



User Manual

6MP Panoramic Network Camera

O6MDP3N

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 only.

Please note: Do not connect two power supplying sources to the device at the same time; it may result in device damage! The product must be grounded to reduce the risk of electric shock.

Improper handling and/or installation could run the risk of fire or electrical shock.

2. Environment

Heavy stress, violent vibration or exposure to water is not allowed during transportation, storage and installation.

This product should be installed in a cool, dry place away from direct sunlight and heat sources.

Do not install the product in extreme temperature conditions.

Do not expose the camera to electromagnetic radiation. Otherwise it may result in CMOS sensor failure.

Do not block any ventilation openings.

Do not allow water and liquid intrusion into the camera.

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.....	4
4	Camera Configuration	8
4.1	System Configuration.....	8
4.1.1	System Information	8
4.1.2	Date and Time.....	8
4.1.3	Local Recording.....	9
4.1.4	Storage.....	9
4.1.5	Configuring Fisheye Parameters.....	11
4.2	Video Configuration.....	11
4.2.1	Image Configuration	11
4.2.2	Video / Audio Configuration.....	13
4.2.3	OSD Configuration	14
4.2.4	Video Mask	15
4.2.5	ROI Configuration	15
4.3	PTZ Configuration	16
4.4	Alarm Setup	16
4.4.1	Motion Detection	16
4.4.2	Other Alarms.....	17
4.4.3	Alarm In (Sensor Input).....	19
4.4.4	Alarm Out	19
4.4.5	Alarm Server	20
4.5	Network Configuration	21
4.5.1	TCP/IP.....	21
4.5.2	Port	22
4.5.3	Server Configuration.....	22
4.5.4	DDNS.....	22
4.5.5	SNMP	23
4.5.6	802.1x	24
4.5.7	RTSP	24
4.5.8	UPNP.....	25
4.5.9	Email	25
4.5.10	FTP	26
4.5.11	HTTPS.....	26
4.5.12	QoS.....	27
4.6	Security Configuration	28
4.6.1	User Admin	28
4.6.2	Online User	29
4.6.3	Block and Allow Lists.....	29
4.6.4	Security Management.....	30
4.7	Maintenance Configuration.....	30
4.7.1	Backup and Restore	30
4.7.2	Reboot	30
4.7.3	Upgrade	31
4.7.4	Operation Log	31
5	Search.....	32
5.1	Image Search	32
5.2	Video Search.....	33

5.2.1	Local Video Search	33
5.2.2	SD Card Video Search.....	34
Appendix	36
Appendix 1 Troubleshooting	36

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)
- 1/2.9" 6MP progressive scan CMOS, 360° panoramic image
- Remote viewing support via web browser, mobile APP, and CMS/VMS

Applications



Installation Recommended Distance:

Performance	Face details	Facial contour	Human movement
			
Object distance	3 m	6 m	12 m

2 Web Access and Login

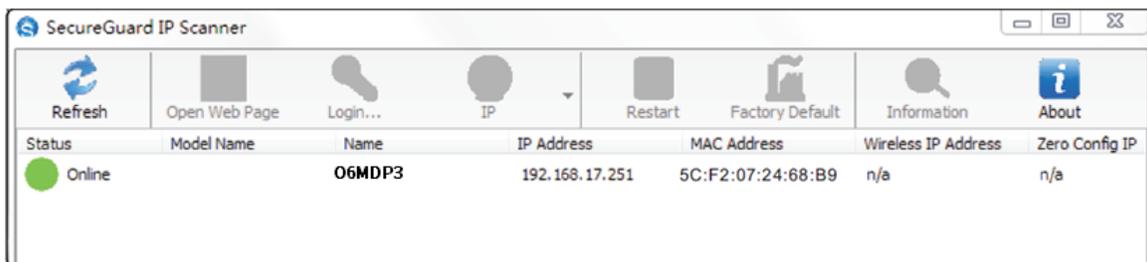
The IP camera settings can be accessed via a web browser (Internet Explorer 8 and up) through the LAN.

- Access through IP Scanner

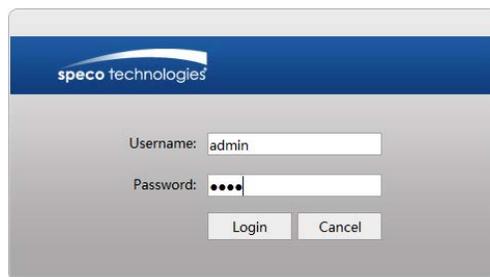
Network connection:



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



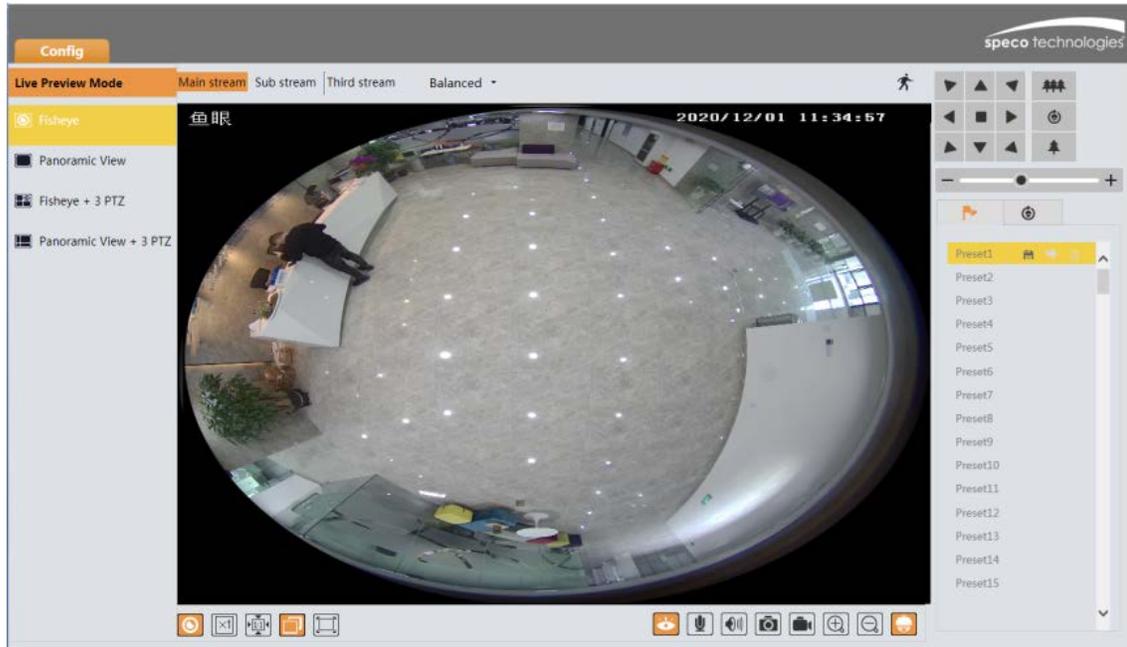
- ③ In the device list, the IP address, model number, and MAC address of each device will be listed. Select the applicable device and double click to open up the web viewer. You can also manually enter the IP address in the address bar of the web browser.



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

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.

