User Manual
2MP License Plate Recognition IP Camera

O2BLP3M

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

Important Safeguards and Warnings

1. Electrical safety

All installation and operation here should conform to local electrical safety codes.
Use a certified/listed 12VDC Class2 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.
The dome cover is an optical device, please do not touch or wipe the cover surface directly during installation and use, please refer to the following methods if dirt is found.
Stained with dirt:
Use an 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 it 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
Quick Start Guide	1
Installation Accessories Bag	1

Table of Contents

1 Introduction

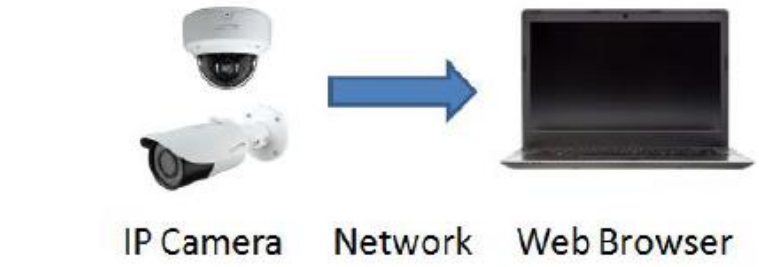
Welcome

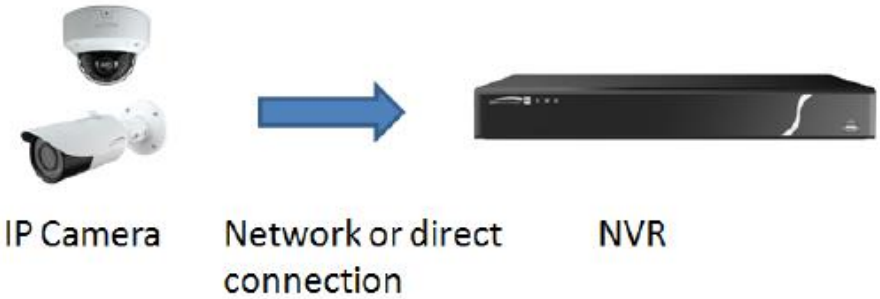
Thank you for purchasing this network camera!
Please read this manual carefully before operating the unit and retain it for further reference.
Should you require any technical assistance, please contact Speco Technologies Technical Support.

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 VMS

Applications





2 Web Access and Login

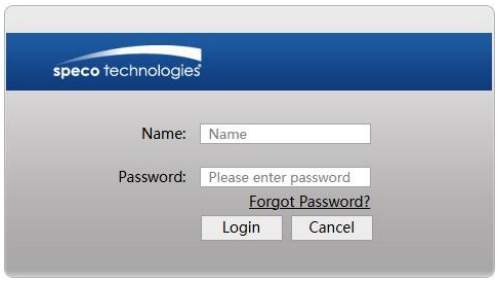
Here we take device access via Web browser for example.
Web browser： Firefox/Edge/Safari/Google Chrome
It is recommended to use the latest version of these web browsers.
The menu display and operation of the camera may be slightly different by using the browser with plug-in or without plug-in. Installing the plug-in will display more functions of the camera.
Connect the IP Camera via LAN or WAN. Here only take the plug-in required browser for example. The details are as follows:

- Access through IP Scanner

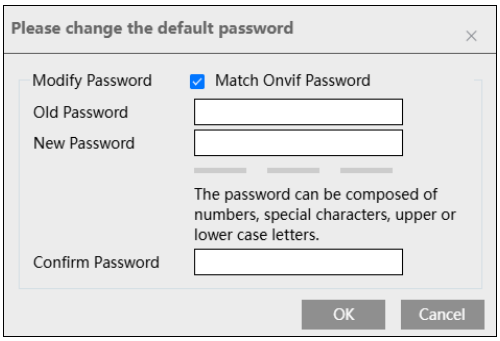
Network connection:

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.

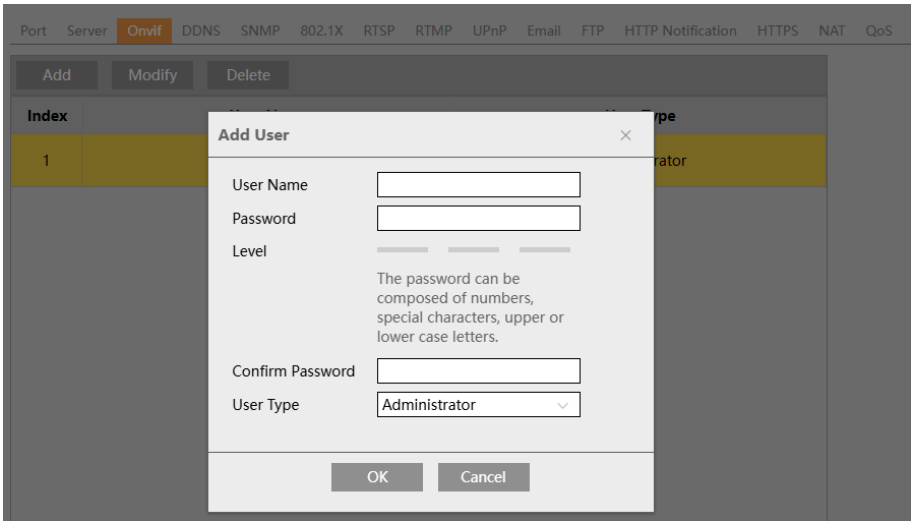
③ In the device list, the IP address, model number, and MAC address of each device will be listed. Select the applicable device and double click to open up the web viewer. You can also manually enter the IP address in the address bar of the web browser.



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



If this is the first time for you to log in, the password prompt may only change the admin password. 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***)



3 License Plate Recognition

3.1 Configuration requirements of camera and surrounding area

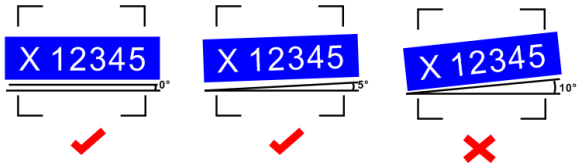
Note: The following installation requirements are based on optimum conditions, your license capture rate may vary depending on lighting, position, license plate designs and other factors.

- The monitoring image should try to cover the lane, entering/exiting vehicles and these vehicles' plate number shall be always seen in the video.
- Try to avoid the objects that will block the camera, such as pillars, obstacles, doors, etc.
- Avoid the scenes with many trees or other moving objects (like humans, non-motor vehicles).
- The monitoring road shall be straight within 165ft in front of/behind the location of the camera installation and make sure the camera points at the front or rear of the vehicle.

The recommended installation height and distance are as follows:

	Overhead		Entrance/Exit	
Lens Type	Recommended Installation Height(H)	Recommended Recognition Distance(L)	Recommended Installation Height(H)	Recommended Recognition Distance(L)
7-22mm	15-20ft	23-98ft	4.2-5ft	8-10ft
5-50mm	13-20ft	16-164ft	4.2-5ft	8-10ft
8-32mm	15-20ft	23-115ft	4.2-5ft	8-10ft

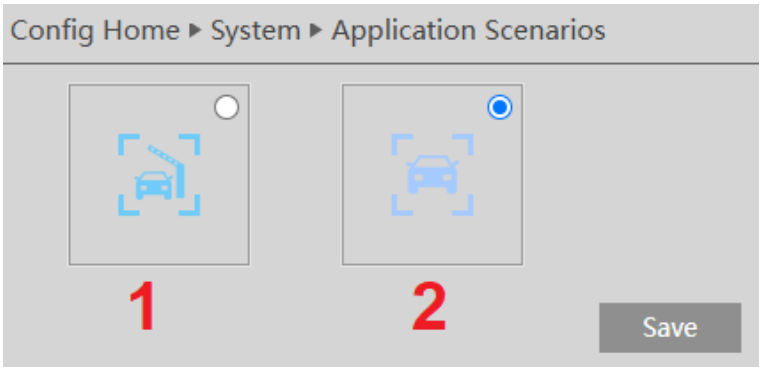
The tilt angle of the license plate
After the camera is installed, you can log in the web client and view whether the license plate tilts in the video. The tilt angle shall range from -5° to 5°.



If the captured license plate doesn't meet the above requirement, you can adjust the pan angle of the camera to correct it.

3.2 Configuring Application Scenarios

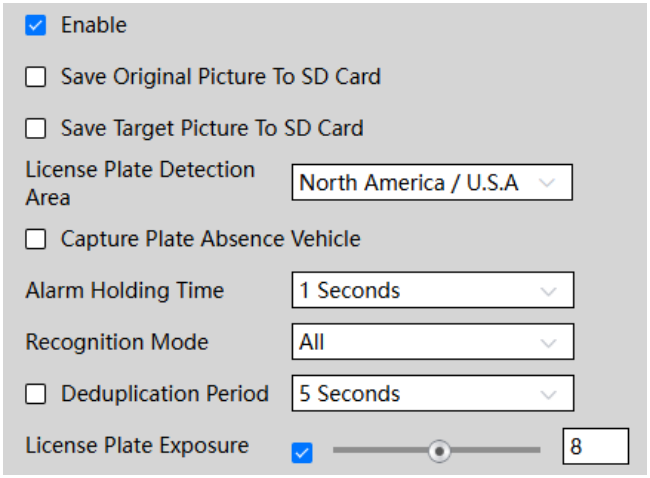
There are two application scenarios can be selected. Please select it as needed.
Click ***Config→System→Application Scenarios*** to choose.



Event Type: 1- Entrance and Exit; 2- License Plate Detection.
If you want to switch the event type, please select it and then click “Save”. After successful reboot, the corresponding event type will be displayed. Select and set as needed.

3.3 License Plate Detection Settings

License plate detection function is to detect and compare license plate numbers. Alarms will be triggered when a license plate is detected.
The setting steps of vehicle license plate detection and comparison are as follows:
1. Go to ***Config→Event→License Plate Detection*** as shown below.



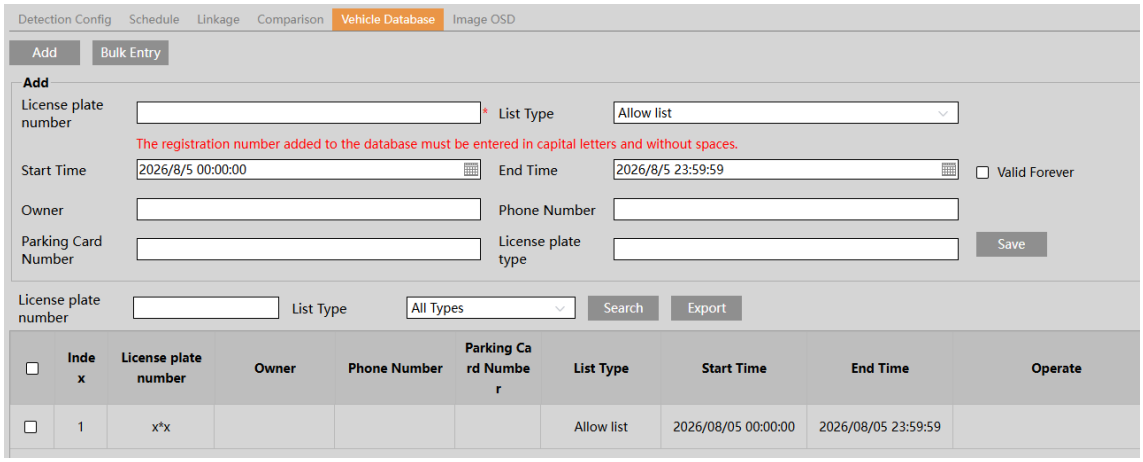
2. Enable license plate detection. Select Save Original Picture/Target Picture to SD Card, License Plate Detection Area, and Capture Plate Absence Vehicle (Capture vehicles missing plates) as needed.
3. Set alarm holding and recognition mode.
Alarm Holding Time: it is the time that the alarm extends after an alarm ends.
Recognition Mode: All, Recognizing when approaching, Recognizing when driving away.
4. Set deduplication period and license plate exposure as needed.
Deduplication Period: In the set period, delete the repeated comparison results.
License Plate Exposure: Set the exposure weight of the license plate in license plate exposure compensation mode. When detecting a license plate in the detection area, the camera will automatically adjust the brightness of the set plate detection area according to the exposure weight. The higher the value is, the higher the exposure weight is.
When the brightness of the captured license plate is not enough or the plate overexposure happens, it can be enabled. Please check and set license plate exposure as needed.
5. Set the alarm detection area, the blocked area and target size filter.

To set the detection area
Check “Detection Area” and click “Draw Area” to draw a closed area. Click “Clear” to clear the area.

To set a blocked area:
Check “Blocked Area” and select the number. Then click “Draw Area” to draw a closed area. Up to 4 areas can be set up. After you set the blocked area, this area will not be detected.

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

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 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 the digital number to directly change the box size. (The default size range of a single number plate image occupies from 1% to 50% of the entire image).
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.
6. Set the schedule of license plate detection. The setup steps of the schedule are the same as the schedule recording setup (See Schedule Recording).
7. Add vehicles to the vehicle Database. Click the vehicle database tab to go to the following interface.

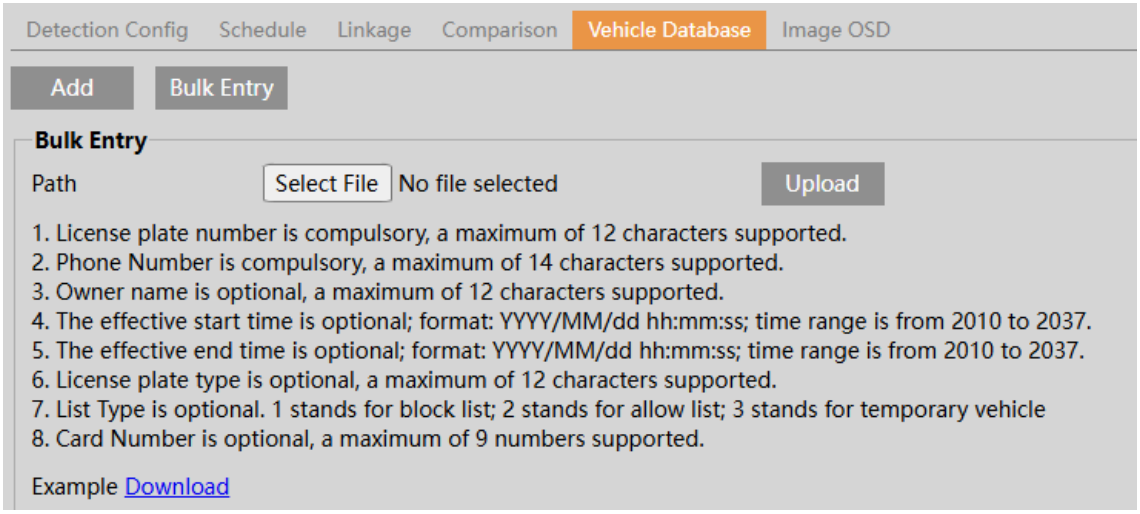


- **Add vehicles**

Click “Add” to extend a vehicle adding box as shown in the above figure. Enter the license plate number, select list type, start and end time, enter owner, license plate type, phone number, parking card number and so on. Then click “Save” to save the vehicle information.

List type: temporary vehicle, allow list and block list can be selected.

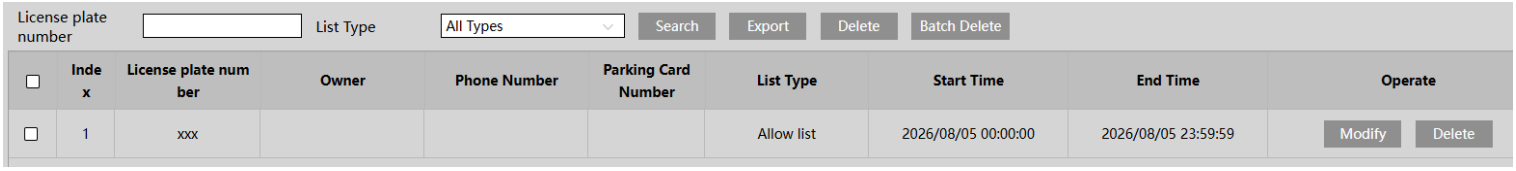
Click “Bulk Entry” to add multiple vehicles at one time as shown below.



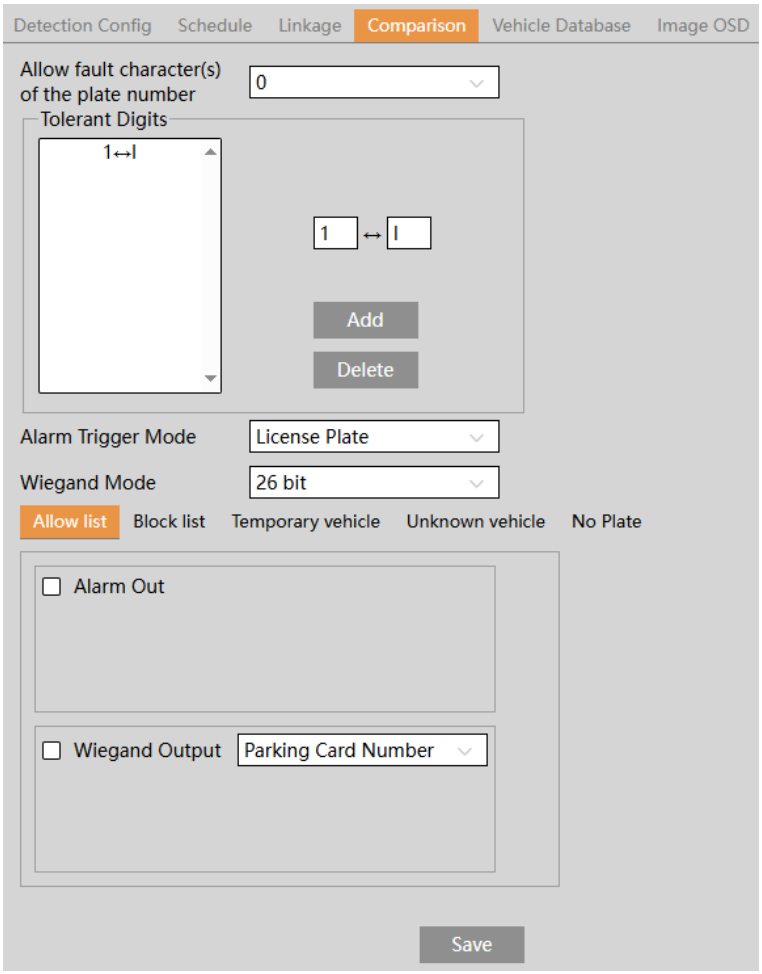
Please edit the vehicle information according to the requirements shown on the above interface. If you don’t know how to edit the file, please click “Download” to download an example file and then follow the example to edit. After that, click “Select File” to choose the vehicle information file and click “Upload” to import all vehicle information.

- **Search vehicles**

After the vehicles are added, you can search them in the vehicle list. Click “Edit” and enter the license plate number and list type and then click “Search” to search the added vehicle information. Click “Modify” to modify its information. Click “Delete” to delete this vehicle information.



8. Set the license plate comparison. Click the “Comparison” tab to go to the following interface.



Set the fault tolerance, alarm list and check “alarm out”. Finally, click “Save” to save all the settings.

Allow fault character(s) of the plate number/Erroneous characters allowed: up to 2 characters are allowed. For example, if “2” is selected, the captured license plate will be matched successfully and trigger the corresponding alarm even if there are 2 characters (or less) of the captured license plate not matched with the license plate of the vehicle list.

Tolerant Digitals: please set the tolerant character pair as needed. For example: 1 and L, supposing that the plate number “ABCL” has been added to the vehicle database, when the plate number “ABC1” is detected by the camera, then these two plate numbers will be matched successfully, and vice versa.

Alarm Trigger Mode: “License Plate” or “License Plate and Parking Card”.

