



User Manual

O4KT1/O8KT1(B)

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

1. Electrical safety

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

2. Environment

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

3. Operation and Daily Maintenance

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

Warning

This camera should be installed by qualified personnel only.
All the examination and repair work should be done by qualified personnel.
Any unauthorized changes or modifications could void the warranty.
This device may potentially trigger seizures for people with photosensitive epilepsy.
This device may emit loud audible alarms, check your local laws before enabling audio.

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

1	Introduction.....	2
2	Web Access and Login.....	3
3	Live View.....	5
4	Camera Configuration	7
4.1	System Configuration	7
4.1.1	System Information.....	7
4.1.2	Date and Time.....	7
4.1.3	Local Recording.....	7
4.1.4	Storage	8
4.2	Video Configuration	9
4.2.1	Image Configuration.....	10
4.2.2	Video / Audio Configuration.....	11
4.2.3	OSD Configuration.....	13
4.2.4	Video Mask	13
4.2.5	ROI Configuration.....	14
4.2.6	Smart Supplement Light Configuration	15
4.3	Alarm Setup	16
4.3.1	Motion Detection.....	16
4.3.2	Exception Alarm.....	17
4.3.3	Alarm Server	18
4.3.4	Light Alarm.....	18
4.3.5	Disarming.....	18
4.4	Analytics Configuration	19
4.4.1	Line Crossing	19
4.4.2	Region Intrusion	22
4.5	Network Configuration	23
4.5.1	TCP/IP	23
4.5.2	Port.....	23
4.5.3	Server Configuration	24
4.5.4	Onvif.....	24
4.5.5	DDNS	25
4.5.6	802.1x.....	25
4.5.7	RTSP.....	26
4.5.8	HTTP Notification	26
4.5.9	NAT.....	28
4.5.10	QoS.....	28
4.6	Security Configuration.....	29
4.6.1	User	29
4.6.2	Online User	30
4.6.3	Block and Allow Lists	30
4.6.4	Security Management	31
4.7	Maintenance Configuration.....	32
4.7.1	Backup and Restore.....	32
4.7.2	Reboot	33
4.7.3	Upgrade	33
4.7.4	Operation Log	34
4.3.6	Serial Output.....	34
4.3.7	Maintenance Information.....	34
5	Search	35
5.4	Image Search.....	35



5.5	Video Search	36
Appendix		38
Appendix 1 Troubleshooting		38

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)
- Integrated IR LEDs for clear vision in low light
- IP67 rated for outdoor installations
- Remote viewing support via web browser, mobile APP, and CMS/VMS

Applications



2 Web Access and Login

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

Available web browser: Firefox/Edge/Safari/Google Chrome

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

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

Installing the plug-in will display more functions of the camera.

Connect IP-Cam via LAN or WAN. Here only take plug-in required browsers for example. The details are as follows:

- 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 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 login interface for Speco Technologies. It features a blue header with the 'speco technologies' logo. Below the header, there are input fields for 'Name' and 'Password'. The 'Name' field has a placeholder 'Name'. The 'Password' field has a placeholder 'Please enter password' and a link for 'Forgot Password?'. At the bottom, there are 'Login' and 'Cancel' buttons.

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

A dialog box titled 'Please change the default password'. It contains a checkbox labeled 'Match Onvif Password' which is checked. Below this, there are input fields for 'Old Password', 'New Password', and 'Confirm Password'. A note states: 'The password can be composed of numbers, special characters, upper or lower case letters.' At the bottom, 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. By default, the ONVIF password will match the admin password that you set. Should you wish to change the ONVIF password to a different password than your admin password, go to the ONVIF section to change the password. (**Config→Network→Ports/Connections→Onvif**)

The screenshot displays a web interface for ONVIF configuration. At the top, a navigation bar includes tabs for Port, Server, Onvif (selected), DDNS, 802.1X, RTSP, HTTP Notification, NAT, and QoS. Below this, a table lists users with columns for Index, User Name, and User Type. A single user with Index 1 and User Name 'admin' is shown. An 'Add User' dialog box is overlaid on the table. The dialog contains input fields for User Name, Password, and Confirm Password, a Level indicator, and a User Type dropdown menu set to 'Administrator'. A note specifies that the password can consist of numbers, special characters, upper or lower case letters. The dialog has OK and Cancel buttons at the bottom.

Index	User Name	User Type
1	admin	

Add User

User Name

Password

Level

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

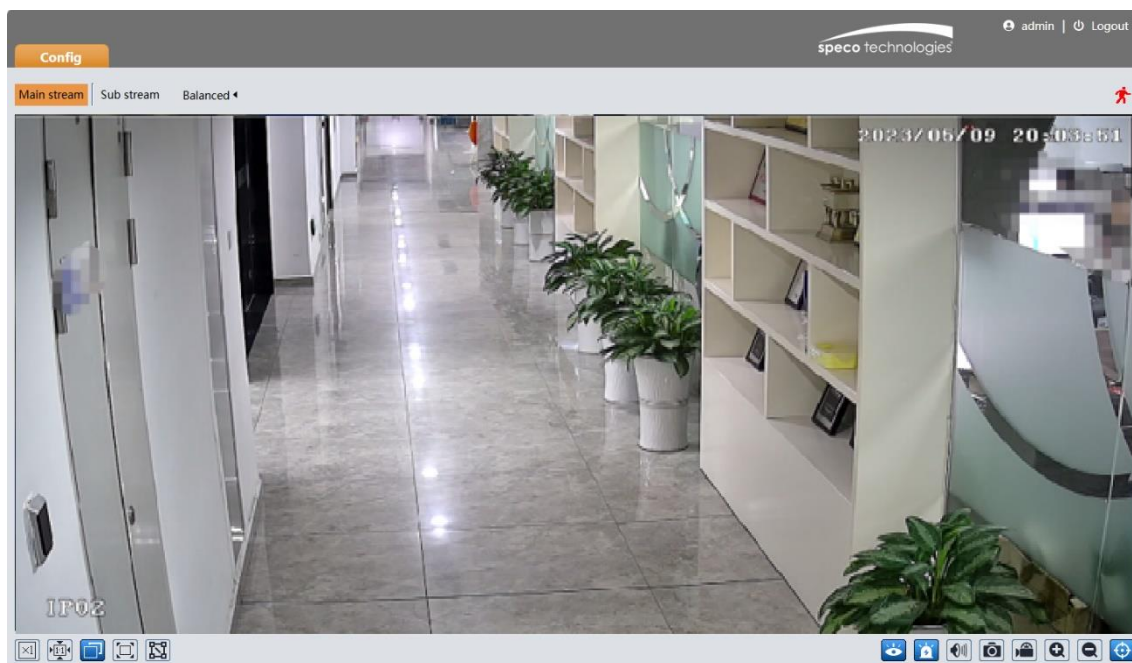
Confirm Password

User Type Administrator

OK Cancel

3 Live View

The window below will be shown after logging in.



The following table describes the icons on the live view interface

Icon	Description	Icon	Description
	Original size of resolution		Zoom in
	Fit (correct scale)		Zoom out
	Auto (fill the window)		Rule information display
	Full screen (show video only)		Enable/disable light alarm
	Measure Tool		SD card recording indicator
	Start/stop live view		Motion alarm indicator
	Start/stop two-way audio		Line crossing indicator
	Enable/disable audio		Region Intrusion indicator
	Snapshot		Light alarm indicator
	Start/stop local recording		

*Measure Tool: get the height and width in pixels of the selected region in the live view interface. (This function is only available for main stream). Click  and drag the mouse on the image to draw a desired box. The width and height in pixels will be directly displayed in the box.

*For the red-blue light alert cameras, after clicking the light alarm icon, the red-blue light will flash alternatively according to the set flashing time (you can set the flashing time by clicking Config→Alarm→Light Alarm). Click this icon again to stop flashing.

