized. If one system fails caused by power failure or other reasons during the upgrade, the other system will not be affected and the camera still can work normally. You can also upgrade your camera through the normal system.

Export Upgrade Log: If upgrade error occurs, the upgrade log can be exported to help the technician to analyze and solve the problem.

4.6.4 Operation Log

To query and export log:

1. Go to Maintenance→Operation Log.

Main Type

All logs

Sub Type

All logs

Start Time

2024-05-10 00:00:00

End Time

2024-05-10 23:59:59

Search

Export

Index	Time	Main Type	Sub Type	User Name	Login IP	Hostname
1	2024-05-10 07:35:20	Alarm	Motion Start			
2	2024-05-10 07:35:15	Alarm	Motion Stop			
3	2024-05-10 07:24:29	Alarm	Motion Start			
4	2024-05-10 07:24:28	Alarm	Motion Stop			
5	2024-05-10 07:02:47	Alarm	Motion Start			
6	2024-05-10 07:02:47	Alarm	Motion Stop			
7	2024-05-10 06:51:57	Alarm	Motion Start			
8	2024-05-10 06:51:52	Alarm	Motion Stop			
9	2024-05-10 06:41:06	Alarm	Motion Start			
10	2024-05-10 06:41:05	Alarm	Motion Stop			
11	2024-05-10 06:30:15	Alarm	Motion Start			

<

1

2

3

4

5

6

...

8

>

20/page

Go to

1

Total

142

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.

4.6.5 Debug Mode

Debug Mode is used to record and collect the required system data, so that the technician can quickly find out and analyze the problem, and help us to improve service.

Before enabling the debug mode, you are advised to consult our technical support.

☒ Open Debug Mode

Debug Level

Ordinary

If the SD card is used as a dump device, SD card related services cannot be used

Save

Note: Once the SD card is used to collect the system data, the SD card will not be used to store snapshots and recorded files. Only when you disable debug mode and format the SD card in the storage interface (Config→System→Storage→ Management) after the device is rebooted, can the SD card be used to store snapshots and recorded files.

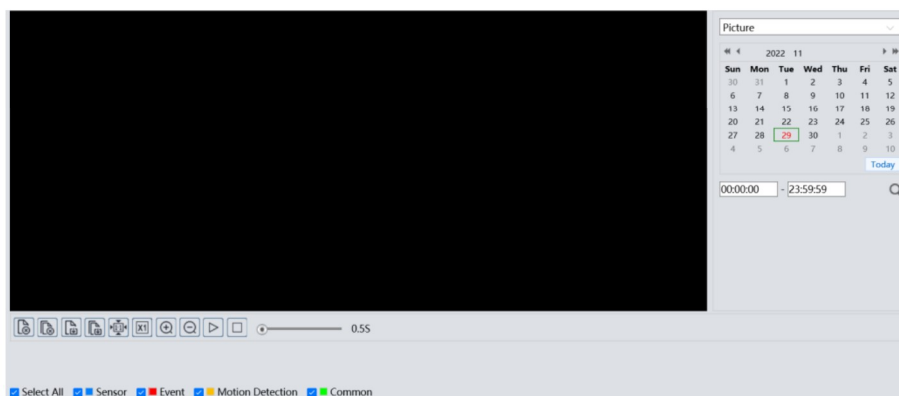
5 Search

5.1 Image Search

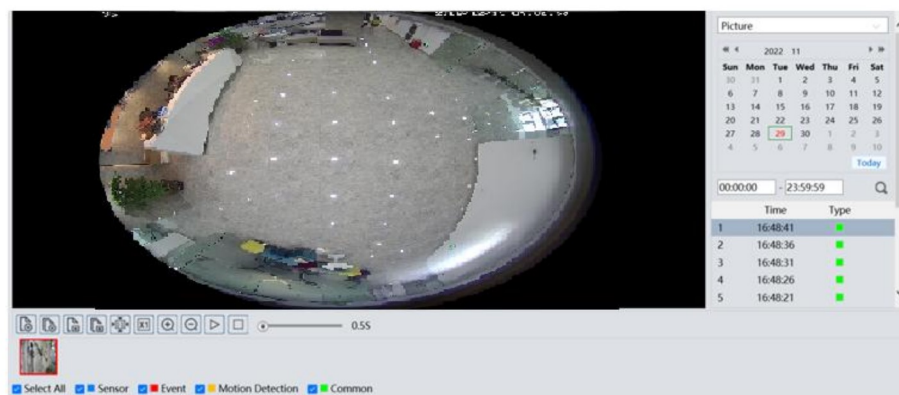
In the Setup interface, click Search to go to the interface as shown below. Images that are saved on the PC or SD card can be found here.