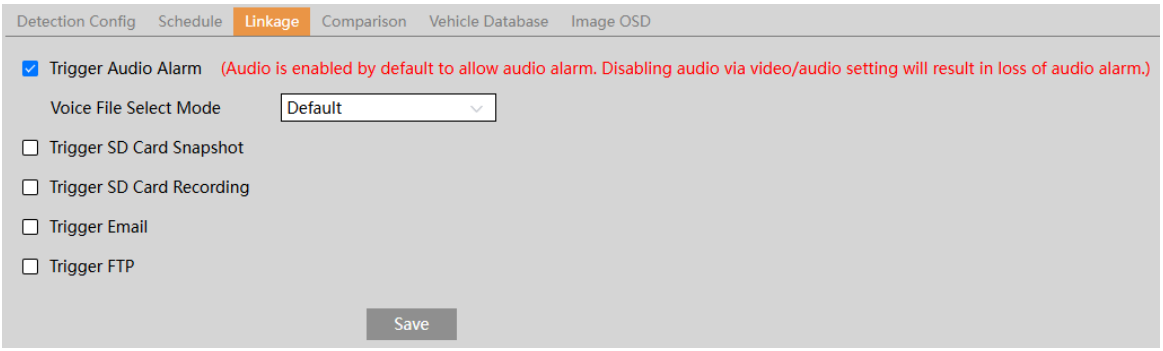
Note: if the “License Plate and Parking Card” mode is selected, the wiegand interface must be connected to the card reader as wiegand input and the parking card no. must be entered when adding the vehicle information.

Wiegand Mode: 26bit, 26bit (10), 34bit, 37bit, 42 bit, 46bit and 58bit can be optional.

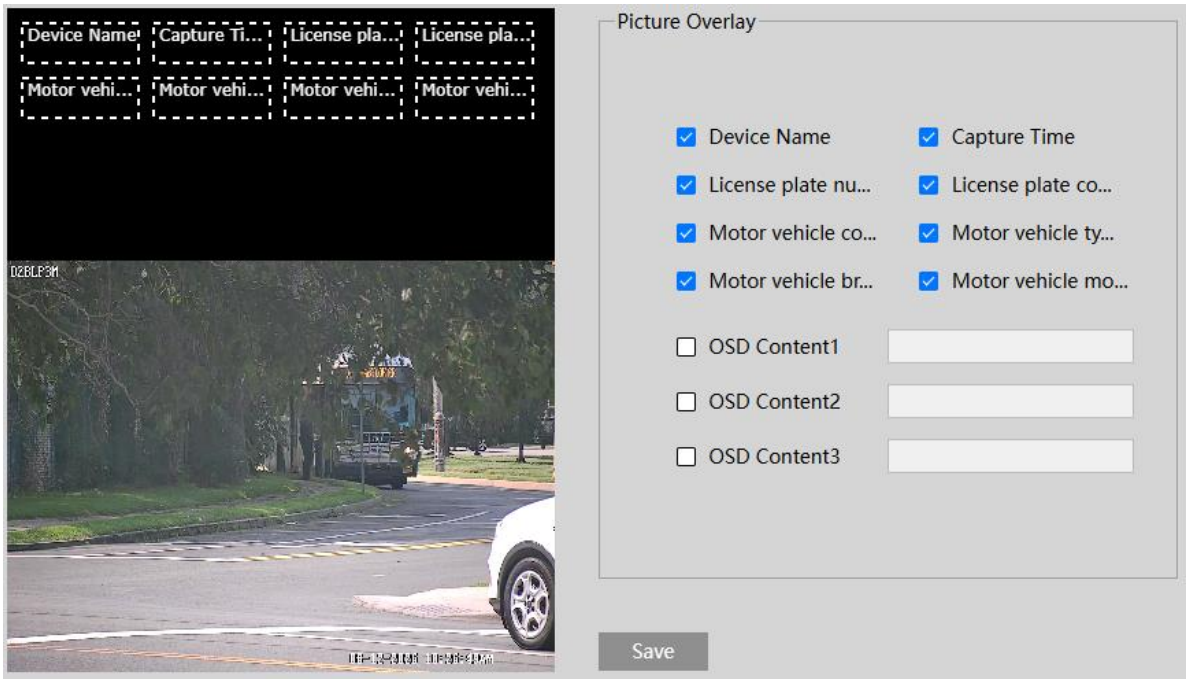
Alarm Out: Select the list type and then checkmark alarm out. Then the alarm output will be triggered when the captured plate number is matched successfully with the plate number of the selected list. If you check the alarm out of the unknown vehicle, the alarm output will be triggered once unknown vehicles (unregistered vehicles) are captured. If “No Plate” is selected, the alarm output will be triggered once the vehicles without license plate are captured.

Wiegand Output: When the alarm trigger mode is “License Plate”, you can enable Wiegand Output. Select the list type and then checkmark wiegand output. Then the wiegand output will be triggered when the captured plate number is matched successfully with the plate number of the selected list. “License plate number (SHA1)” or “Parking Card Number” can be selected.

9. Set alarm trigger options. Click the “Linkage” tab to go to the following interface. The alarm trigger setup steps are the same as motion detection setup. Please refer to motion detection for details.



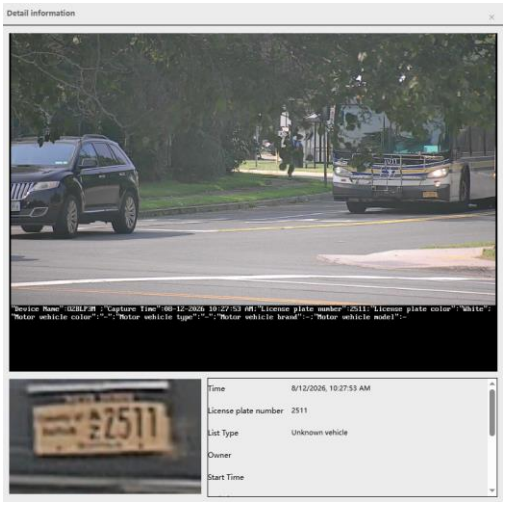
10. Select the attribute information of the target and set OSD contents as needed. Click “Image OSD” and then select the relevant attribute information.



Additionally, you can enter some OSD contents as needed. When the target is detected, the information you select will be displayed under the original snapshot in the detail page of the snapshot.

After the above items are set, go to the live interface and click  to see the captured pictures as shown below.

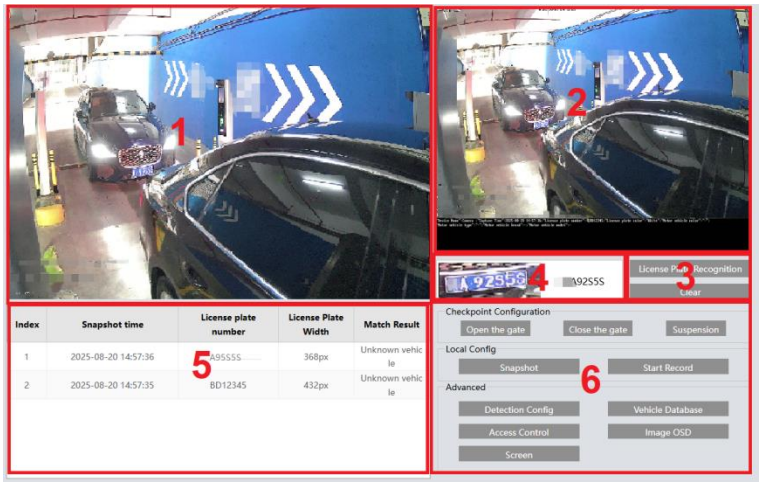
When the captured license plate is matched with the license plate of the vehicle database, the list type will be displayed under the license plate number. Click the captured license plate picture, and then the detailed information page will be displayed as shown below.



In the detailed information page, you can view the snapshot time, the captured original image, the captured plate image, motor vehicle color, license plate color, motor vehicle brand/model, etc.

3.4 Entrance and Exit

3.4.1 Real-time Image



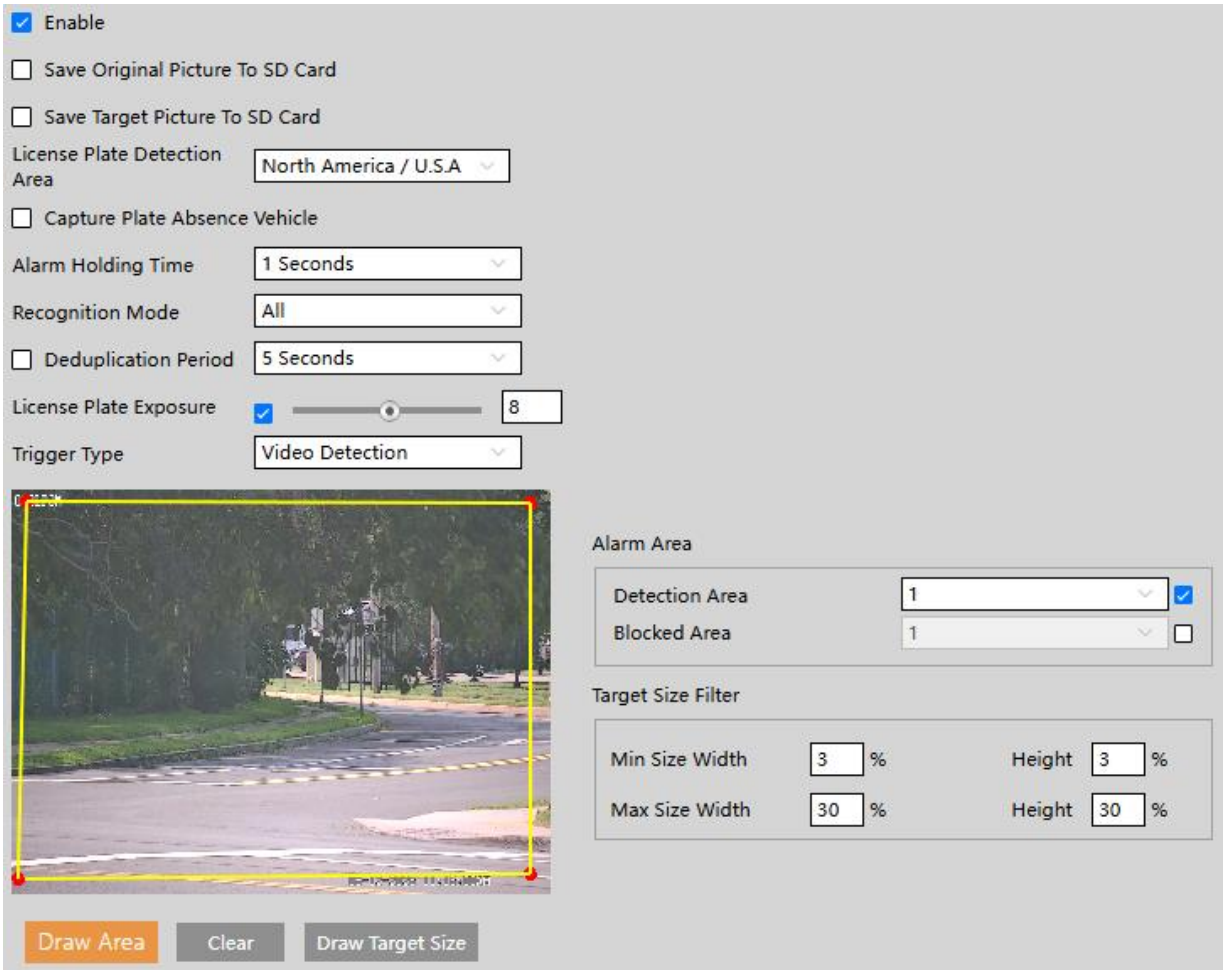
Area	Description	Area	Description
1	Live view window	4	Plate snapshot
2	Original image	5	Vehicle capture and match result display area
3	License plate recognition and clear	6	Functional areas

License Plate recognition: click “License Plate recognition” to manually trigger license plate recognition function (capture and compare the current license plate appearing in the window).
Clear: clear the current captured plate image and information.
When the vehicle cannot be successfully captured, you can manually close, open, or suspend the barrier gate.
Open the gate: manually open the gate
Close the gate: manually close the gate

Suspension: the gate is suspended by clicking the button.
Snapshot: manually capture the current image to the local PC.
Start Recording: click it to start recording and save to the local PC.

3.4.2 Detection Configuration

In the real-time image page, click "Detection Config" or click ***Config→Entrance and Exit→Detection Config*** to go to the following interface.



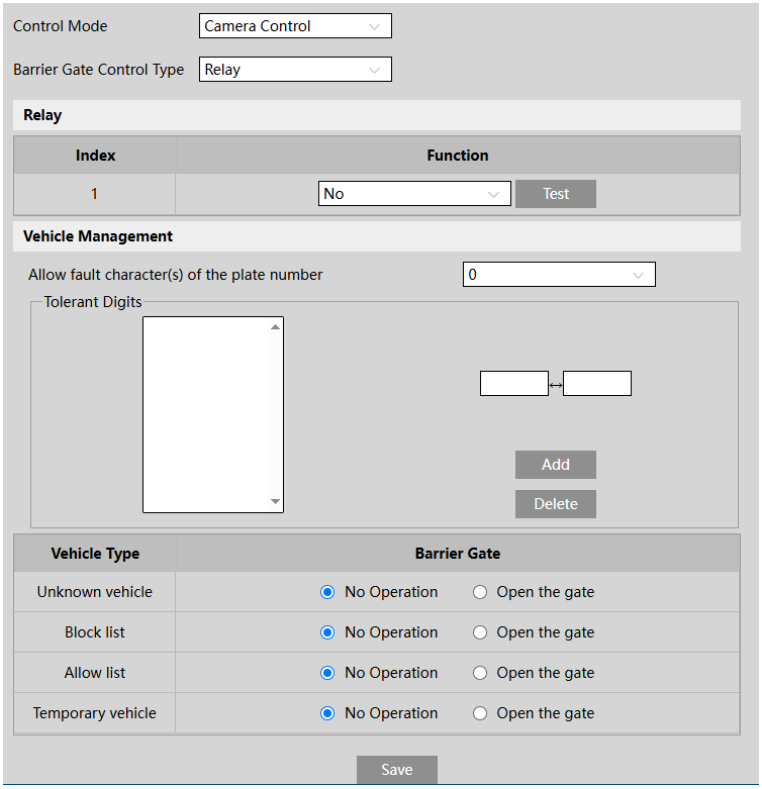
Trigger Type: video detection and IO coil.
Video Detection: Capture vehicle plates by video detection.
IO Coil: If the IO coil is connected to the camera, the trigger type could be set to "IO Coil" and then you can set the linked IO number and trigger status.

If the trigger type is set to "IO Coil", the "License Plate Recognition" button in the real-time image page will be disabled. Vehicles can be recognized and captured only when they enter the inductive zone of the induction coil.
Other detection configurations of Entrance and Exit are the same as the detection setup of license plate detection (See License Plate Detection Settings-Point 1~6 for details).

3.4.3 Access Control Settings

Only when the application scenario is "Entrance and Control", can the access control menu be displayed. In the alarm out interface, the alarm out mode is "Access Control" by default and the alarm out linkage will not take effect. If the alarm out mode is selected to other modes, the barrier gate switch will be ineffective.

In the real-time image page, click “Access Control” or click ***Config→Entrance and Exit→Access Control*** to go to the following interface.



Control Mode: Camera control or platform control.
Barrier Gate Control Type: Relay or Wiegand.

Camera Control

Relay: Some models support 2CH relay output control. Please choose “Open the gate”, “Close the gate” or “Suspension” as needed. Click “Test” to test whether the relay output control is effective.

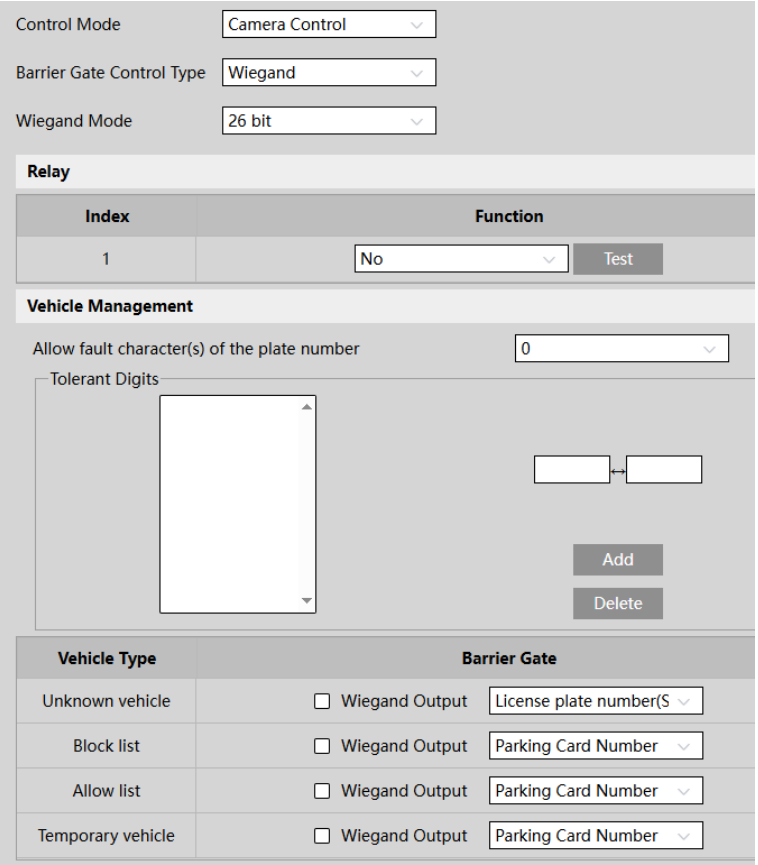
Vehicle Management

The fault tolerance setup here is the same as the fault tolerance setup of the license plate detection. (See License Plate Detection Settings-Point 8 for details)

Additionally, you can set whether to open the gate or not for vehicles of different types. It is recommended to set “No Operation” for block list so that the barrier gate will not be opened once the vehicle is matched from the block list.

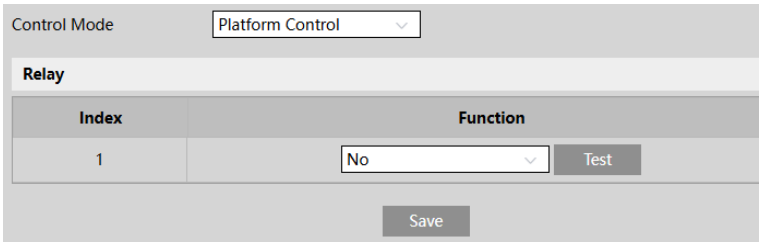
“Open the gate”: if enabled, the barrier gate will be opened automatically once the vehicle is matched successfully.

Wiegand: If the barrier gate control type is set to “Wiegand”, please set the Wiegand mode as needed.



You can set the wiegand output type for the captured unknown vehicle/blocklist/allowlist/ temporary vehicle. Only license plate number (SHA1) can be selected for unknown vehicles.

- **Platform Control**



If you add your camera into the platform and link it to the parking lot management module, the control mode can be set to "Platform control". Then set the relay output as needed.

3.4.4 Vehicle Database Management

In the real-time image page, click "Vehicle Database" or click ***Config→Entrance and Exit→Vehicle Database***. The vehicle database management here is the same as the database management of license plate detection (See License Plate Detection Settings- Point 7 for details).

3.4.5 Image OSD Settings

In the real-time image page, click "Image OSD" or click ***Config→Entrance and Exit→Image OSD***. The image OSD setup here is the same as the image OSD setup of license plate detection (See License Plate Detection Settings- Point 10 for details).

3.4.6 Screen

You can connect a RS485/RS232 screen to display the captured license plate. Go to ***Config→Entrance and Exit→Screen*** to enable it. Before you enable this function, please connect a specific screen through RS485/RS232 interface first. After that, click ***Config→System→Serial Port*** to set the Baud-Rate. The baud rate of the camera and the screen must be the same (See Serial Port Settings for details).