* After clicking the light alarm icon, the white light will flash according to the set flashing time (you can set the flashing time by clicking Config→Alarm→Light Alarm). Click this icon again to stop flashing. (Only when the illumination mode in Display Settings is set to "Infrared light", can this function be displayed)

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

- All indicator icons above will flash in live view interface only when the corresponding events are enabled.
- In full screen mode, to exit, double click on the mouse or press the ESC key on the keyboard.

4 Camera Configuration

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

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

4.1 System Configuration

4.1.1 System Information

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

4.1.2 Date and Time

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

Date and Time Summer Time

Zone: GMT-05 (New York, Toronto, Washington DC, Mid-Atlantic) ⚠ 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: 2026/8/31 01:37:51 ☐ Sync with computer local time

Save

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

Date and Time Summer Time

☒ DST

☒ Auto DST

☐ Manual DST

Start Time: January First Sunday 00:00 Hour

End Time: February First Monday 00:00 Hour

Time Offset: 120 Minutes

Save

4.1.3 Local Recording

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

Picture Path: C:\Program Files\NetIPCamera\Picture Browse

Record Path: C:\Program Files\NetIPCamera\Record Browse

Video Audio Settings: ☐ Open ☒ Close

Show Bitrate: ☐ Open ☒ Close

Local Smart Snapshot Storage: ☐ Open ☒ Close

Save

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.

Management	Record	Snapshot
Total picture capacity	6090 MB	
Picture remaining space	834 MB	
Total recording capacity	54720 MB	
Record remaining space	128 MB	
State	Normal	
Snapshot Quota	10 %	
Video Quota	90 %	
Changes in the quota ratio need to be formatted before they become effective.		
Eject Format		

● 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.

● Record Parameters

Go to Config→System→Storage→Record Parameters.

Overwrite (Cycle Write): the earliest record data will be replaced by the latest when the SD card is full.

● Schedule Recording Settings

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

Management	Record Parameters	Schedule Record	Snapshot
Parameter Settings			
Record Stream	Main stream		
Pre Record Time	No Pre Record		(H.264,H.265,MJPEG)
Timing			
☐ Enable Schedule Record			

2. Set record stream, pre-record time and schedule record.

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

Schedule Record: Check “Enable Schedule Record” and set the schedule.

☐ 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																								
Mon.	00:00-24:00																								
Tue.	00:00-24:00																								
Wed.	00:00-24:00																								
Thu.	00:00-24:00																								
Fri.	00:00-24:00																								
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

Weekly schedule

Set the alarm time from Monday to Sunday for a single week. Each day is divided into 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 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 Parameters Schedule Record **Snapshot**

Snapshot Parameters

Image Format

Resolution

Event Trigger

Snapshot Interval Second

Snapshot Quantity

Timing

☐ Enable Timing Snapshot

Snapshot Interval Second (0 Day 00 Hour 00 Minute 05 Second)

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

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

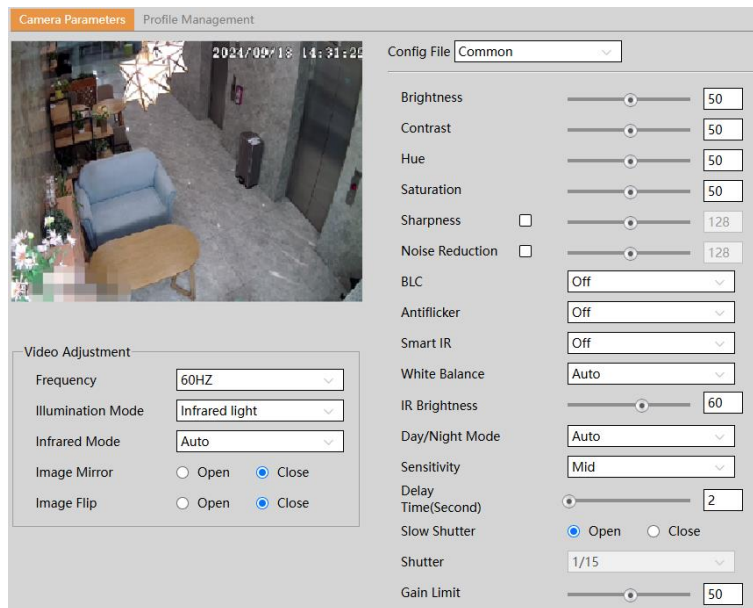
Timing Snapshot: Enable timing snapshot first and then set the snapshot interval and schedule. The setup steps of the schedule are the same as the schedule recording (See [Schedule Recording](#)).

4.2 Video Configuration

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

4.2.1 Image Configuration

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



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

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

Hue: Set the total color degree of the image.

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

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

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

Backlight Compensation (BLC):

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

Antiflicker:

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

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

Slow Shutter: If enabled, when the ambient light drops to a certain level, the frame rate will be gradually reduced to maintain the brightness of the camera. It is recommended to enable this function for scenarios with high requirements in a low-light environment.

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 Limit: 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.

Illumination Mode: choose "White light", "Infrared light" or "Smart supplement light" as needed.

Smart supplement light: If selected, in low ambient light, the system will automatically turn on the visible infrared light. Once there are people/vehicles appearing/staying in the detection area, it will automatically switch to full-brightness visible white light. When people/vehicles leaving the detection area exceeds the set duration, it will resume to infrared light. See [Smart Supplement Light Configuration](#) for details.

If “White light” is selected, overexposure control and white light mode can be set.

White light mode: Choose “Off”, “Auto” or “Manual”. Please select it as needed.

Overexposure control: Choose “OFF”, “Low”, “Mid” or “High”. This function can automatically adjust the exposure parameter according to the actual effect of the image, effectively avoiding detail loss caused by image overexposure, so that the image will be more vivid. Please set it as needed.

If “Infrared light” is selected, “Smart IR”, “IR Brightness”, “Day/Night Mode” and “Infrared Mode” can be configured.

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

IR Brightness: The value ranges from 1 to 100. Please set it as needed.

Day/Night Mode: Choose “Auto”, “Day”, “Night”, or “Timing”.

If “Timing” is selected, you need to set daytime and night time. For example: if “Daytime” is set to “7:00”, the camera will switch to Day mode at 7:00 o’clock; if “Night time” is set to “17:00”, the camera will switch from Day mode to Night mode at 17:00 o’clock.

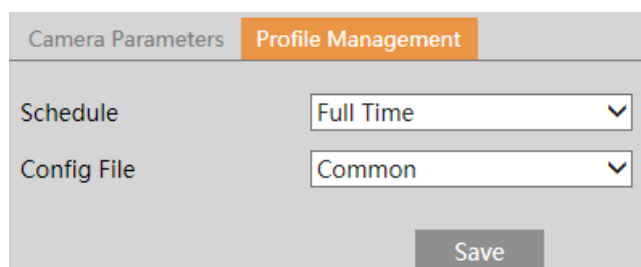
Infrared Mode: Choose “Auto”, “ON” or “OFF”.

Image Mirror: Turn the current video image horizontally.

Image Flip: Turn the current video image vertically.

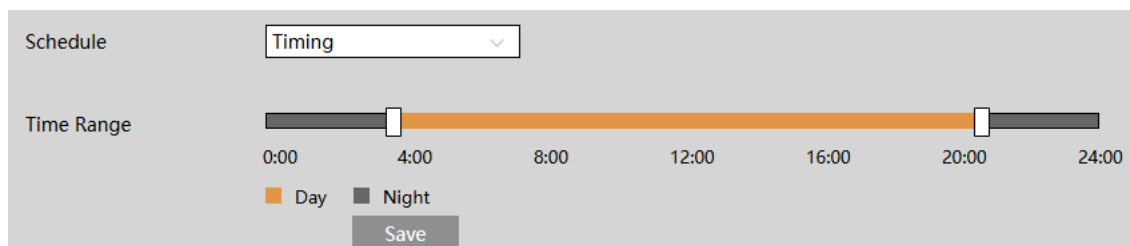
Schedule Settings of Image Parameters:

Click the “Profile Management” tab as shown below.