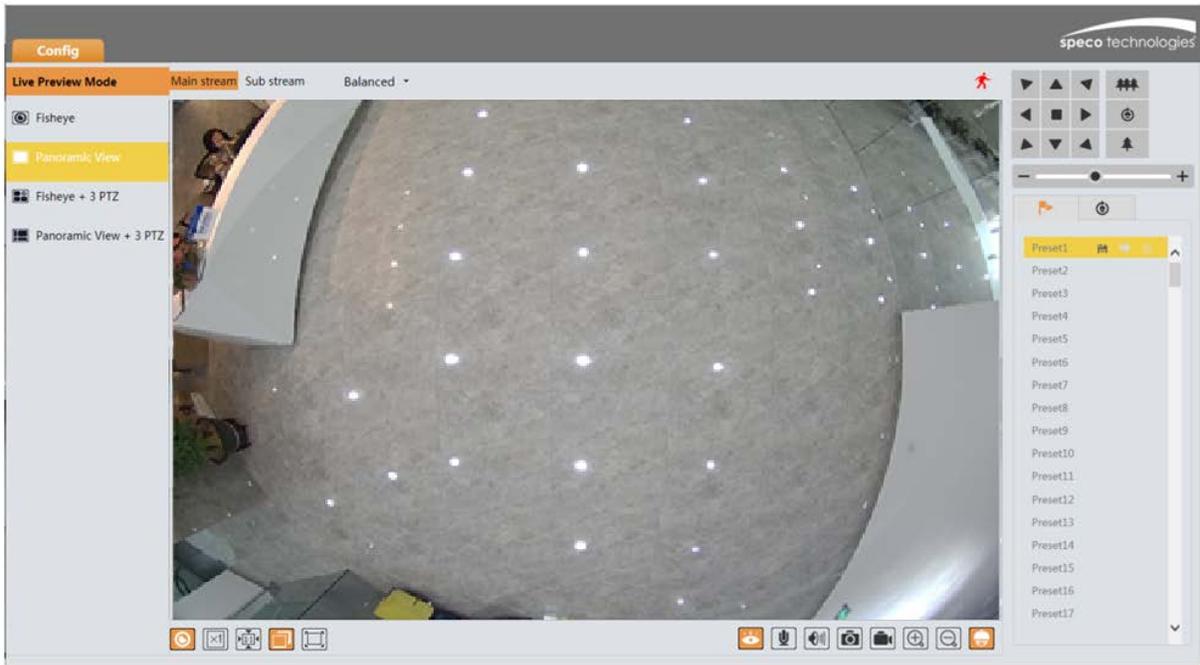
Icon	Description	Icon	Description
	Select live preview mode		Snapshot
	Original size of resolution		Start/stop local recording
	Fit (correct scale)		Zoom in (for motorized models)
	Auto (fill the window)		Zoom out (for motorized models)
	Full screen (show video only)		PTZ control
	Start/stop live view		Sensor alarm indicator
	Start/stop two-way audio		Motion alarm indicator
	Enable/disable audio		

- 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



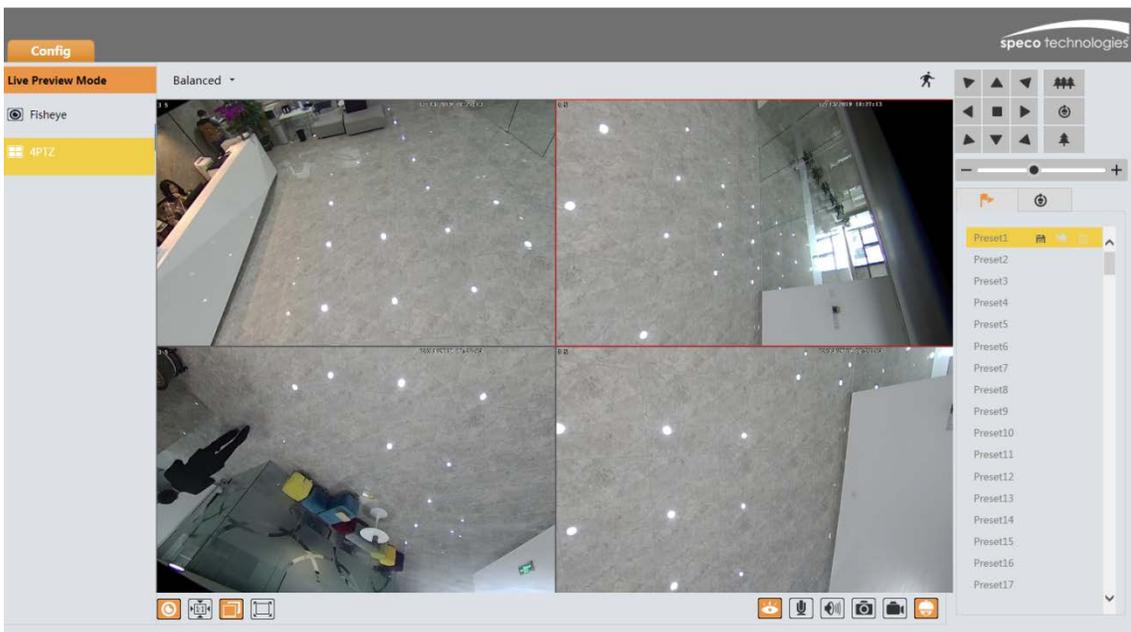
Fisheye+ 3PTZ view mode



Panoramic + 3PTZ view mode



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



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.

Click  to display the control panel. The descriptions of the 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 preset and click  to call the preset. Select and set the preset and then click  to save the position of the preset. Select the set preset and click  to delete it.

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	O6MDP3N
Product Model	O6MDP3N
Brand	Speco
Software Version	4.2.1.0
Software Build Date	2021-12-20
Kernel Version	20
Hardware Version	1.3-1516805
Onvif Version	20.06
OCX Version	2.0.3.4
MAC	5C:F2:07:24:68:B9

4.1.2 Date and Time

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

Zone Date and Time

Zone

DST

Auto DST

Manual DST

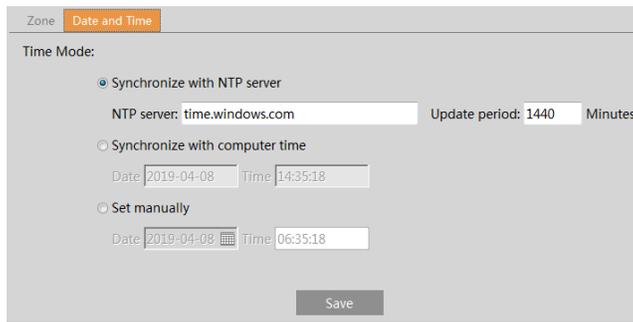
Start Time Hour

End Time Hour

Time Offset

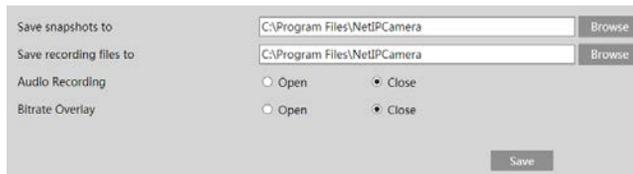
Select the applicable time zone and enable / disable DST as needed.

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



4.1.3 Local Recording

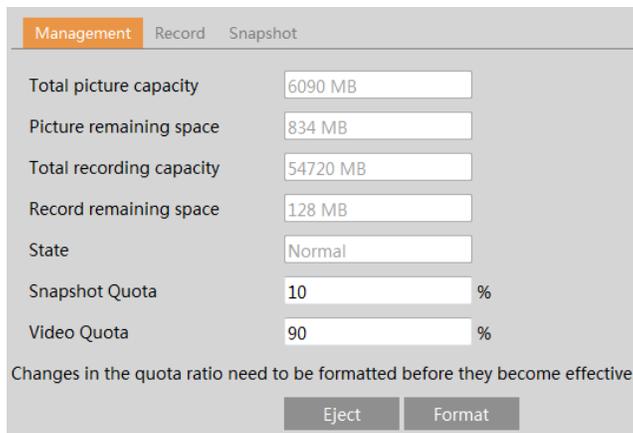
Go to System→Local Recording to set up the storage path of captured pictures and recorded videos on the local PC. There is also an option to enable or disable the bitrate display in the recorded files.



Additionally, the snapshots triggered by smart events (including face detection, line crossing detection and 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.

Management	Record	Snapshot
Record Parameters		
Record Stream	Main stream ▼	
Pre Record Time	No Pre Record ▼ (H264,H265,MJPEG)	
Cycle Write	Yes ▼	

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

Pre Record Time: Set the time to record before the actual recording begins.

3. Set schedule recording. Check “Enable Schedule Record” and set the schedule.

Timing

Enable Schedule Record Erase Add

Week Schedule

Sun.	00:00-24:00	Manual Input
Mon.	00:00-24:00	Manual Input
Tue.	00:00-24:00	Manual Input
Wed.	00:00-24:00	Manual Input
Thu.	00:00-24:00	Manual Input
Fri.	00:00-24:00	Manual Input
Sat.	00:00-24:00	Manual Input

Holiday Schedule

Date:

00:00-24:00	Manual Input
-------------	--------------

Weekly schedule

Set the alarm time from Monday to Sunday for a single week. Each day is divided in one hour increments. Green means scheduled. Blank means unscheduled.

“Add”: Add the schedule for a special day. Drag the mouse to set the time on the timeline.

“Erase”: Delete the schedule. Drag the mouse to erase the time on the timeline.

Manual Input: Click it for a specific day to enter specific start and end times. This adds more granularities (minutes).

Day schedule

Set the alarm time for alarm a special day, such as a holiday.

Note: Holiday schedule takes priority over weekly schedule.