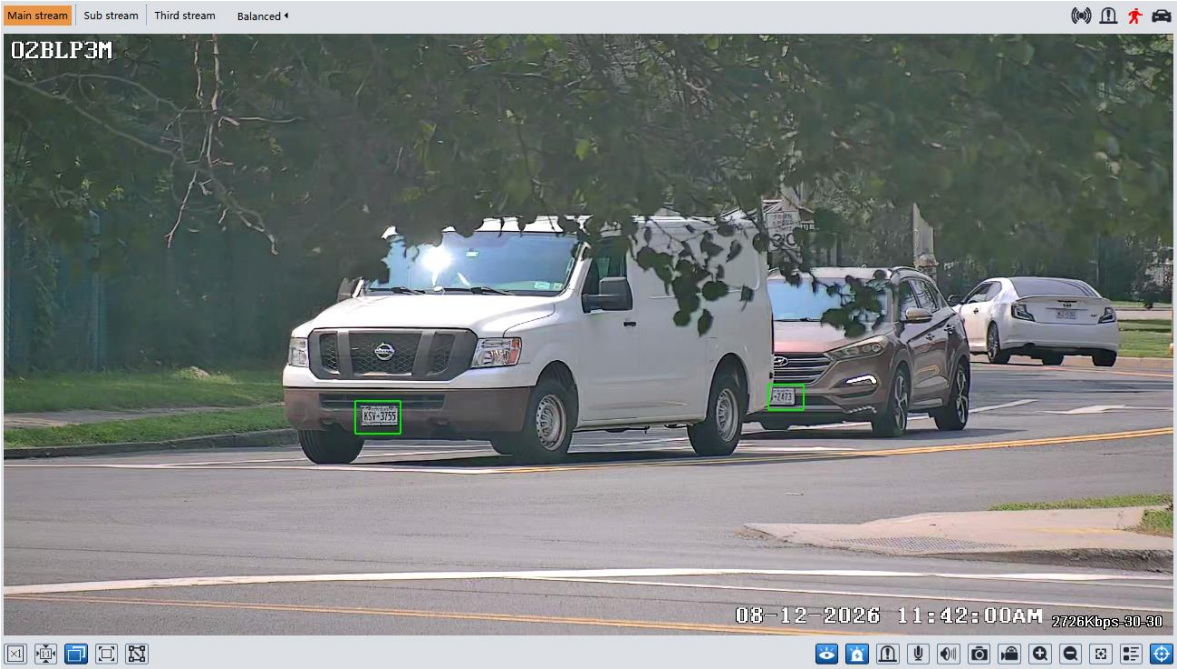
Note:

* Only some models support RS232 interface.

* Only some specific screens are supported. For the compatible screen brands, please contact the camera manufacturer or your supplier for details.

4 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		Zoom out
	Fit correct scale		Zoom/Focus control
	Auto (fill the window)		License plate detection
	Full screen		Rule information display
	Measure Tool		SD card recording indicator
	Start/stop live view		Sensor alarm indicator
	Enable/disable alarm status display		License plate detection indicator
	Enable/disable alarm output		Alarm output indicator
	Enable or disable audio alarm		Audio alarm indicator
	Start/stop two-way audio		Motion alarm indicator
	Enable/disable audio		Color abnormal indicator
	Snapshot		Abnormal clarity indicator
	Start/stop local recording		Scene change indicator
	Zoom in		

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

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

Click the zoom/focus control button to show the control panel. The descriptions of the control panel are as follows:

Icon	Description	Icon	Description
	Zoom -		Zoom +
	Focus -		Focus +
	One key focus (used when image is out of focus after manual adjustment)		

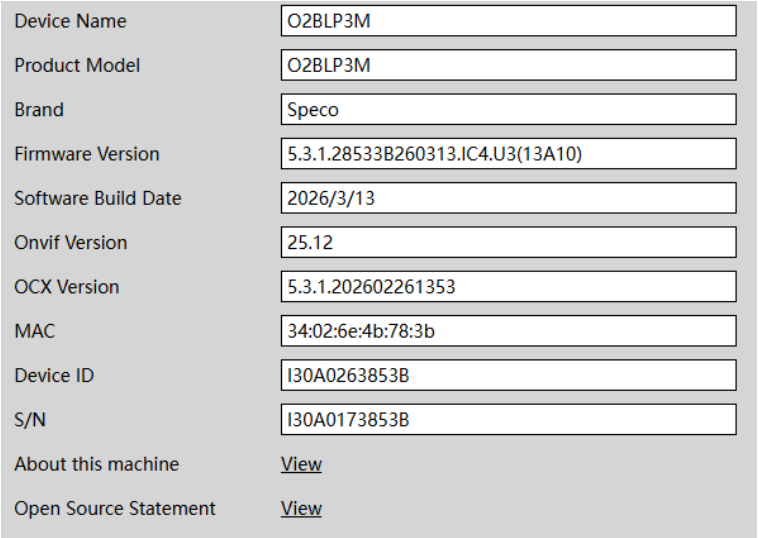
5 Camera Configuration

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

5.1 System Configuration

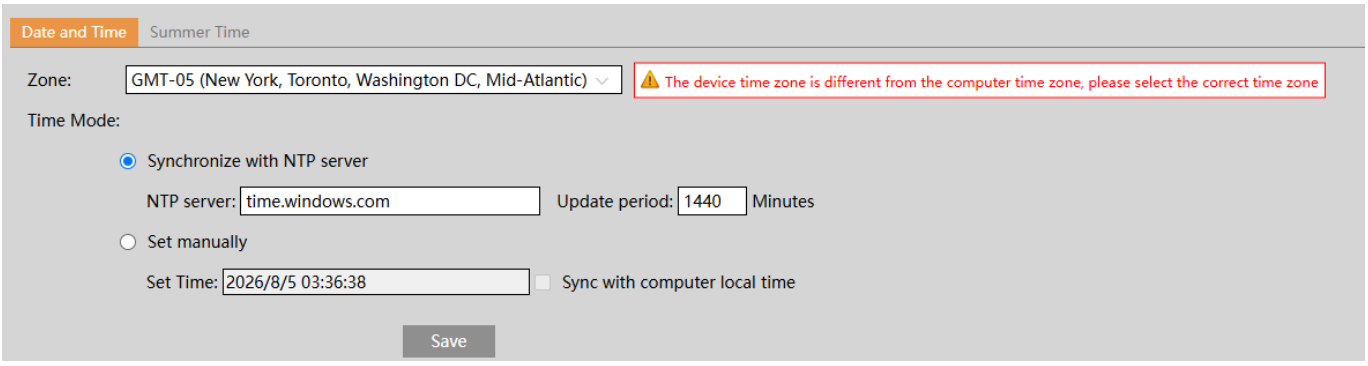
5.1.1 System Information

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



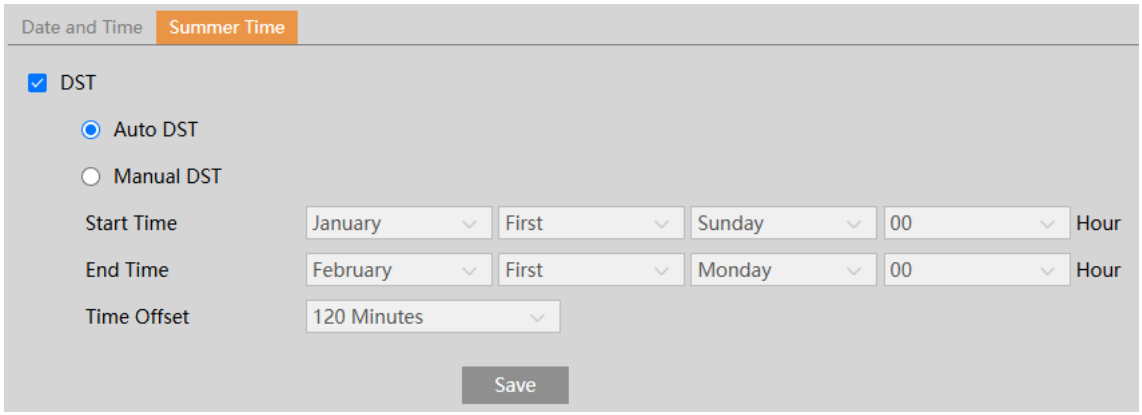
5.1.2 Date and Time

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



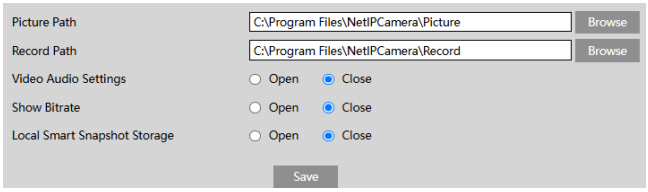
Select the time zone and time mode as needed.
Note: The time zone of the camera and the computer must be the same. It is recommended to modify the time zone of the camera according to the time zone of the computer. If the time zone of the computer is modified, the current web client needs to be closed. Then re-open it and log in again.

Time Mode:
NTP: Specify an NTP server to synchronize the time.
Manual: Set the system time manually or you can synchronize the time with the time of the local computer.
Click the “Summer Time” tab to set DST (Daylight Saving Time) as needed.



5.1.3 Local Config

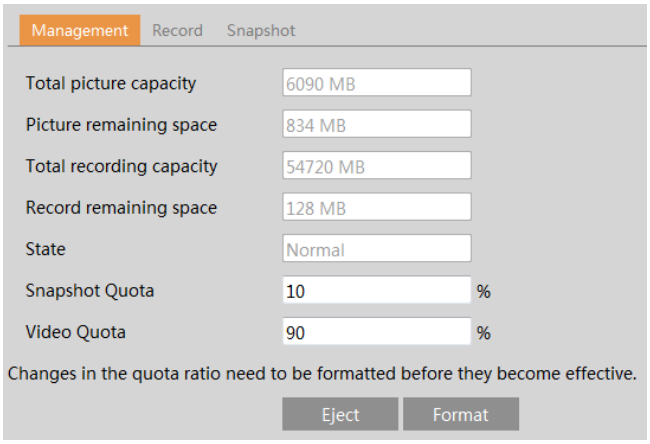
Go to ***System→Local Config*** to set up the storage path of captured pictures and recorded videos on the local PC. There is also an option to enable or disable the bitrate display in the recorded files.



Show Bitrate: enable or disable bitrate display in the live video.
Additionally, "Local smart snapshot storage" can be enabled or disabled here. If enabled, the captured pictures triggered by smart events (like line crossing detection, region intrusion, etc.) will be saved to the local PC.
Note: when you access your camera by the web browser without the plug-in, only Show Bitrate can be set in the above interface.

5.1.4 Storage

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



- **SD Card Management**

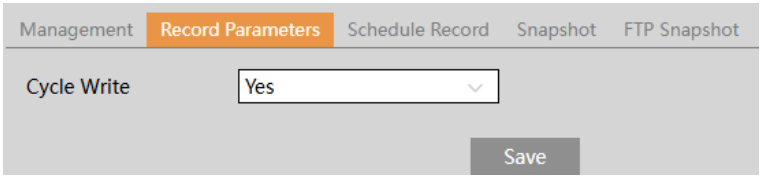
Click the "Format" button to format the SD card. All data will be cleared by clicking this button.
Click the "Eject" button to stop writing data to the SD card. Then the SD card can be ejected safely.
Snapshot Quota: Set the capacity proportion of captured pictures on the SD card.
Video Quota: Set the capacity proportion of record files on the SD card.

Note: This series of products support ANR (Automatic Network Replenishment) function.
1. When the network of the camera is disconnected (for example, the network cable is unplugged), the camera will automatically

trigger record and store the recorded files to the SD card.
2. After the IPC is added to the NVR supporting ANR function and the ANR function of the IPC is enabled in the NVR, the IPC will automatically trigger record and store the recorded files to the SD card when the network between the NVR and the IPC is disconnected. After resuming connection, the IPC will automatically upload the recorded files during the offline period to the NVR.

- **Configuring Record Parameters**

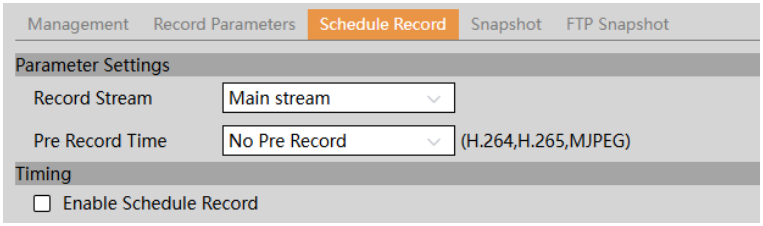
Go to ***Config→System→Storage→Record Parameters***.



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

- **Schedule Recording Settings**

Go to ***Config→System→Storage→Schedule Record*** to go to the interface as shown below.



Pre-Record Time: Set the time to record before the actual recording begins.
Schedule Record: Check "Enable Schedule Record" and set the schedule.

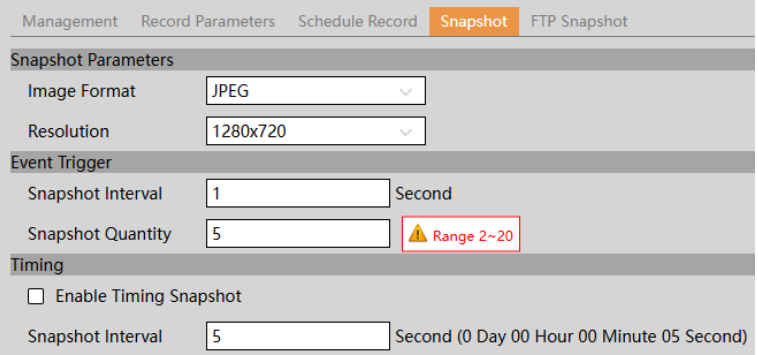
Weekly schedule
Set the alarm time from Monday to Sunday for a single week. Each day is divided into one-hour increments. Green means scheduled. Blank means unscheduled.
"Add": Add the schedule for a special day. Drag the mouse to set the time on the timeline.

"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**

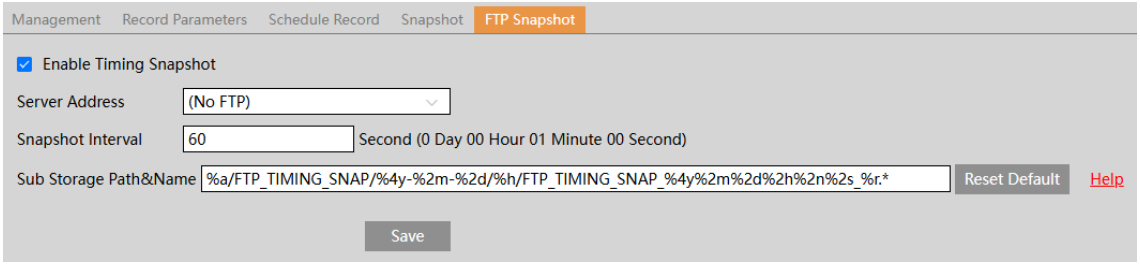
Go to ***System→Storage→Snapshot*** to go to the interface as shown below.



Set the format, resolution and quality of the image saved on the SD card and the snapshot interval and quantity and the timing snapshot here.
Snapshot Quantity: The number you set here is the maximum quantity of snapshots. The actual quantity of snapshots may be less than this number. Supposing the occurrence time of an alarm event is less than the time of capturing pictures, the actual quantity of snapshots is less than the set quantity of snapshots.
Timing Snapshot: Enable timing snapshot first and then set the snapshot interval and schedule. The setup steps of schedule are the same as the schedule recording (See Schedule Recording).

- **FTP Snapshot**

Enable timing snapshot. If enabled, the system will upload snapshots to the FTP server according to the set snapshot interval.



Server Address: select the set FTP server. See the FTP section for the FTP server setting.
Sub Storage Path& Name: Click "Help" to view the rule and then set it as needed.
Meanings of the default Path & Name Settings:
"%a/FTP_TIMING_SNAP/%4y-%2m-%2d/%h" stands for sub storage path
"FTP_TIMING_SNAP_%4y%2m%2d%2h%2n%2s_%r.* " stands for file name
The entire default value means that a jpg file named "FTP_TIMING SNAP _Year Month Day Hour Minute Second_Random number" will be generated under FTP root directory> MAC address>FTP_TIMING SNAP>Year-Month-Day>Hour
"FTP_TIMING SNAP" refers to the event type. You can modify the event name as needed (for example: FTP Snapshot).
If the sub storage path and name box is empty, the snapshot will be uploaded and named according to the default settings.
If you only enter the file name rule, the snapshot will be uploaded to the root directory of the FTP server.

5.1.5 Serial Port Settings

Go to ***Config→System→Serial Port*** to configure RS485/RS232 protocol.

- **RS 485 settings**

You can connect a RS485 screen to display the captured license plate in entrance and exit control mode. The baud rate must be the same as the screen. Other parameters are suggested to use the default settings. When the IPC connected a RS485 screen is added to the platform and the IPC is linked to a lane in the parking management module, the transparent mode should be enabled.
Additionally, you can use RS485 to transmit the data between the camera and the computer or terminal. Before using this function, please connect the camera and computer or terminal with RS485 cable. Please set the parameters of RS485 as needed. Note that you should keep the parameters of the camera and the computer or terminal all the same.

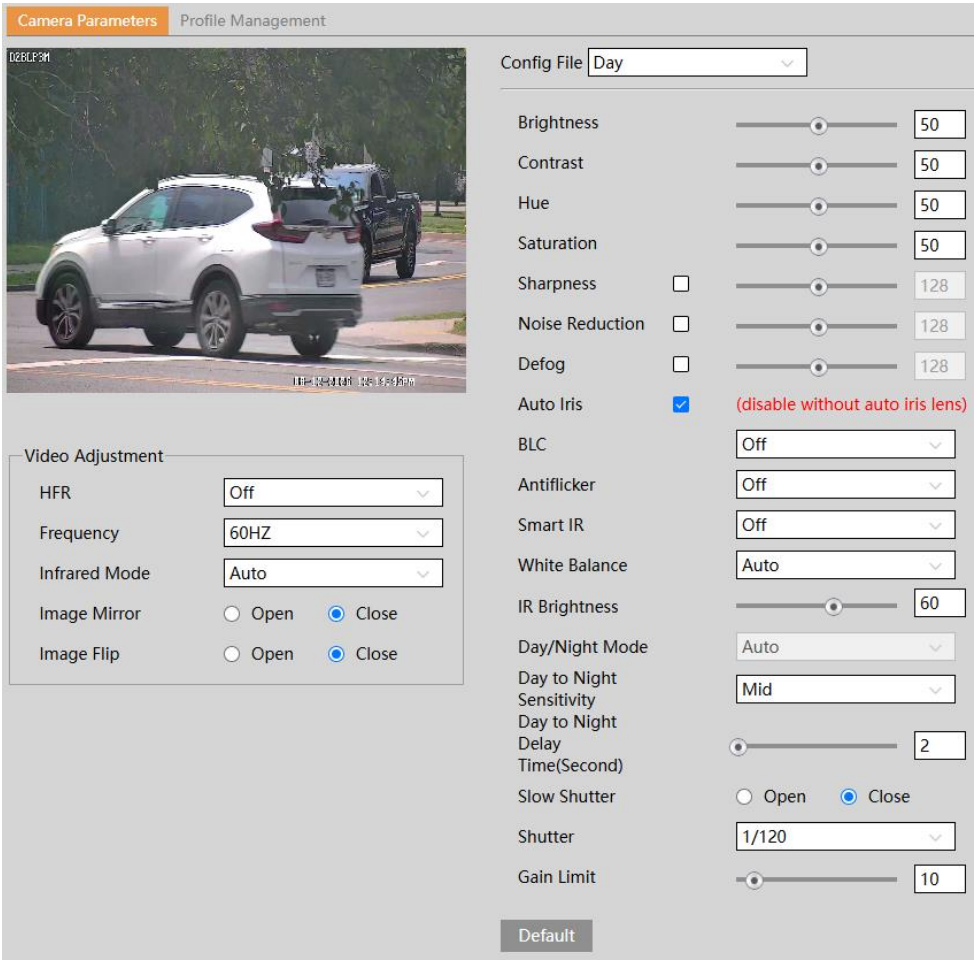
- **RS232 settings**

This function is only available for the model with RS232 interface.
It is used to connect the LED screen, card reader or other third-party device. Please set the relevant parameters according to the device you connect. In addition, you can also use RS232 to transmit the data between the camera and the computer or terminal.
Note：Transparent mode should be enabled when you use RS232/RS485 to transmit the data between the camera and the computer or terminal.

5.2 Video Configuration

5.2.1 Image Configuration

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



Brightness: Set the brightness level of the camera's image.
Contrast: Set the color difference between the brightest and darkest parts.
Hue: Set the total color degree of the image.
Saturation: Set the degree of color purity. The purer the color, the brighter the image is.
Sharpness: Set the resolution level of the image plane and the sharpness level of the image edge.
Noise Reduction: Decrease the noise and make the image more thorough. Increasing the value will make the noise reduction effect better but it will reduce the image resolution.
Defog: Activating this function and setting an appropriate value as needed in foggy, dusty, smoggy, or rainy environments to get clear images.
Auto Iris: If your camera is auto Iris, please enable it.
Backlight Compensation (BLC):

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

Note: After enabling HWDR, the shutter and gain limit cannot be modified. Additionally, the anti-flicker function is automatically turned off and cannot be set.