Set a full-time schedule for common, and specified time schedule for day and night.

Choose “Timing” in the drop-down box of the schedule as shown below.



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

4.2.2 Video / Audio Configuration

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

Video Audio

Index	Stream Name	Resolution	Frame Rate	Bitrate Type	Bitrate(Kbps)	Video Quality	I Frame Interval	Video Compression	Profile
1	Main stream	3840x2160	20	CBR	8192	Medium	80	H.264	High Profile
2	Sub stream	1280x720	20	CBR	1536	Medium	80	H.264	High Profile

Send Snapshot Sub stream Size:(1280x720)

☐ Video encode slice split

☐ Watermark(Only supports H.264, H.265) Watermark content:

Save

Two video streams can be adjustable.

Resolution: The size of image.

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

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 network bandwidth usage.

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

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

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

Video Compression: MJPEG, H264+, H264, H265or H265+can be optional. MJPEG is not available for main stream. If H.265/H.265+ is chosen, make sure the client system is able to decode H.265/H.265+. Compared to H.265, H.265+ saves more storage space with the same maximum bitrate in most scenes. Compared to H.264, H.265 reduces the transmission bitrate under the same resolution, frame rate and image quality.

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

Send Snapshot: Set the snapshot stream.

Video encode slice split: If this function is enabled, a smooth image can be obtained even when using a low-performance PC.

Watermark: When playing back the locally 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.

Video Audio

☒ Enable

Audio Encoding G711A

Audio Type MIC

Environmental Noise Filter Normal

MIC In Volume 0

Save

Audio Encoding: G711A and G711U are selectable.

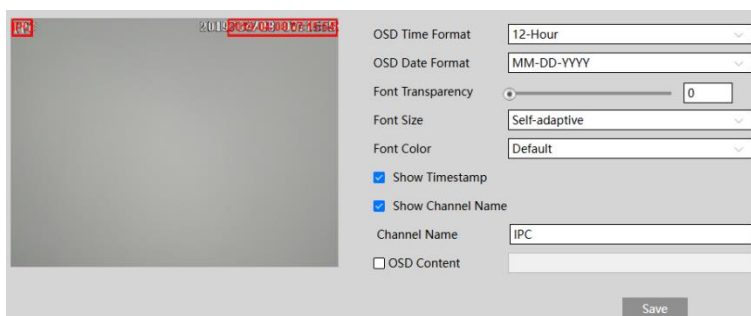
Audio Type: LIN or MIC. (If the internal MIC is used, choose “MIC”. If you want to use an external line-level audio input device, choose “LIN”.)

Environmental Noise Filter: “Normal” or Enhanced” can be optional. If the camera is installed near the seaside or in a windy sports field, you can select enhanced mode to filter out environmental noise.

MIC IN/Audio Out Volume: Set the volume as needed.

4.2.3 OSD Configuration

Go to Video→OSD as shown below.



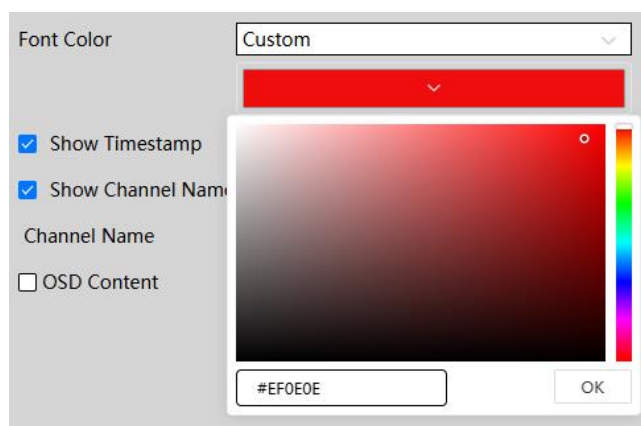
Set OSD time format, OSD date format, OSD content and font transparency/size/color here. After enabling the corresponding display and entering the content, drag them to change their position. Then click the “Save” button to save the settings.

Note: The quantities of the OSD items are different for different models.

Font Size: When the image resolution is less than 720P, the font size will be automatically changed to 16*16 and will not follow the font size you have set.

Font Color: You can use the default font color (white) or customize the font color as needed.

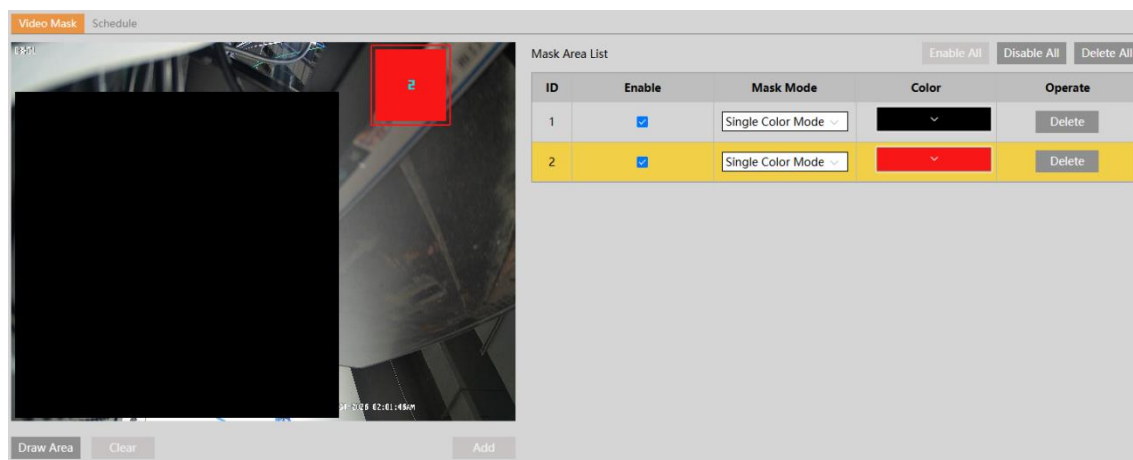
To customize the font color:



1. Select “Custom” and then click on the blank box under it.
2. Select a color on the colorful bar (right).
3. Click on the left color box to choose the desired color. Or you can directly enter the hexadecimal color code to set the color.
4. Click “OK” to save the font color settings.

4.2.4 Video Mask

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

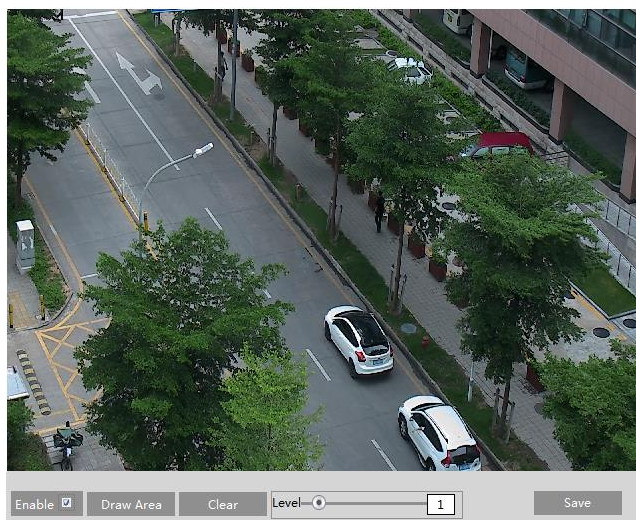


To set up a video mask:

1. Click the “Draw Area” button and then drag the mouse on the left window to draw rectangle mask areas.
2. Click the color block to select the desired color.
3. Enable/disable the mask area as needed. After the video mask areas are set, you can enable/disable/delete mask areas as needed.
4. Set the schedule. The mask areas only take effect during the scheduled period. The setup steps of the schedule are the same as the schedule recording setup. (See [Schedule Recording](#)).
5. Return to the live to verify that the area has been drawn as shown, as blocked out in the image.