● Snapshot Settings

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

Management Record **Snapshot**

Snapshot Parameters

Image Format JPEG

Resolution 704x480

Image Quality Low

Event Trigger

Snapshot Interval 1 Second

Snapshot Quantity 5

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

Snapshot Quantity: The number you set here is the maximum quantity of snapshots. The actual quantity of snapshots may be less than this number. Supposing the occurrence time of an alarm event is less than the time of capturing pictures, the actual quantity of snapshots is less than the set quantity of snapshots.

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

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 or 4 PTZ

Installation Method Ceiling

Notice: To modify installation method will affect live preview, image effect, PTZ mode and Preset, etc.

Save

Stream mode: Fisheye + Panoramic view + 3PTZ and Fisheye or 4PTZ mode are optional.

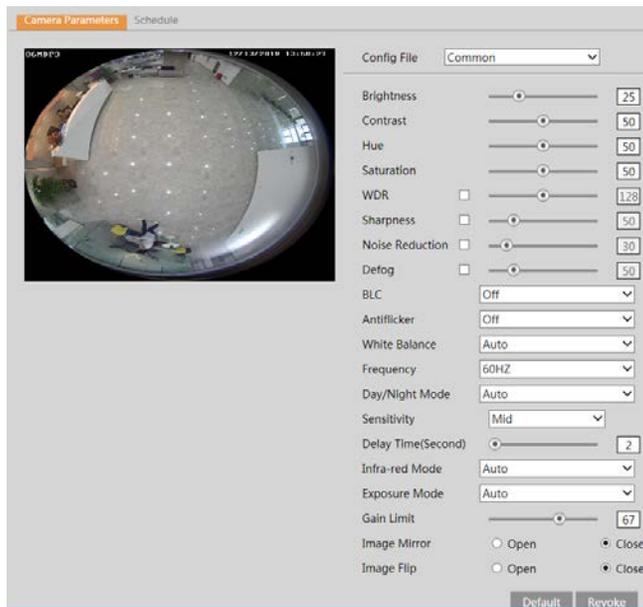
Installation method: ceiling and desktop are optional. Please select the installation mode according to the actual way of installation.

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.

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

Recording will be stopped for a few seconds while the mode is changing from non-WDR to WDR mode.

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

DNR: Digital noise reduction.

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

Backlight Compensation (BLC):

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

Antiflicker:

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

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

Frequency: 50Hz and 60Hz can be optional.

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

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

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

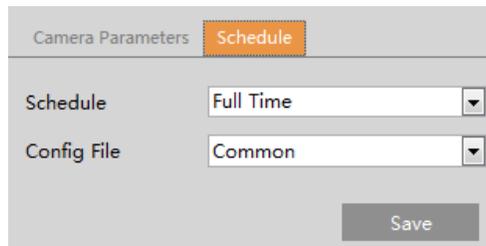
Gain Limit: The higher the value is, the brighter the image is.

Image Mirror: Turn the current video image horizontally.

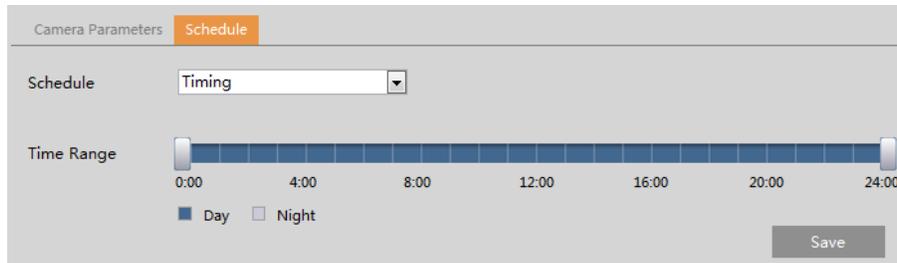
Image Flip: Turn the current video image vertically.

Schedule Settings of Image Parameters:

Click the "Schedule" tab as shown below.



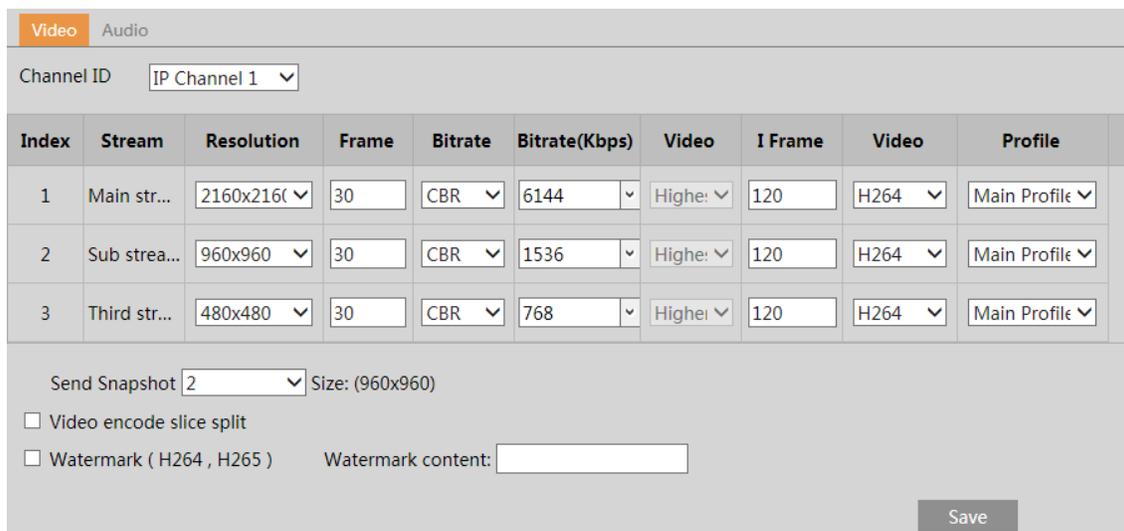
Set full time schedule for common, day or night mode and specified time schedule for day and night. Choose “Timing” in the drop-down box of schedule as shown below.



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



You can select streams for different channels.

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, 2 streams can be set. Please set them according to the actual network condition.

IP Channel 3/4/5: PTZ view channel, 2 streams 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 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.

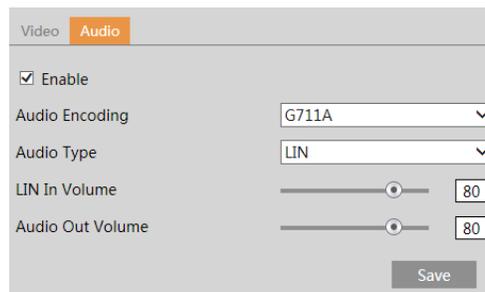
Profile: For H.264. Baseline, main and high profiles are selectable.

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.

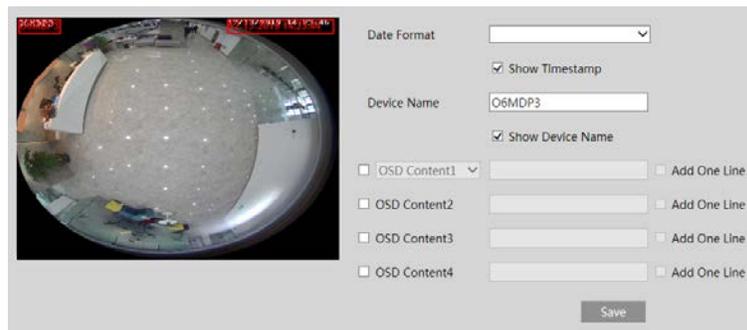


Audio Encoding: G711A and G711U are selectable.

Audio Type: LIN and MIC. Additionally, audio input/output volume can be set here.

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.

Picture Overlap Settings:

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

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.

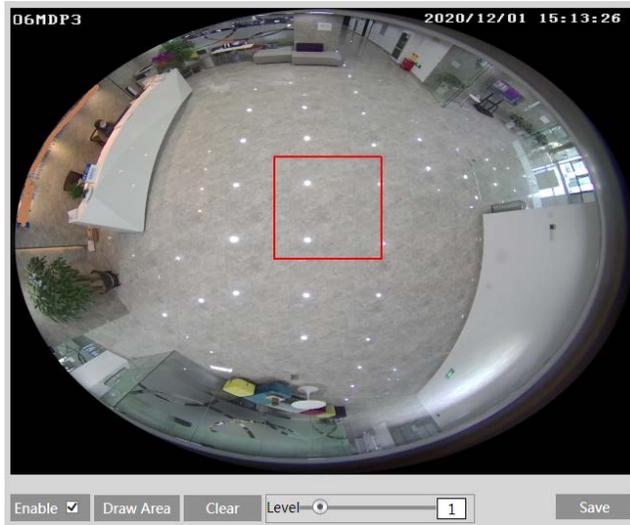


To clear the video mask:

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 PTZ Configuration

Go to PTZ→Protocol interface. The PTZ of this camera can be controlled by the keyboard. Connect the keyboard and the camera through RS485 interface and then set the corresponding protocol and baud-rate in the camera and keyboard.