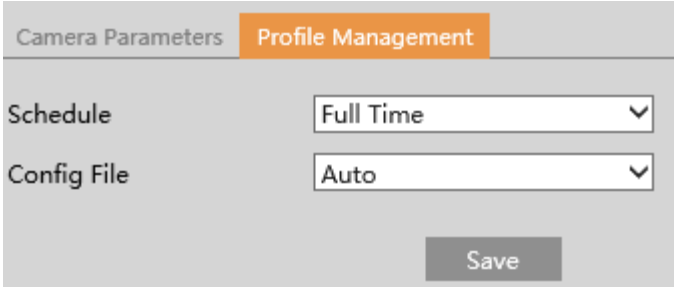
- HLC: lowers the brightness of the entire image by suppressing the brightness of the image's bright area and reducing the size of the halo area.
- BLC: If enabled, the auto exposure will activate according to the scene so that the object of the image in the darkest area will be seen clearly.

Antiflicker:

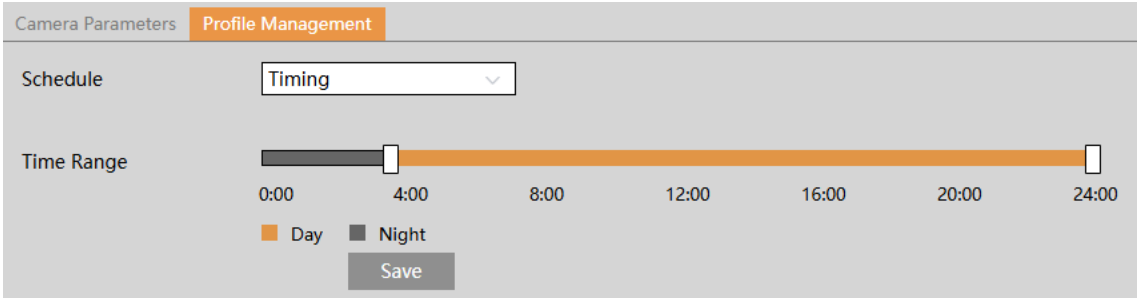
- Off: disables the anti-flicker function. This is used mostly in outdoor installations.
- 50Hz: reduces flicker in 50Hz lighting conditions.
- 60Hz: reduces flicker in 60Hz lighting conditions.

Smart IR: Choose "ON" or "OFF". This function can effectively avoid image overexposure to make the image more realistic. The higher the level is, the more overexposure compensation will be given.
White Balance: Adjust the color temperature according to the environment automatically.
Day/Night Mode: Choose "Auto", "Day", "Night" or "Timing (Schedule)".
If "Timing (Schedule)" 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.
Slow Shutter: If enabled, the camera will slowly decrease the frame rate to keep a certain level of brightness in low light environments.
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.
HFR: High Frame Rate. If "ON" is selected, the system will restart and then the maximum value of the frame rate of the main stream can be set to 1080P@ 60 fps /50fps.
Frequency: 50Hz and 60Hz can be optional.
Infrared Mode: Choose "Auto", "ON" or "OFF".
Image Mirror/Flip Vertically: Turn the current video image horizontally.
Image Flip/Flip Horizontally: Turn the current video image vertically.

Schedule Settings of Image Parameters:
Click the "Profile Management" tab as shown below.



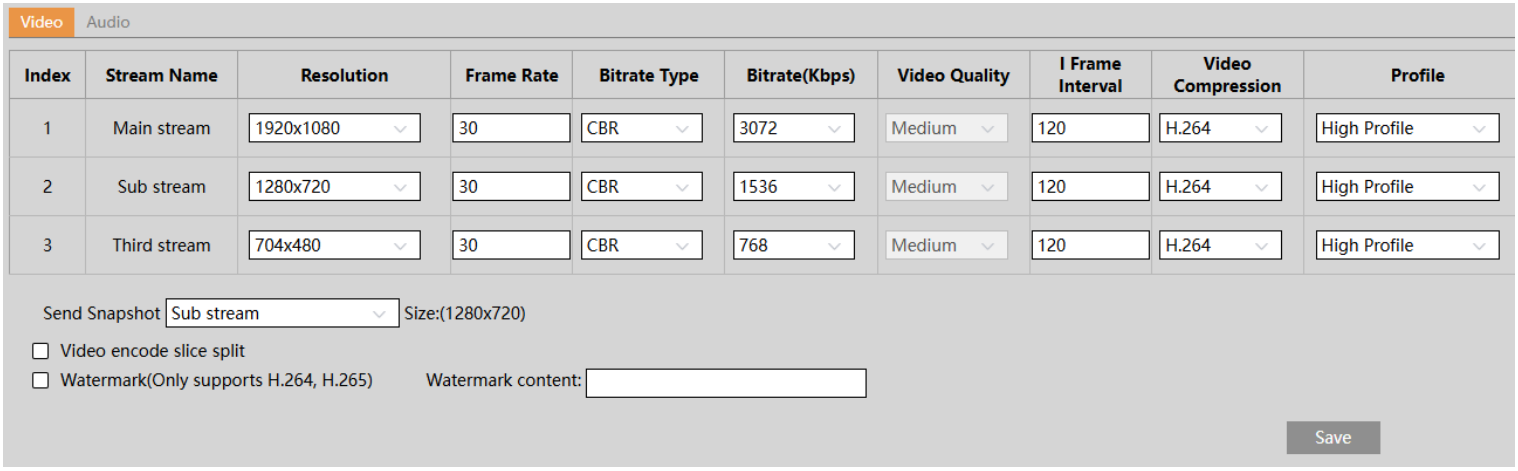
Set full Time schedule for common, day or night mode and specified time schedule for day and night. Choose “Timing” in the drop-down box of schedule as shown below.



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.

5.2.2 Video / Audio Configuration

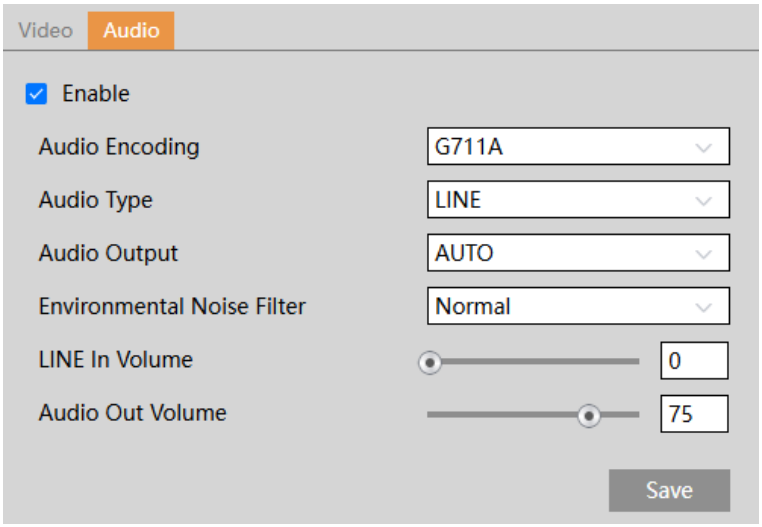
Go to ***Image→Video / Audio*** as shown below. In this interface, set the resolution, frame rate, bitrate type, video quality and so on subject to the actual network condition.



Three video streams can be adjustable.
Resolution: The size of image.
Frame rate: The higher the frame rate, the video is smoother.
Bitrate type: CBR and VBR are optional. Bitrate is related to image quality. CBR means that no matter how much change is seen in the video scene, the compression bitrate will be kept constant. VBR means that the compression bitrate will be adjusted according to scene changes. For example, for scenes that do not have much movement, the bitrate will be kept at a lower value. This can help optimize network bandwidth usage.
Bitrate: it can be adjusted when the mode is set to CBR. The higher the bitrate, the better the image quality will be.
Video Quality: It can be adjusted when the mode is set to VBR. The higher the image quality, the more bitrate will be required.

I Frame interval: It determines how many frames are allowed between a “group of pictures”. When a new scene begins in a video, until that scene ends, the entire group of frames (or pictures) can be considered as a group of pictures. If there is not much movement in the scene, setting the value higher than the frame rate is fine, potentially resulting in less bandwidth usage. However, if the value is set too high, and there is a high frequency of movement in the video, there is a risk of frame skipping.
Video Compression: MJPEG, H264+, H264, H265 or H265+ can be optional. MJPEG is not available for main stream. If H.265/H.265+ is chosen, make sure the client system is able to decode H.265/H.265+. Compared to H.265, H.265+ saves more storage space with the same maximum bitrate in most scenes. Compared to H.264, H.265 reduces the transmission bitrate under the same resolution, frame rate and image quality.
Profile: For H.264. Baseline, main and high profiles are selectable.
Send Snapshot: Set the snapshot stream.
Video encode slice split: If this function is enabled, smooth image can be gotten even though using the low-performance PC.
Watermark: When playing back the local recorded video in the search interface, the watermark can be displayed. To enable it, check the watermark box and enter the watermark text.

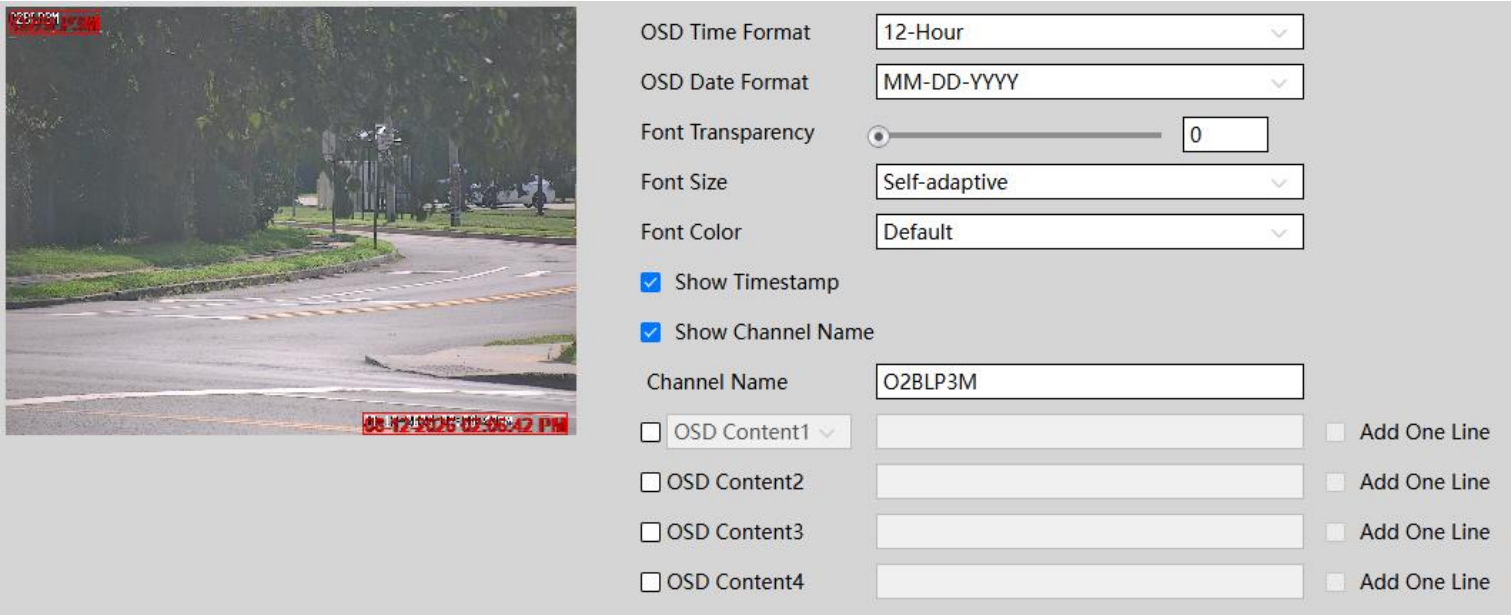
Click the “Audio” tab to go to the interface as shown below.



Audio Encoding: G711A and G711U are selectable.
Audio Type: LINE
Audio Output: Talkback, warning or auto can be optional. If “Talkback” is selected, the audio output will be used for two-way audio. If “Warning” is selected, the audio output will be used to play the pre-defined audio alarm. If “Auto” is selected, the system will output sound for two-way audio or warning voice as needed. But when it is warning and two-way audio is being enabled simultaneously, two-way audio will be output first.
Environmental Nosie 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.
LINE IN/Audio Out Volume: Set the volume as needed.

5.2.3 OSD Configuration

Go to ***Image→OSD*** as shown below.



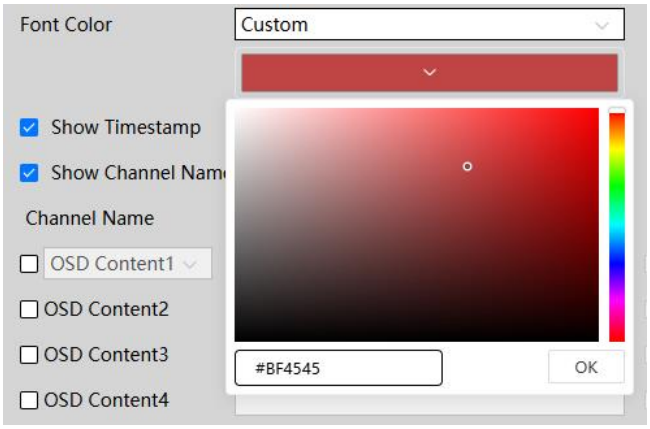
Set OSD time format, OSD date format, OSD content and font transparency/size/color here. After enabling the corresponding display and entering the content, drag them to change their position. Then click the "Save" button to save the settings.

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 change of 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 size color:



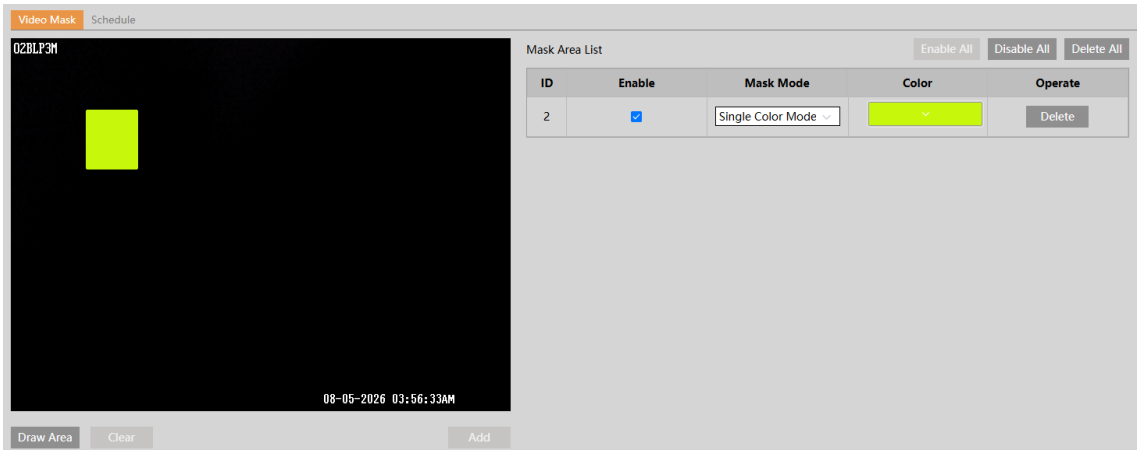
1. Select "Custom" and then click on the blank box under it.
2. Select a color on the colorful bar (right).
3. Click on the left color box to choose the desired color. Or you can directly enter the hexadecimal color code to set the color.
4. Click "OK" to save the OSD font color settings.

Picture Overlap Settings:

Check "OSD Content1", choose "Picture Overlay" and click to select the overlapping picture. Then click "Open" to upload the overlapping picture. The pixel of the image shall not exceed 200*200, or it cannot be uploaded.

5.2.4 Video Mask

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

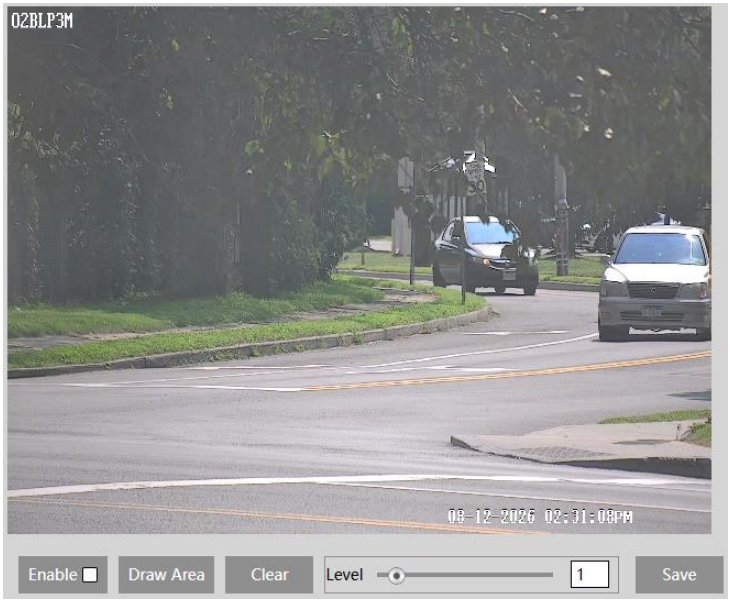


To set up a video mask:

1. Click the "Draw Area" button and then drag the mouse on the left window to draw the video mask area.
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.

5.2.5 ROI Configuration

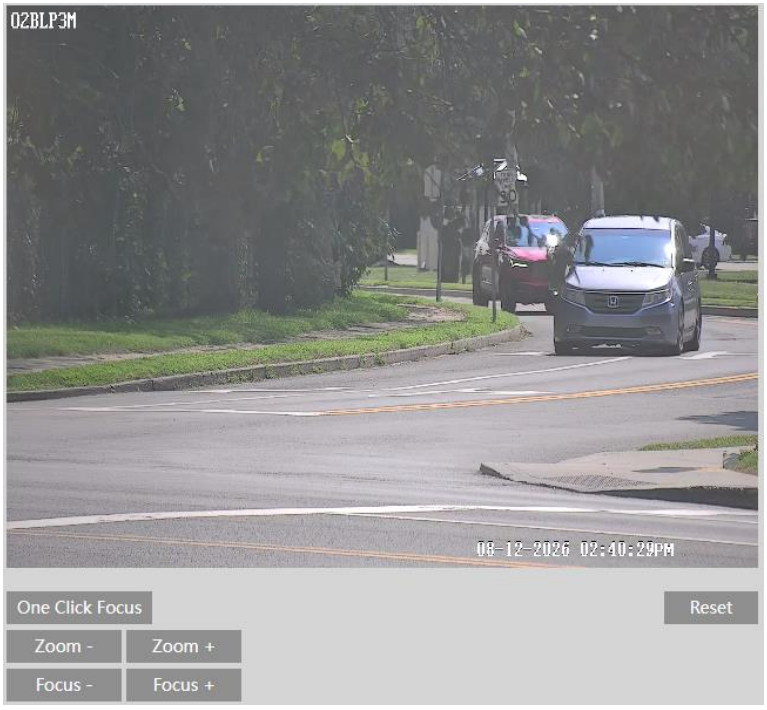
Go to ***Image→ROI Config*** as shown below. An area in the image can be set as a region of interest. This area will have a higher bitrate than the rest of the image, resulting in better image quality for the identified area.



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.

5.2.6 Zoom/Focus

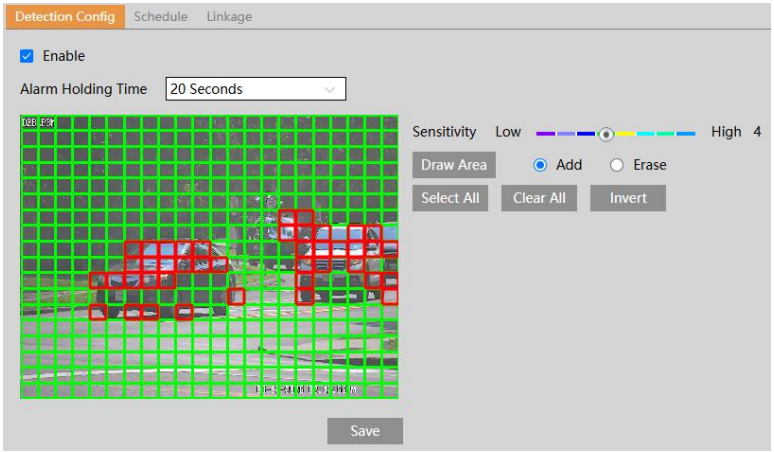
This function is only available for the model with motorized zoom lens. Within this section, zoom and focus can be controlled. If the image is out of focus after a manual adjustment, one key focus can be used to set the focus automatically.