4.2.5 ROI Configuration

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



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



4.2.6 Smart Supplement Light Configuration

This function is only available for some models.

1. Set the illumination mode to “Smart Supplement Light” in the Display Setting interface.
2. Go to **Config→Image→Smart Supplement Light**.

3. Select the trigger mode. “Moving object” or “All objects” can be selected.
4. Set the detection target and sensitivity. “Human” is selected by default. You can also select “Motor Vehicle” or “Motorcycle/Bicycle” as needed.

Target Detection Sensitivity: The higher the value is, the more likely it is that targets will trigger the white light.

5. Set the duration of the white light. In low ambient light, the system will automatically turn on the visible infrared light. If “Moving object” is selected, once people/vehicles appear and move in the set alarm area, it will automatically switch to full-brightness visible white light. When people/vehicles stay and do not move in the alarm area, or when leaving the alarm area exceeds the set duration, it will resume the infrared light.

If “All objects” is selected, once people/vehicles appear (moving or not moving) in the set alarm area, it will automatically switch to full-brightness visible white light. When people/vehicles leaving the alarm area exceed the set duration and no other targets are detected during the period, it will resume to infrared light.

6. Set alarm areas. Select the alarm area number. Four alarm areas can be added.

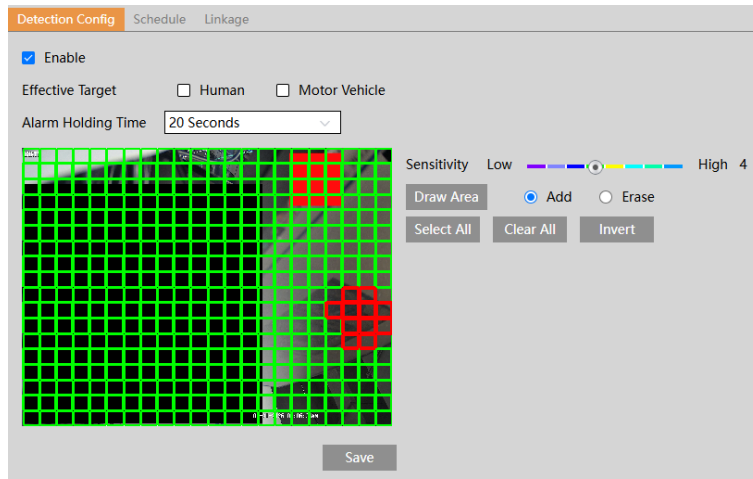
Click the “Draw Area” button and then click around the area where you want to set as the alarm area in the image (the alarm area should be a closed area). Click the “Stop Draw” button to stop drawing. Click the “Clear” button to delete the alarm area.

7. Click “Save” to save the settings.

4.3 Alarm Setup

4.3.1 Motion Detection

Go to Alarm→Motion Detection to set a 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.

Effective Target: Choose “Human” or “Motor Vehicle”. If “Human/Motor Vehicle” is enabled, the camera will only detect the movement of a human/motor vehicle. If no target is enabled, alarms will be triggered when a moving object appears in the image, including a human, a vehicle or other moving objects. (Some models only support “Human”)

Alarm Holding Time: It refers to the time that the alarm remains active after an alarm ends. For instance, if the alarm holding time is set to 20 seconds, once the camera detects motion, an alarm will be activated once, and no additional motion will be detected for 20 seconds. If another motion is detected during this period, it will be considered continuous movement; otherwise, it will be considered a single motion.

2. Set motion detection area and sensitivity.

Clear all grids. Then move the “Sensitivity” scroll bar to set the sensitivity. A 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.

You can set different sensitivity levels for different areas.

After that, click the “Save” to save the settings.

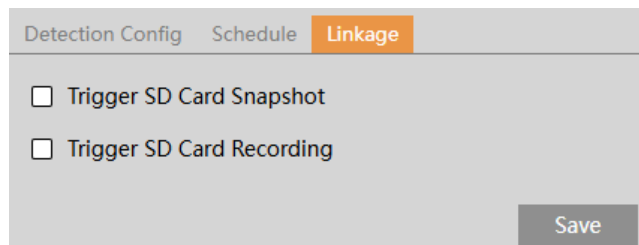
Note:

a) The area without colored grids means the sensitivity value is 0, which will be considered as a blocked area.

b) After detecting a moving object in the area covered with grid lines, an alarm will be triggered when the number of the red grid lines exceeds the threshold of the sensitivity level.

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

4. Click “Linkage” to configure the alarm linkage items.



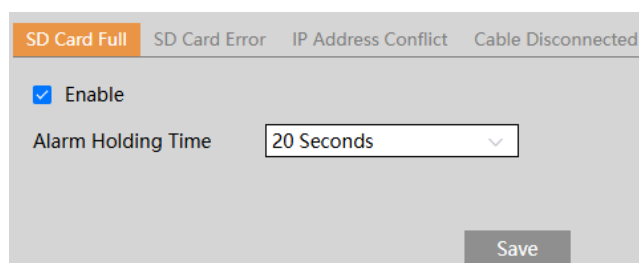
Trigger SD Card Snapshot: If selected, the system will capture images on motion detection and save the images on an SD card.

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

4.3.2 Exception Alarm

- **SD Card Full**

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



The screenshot shows the configuration page for the 'SD Card Full' exception alarm. At the top, there are four tabs: 'SD Card Full' (highlighted in orange), 'SD Card Error', 'IP Address Conflict', and 'Cable Disconnected'. Below the tabs, there is a checkbox labeled 'Enable' which is checked. Underneath, there is a label 'Alarm Holding Time' followed by a dropdown menu currently set to '20 Seconds'. At the bottom right, there is a 'Save' button.

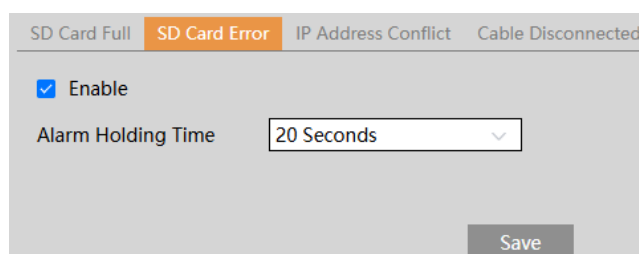
2. Click “Enable” and set the alarm holding time.

You can go to Config→Maintenance→ Operation Log to check the relevant alarm information after enabling this function.

- **SD Card Error**

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

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



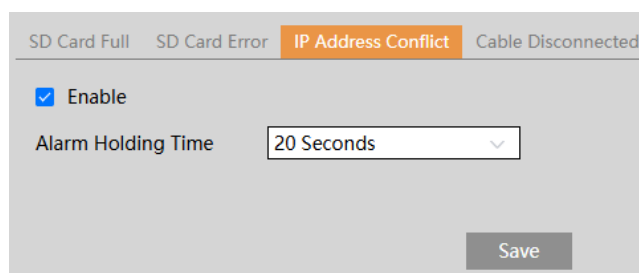
The screenshot shows the configuration page for the 'SD Card Error' exception alarm. At the top, there are four tabs: 'SD Card Full', 'SD Card Error' (highlighted in orange), 'IP Address Conflict', and 'Cable Disconnected'. Below the tabs, there is a checkbox labeled 'Enable' which is checked. Underneath, there is a label 'Alarm Holding Time' followed by a dropdown menu currently set to '20 Seconds'. At the bottom right, there is a 'Save' button.