Here the protocol and baud-rate must be the same with these of the keyboard.

Address: 1; you can control PTZ channel 1 by using this address in the keyboard.

Address: 2; you can control PTZ channel 2 by using this address in the keyboard.

.....

4.4 Alarm Setup

4.4.1 Motion Detection

Go to Event Setup→Motion Detection to set motion detection alarm.

Alarm Config
Area and Sensitivity
Schedule

Enable

Alarm Holding Time v

Trigger Alarm Out

Alarm Out

Trigger Snap

Trigger SD Recording

Trigger Email

Trigger FTP

Save

1. Check “Enable” check box to activate motion based alarms. If unchecked, the camera will not send out any signals to trigger motion-based recording to the NVR or CMS, even if there is motion in the video.

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

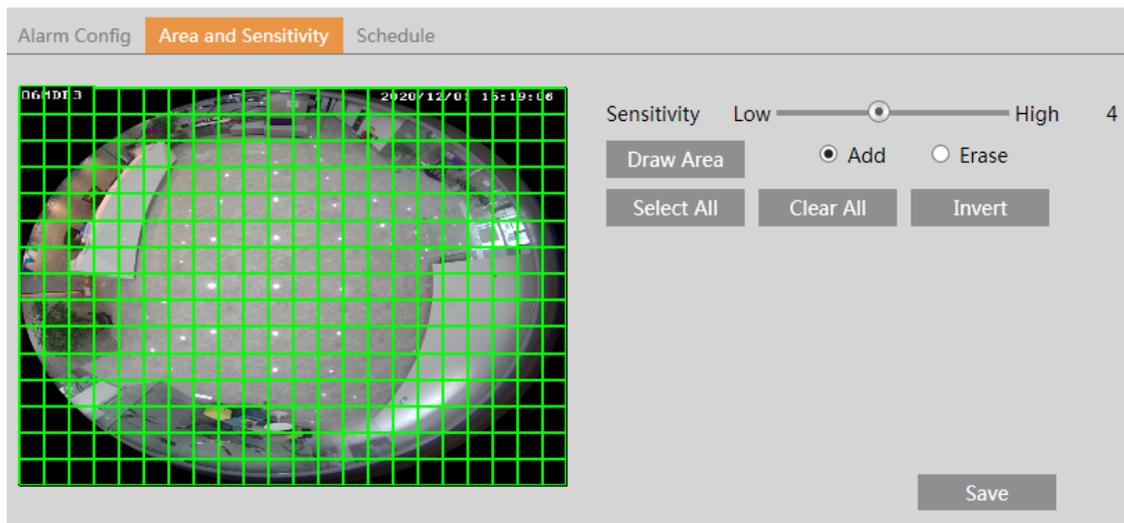
Trigger Snap: If selected, the system will capture images on motion detection and save the images on an SD card.

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

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

Trigger FTP: If “Trigger FTP” 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.

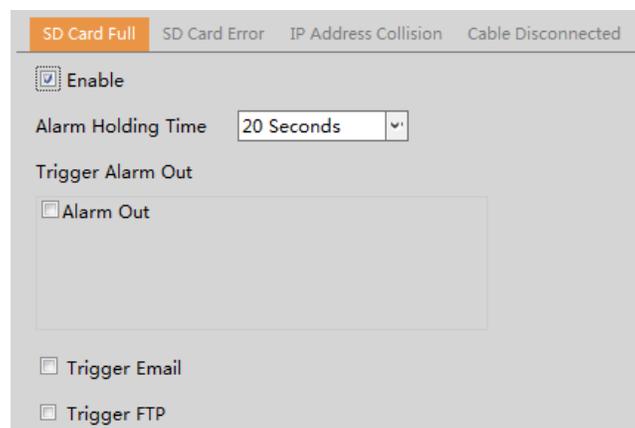
After that, click the “Save” to save the settings. “Clear All” can be used to clear out the entire motion zone.

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](#)).

4.4.2 Other Alarms

● SD Card Full

1. Go to Event Setup→Anomaly→SD Card Full.

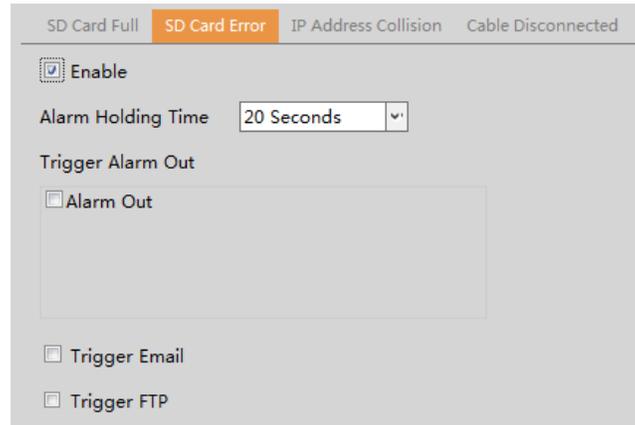


2. Click “Enable” and set the alarm holding time.
3. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection chapter for details.

- **SD Card Error**

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

1. Go to Event Setup→Anomaly→SD Card Error as shown below.

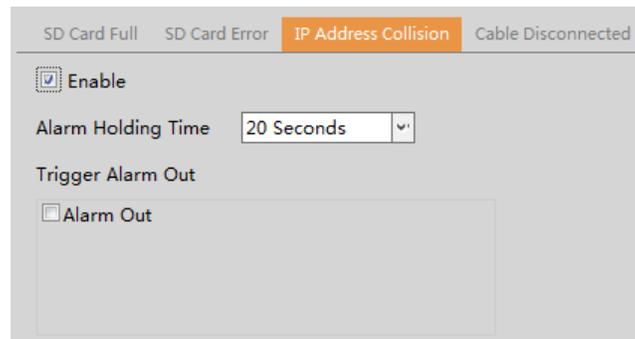


The screenshot shows the configuration page for 'SD Card Error'. At the top, there are four tabs: 'SD Card Full', 'SD Card Error' (which is selected and highlighted in orange), 'IP Address Collision', and 'Cable Disconnected'. Below the tabs, there is a section for 'SD Card Error' configuration. It includes an 'Enable' checkbox which is checked. Below that is an 'Alarm Holding Time' dropdown menu set to '20 Seconds'. Underneath is a 'Trigger Alarm Out' section with an 'Alarm Out' checkbox which is unchecked. At the bottom, there are two more checkboxes: 'Trigger Email' and 'Trigger FTP', both of which are unchecked.

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 Event Setup→Anomaly→IP Address Collision as shown below.



The screenshot shows the configuration page for 'IP Address Collision'. At the top, there are four tabs: 'SD Card Full', 'SD Card Error', 'IP Address Collision' (which is selected and highlighted in orange), and 'Cable Disconnected'. Below the tabs, there is a section for 'IP Address Collision' configuration. It includes an 'Enable' checkbox which is checked. Below that is an 'Alarm Holding Time' dropdown menu set to '20 Seconds'. Underneath is a 'Trigger Alarm Out' section with an 'Alarm Out' checkbox which is unchecked. At the bottom, there are two more checkboxes: 'Trigger Email' and 'Trigger FTP', both of which are unchecked.

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 Event Setup→Anomaly→Cable Disconnected as shown below.

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.

4.4.3 Alarm In (Sensor Input)

This function is only available for some models. To set sensor alarm (alarm in): Go to Event Setup→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](#)).

4.4.4 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.

The screenshot shows a configuration window for 'Alarm Out Mode'. The 'Alarm Out Mode' dropdown menu is set to 'Manual Operation'. Below this, there are two buttons: 'Open' and 'Close'. At the bottom right, there is a 'Save' button.

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.

The screenshot shows a configuration window for 'Alarm Out Mode'. The 'Alarm Out Mode' dropdown menu is set to 'Day/night switch linkage'. Below this, there are two dropdown menus: 'Day' and 'Night', both set to 'Close'. At the bottom right, there is a 'Save' button.