5.3 Alarm Setup

5.3.1 Motion Detection

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



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

Alarm Holding Time: it refers to the time that the alarm extends after an alarm ends. For instance, if the alarm holding time is set to 20 seconds, once the camera detects a motion, it will go to alarm and will not detect any other motion in 20 seconds. If there is another motion detected during this period, it will be considered as continuous movement; otherwise, it will be considered as a single motion.

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.

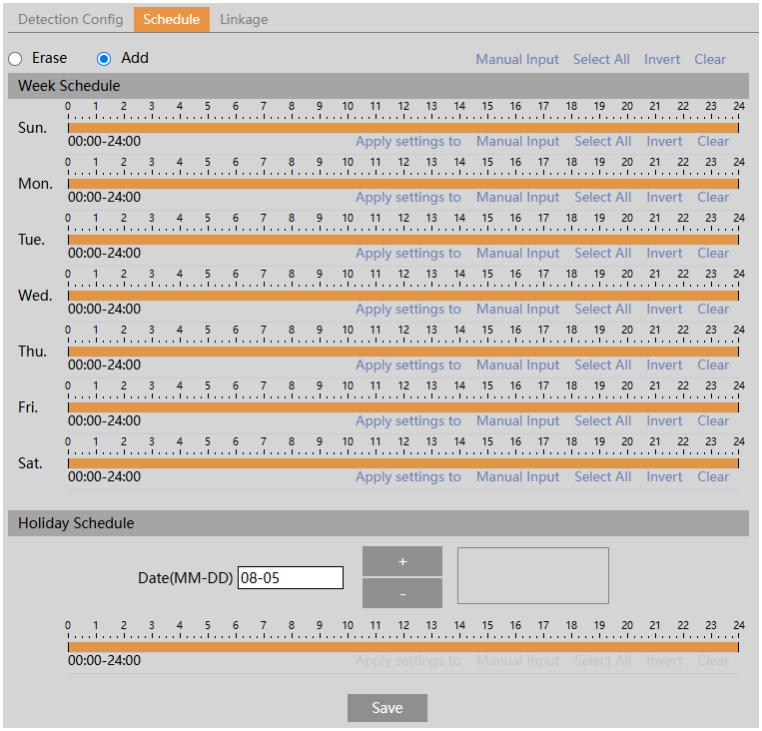
After that, click the “Save” to save the settings.

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.



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.

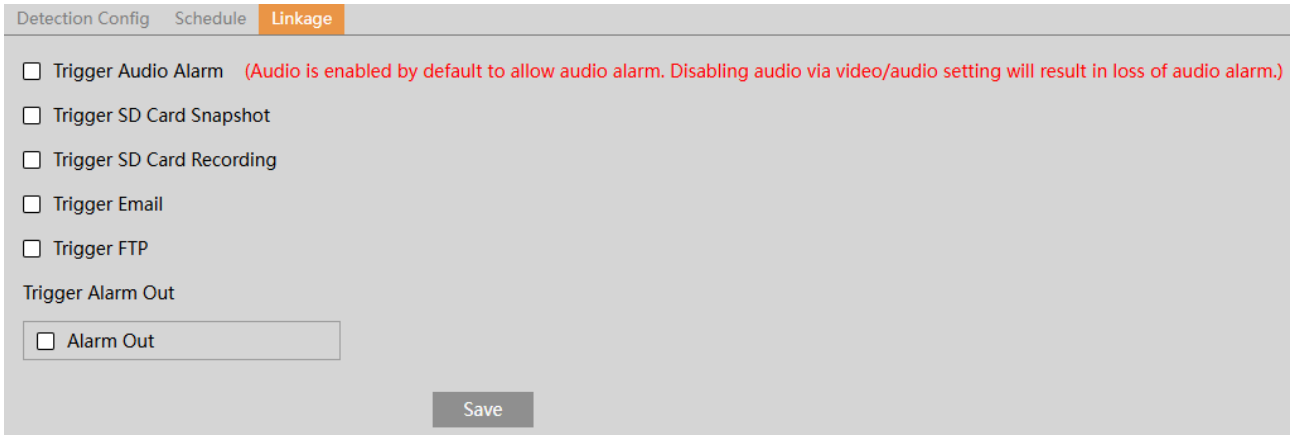
Manual Input: Click it for a specific day to enter specific start and end times. This adds more granularities (minutes).

Day schedule

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

Note: Holiday schedule takes priority over weekly schedule.

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

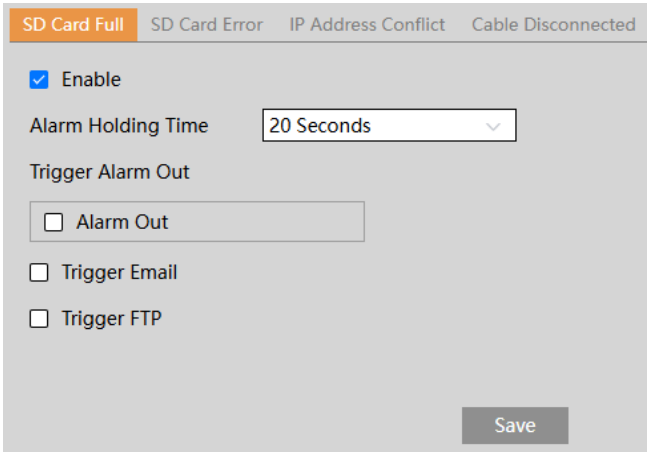


Trigger Audio Alarm: If selected, the warning voice will be played on detecting a motion-based alarm. After checking it, you need to select the voice file as needed. If "Default" is selected, the voice file is the voice set in the audio alarm interface (see Audio Alarm for details). If "Specified" is selected, you can specify the warning voice and language for the motion alarm.
Trigger SD Card Snapshot: If selected, the system will capture images on motion detection and save the images on an SD card.
Trigger SD Card Recording: If selected, the 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 to those addresses.
Trigger FTP: If "Trigger FTP" and "Attach Picture" are checked, the captured pictures will be sent to the FTP server address. You can set the sub storage path and name as needed. Please refer to the FTP configuration for more details.
Trigger Alarm Out: If selected, this would trigger an external relay output that is connected to the camera on detecting a motion-based alarm. (For the models with two alarm output interfaces, two alarm out can be selected)

5.3.2 Other Alarms

- **SD Card Full**

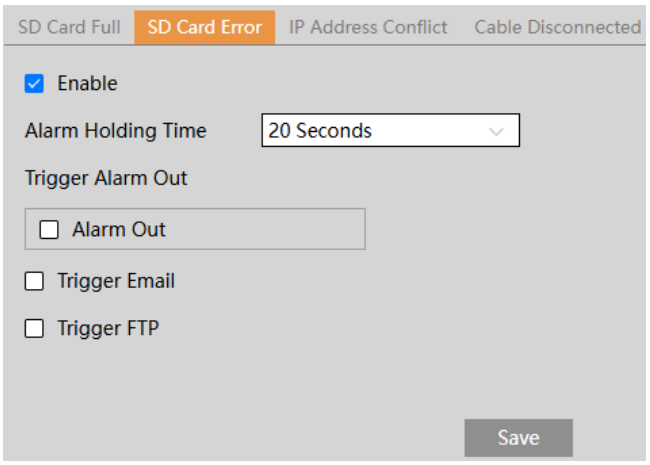
1. Go to ***Config →Alarm →Exception Alarm →SD Card Full***.



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

- **SD Card Error**

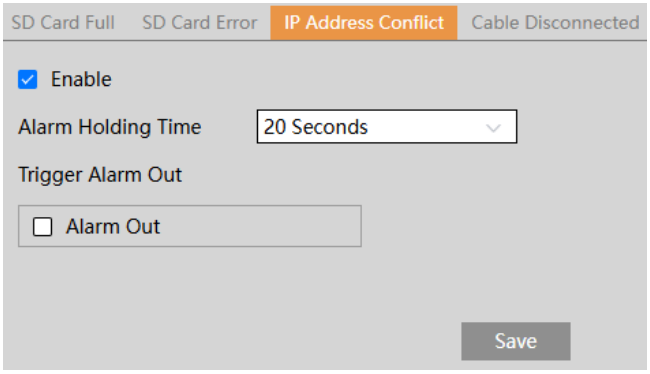
When there are some errors in writing to the SD card, the corresponding alarms will be triggered.
1. Go to ***Alarm →Exception Alarm →SD Card Error*** as shown below.



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 for details.

- **IP Address Conflict**

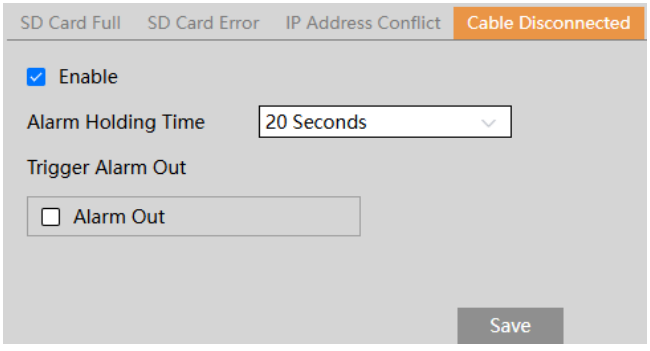
1. Go to ***Alarm →Exception Alarm →IP Address Conflict*** as shown below.



2. Click “Enable alarm” and set the alarm holding time.
3. Trigger alarm out. When the IP address of the camera is in conflict with the IP address of other devices, the system will trigger the alarm out.

- **Cable Disconnection**

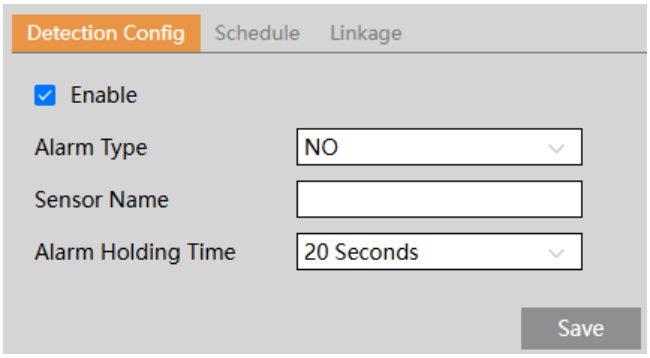
1. Go to ***Alarm →Exception Alarm →Cable Disconnected*** as shown below.



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.

5.3.3 Alarm In (Sensor Input)

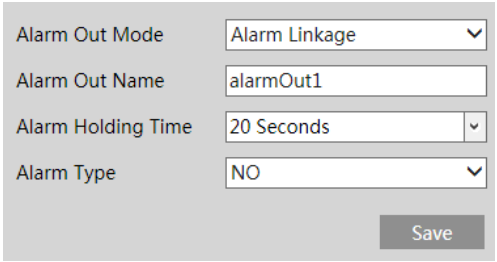
This function is only available for some models. To set sensor alarm (alarm in):
Go to ***Config→Alarm→Alarm In*** as shown below.



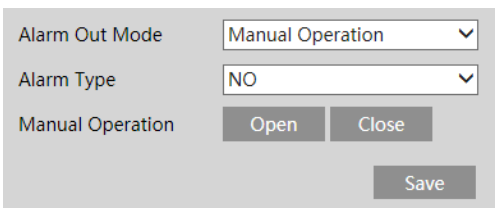
1. Click “Enable” and set the alarm type, alarm holding/latch time and sensor name.
2. Click the “Save” button to save the settings.
3. Set the schedule of the sensor alarm. The setup steps of the schedule are the same as the schedule recording setup (See Schedule Recording).
4. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as motion detection. Please refer to motion detection for details.

5.3.4 Alarm Out

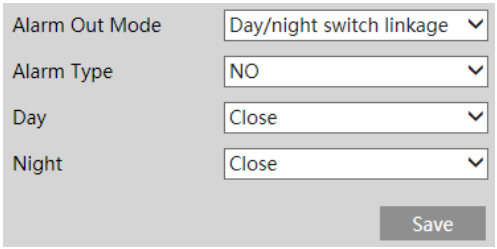
This function is only available for some models. Go to ***Alarm→Alarm Out***.



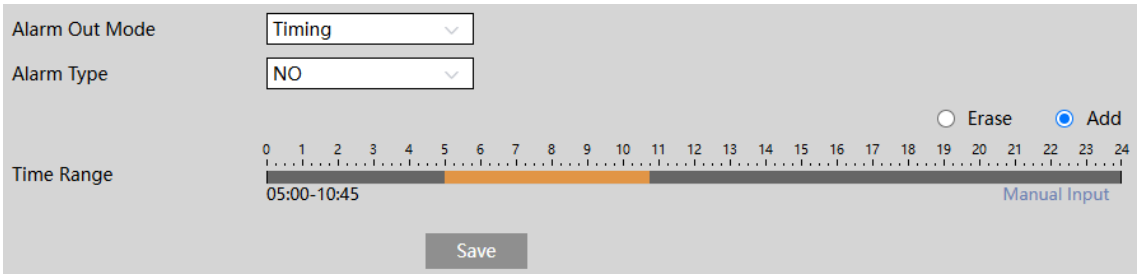
Alarm Out ID: Some models may support two alarm output interfaces. The alarm out can be set respectively by selecting alarm out ID.
Alarm Out Mode: Alarm linkage, manual operation, day/night switch linkage (day/night indicator via alarm in) and timing (schedule) are optional.
Note: In Entrance and Exit mode, “Access Control” alarm out mode will be selected by default. If a barrier gate is connected through the alarm output interface, please select “Access Control”. If the alarm out mode is selected to other modes, the barrier gate switch will be ineffective. If “Access Control” is selected, alarm linkage actions will not take effect.
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 the alarm type and click “Open” to trigger the alarm out immediately; click “Close” to stop alarm.



Day/Night Switch Linkage: Having selected this mode, select the alarm type and then choose to open or close alarm out when the camera switches to day mode or night mode. (For white light models, this function is not available)

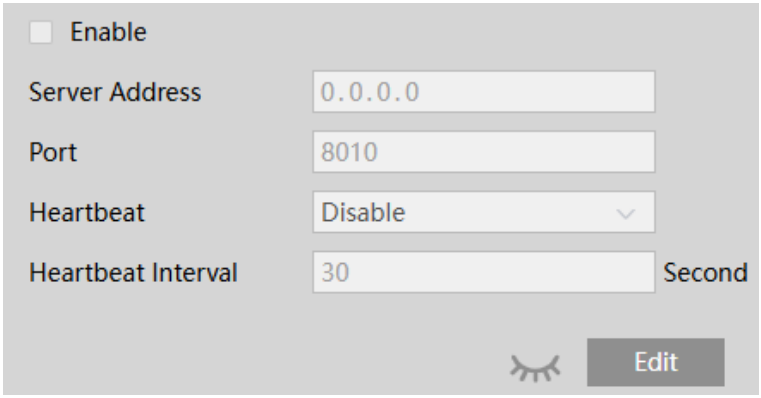


Timing (Schedule): Select the alarm type. Then click "Add" and drag the mouse on the timeline to set the schedule of alarm out; click "Erase" and drag the mouse on the timeline to erase the set time schedule. After this schedule is saved, the alarm out will be triggered in the specified time.



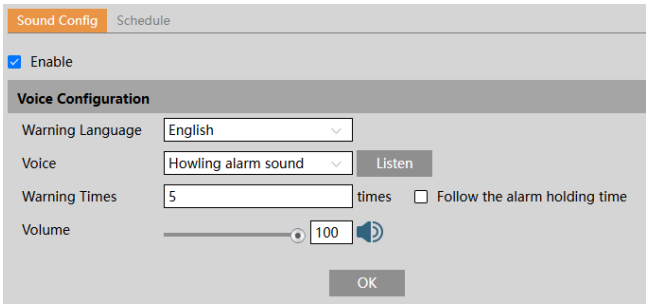
5.3.5 Alarm Server

Go to ***Alarm→Alarm Server*** 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.

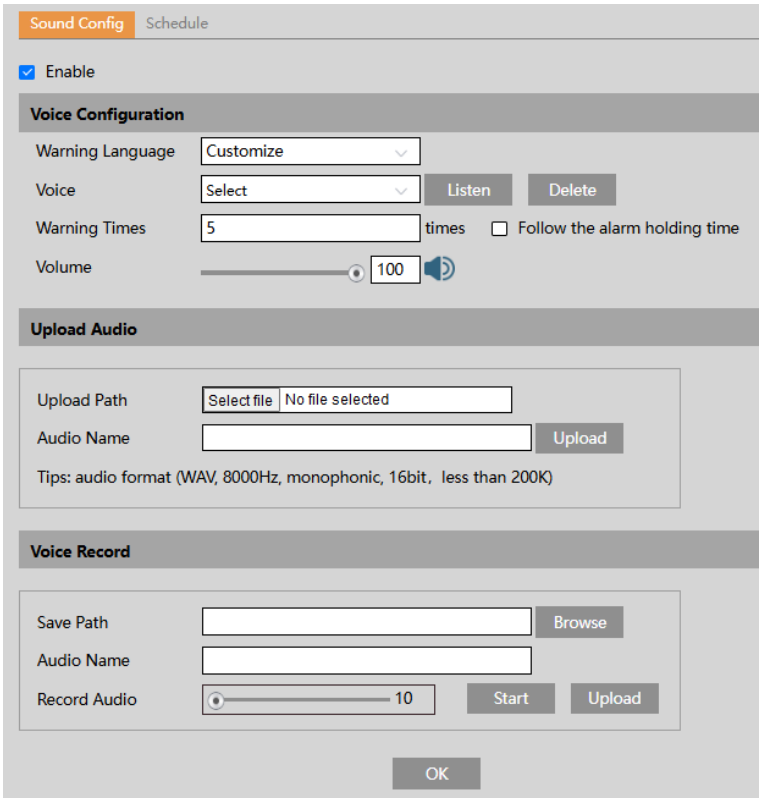


5.3.6 Audio Alarm

Go to ***Alarm→Audio Alarm*** as shown below.
Enable audio alarm. If disabled, the camera will not play the desired warning voice even if an event triggers audio alarm. Additionally, you need to enable audio in the audio configuration interface and the alarm output type should be "Warning" or "Auto", or the warning voice cannot play too.



① Select the warning voice. If you want to customize the voice, you can choose “Customize”. Click “Select File” or “Browse” to choose the audio file you want to upload and then enter the audio name. Finally, click “Upload” to upload the audio file. Note that the format of the audio file must meet the requirement (see Tips), or it will not be uploaded. After you upload the audio file, you can select the audio name from the audio list and click “Listen” to listen to it. Click “Delete” to delete the audio.
Follow the alarm holding time: if enabled, the warning voice will stop when the alarm holding time ends.



You can also record your own voice in the above interface and then upload.

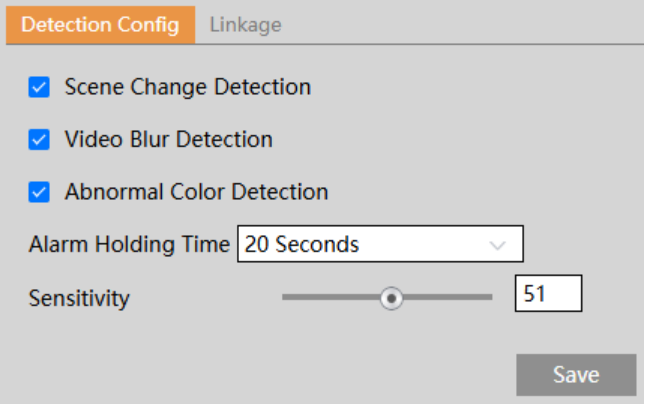
- Insert the microphone into your PC.
- Click “Browse” to choose the save path of the audio you want to record.
- Set the record audio volume and then click “Start” to start recording your voice.
- Click “Upload” to upload your customized voice.