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

You can go to Config→Maintenance→ Operation Log to check the relevant alarm information after enabling this function.

- **IP Address Conflict**

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



The screenshot shows the configuration page for the 'IP Address Conflict' exception alarm. At the top, there are four tabs: 'SD Card Full', 'SD Card Error', 'IP Address Conflict' (highlighted in orange), and 'Cable Disconnected'. Below the tabs, there is a checkbox labeled 'Enable' which is checked. Underneath, there is a label 'Alarm Holding Time' followed by a dropdown menu currently set to '20 Seconds'. At the bottom right, there is a 'Save' button.

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

You can go to Config→Maintenance→ Operation Log to check the relevant alarm information after enabling this function.

- **Cable Disconnection**

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

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

You can go to Config→Maintenance→ Operation Log to check the relevant alarm information after enabling this function.

4.3.3 Alarm Server

Go to Alarm→Alarm Server as shown below.

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.

4.3.4 Light Alarm

Only when the illumination mode in Display Settings is set to “Infrared light”, can this function be displayed

Go to Alarm→Light Alarm as shown below.

Set the flashing time and frequency of the light.

Flashing time: the flashing time ranges from 1 second to 60 seconds.

Follow Alarm Holding time: if enabled, the warning voice will stop when the alarm holding time ends.

Flashing Frequency: three options- low, middle and high

4.3.5 Disarming

You can disarm alarm linkage actions quickly in this interface.

Disarming: The system stops triggering alarm linkage actions immediately.

Scheduled Disarming: The system stops triggering alarm linkage actions in the selected period. Click “Schedule” to set the schedule. The schedule setup steps are the same as the schedule recording setup (See [Schedule Recording](#)).

After “Disarming” or “Scheduled Disarming” is enabled, the reported general alarms (the alarm start time and end time of alarm out and audio alarm) will probably not match the actual situation. You need to handle it manually.

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 has adequate and even light, avoiding overexposure or too much darkness on both sides.

4.4.1 Line Crossing

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

Go to Event→Line Crossing as shown below.

Detection Config
Schedule
Linkage

☒ Enable
☐ Save Original Picture To SD Card
☐ Save Target Picture To SD Card

Trigger mode
Moving object

Alarm Holding Time
3 Seconds

Draw Area
Clear
Draw Target Size

Alarm Line
1

Direction
A->B

Alarm Line Parameters

Detection target and sensitivity

Target
Target detection sensitivity

☒ Human
☐ Motor Vehicle
☒ Motorcycle/Bicycle

50
50
50

Event Detection

Event-triggered sensitivity
50

Target Size Filter

Target
Human

Min Size Width
1 %
Height
1 %

Max Size Width
90 %
Height
90 %

Save

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

Save Original Picture to SD Card: If it is enabled, the detected original pictures will be captured and saved to the SD card when the targets cross the alarm line.

Save Target Picture to SD Card: If it is enabled, the detected target cutout pictures will be captured and saved to the SD card when the targets cross the alarm line.

Note: To save snapshots to the local PC, please enable “Local Smart Snapshot Storage” in the local config interface first. To save snapshots to the SD card, please install an SD card first.

2. Set alarm holding time.

3. Set alarm lines, targets, sensitivity and target size filter for line crossing detection.

Set the alarm line number and direction. Four 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 **will** 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.

Note: If the set rule line is very close to the edge of the screen, it may be difficult for the target to trigger the alarm. Please make sure that there is at least one full target-sized space between the rule line and the edge of the screen.

Detection Target:

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

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

Motorcycle/Bicycle: Select it and then alarms will be triggered if a vehicle with two wheels (eg. a motorcycle or bicycle) crosses the pre-defined alarm lines.

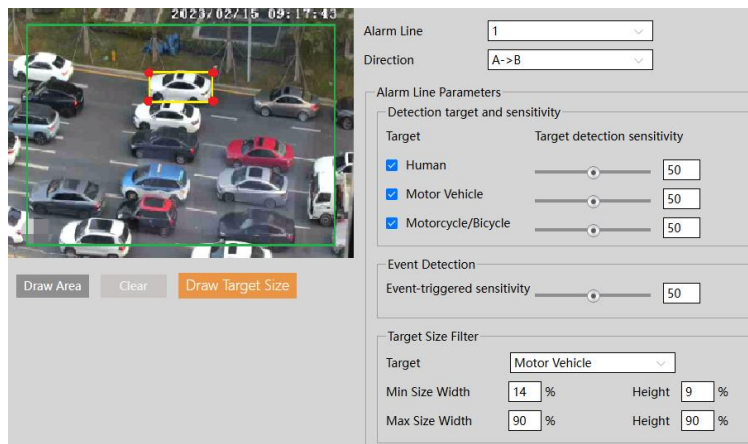
All three types of objects can be selected simultaneously. Please select the detection objects as needed. If no object/target is selected, alarms will not be triggered even if line crossing detection is enabled.

Target Detection Sensitivity: The higher the value, the easier it is for the alarm to be triggered by targets.

Event Triggered Sensitivity: It refers to the percentage of the body part of an object that goes across the alarm line. The higher the value of sensitivity is, the more easily the alarm can be triggered.

To set target size filter:

Click “Draw Target Size” to draw the maximum and minimum size of a specific target as shown below.



Target: choose “Human”, “Motor Vehicle” or “Motorcycle/Bicycle” as needed.

Green box is the maximum target detection box; yellow box is the minimum target detection box.

Click the green box to edit the maximum target detection box; click the yellow box to edit the minimum target detection box.

Drag one of the four corners of the green or yellow box to change the box size. The corresponding size value on the right will be changed too. You can also enter a digital number to change the box size directly.

Click and drag the green or yellow box to move its position.

Finally, click “Save” to save the settings.

After the target size range is set, only the target whose size is between the minimum value and the maximum value can be detected.

After the target size range is set, only the target whose size is between the minimum value and the maximum value can be detected.

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

5. Click “Linkage” to set the alarm linkage options for line crossing detection.

Trigger Light Alarm: If selected, the light of the camera will flash when an object crosses over the alarm line. The light flashing time and frequency shall be set first in the light alarm interface. See [Light Alarm](#) for details.

Note: Only when the illumination mode in Display Settings is set to “Infrared light”, can this function be displayed.

Trigger SD Card Snapshot: If selected, the system will capture images when the target crosses over the alarm line and save the images on an SD card.

Trigger SD Card Recording: If selected, videos will be recorded on an SD card when the target crosses over the alarm line.

※ Configuration of the camera and surrounding area

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

2. Avoid scenes with many trees or 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 as shown below.

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

Save Original Picture to SD Card: If it is enabled, the detected original pictures will be captured and saved to the SD card when the target intrudes into the pre-defined areas.

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

2. Set trigger mode, time threshold and alarm holding time.

Trigger Mode: Choose “Moving object” or “All objects” as needed. If “Moving object” is selected, alarms will be triggered when an object intrudes into the pre-defined area; if the object stops moving on the alarm line, the region intrusion alarm stops too. If “All objects” is selected, alarms will be triggered when an object remains still on the alarm line or intrudes into the pre-defined area.

Time Threshold: It refers to the threshold for the time of the object/target stays in the region. If one object entering and staying in the pre-defined area exceeds the time threshold, alarms will be triggered.

Alarm Holding Time: It is the time that the alarm remains active after an alarm ends.

3. Set alarm areas, targets, sensitivity and target size filter for region intrusion detection.

Set the alarm area number. Four 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 (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.

Note: If the set rule line is very close to the edge of the screen, it may be difficult for the target to trigger the alarm. Please make sure that there is at least one full target-sized space between the rule line and the edge of the screen.