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.

The screenshot shows a configuration window for 'Alarm Out Mode'. The 'Alarm Out Mode' dropdown menu is set to 'Timing'. Below this, there are two radio buttons: 'Erase' and 'Add', with 'Add' selected. A timeline is shown with a range from 0 to 24 hours. A blue bar highlights the time range from 02:00 to 13:15. The label 'Manual Input' is visible at the end of the timeline. At the bottom right, there is a 'Save' button.

4.4.5 Alarm Server

Go to Alarm→Alarm Server interface as shown below.

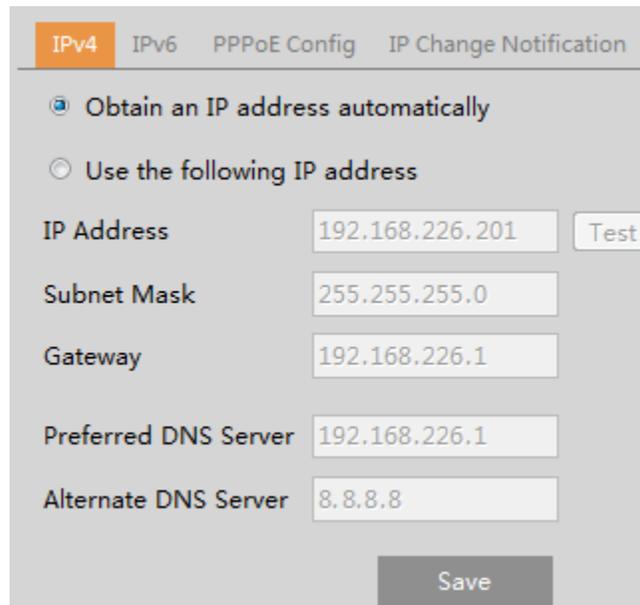
Set the server address, port, heartbeat and heartbeat interval. When an alarm occurs, the camera will transfer the alarm event to the alarm server. If an alarm server is not needed, there is no need to configure this section.

The screenshot shows the 'Alarm Server' configuration interface. The breadcrumb path is 'Setup > Event Setup > Alarm Server'. The fields are: 'Server Address' (text input), 'Port' (text input with value 0), 'Heartbeat' (dropdown menu with value Disable), and 'Heartbeat interval' (text input with value 30 and unit Second). At the bottom, there is an 'OK' button.

4.5 Network Configuration

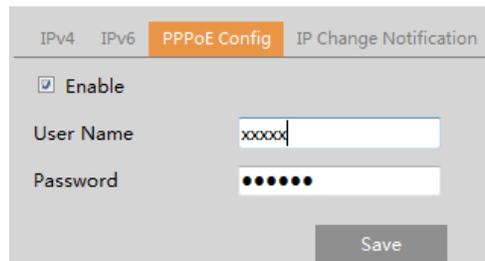
4.5.1 TCP/IP

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.

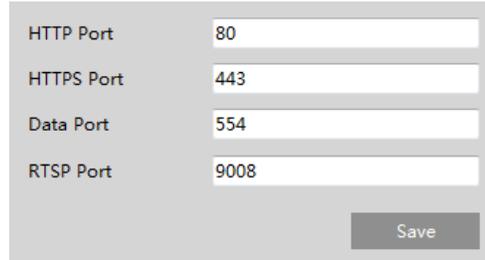


Trigger Email: when the IP address of the device is changed, the new IP address will be sent to the email address that has been set up.

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→Advanced interface as shown below. HTTP port, Data port and RTSP port can be set.



A screenshot of a web interface for configuring network ports. It features four input fields: 'HTTP Port' with the value '80', 'HTTPS Port' with '443', 'Data Port' with '554', and 'RTSP Port' with '9008'. A 'Save' button is located at the bottom right of the form.

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

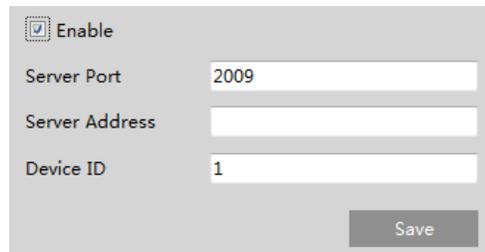
HTTPS Port: The default HTTPS port is 443. It can be changed to any port which is not occupied.

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.

4.5.3 Server Configuration

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



A screenshot of a web interface for server configuration. It includes a checked 'Enable' checkbox, a 'Server Port' field with '2009', an empty 'Server Address' field, and a 'Device ID' field with '1'. A 'Save' button is at the bottom right.

1. Check “Enable”.

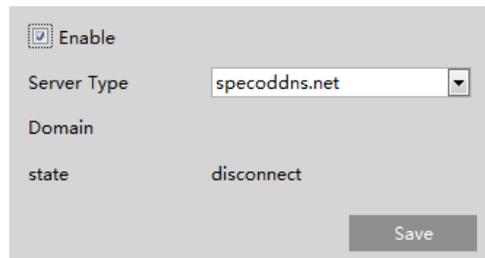
2. Check the IP address and port of the transfer media server in the VMS. Then enable the auto report in the VMS when adding a new device. Next, enter the remaining information of the device in the VMS. After that, the system will automatically allot a device ID. Please check it in the VMS.

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 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.



A screenshot of a web interface for DDNS configuration. It features a checked 'Enable' checkbox, a 'Server Type' dropdown menu with 'specoddns.net' selected, an empty 'Domain' field, and a 'state' field with 'disconnect'. A 'Save' button is at the bottom right.

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

<input checked="" type="checkbox"/> Enable	
Server Type	specoddns.net
Domain	speco008954.specoddns.net
State	connect(210.21.229.138)
<input type="button" value="Save"/>	

4.5.5 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.

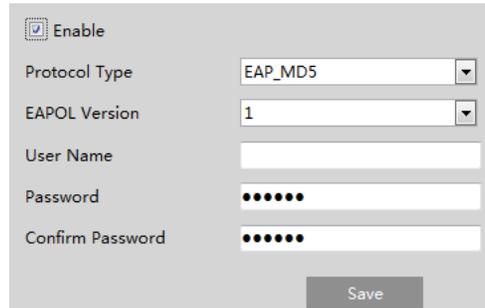
SNMP v1/v2	
<input type="checkbox"/> Enable SNMPv1	
<input type="checkbox"/> Enable SNMPv2	
Read SNMP Community	public
Write SNMP Community	private
Trap Address	192.168.226.201
Trap Port	162
Trap community	public
SNMP v3	
<input type="checkbox"/> Enable SNMPv3	
Read User Name	public
Security Level	auth, priv
Authentication Algorithm	<input checked="" type="radio"/> MDS <input type="radio"/> SHA
Authentication Password	••••••••
Private-key Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES
Private-key Algorithm	••••••••
Write User Name	private
Security Level	auth, priv
Authentication Algorithm	<input checked="" type="radio"/> MDS <input type="radio"/> SHA
Authentication Password	••••••••
Private-key Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES
Private-key Algorithm	••••••••
Other Settings	
SNMP Port	161
<input type="button" value="Save"/>	

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.

4.5.6 802.1x

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.