Note: when you access your camera by the web browser without the plug-in, “video record” is not available in the above interface.

② Select the voice and then set the warning times and volume as needed.
Warning times: it ranges from 1 to 50.
③ Set the schedule of audio alarm. The setup steps of the schedule are the same as the schedule recording setup. (See Schedule Recording).
④ Click “OK” to save the settings.

5.3.7 Video Exception

This function can detect changes in the surveillance environment affected by external factors.
To set video exception detection:
Go to ***Config→Event→Video Exception*** as shown below.

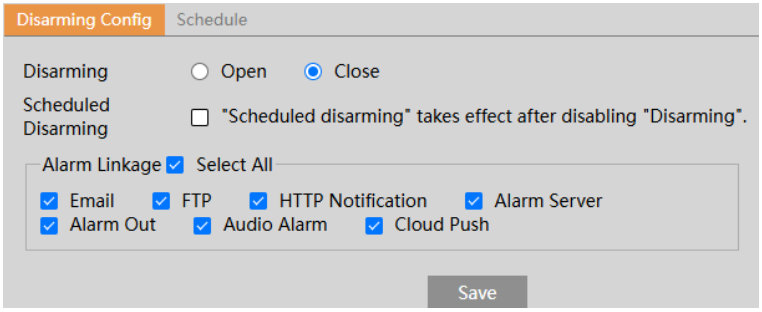


1. Enable the applicable detection that's desired.
Scene Change Detection: Alarms will be triggered if the scene of the monitor video has changed.
Video Blur Detection: Alarms will be triggered if the video becomes blurry.
Abnormal Color Detection: Alarms will be triggered if the image is abnormal because of color deviation.
2. Set the alarm holding time.
3. Set the sensitivity of the exception detection.
Drag the slider to set the sensitivity value or directly enter the sensitivity value in the textbox.
The sensitivity value of Scene Change Detection: The higher the value is, the more sensitive the system responds to the amplitude of the scene change.
The sensitivity value of Video Blur Detection: The higher the value is, the more sensitive the system responds to the blurriness of the image.
The sensitivity value of Abnormal Color Detection: The higher the value is, the more sensitive the system responds to the color shift of the image.
4. Click "Linkage" to configure the alarm linkage items. The setup steps are the same as motion detection. Please refer to motion detection for details.
After checking "Trigger SD Card Snapshot" and/or "Trigger SD Card Recording", you can search the recorded files or snapshots of video exception by selecting the "Common" event.

※ The requirements of camera and surrounding area
1. Auto-focusing function should not be enabled for exception detection.
2. Try not to enable exception detection when light changes greatly in the scene.
3. Please contact us for more detailed application scenarios.

5.3.8 Disarming

You can disarm alarm linkage actions quickly in this interface.

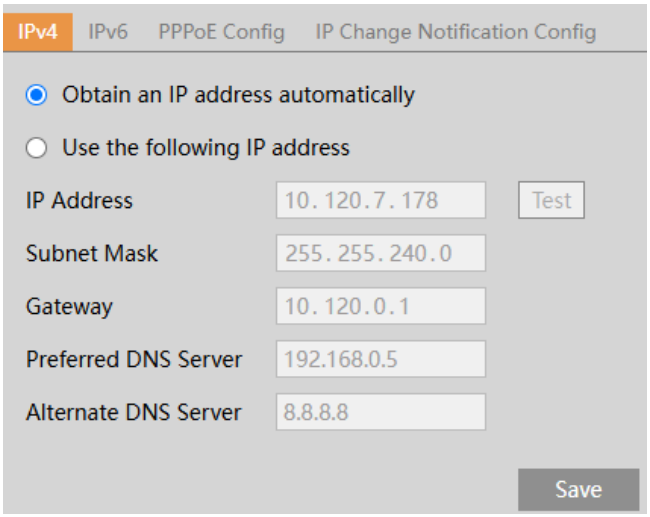


Disarming: The system stops triggering alarm linkage actions immediately.
Scheduled Disarming: The system stops triggering alarm linkage actions in the selected period. Click "Schedule" to set the schedule. The setup steps of schedule are the same as the motion detection schedule settings (See the Motion Detection section for details).
Note: 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.

5.4 Network Configuration

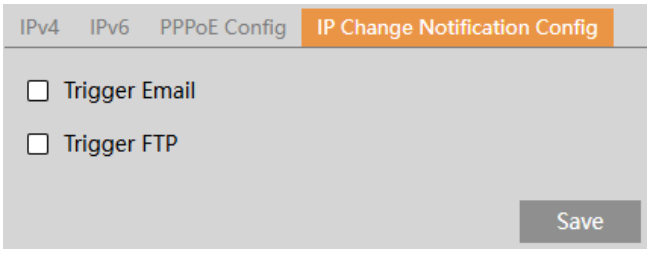
5.4.1 TCP/IP

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



Use IP address (take IPv4 for example)-There are two options for IP setup: obtain an IP address automatically by DHCP and use the following IP address. Please choose one of the options as needed.
Test: Test the effectiveness of the IP address by clicking this button.
Use PPPoE-Click the "PPPoE Config" tab to go to the interface as shown below. Click "Edit", enable PPPoE and then enter the user name and password from your ISP. (Only some models support the PPPoE function)

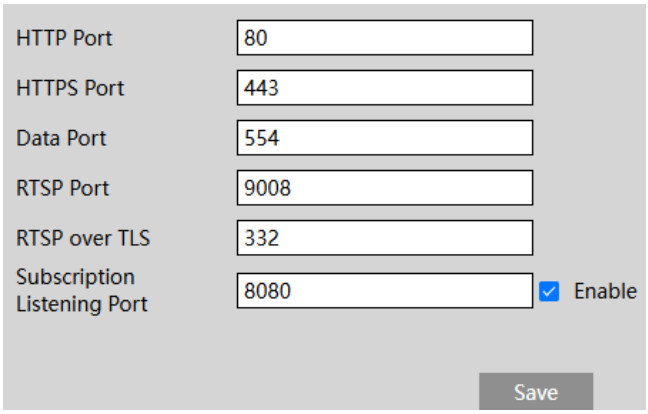
Either one of these two network connection methods can be used. If PPPoE is used to connect to the internet, the camera will get a dynamic WAN IP address. This IP address will change frequently. To be notified, the IP change notification function can be used. Click "IP Change Notification Config" to 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 the FTP server that has been set up.

5.4.2 Port

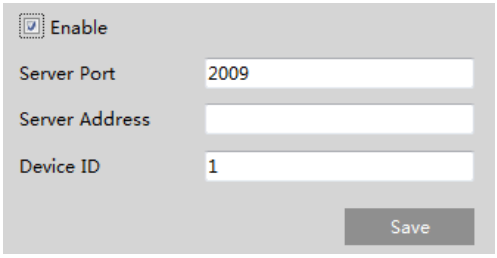
Go to ***Network→Port/Connections*** as shown below.



HTTP Port: The default HTTP port is 80. It can be changed to any port which is not occupied.
HTTPS Port: The default HTTPs port is 443. It can be changed to any port which is not occupied.
Data Port: The default data port is 9008. Please change it as necessary.
RTSP Port: The default port is 554. Please change it as necessary.
RTSP over TLS: Supports media stream transmission based on TLS channel encryption protection.
Subscription Listening Port: The port is used for a persistent connection of the third-party platform to push smart data.

5.4.3 Server Configuration

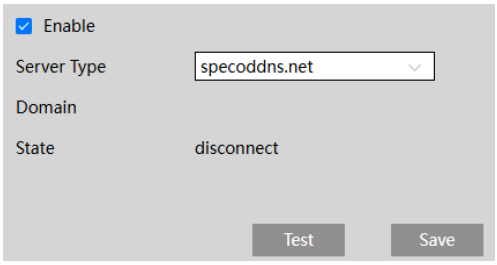
This function is mainly used for connecting network video management systems.



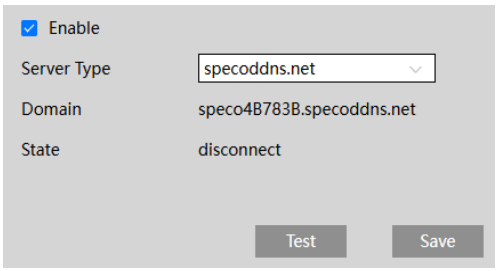
1. Click “Edit” and then check “Enable”.
2. Check the IP address and port of the transfer media server in the VMS. Then enable the auto report in the VMS when adding a new device. Next, enter the remaining information of the device in the VMS. After that, the system will automatically allot a device ID. Please check it in the VMS.
3. Enter the above-mentioned server address, server port and device ID in the corresponding boxes. Click the “Save” button to save the settings.

5.4.4 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→Ports/Connections→ DDNS***.



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



5.4.5 SNMP

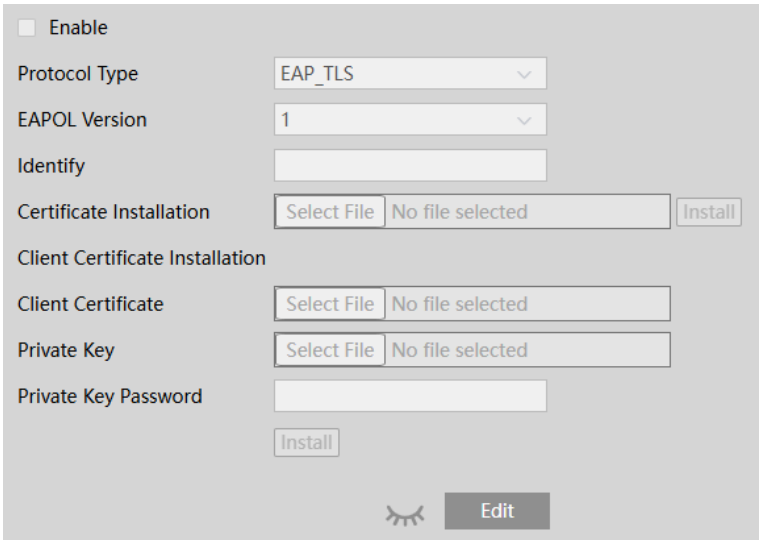
To get camera status, parameters and alarm information and remotely manage the camera, the SNMP function can be used. Before using SNMP, please install an SNMP management tool and set the parameters of the SNMP, such as SNMP port, trap address.

1. Go to ***Network→Ports/Connections→SNMP***.

2. Click “Edit” and then check the corresponding version checkbox (Enable SNMPv1, Enable SNMPv2, Enable SNMPv3) according to the version of the SNMP software that will be used.
3. Set the values for “Read SNMP Community”, “Write SNMP Community”, “Trap Address”, “Trap Port” and so on. Please make sure the settings are the same as those of the SNMP software.
Note: Please use the different version in accordance with the security level you required. The higher the version is, the higher the level of the security is.

5.4.6 802.1x

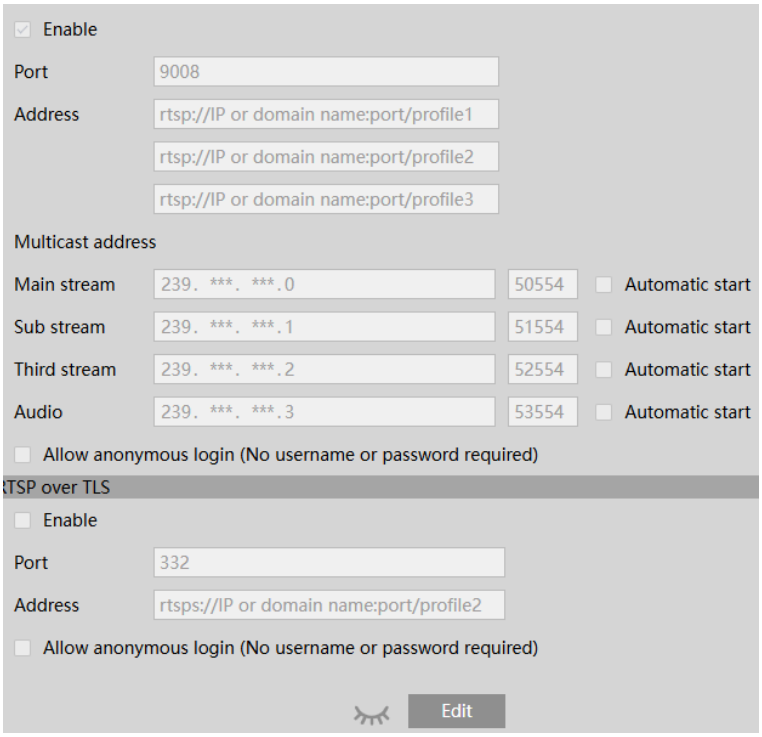
If it is enabled, the camera’s data can be protected. When the camera is connected to the network protected by IEE802.1x, user authentication is needed.



To use this function, the camera should 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 related CA certificate, device certificate and private key. Before connecting the camera to the protected network with 802.1x, apply a digital certificate from a Certificate Authority (i.e., your network administrator) which 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 user name and password must be the same as the user name and password applied for and registered in the authentication server.

5.4.7 RTSP

Go to ***Network→Ports/Connections→RTSP***.

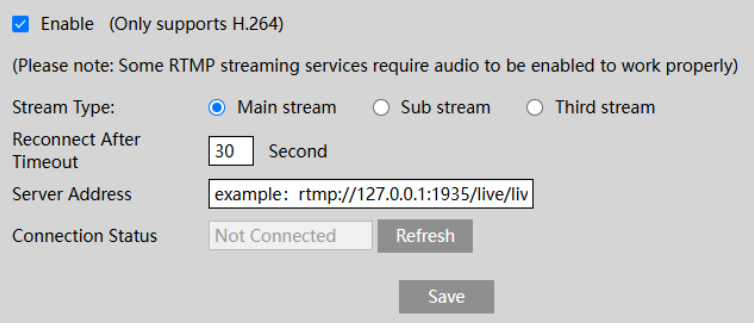


Select “Enable” to enable the RTSP function.
Port: Access port of the streaming media. The default number is 554.
RTSP Address: The RTSP address (unicast) format that can be used to play the stream in a media player.

Multicast Address
Main stream: The address format is
“rtsp://IP address: rtsp port/profile1?transportmode=mcast”.
Sub stream: The address format is
“rtsp://IP address: rtsp port/profile2?transportmode=mcast”.
Third stream: The address format is
“rtsp://IP address: rtsp port/profile3?transportmode=mcast”.
Audio: Having entered the main/sub stream in a media player(like VLC), the video and audio will play automatically.
If “Allow anonymous login…” is checked, there is no need to enter the username and password to view the video.
If “auto start” is enabled, the multicast received data should be added into a VLC player to play the video.
RTSP over TLS: Enable RTSP stream encryption by using TLS.

5.4.8 RTMP

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



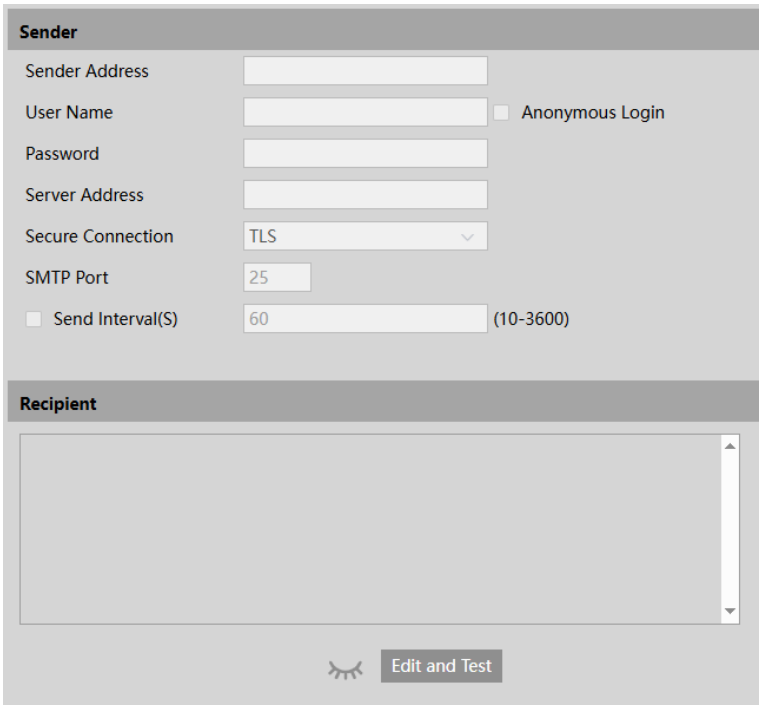
Click “Edit” and then check “Enable”, select stream type and set the reconnection time after timeout and server address as needed.
Server address: Enter the server address allocated by the third-party server.
After that, click “Save” to save the settings. Then click “Refresh” to view the connection status.

5.4.9 UPNP

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

5.4.10 Email

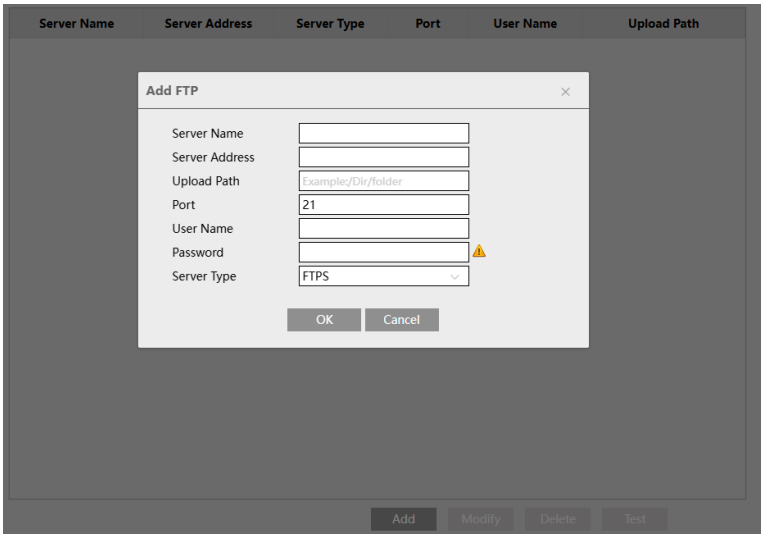
If you need to trigger Email when an alarm happens or IP address is changed, please set the Email here first.
Go to ***Network→Ports/Connections→Email***.



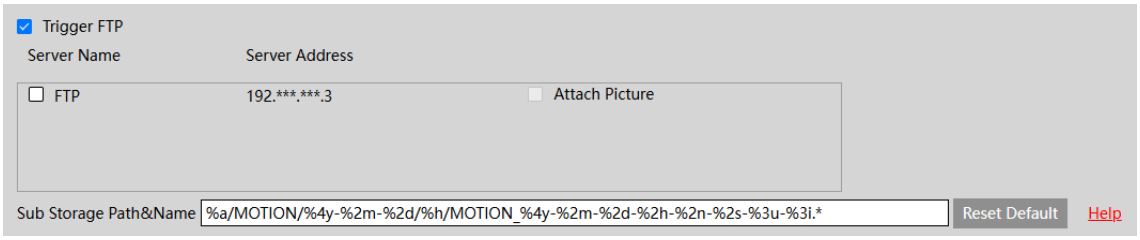
Click “Edit and Test” to set the sender and the recipient.
Sender Address: sender’s e-mail address.
User name and password: sender’s user name and password (you don’t have to enter the username and password if “Anonymous Login” is enabled).
Server Address: The SMTP IP address or host name.
Select the secure connection type at the “Secure Connection” pull-down list according to what’s required.
SMTP Port: The SMTP port.
Send Interval(S): The time interval of sending email. For example, if it is set to 60 seconds and multiple motion detection alarms are triggered within 60 seconds, they will be considered as only one alarm event and only one email will be sent. If one motion alarm event is triggered and then another motion detection alarm event is triggered after 60 seconds, two emails will be sent. When different alarms are triggered at the same time, multiple emails will be sent separately.
Click the “Test” button to test the connection of the account.
Recipient Address: receiver’s e-mail address.