Detection Target:

Human: Select it, and then alarms will be triggered if someone intrudes into the pre-defined area.

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

Motorcycle/Bicycle: Select it and then alarms will be triggered if a vehicle with two wheels (eg. a motorcycle or bicycle) intrudes into

the pre-defined area.

All 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.

Target Detection Sensitivity: The higher the value is, the easier it is for the alarm to be triggered by targets.

Event Triggered Sensitivity: It refers to the percentage of the body part of an object that enters the alarm area. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Target size setup: The setup steps of the target size are the same as the line crossing target size setup (See [Line Crossing](#) for details).

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

5. Click “Linkage” to set the alarm linkage options for region intrusion detection. The setup steps are the same as the line crossing linkage settings. Please refer to [Line Crossing](#) for details.

※ Configuration requirements of the 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.

4.5 Network Configuration

4.5.1 TCP/IP

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

IPv4 IPv6

☐ Obtain an IP address automatically

☒ Use the following IP address

IP Address

Subnet Mask

Gateway

Preferred DNS Server

Alternate DNS Server

Use IP address (take IPv4 for example)-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.

4.5.2 Port

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

HTTP Port	80
Data Port	554
RTSP Port	9008
Subscription Listening Port	8080 ☒ Enable

HTTP Port: The default HTTP port is 80. 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.

Subscription Listening Port: The port is used for a persistent connection of the third-party platform to push smart data.

4.5.3 Server Configuration

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

☐ Enable

Server Port	2009
Server Address	
Device ID	1



1. Check "Enable".

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

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

4.5.4 Onvif

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

Port Server **Onvif** DDNS 802.1X RTSP HTTP Notification NAT QoS

Add Modify Delete

Index	User Name	User Type
1		

Add User ✕

User Name

Password

Level

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

Confirm Password

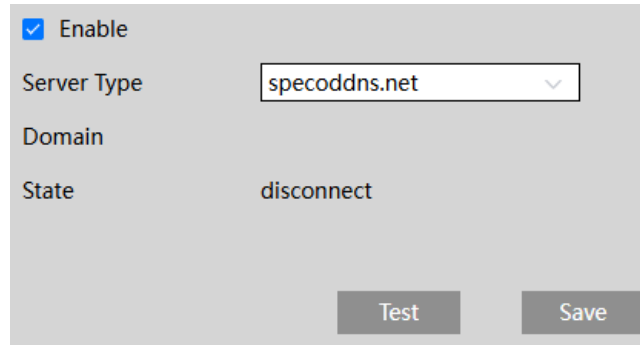
User Type

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

4.5.5 DDNS

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

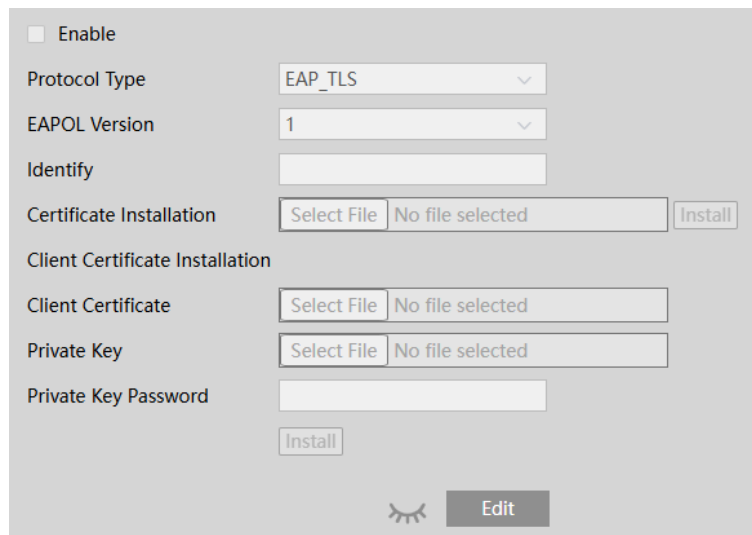
1. Go to Network→ Ports/Connections→ DDNS. Click “Edit”.



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

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 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 regarded 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.

Click “Edit” to start the setup.

Protocol type: Choose “EAP_MD5” or “EAP_TLS” as needed.

Select EAP-TLS as the EAP method. Enter your ID issued by the CA and then upload the related certificate, device certificate and private key. Before connecting the camera to the protected network with 802.1x, apply for a digital certificate from a Certificate Authority (i.e., your network administrator) that can be validated by a RADIUS server.

Select EAP_MD5 as the EAP method. You need to enter the username and password.

User name and password: The username and password must be the same as the username and password applied for and registered

in the authentication server.

4.5.7 RTSP

Go to Network→ Ports/Connections→RTSP.

☒ Enable

Port: 9008

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

Multicast address

Main stream: 239.***.***.0 50554 ☐ Automatic start

Sub stream: 239.***.***.1 51554 ☐ Automatic start

Audio: 239.***.***.3 53554 ☐ Automatic start

☐ Allow anonymous login (No username or password required)

Edit

Click “Edit” and 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: After entering 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 HTTP Notification

Go to Config→Network →Ports/Connections→HTTP Notification.

Push Protocol Version: V1

Push Type: ☒ Push by Subscription ☒ Actively Push

Push by Subscription

Subscription Listening Port: 8080

Actively Push

Index	Enable	IP address/domain	Port	Path	Connection Status	Connection Type	Send Heartbeat	Heartbeat Interval (Second)	Smart Alarm Type

Edit

Click “Edit”.

Push Protocol Version: Choose “V1” or “V2” as needed. It is recommended to use V2.

Push Type: “Push by Subscription” and/or “Actively Push” can be selected.

Push by Subscription: Push target trajectory (moving coordinate) to the 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 a smart event (such as line crossing detection, region intrusion detection, etc.)

If the subscription listening port is occupied, you can modify it.

Actively Push: Click “Add” to add an HTTP notification.

Add HTTP Notification

☒ Enable

Protocol Type: HTTP

HTTP Request Method: POST

Domain/IP: 0.0.0.0

Server Port: 80

Path:

User Name: ☐ Enable

Password:

Connection Type: Persistent connection

Heartbeat Interval(Second): 90 ☒ Send Heartbeat

Smart Alarm Data ☐ Select All

☒ Alarm status data

☐ Smart track data

☒ Smart event data ☒ Original picture ☒ Target picture

Smart Alarm Type ☒ Select All

☒ Motion Detection ☒ Region Intrusion ☒ Line Crossing

Save Cancel

Protocol type: HTTP

HTTP Request Method: Choose “POST” or “GET” as needed.

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

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

Path: Enter the subdomain of the above server, for example, the URL of alarm information push: “/SendAlarmStatus”.

Username and password: Please enable and enter as needed.

Connection Type: Choose “Persistent connection” or “Short connection” as needed. A persistent connection is always pushed with

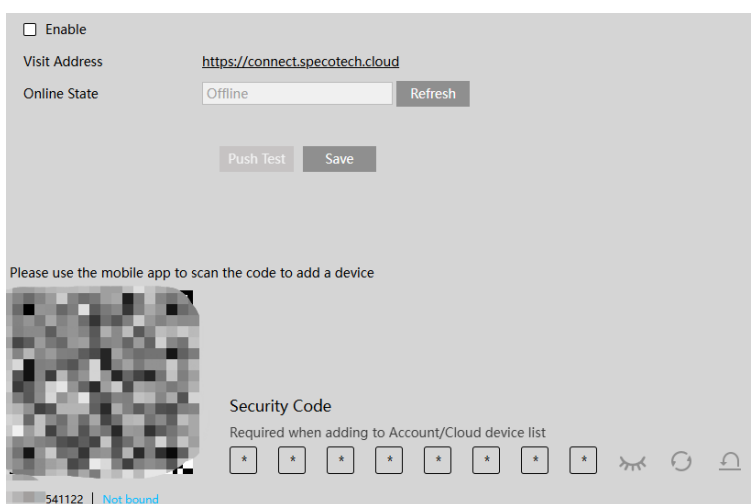
an established connection. A short connection will be disconnected after it is successfully pushed and re-established for the next push.