Enable

Protocol Type: EAP_MD5

EAPOL Version: 1

User Name: _____

Password: ●●●●●●

Confirm Password: ●●●●●●

Save

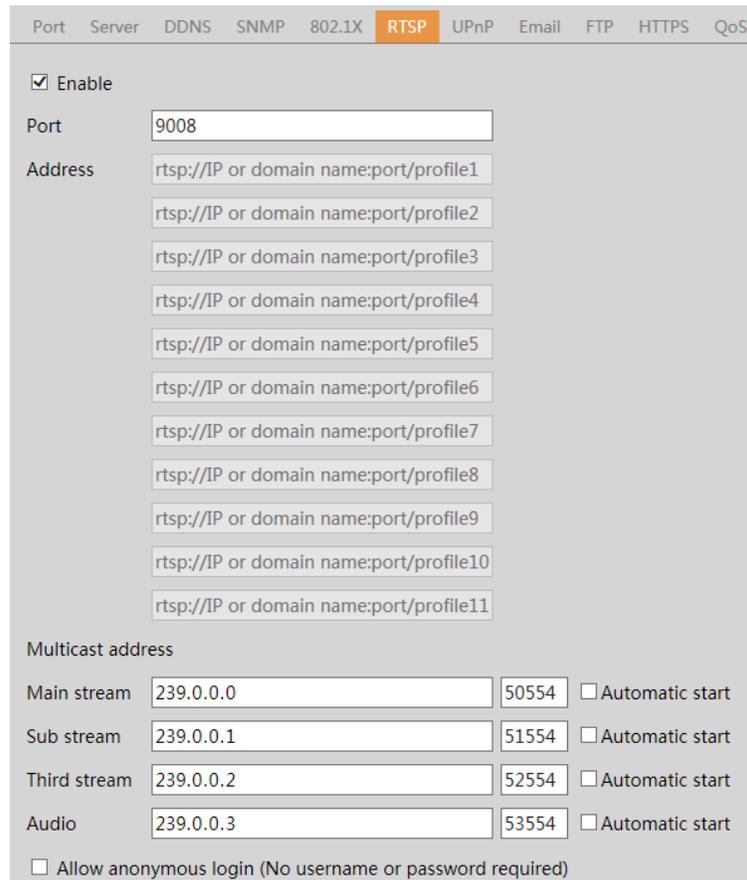
To use this function, the camera shall be connected to a switch supporting 802.1x protocol. The switch can be reckoned as an authentication system to identify the device in a local network. If the camera connected to the network interface of the switch has passed the authentication of the switch, it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

4.5.7 RTSP

Go to Network→RTSP.



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

Enable

Port: 9008

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

rtsp://IP or domain name:port/profile2

rtsp://IP or domain name:port/profile3

rtsp://IP or domain name:port/profile4

rtsp://IP or domain name:port/profile5

rtsp://IP or domain name:port/profile6

rtsp://IP or domain name:port/profile7

rtsp://IP or domain name:port/profile8

rtsp://IP or domain name:port/profile9

rtsp://IP or domain name:port/profile10

rtsp://IP or domain name:port/profile11

Multicast address

Main stream: 239.0.0.0 50554 Automatic start

Sub stream: 239.0.0.1 51554 Automatic start

Third stream: 239.0.0.2 52554 Automatic start

Audio: 239.0.0.3 53554 Automatic start

Allow anonymous login (No username or password required)

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.

4.5.8 UPNP

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

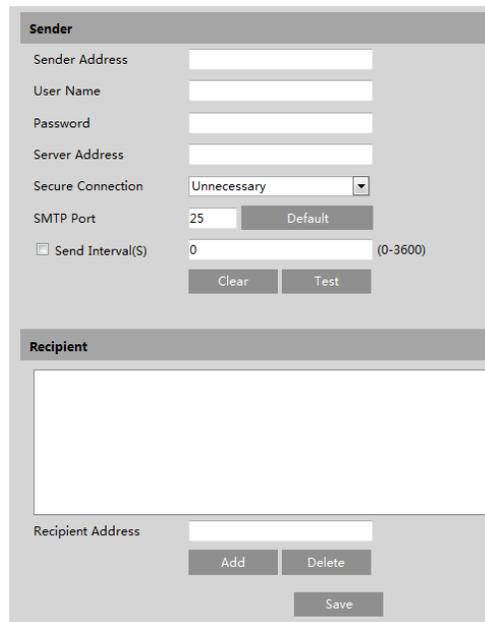
Go to Network→UPnP. Enable UPnP and then enter UPnP name.



4.5.9 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 Address: sender’s e-mail address.

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

Server Address: The SMTP IP address or host name.

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

SMTP Port: The SMTP port.

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

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

Recipient Address: receiver’s e-mail address.

4.5.10 FTP

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

Go to Network→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.

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

4.5.11 HTTPS

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

Go to Network→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.

4.5.12 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: The range is from 0 to 63.

Alarm DSCP: The range is from 0 to 63.

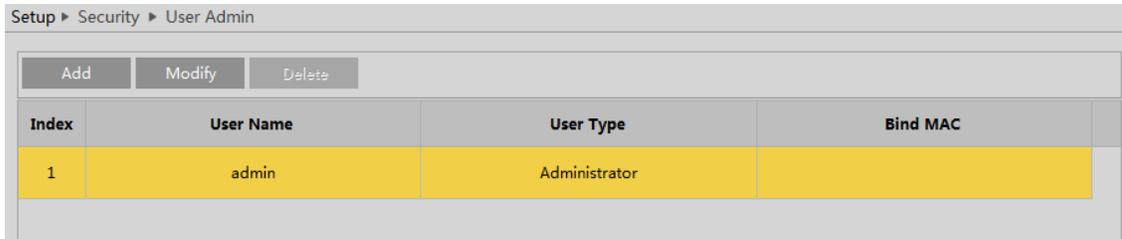
Manager DSCP: The range is from 0 to 63.

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.



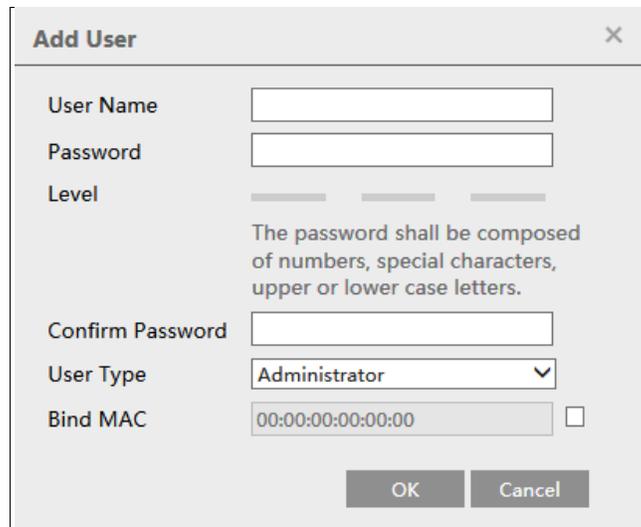
Setup ▶ Security ▶ User Admin

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 [X]

User Name

Password

Level

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

Confirm Password

User Type

Bind MAC

OK Cancel

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

3. Enter letters or numbers in “Password” and “Confirm Password” textbox.

4. Choose the user type. Administrator has all permissions. Normal user can only view the live video. Advanced user has the same permissions as an Administrator except for; user, backup settings, factory reset, and upgrading the firmware.

5. Enter the MAC address of the PC in “Bind MAC” textbox.

If this option is enabled, only the PC with the specified MAC address can access the camera for that user.

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

Modify user:

1. Select a user to modify password and MAC address if necessary in the user configuration list box.

2. The “Edit user” dialog box pops up by clicking the “Modify” button.

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

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

Delete user:

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

Note: The default administrator account cannot be deleted.

4.6.2 Online User

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

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

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

4.6.3 Block and Allow Lists

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

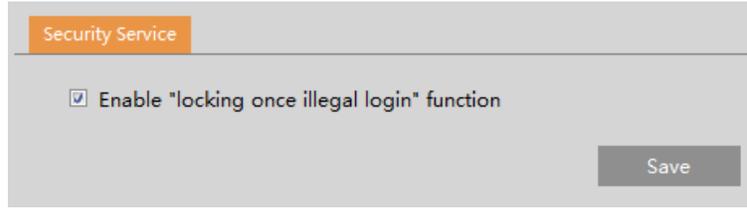
The setup steps are as follows:

Check the “Enable address filtering” check box.

Select “Block/Allow the following address”, IPV4/IPV6/MAC and then enter IP address or MAC address in the address box and click the “Add” button.

4.6.4 Security Management

Go to Security→Security Management as shown below.

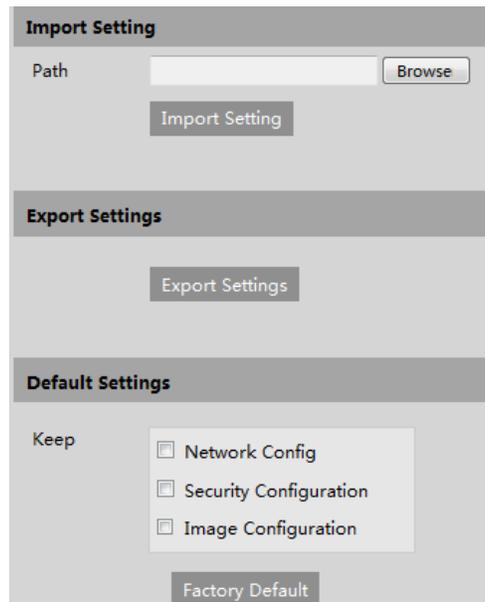


In order to prevent against malicious password unlocking, “locking once illegal login” function can be enabled here. If this function is enabled, login failure after trying six times will make the login interface locked. The camera can be logged in again after a half hour or after the camera reboots.