5.4.11 FTP

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



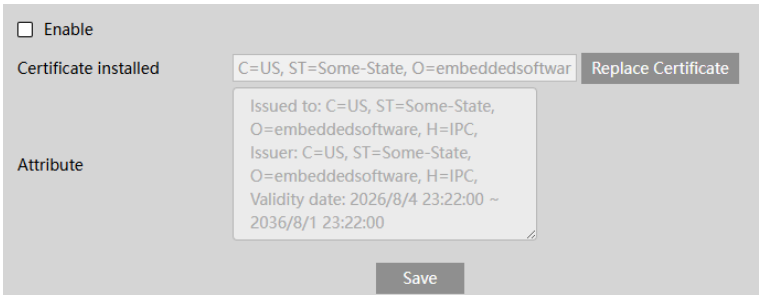
2. Click “Edit and Test” and then click “Add” to add the information of the FTP. After that, click “Save” to save the settings.
Server Name: The name of the FTP server.
Server Address: The IP address or domain name of the FTP.
Upload Path: The directory where files will be uploaded to.
Port: The port of the FTP server.
User Name and Password: The username and password that are used to login to the FTP server.
Server Type: FTP or FTPS
3. In the event setting interface (like motion detection, region intrusion, line crossing, etc.), trigger FTP as shown below.



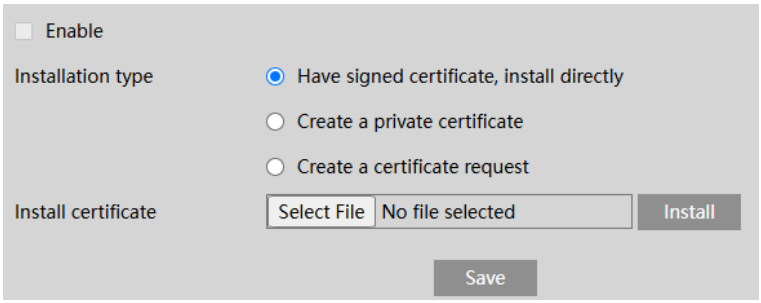
If “Trigger FTP” and “Attach Picture” are checked, the captured pictures will be sent to the FTP server address.
Sub Storage Path& Name: Click “Help” to view the rule and then set it as needed.
Meanings of the default Path & Name Settings (taking motion detection as an example):
“%a/MOTION/%4y-%2m-%2d/%h” stands for sub storage path
“MOTION_%4y-%2m-%2d-%2h-%2n-%2s-%3u-%3i.* ” stands for file name
When an motion alarm is triggered and “Trigger FTP” and “Attach Picture” are checked, a jpg file named “MOTION_Year Month Day Hour Minute Second_Event number” and a txt file named “MOTION_Year Month Day Hour Minute Second_Event number” will be generated under FTP root directory> MAC address>MOTION>Year-Month-Day>Hour
“MOTION” refers to the event type. You can modify the event name as needed (for example: Motion). You can also change the display order and contents of the sub storage path and file name.
If the sub storage path and name box is empty, the snapshot will be uploaded and named according to the default settings.
If you only enter the file name rule, the snapshot will be uploaded to the root directory of the FTP server.

5.4.12 HTTPS

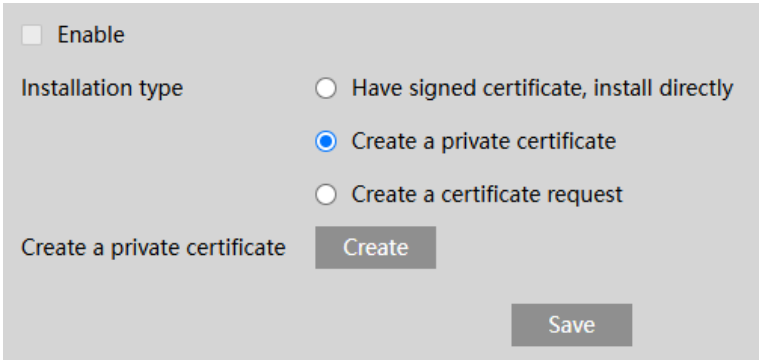
HTTPs provides authentication of the web site and protects user privacy.
Go to ***Network→Ports/Connections→HTTPS*** as shown below.



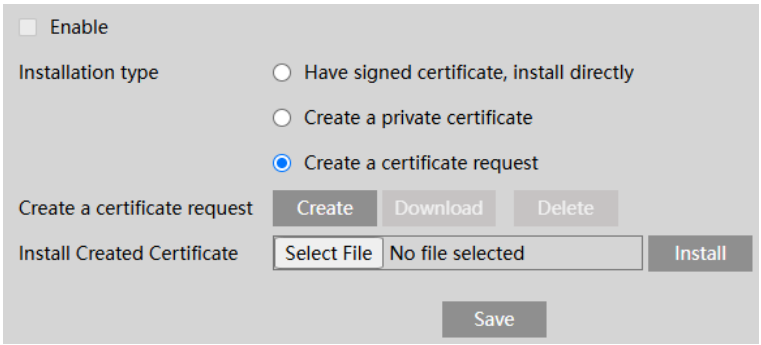
There is a certificate installed by default as shown above. Enable this function and save it. Then the camera can be accessed by entering https://IP: https port via the web browser (eg. https://192.168.226.201:443).
A private certificate can be created if users don't want to use the default one. Click "Replace Certificate" 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.

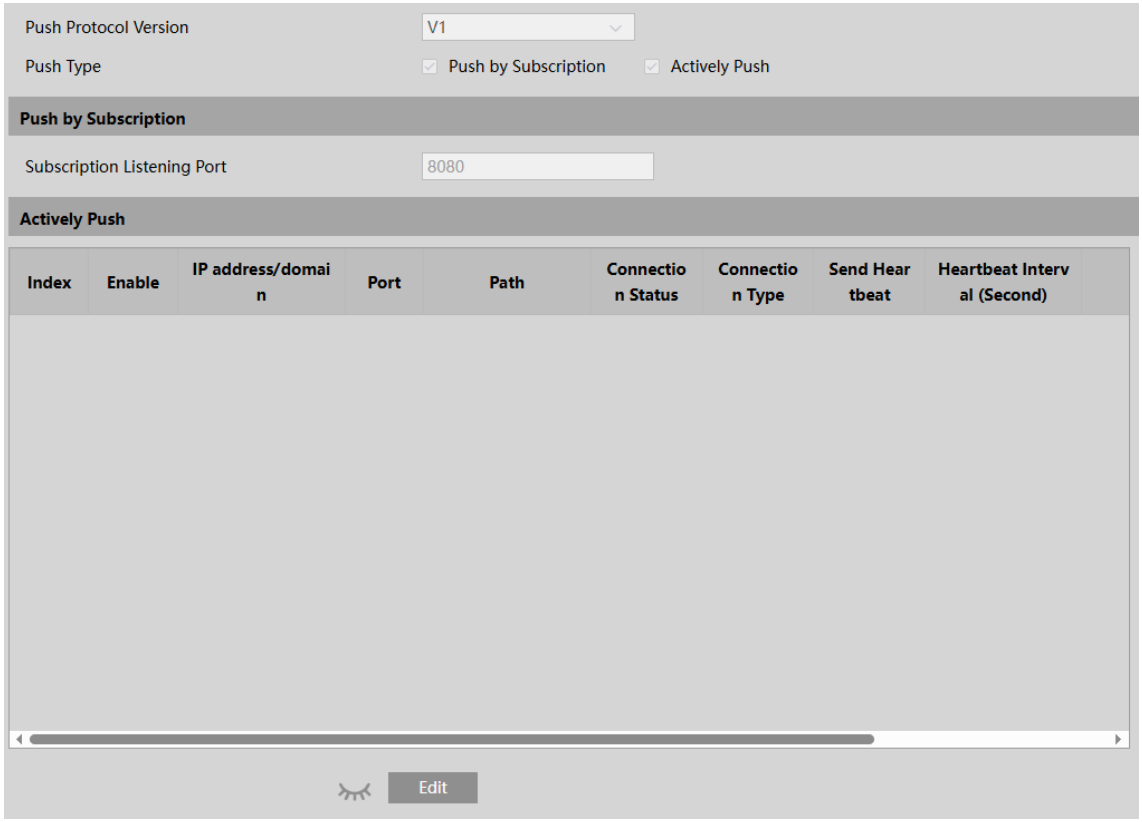


Click "Create" to create the certificate request. Then download the certificate request and submit it to the trusted certificate

authority for signature. After receiving the signed certificate, import the certificate to the device.

5.4.13 HTTP Notification

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



Click “Edit”.

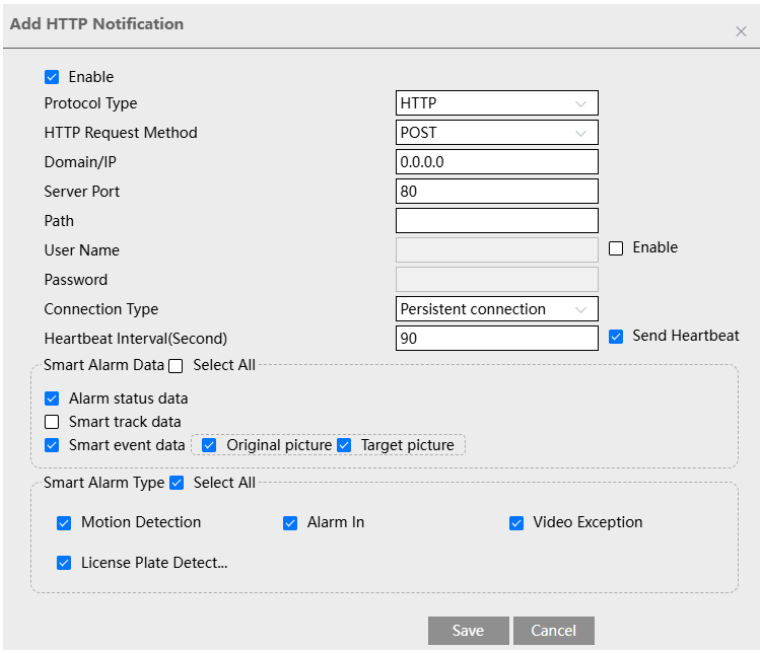
Push Protocol Version: Choose “V1” or “V2” as needed. It is recommended to use V2.

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

Push by Subscription: Push target trajectory (moving coordinate) to 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 a HTTP notification.



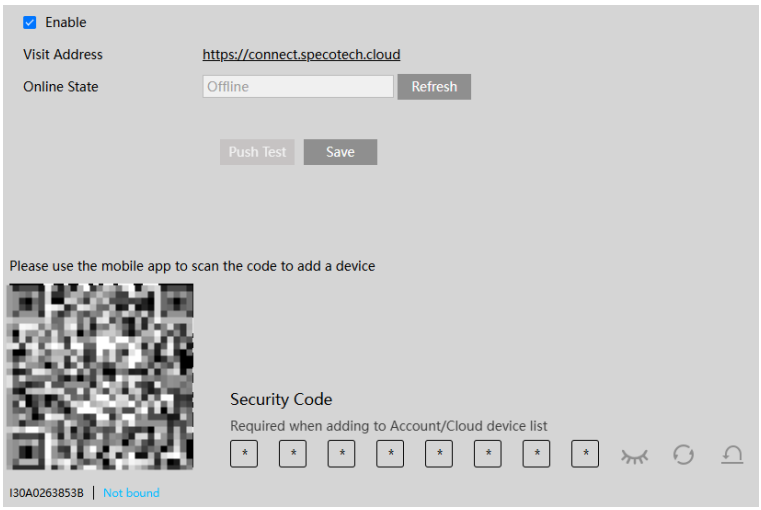
Protocol type: HTTP
HTTP Request Method: Choose “POST” or “GET” as needed.
Domain/IP: the IP address/domain name of the third-party platform.
Server port: the server port of the third-party platform.

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.

5.4.14 NAT

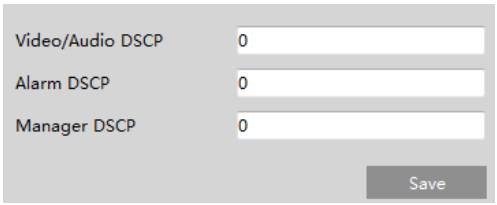
If this function is enabled, the network camera can be quickly accessed by scanning the QR Code and entering the security code in the mobile APP via WAN. In addition, you can also enter the visit address in the address bar of a web browser to log in the camera via WAN. Enable this function by going to ***Config→Network→NAT***.



After the device is successfully bound, you can unbind it via APP (go to the server list of the APP and delete the device).
Note that after you bind the camera to your APP account, a verification code will be required when logging onto the web client by using the above-mentioned visit address.

5.4.15 QoS

QoS (Quality of Service) function is used to provide different quality services for different network applications. With 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.

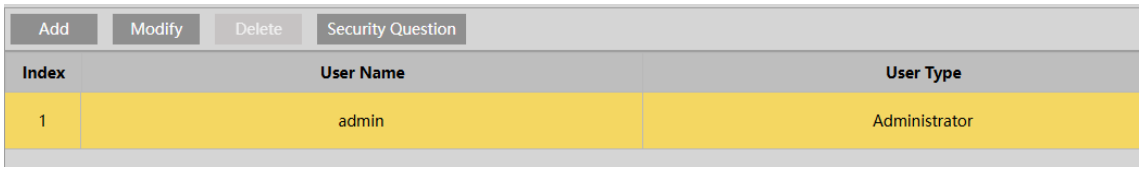


Video/Audio DSCP: The range is from 0 to 63.
Alarm DSCP: The range is from 0 to 63.
Manager DSCP: The range is from 0 to 63.
Generally speaking, the larger the number is, the higher the priority is.

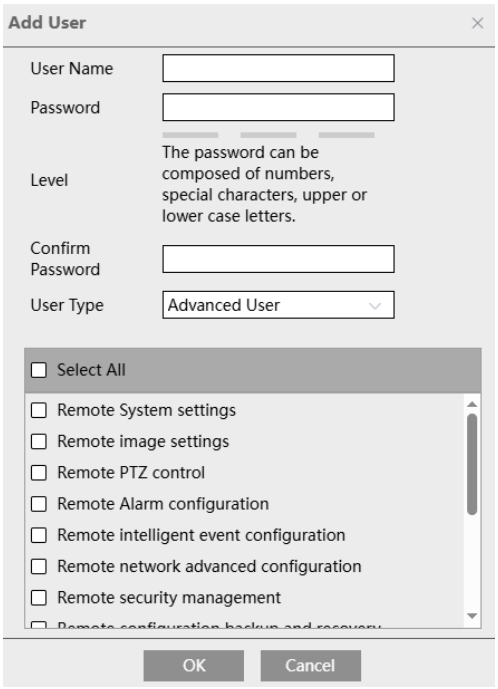
5.5 Security Configuration

5.5.1 User

Go to ***Security→User*** as shown below.



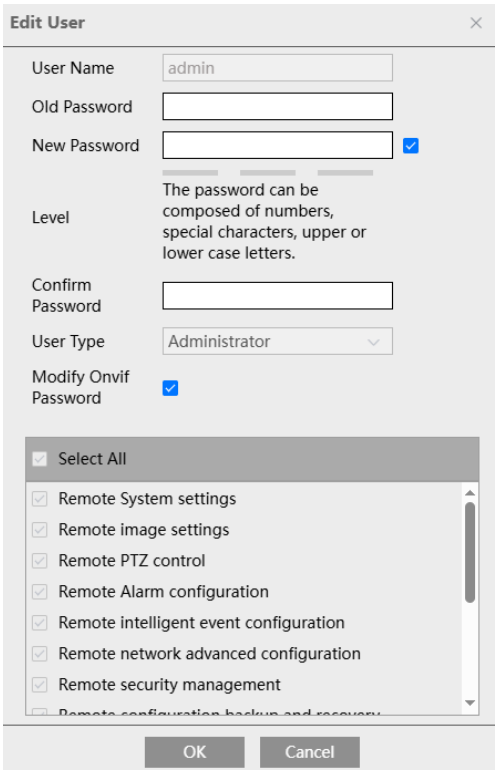
Add user:
1. Click “Add” to pop up the following textbox.



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

Modify user:

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



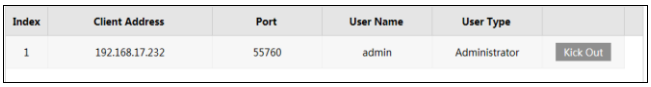
3. Enter the old password of the user in the “Old Password” text box.
4. Enter the new password in the “New password” and “Confirm Password” text box.
5. Modify the permission as necessary.
6. Click the “OK” button to save the settings.
Note: To change the access level of a user, the user must be deleted and added again with the new access level.

Delete user:
1. Select the user to be deleted in the user configuration list box.
2. Click the “Delete” button to delete the user.
Note: The default administrator account cannot be deleted.

Safety Question
You can set the safety questions and answers here for the admin user.

5.5.2 Online User

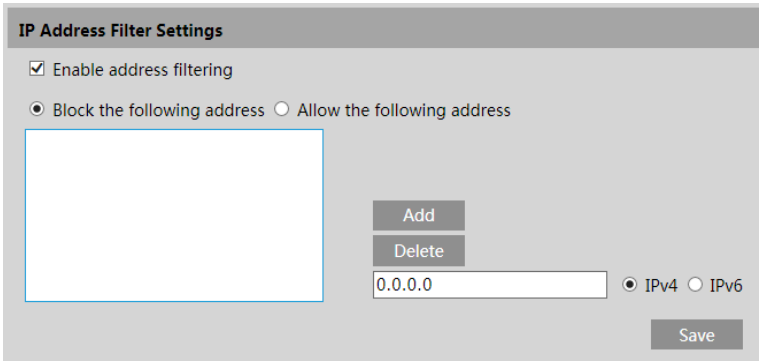
Go to ***Security→Online User*** to view the user who is viewing the live video.



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

5.5.3 Block and Allow Lists

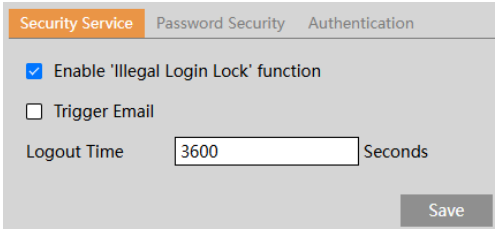
Go to ***Security→Block and Allow Lists*** as shown below.



The setup steps are as follows:
Check the “Enable address filtering” check box.
Select “Block/Allow the following address”, IPv4/IPv6 and then enter IP address in the address box and click the “Add” button.

5.5.4 Security Management

Go to ***Security→Security Management*** as shown below.



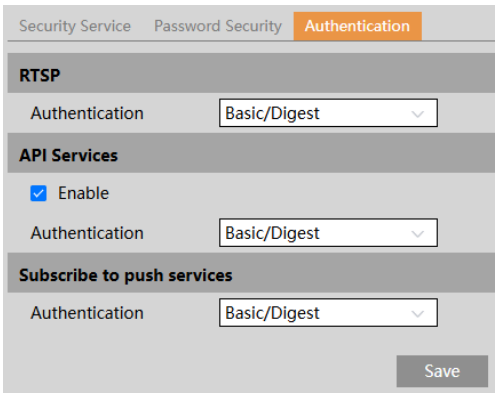
In order to prevent against malicious password unlocking, “locking once illegal login” function can be enabled here. If this function is

enabled, login failure after trying five times will make the login interface locked. The camera can be logged in again after a half hour or after the camera reboots.
Trigger Email: if enabled, e-mail will be sent when logging in/out or illegal login lock occurs.
Logout time: Set the logout time as needed. For example: 3600s, you will be automatically logged out after 3600s and then you need to enter the username and password again to log in.

- **Password Security**

Please set the password level and expiration time as needed.
Password Level: Weak, Medium or Strong.
Weak level: Numbers, special characters, upper or lower case letters can be used. You can choose one of them or any combination of them when setting the password.
Medium Level: 8~16 characters, including at least two of the following categories: numbers, special characters, upper case letters, lower case letters.
Strong Level: 8~16 characters. Numbers, special characters, upper case letters and lower case letters must be included.
For your account security, it is recommended to set a strong password and change your password regularly.