If “Persistent Connection” is selected, enable “Send heartbeat” and set heartbeat interval as needed to maintain the connection. A short connection doesn’t have heartbeat sending or heartbeat interval options.

Enable “Send heartbeat” and set heartbeat interval as needed. Check smart alarm data and type. After the above parameters are set, click “Save” to save the settings. Select one URL and click “Test” to test the connection of the URL. Then the camera will automatically connect to the third-party platform. The online state can be viewed in the above interface. After the camera is successfully connected, it will send the selected alarm data to the third-party platform once the selected smart alarm is triggered.

4.5.9 NAT

If this function is enabled, the network camera can be quickly accessed by scanning the QR Code in the mobile APP via WAN. Enable this function by going to Config→Network→Ports/Connections→NAT. After this function is enabled, you can view the visit address and whether it is online.

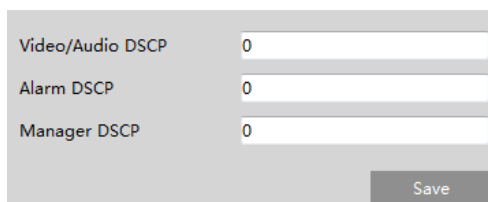


Additionally, you can use the visit address and device ID to visit the web client remotely.

4.5.10 QoS

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

Go to Network→ Ports/Connections→QoS.



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

Alarm DSCP: The range is from 0 to 63.

Manager DSCP: The range is from 0 to 63.

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

4.6 Security Configuration

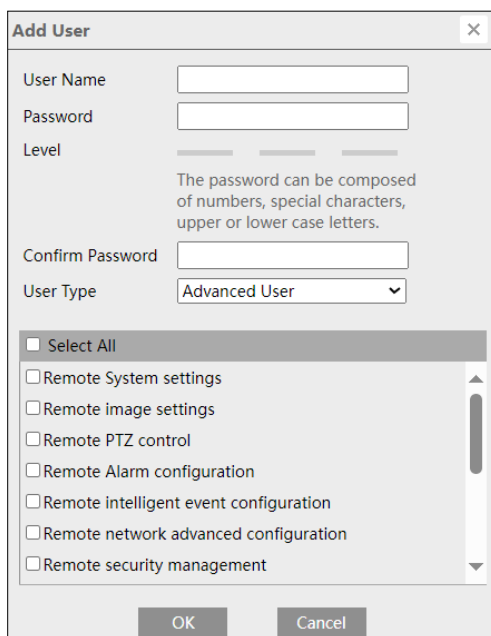
4.6.1 User

Go to Security→User as shown below.

Add Modify Delete Security Question		
Index	User Name	User Type
1	admin	Administrator

Add user:

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



The "Add User" dialog box contains the following fields and options:

- User Name:** A text input field.
- Password:** A text input field.
- Level:** A dropdown menu.
- Confirm Password:** A text input field.
- User Type:** A dropdown menu with "Advanced User" selected.
- Permissions:** A list of checkboxes under the "Select All" header:
 - ☐ Remote System settings
 - ☐ Remote image settings
 - ☐ Remote PTZ control
 - ☐ Remote Alarm configuration
 - ☐ Remote intelligent event configuration
 - ☐ Remote network advanced configuration
 - ☐ Remote security management
- Buttons:** "OK" and "Cancel" at the bottom.

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

Modify user:

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

Edit User

User Name: admin

Old Password:

New Password: ☒

Level:

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

Confirm Password:

User Type: Administrator

Modify Onvif User: ☒

☒ Select All

- ☒ Remote System settings
- ☒ Remote image settings
- ☒ Remote PTZ control
- ☒ Remote Alarm configuration
- ☒ Remote intelligent event configuration
- ☒ Remote network advanced configuration
- ☒ Remote security management

OK Cancel

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

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

Delete user:

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

Note: The default administrator account cannot be deleted.

Security Question Settings: Set the questions and answers for the admin to reset the password after you forget it.

4.6.2 Online User

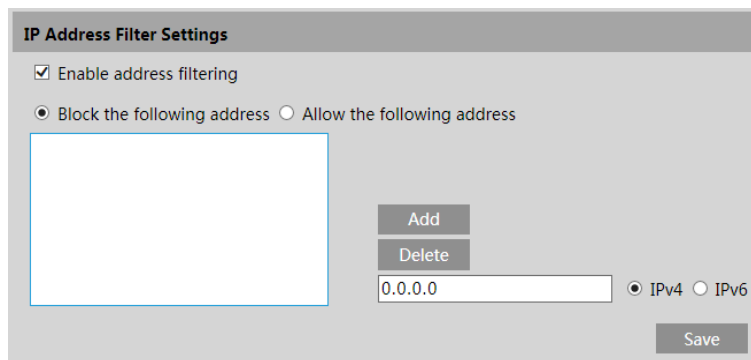
Go to Security→Online User to view the user who is viewing the live video.

Index	Client Address	User Name	User Type	Video Stream Count	
1	10.1.20.221	admin	Administrator	1	Kick Out

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

4.6.3 Block and Allow Lists

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



The screenshot shows the 'IP Address Filter Settings' window. It has a title bar with the same name. Inside, there's a checked checkbox for 'Enable address filtering'. Below it are two radio buttons: 'Block the following address' (selected) and 'Allow the following address'. A large empty rectangular box is provided for listing addresses. To the right of this box are 'Add' and 'Delete' buttons. Below these is a text 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.

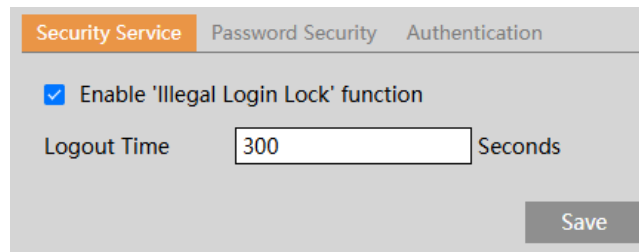
The setup steps are as follows:

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.

4.6.4 Security Management

Go to Security→Security Management as shown below.



The screenshot shows the 'Security Service' tab in the 'Security Management' section. It has sub-tabs: 'Security Service' (active), 'Password Security', and 'Authentication'. Under 'Security Service', there's a checked checkbox for 'Enable 'Illegal Login Lock' function'. Below it is a 'Logout Time' label followed by a text input field containing '300' and the word 'Seconds'. At the bottom right is a 'Save' button.

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

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

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

● Password Security



The screenshot shows the 'Password Security' sub-tab. It has labels for 'Password Level' and 'Expiration Time'. 'Password Level' has a dropdown menu showing 'Weak'. 'Expiration Time' has 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, 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.

● Authentication

You can improve the network access security by setting RTSP and API service authentication.

Security Service Password Security **Authentication**

RTSP

Authentication Basic/Digest

API Services

☒ Enable

Authentication Basic/Digest

Subscribe to push services

Authentication Basic/Digest

Save

RTSP Authentication: “Digest” or “Basic/Digest” can be selected.

API Service Authentication: “Digest” or “Basic/Digest” can be selected.

Push Subscription Authentication: “Digest” or “Basic/Digest” can be selected.

4.7 Maintenance Configuration

4.7.1 Backup and Restore

Go to Maintenance→Backup and Restore.

Import Setting

Path Select File No file selected

Import Setting

Export Settings

Export Settings

Restore Default Parameters

Keep

☐ Network Config

☐ Security Configuration

☐ Image Configuration

Info: The "Restore default Parameters" option does not reset the password and does not remove activation.