4.7 Maintenance Configuration

4.7.1 Backup and Restore

Go to Maintenance→Backup & Restore.



- **Import & Export Settings**

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

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

- **Default Settings**

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

4.7.2 Reboot

Go to Maintenance→Reboot.

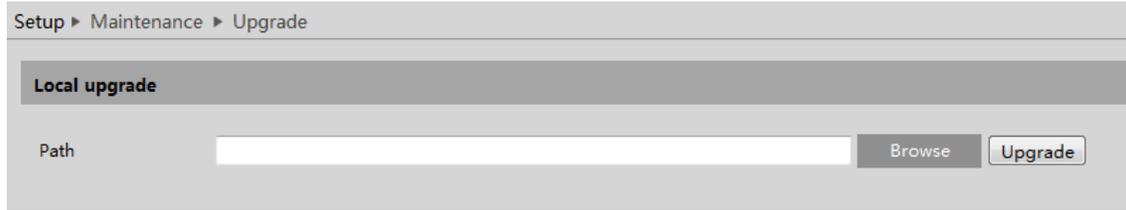
Click the “Reboot” button to reboot the device.

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.



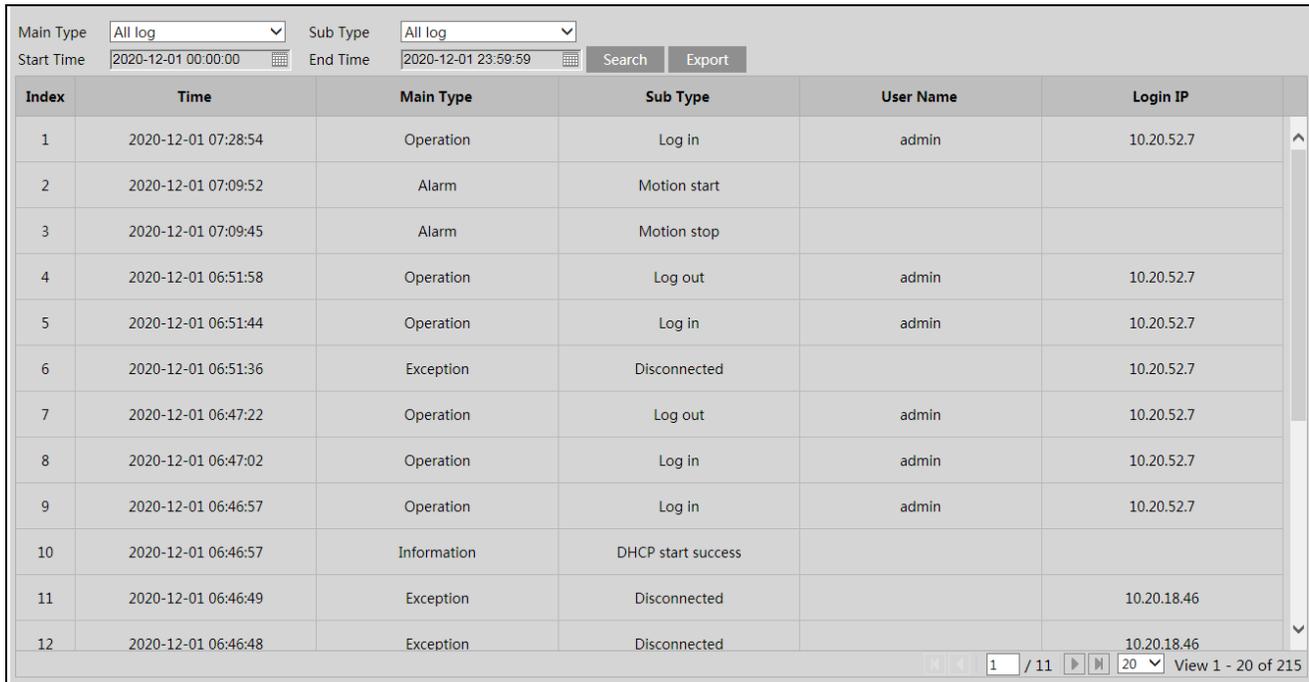
1. Click the “Browse” button to select the save path of the upgrade file
2. Click the “Upgrade” button to start upgrading the firmware.
3. The device will restart automatically

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.



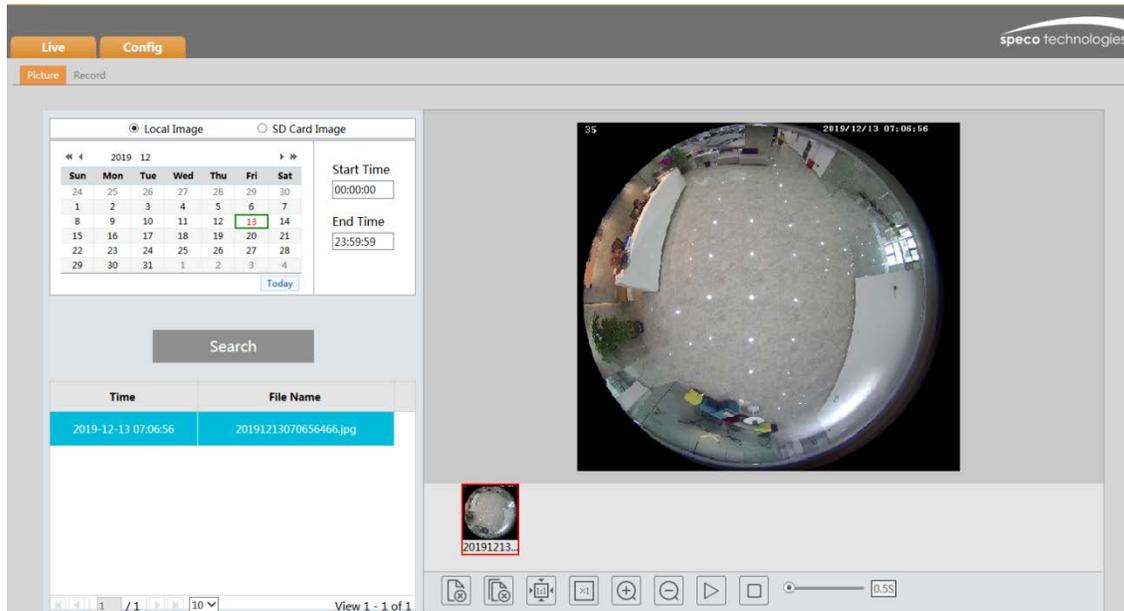
Index	Time	Main Type	Sub Type	User Name	Login IP
1	2020-12-01 07:28:54	Operation	Log in	admin	10.20.52.7
2	2020-12-01 07:09:52	Alarm	Motion start		
3	2020-12-01 07:09:45	Alarm	Motion stop		
4	2020-12-01 06:51:58	Operation	Log out	admin	10.20.52.7
5	2020-12-01 06:51:44	Operation	Log in	admin	10.20.52.7
6	2020-12-01 06:51:36	Exception	Disconnected		10.20.52.7
7	2020-12-01 06:47:22	Operation	Log out	admin	10.20.52.7
8	2020-12-01 06:47:02	Operation	Log in	admin	10.20.52.7
9	2020-12-01 06:46:57	Operation	Log in	admin	10.20.52.7
10	2020-12-01 06:46:57	Information	DHCP start success		
11	2020-12-01 06:46:49	Exception	Disconnected		10.20.18.46
12	2020-12-01 06:46:48	Exception	Disconnected		10.20.18.46

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.