- **Authentication**

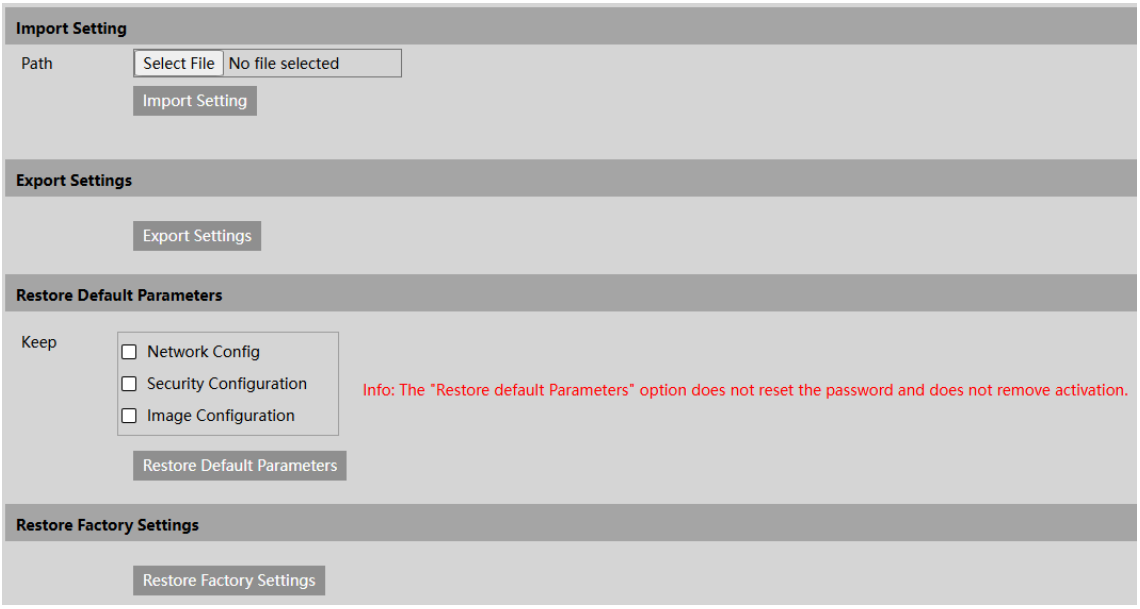


RTSP Authentication: “Digest” or “Basic/Digest” can be selected.
API Service Authentication: “Digest” or “Basic/Digest” can be selected.
Push Subscription Authentication: “Digest” or “Basic/Digest” can be selected.

5.6 Maintenance Configuration

5.6.1 Backup and Restore

Go to ***Maintenance→Backup and Restore***.



- **Import & Export Settings**

Configuration settings of the camera can be exported from one camera into another camera.
1. Click “Select File” 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.
* The customized audio files are not supported to export or import.

- **Restore Default Parameters**

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

- **Restore Factory Settings**

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

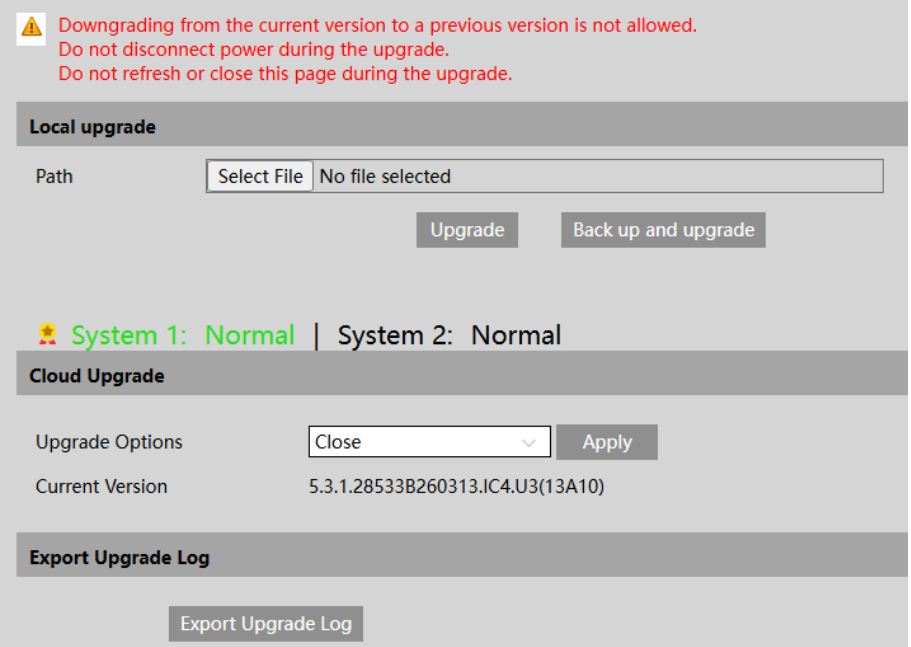
5.6.2 Reboot

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.

5.6.3 Upgrade

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



- **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 upgrading.

- **Cloud Upgrade**

Only some models support this function.

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

After the cloud server pushes the latest version, you can upgrade the camera by itself or NVR.

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 system failure. After the device is successfully upgraded, there are ten minutes of observation. During this observation period, do not upgrade the device again.

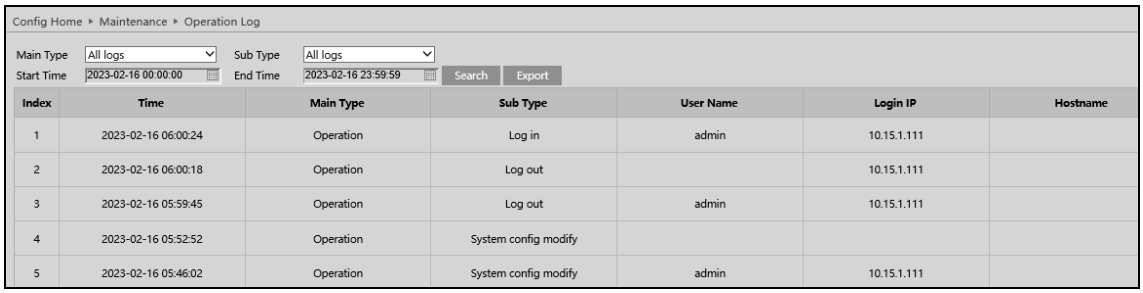
Note: To decrease the upgrade risk, this series of cameras adopts two systems. After one system is successfully upgraded, the other system will be synchronized. If one system fails caused by power failure or other reasons during the upgrade, the other system will not be affected, and the camera still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

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

5.6.4 Operation Log

To query and export log:

1. Go to ***Config→Maintenance→Operation Log***.



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

5.6.5 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.

5.6.6 Maintenance Information

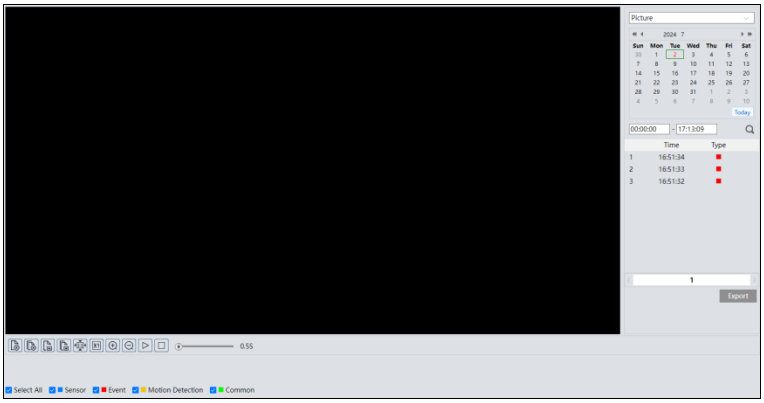
When the device failure occurs, you can export the maintenance information and send it to the technicians, so that they can quickly find out and analyze the problem. Go to ***Config→Maintenance Information*** to export.

6 Search

6.1 Image Search

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

1. Choose “Picture”.



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

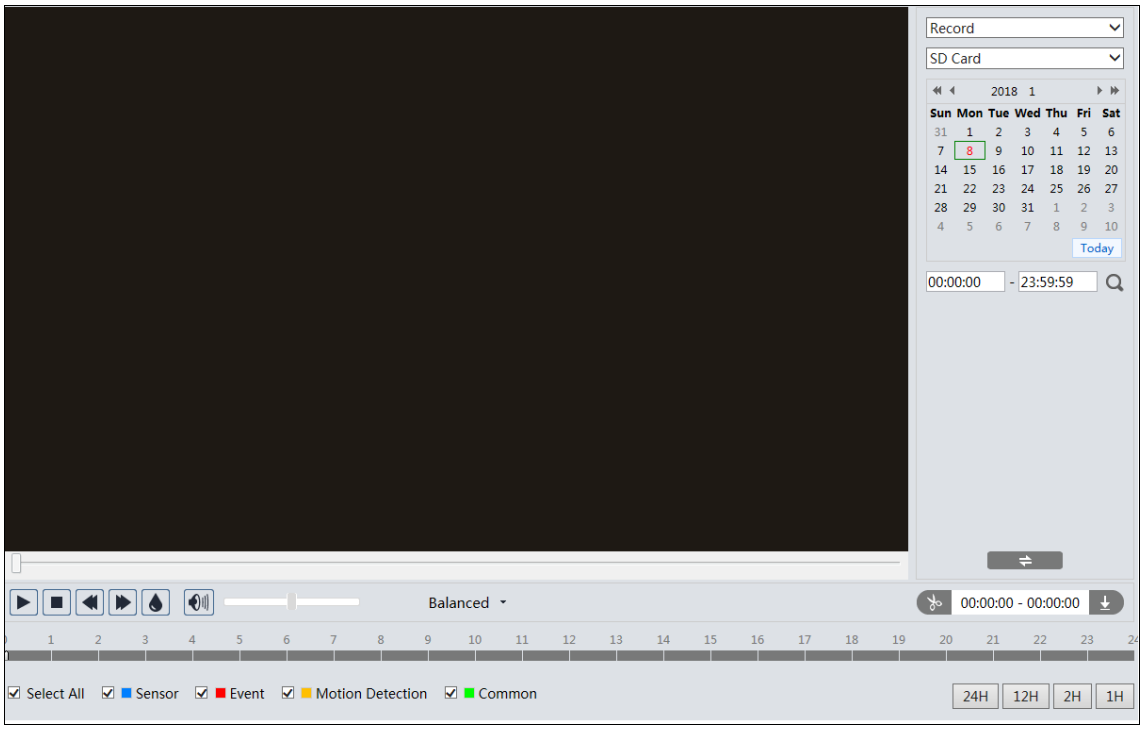
You can export all the searched pictures by clicking “Export”.

The descriptions of the buttons are shown as follows.

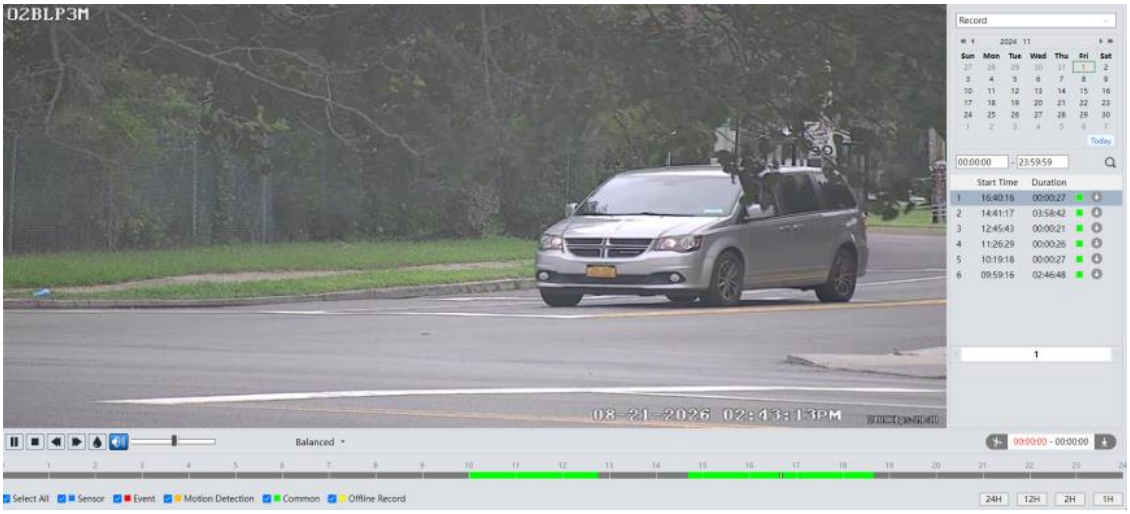
Icon	Description	Icon	Description
	Close: Select an image and click this button to close the image.		Close all: Click this button to close all images.
	Save: Click this button to select the path for saving the image on the PC.		Save all: Click this button to select the path for saving all pictures on the PC.
	Fit size: Click to fit the image on the screen.		Actual size: Click this button to display the actual size of the image.
	Zoom in: Click this button to digitally zoom in.		Zoom out: Click this button to digitally zoom out.
	Slide show play: Click this button to start the slide show mode.		Stop: Click this button to stop the slide show.
5.5S	Play speed: Play speed of the slide show.		

6.2 Video Search

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



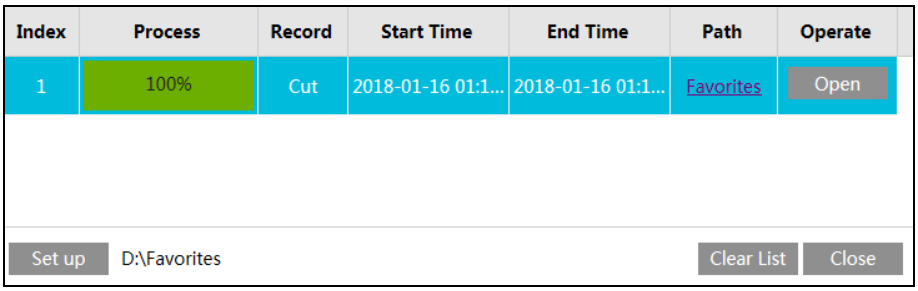
1. Choose “Record”.
2. Set search time: Select the date and choose the start and end time.
3. Select the alarm events at the bottom of the interface.
4. Click to search the images.
5. Double click on a file name in the list to start playback.



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.		

The timetable can be shown in 24H/12H/2H/1H format by clicking the corresponding buttons.
Video clip and downloading

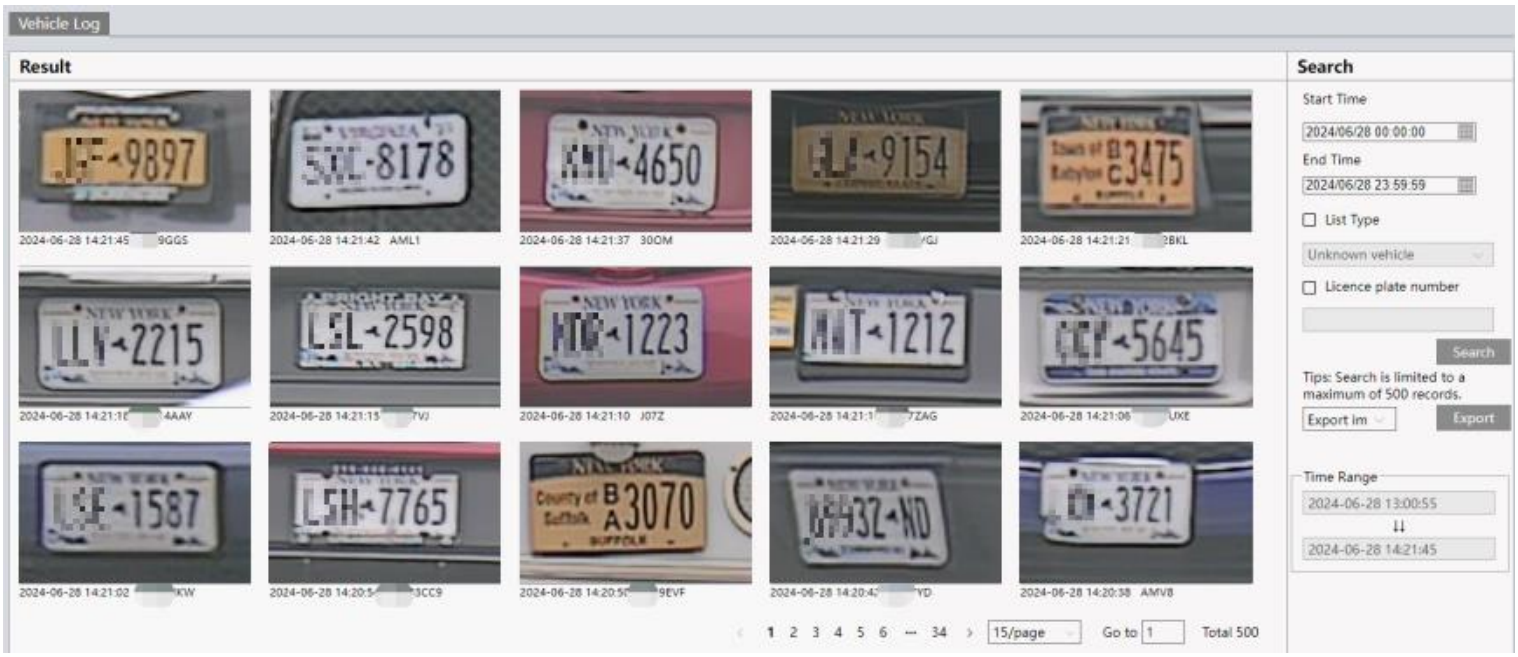
1. Search the video files according to the above-mentioned steps.
2. Select the start time by clicking on the timetable.
3. Click to set the start time and then this button turns blue ( ).
4. Select the end time by clicking on the timetable. Then click to set the end time.
5. Click to download the video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



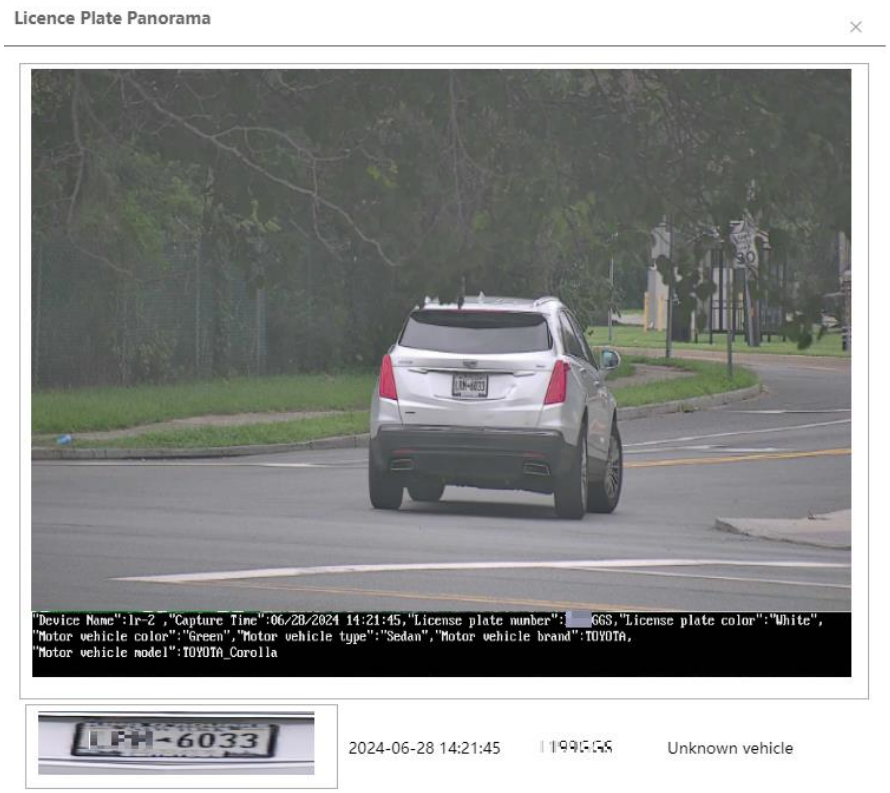
Click “Set up” to set the storage directory of the video files.
Click “Open” to play the video.
Click “Clear List” to clear the downloading list.
Click “Close” to close the downloading window.

6.3 Vehicle Data Search

Click “Data Record” to enter the vehicle log search interface.
Set the start time and end time and click “Search” to view the license plate recognition result.
You can also filter the plate number by selecting the list type or entering the desired license plate number.



Please export image and file as needed. Click the searched license plate picture to view the original picture.



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.

No sound can be heard.
1. Audio input device is not connected. Please connect and try again.
2. The audio function is not enabled at the corresponding channel. Please enable this function.

Models: O2BLP3M

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