● SD Card Image Search

1. Choose "Picture".



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.



The descriptions of the buttons are shown as follows.

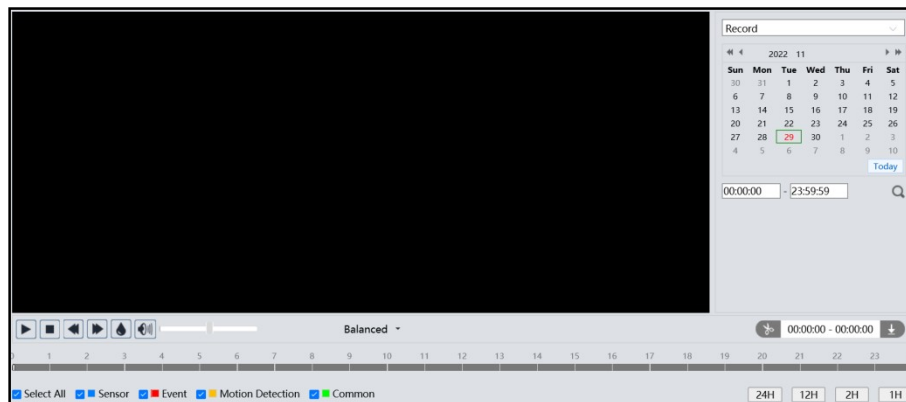
Icon	Description	Icon	Description
	Close: Select an image and click this button to close the image.		Close all: Click this button to close all images.
	Save: Click this button to select the path for saving the image on the PC.		Save all: Click this button to select the path for saving all pictures on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

Icon	Description	Icon	Description
	Zoom in: Click this button to digitally zoom in.		Zoom out: Click this button to digitally zoom out.
	Slide show play: Click this button to start the slide show mode.		Stop: Click this button to stop the slide show.
	Play speed: Play speed of the slide show.		

5.2 Video Search

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”.
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. Double click on a file name in the list to start playback.



Choose the date and the start time and end time and then click “Search” button to search the record files. Double click the record file to play the record.

Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button
	Stop button		Speed down

Icon	Description	Icon	Description
	Speed up		Watermark display
	Click it to play the next record.		Click it to play the previous record.
	Enable / disable audio; drag the slider to adjust the volume after enabling audio.		

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

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

Video clip and downloading

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

Index	Process	Record Type	Start Time	End Time	Path	Operate
1	94%	Motion Detection	2022-10-13 11:00:31	2022-10-13 11:00:48	Record	Cancel
Setting C:\Program Files\NetIPCamera\Record Clear List Close						

Click “Setting” 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

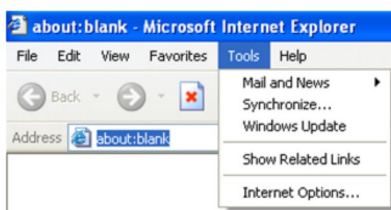
IP Scanner does not show any device.

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.

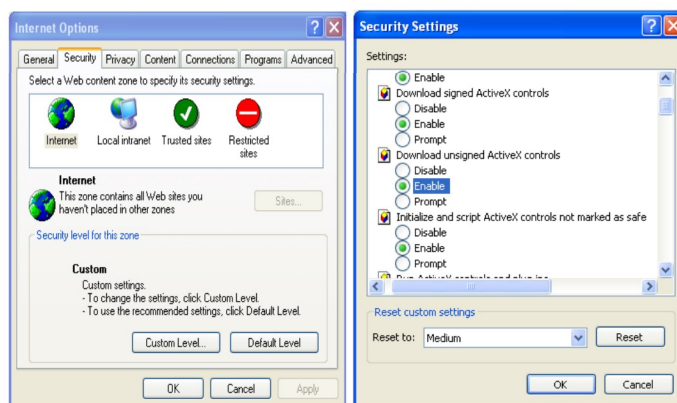
1. Open IE browser and then click Tools→Internet Options.



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: O6MDP4

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