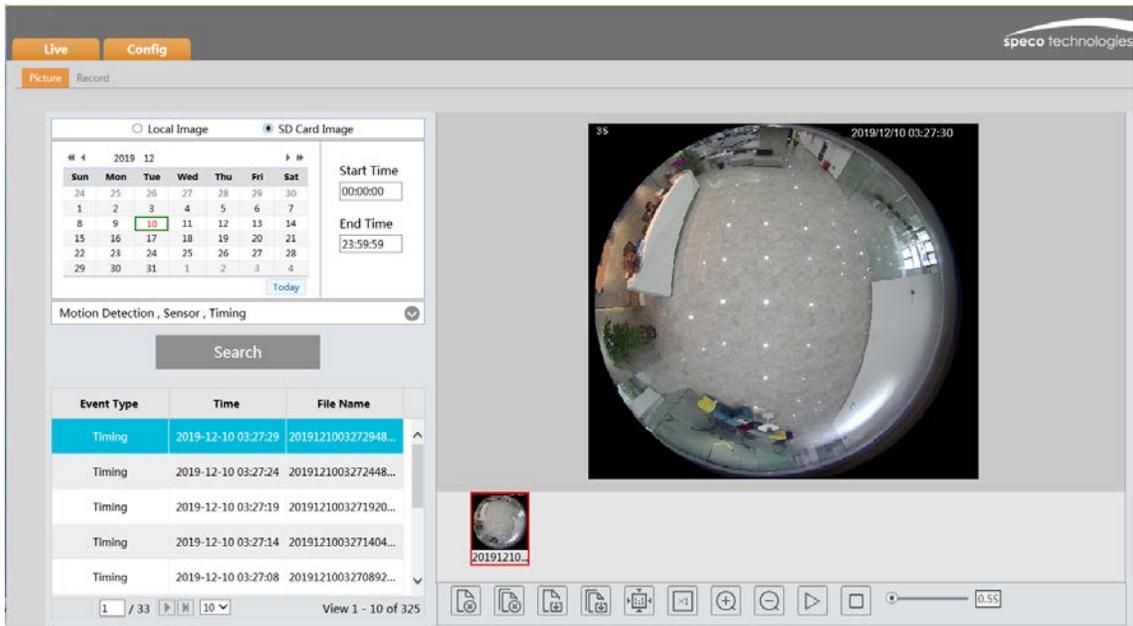


Local Image Search

1. Set time: Select date and choose the start and end time in the top left corner.
2. Click "Search" button to search the pictures.
3. Click a file name in the list to view captured pictures as shown above.

SD Card Image Search

1. Set time: Select date and choose the start and end time in the top left corner.
2. Check events.
3. Click "Search" button to search the pictures.
4. Click a file name in the list to view captured pictures as shown below.
4. Double click a file name in the list to view the captured photos as shown above.



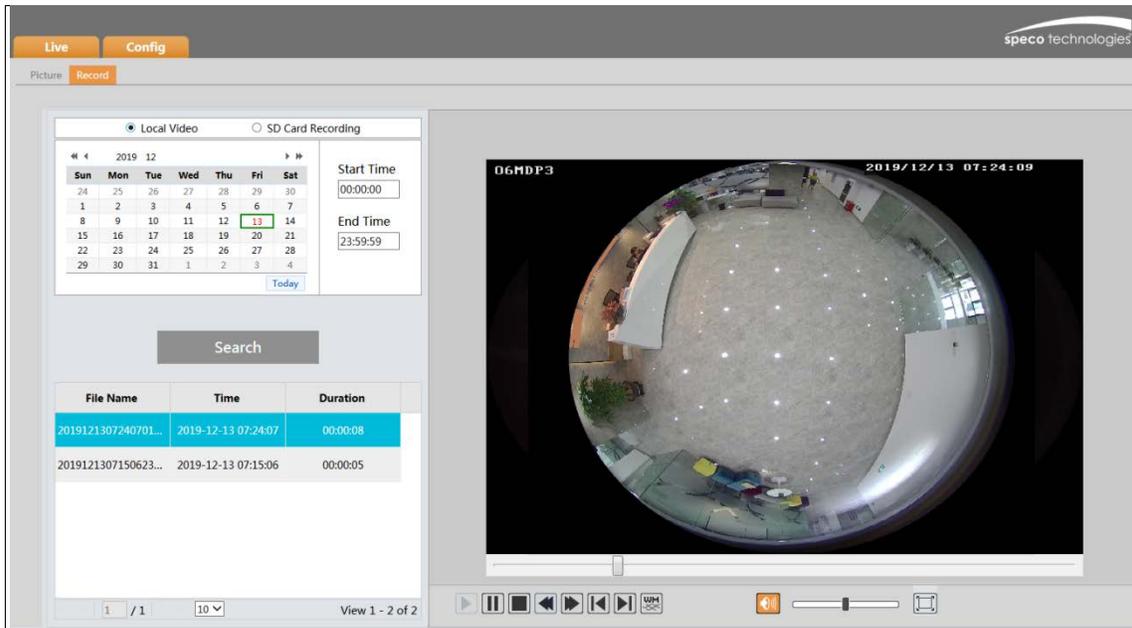
The descriptions of the buttons are shown as follows.

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

5.2 Video Search

5.2.1 Local Video Search

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



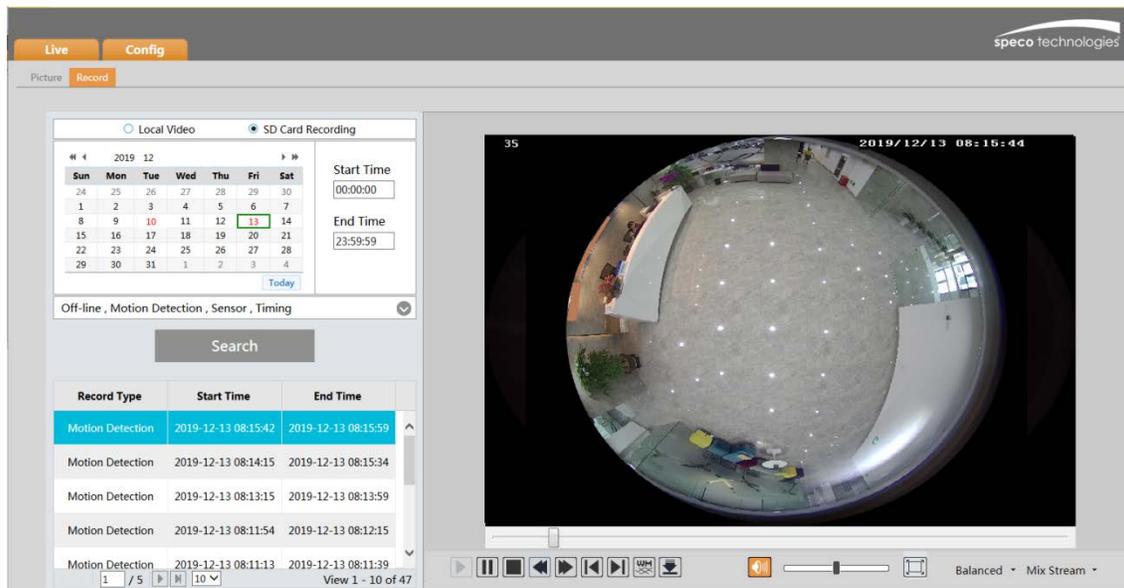
Choose the date and the start time and end time and then click “Search” button to search the record files. Double click the record file to play the record.

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

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.

Choose “Record” — “SD Card Recording”.



1. Set the date and the start and end time, select the record type and then click “Search” button to search the record.

2. Double click the searched file name to play the record.

Please refer to Local Video Search for the descriptions of the buttons on the playback interface.

Click  button to download the record saved in the SD card.

Appendix

Appendix 1 Troubleshooting

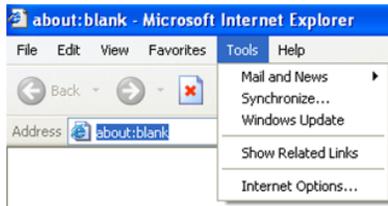
IP Scanner does not show any device.

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.

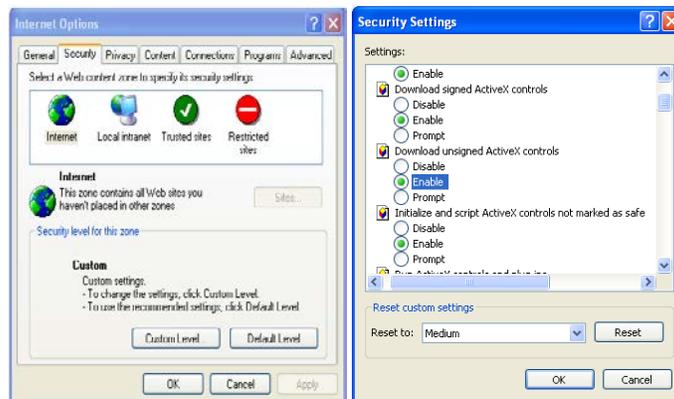
1. Open IE browser and then click Tools→Internet Options.



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:O6MDP3N

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