Restore Default Parameters

Restore Factory Settings

Restore Factory Settings

- **Import & Export Settings**

Configuration settings of the camera can be exported from one 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.

- **Export Maintenance Information**

When the device error occurs, you can export the relevant maintenance information as needed and send it to the technician to find out the problem.

The historical running log can be exported only when your SD card is inserted, and the maintenance information has been stored on your SD card (Go to Config→Storage to view the storage capacity of maintenance information).

- **Default Settings**

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

4.7.2 Reboot

Go to Maintenance→Reboot.

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

Timed Reboot Setting:

If necessary, the 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.

4.7.3 Upgrade

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

The screenshot displays the 'Upgrade' interface. At the top, a warning message states: 'Downgrading from the current version to a previous version is not allowed. Do not disconnect power during the upgrade. Do not refresh or close this page during the upgrade.' Below this, the 'Local upgrade' section includes a 'Path' field with a 'Select File' button and 'No file selected' text, and two buttons: 'Upgrade' and 'Back up and upgrade'. The status bar shows 'System 1: Normal' and 'System 2: Normal'. The 'Cloud Upgrade' section features an 'Upgrade Options' dropdown menu set to 'Close' and an 'Apply' button. Below this, the 'Current Version' is listed as '5.3.1.36704B260417.ID18.U3(07A09)'. At the bottom, the 'Export Upgrade Log' section contains an 'Export Upgrade Log' button.

- **Local Upgrade**

1. Click the “Select File” 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 the upgrade.

- **Cloud Upgrade**

Only some models support this function.

Note: Before you use the cloud upgrade, please make sure the cloud service is enabled successfully.

After the cloud server pushes the latest version, you can upgrade the camera.

1. Go to **Config→Maintenance→Upgrade**.
2. Select “Notify Only” in the cloud upgrade options or click “Manual Check” to check whether the current version is the latest. If your software version is not the latest, click “Upgrade” to download and upgrade from the cloud server.

Caution:

1. You cannot downgrade to a lower version.
 2. Do not refresh/close the browser or disconnect the camera from the network during the upgrade, or it will cause a system failure.
- After the device is successfully upgraded, there is a ten-minute observation period. 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.

4.7.4 Operation Log

To query and export log:

- 1. Go to Maintenance→Operation Log.

Main Type

All logs

Sub Type

All logs

Start Time

2026/8/31 00:00:00

End Time

2026/8/31 23:59:59

Search

Export

Index	Time	Main Type	Sub Type	User Name	Login IP	Hostname
1	2026/8/31 02:58:43	Operation	Log in	admin	10.1.20.221	
2	2026/8/31 02:51:03	Operation	Log out		10.1.20.221	
3	2026/8/31 02:50:17	Operation	Log out	admin	10.1.20.221	
4	2026/8/31 02:50:03	Operation	Log out		10.1.20.221	
5	2026/8/31 02:50:00	Operation	Net Config Modify	admin	10.1.20.221	
6	2026/8/31 02:46:02	Operation	Log in	admin	10.1.20.221	

- 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.

4.3.6 Serial Output

Serial output 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 mode, you are advised to consult our technical support.

☐ Enable

Log Level

RUN/WARN/ERROR

Save

4.3.7 Maintenance Information

When a device failure occurs, you can export the maintenance information and send it to the technicians, so that they can quickly find out and analyze the problem. Go to **Config→Maintenance Information** to export.

5 Search

5.4 Image Search

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

● SD Card Image Search

1. Choose “Picture”—“SD Card”.



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

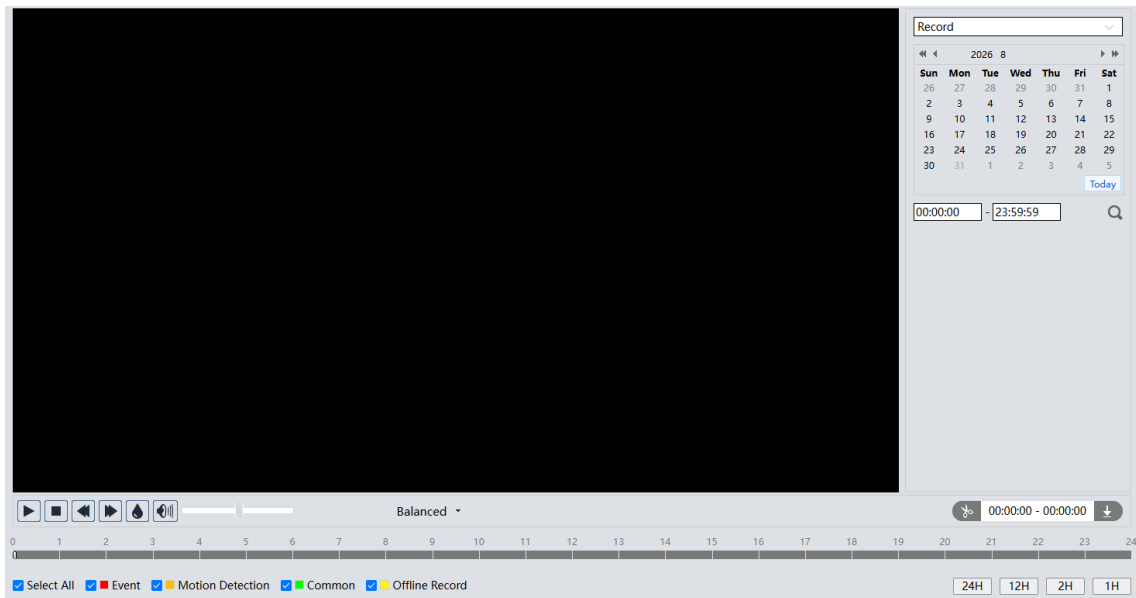
The descriptions of the buttons are shown as follows.

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

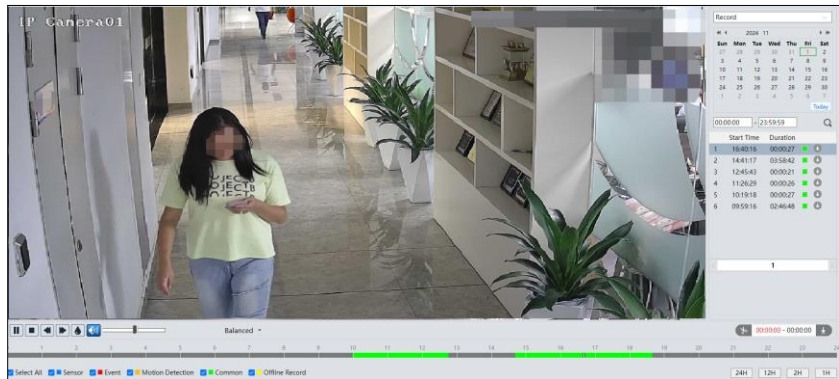
5.5 Video Search

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

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



- 4. Select the alarm events at the bottom of the interface.
- 5. Double-click on a file name in the list to start playback.



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

© 2014 Pearson Education, Inc. or its affiliate(s). All rights reserved.

Video clip and downloading

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

Index	Process	Record	Start Time	End Time	Path	Operate
1	100%	Cut	2018-01-16 01:1...	2018-01-16 01:1...	Favorites	Open

Set up

D:\Favorites

Clear List

Close

Click “Set up” to set the storage directory for 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.

Fail to connect devices via a web browser.

A: The network is not properly connected. Check the connection and make sure it is connected properly.

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

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

D: Exclude the above reasons. Restore the default setting using the IP Scanner.

No sound can be heard.

A: The audio input device is not connected. Please connect and try again.

B: The audio function is not enabled on the corresponding channel. Please enable this function.

Models: O8KT1/ O8KT1B

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