LICENSE PLATE RECOGNITION NETWORK CAMERA

User Manual

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

The following symbols or words may be found in this manual.

Symbols/Words	Description
⚠ **Warning**	Indicates a medium or low potential hazardous situation which , if not avoided, will or could result in slight or moderate injury
⚠ **Caution**	Indicates a potential risk which, if not avoided, will or could result in device damage, data loss, lower performance or unexpected results
☞ **Note**	Provides additional information to emphasize or supplement important points of the text.

About the Manual

- This manual is suitable for many models. All examples, screenshots, figures, charts, and illustrations used in the manual are for reference purpose, and actual products may be different with this Manual.
- Please read this user manual carefully to ensure that you can use the device correctly and safely.
- Within the maximum scope permitted by the law, the products described in this Manual (including hardware, software, firmware, etc.) are provided “AS IS”. The information in this document (including URL and other Internet site reference data) is subject to change without notice. This Manual may contain technical incorrect places or printing errors. This information will be periodically updated, and these changes will be added into the latest version of this Manual without prior notice.
- In this manual, the trademarks, product names, service names and company names that are not owned by our company are the properties of their respective owners.

Use of the Product

- This product should not be used for illegal purposes.
- The company does not allow anyone to use the Company's products to infringe the privacy, personal information, and portrait rights of others. The user shall not use this product for any illegal use or any prohibited use under these terms, conditions, and declarations. When using this product, the user shall not damage, disable, overload or obstruct any of the hardware of this product in any way, or interfere with the use of this product by any other users. Also, the user should not attempt to use the product or the software, by hacking, stealing the password, or any other means.

Electrical Safety

- This product is intended to be supplied by a Listed Power Unit, marked with 'Limited Power Source', 'LPS' on unit, output rated minimum 12V/2 A or POE 48V/ 350mA or AC24V (depending on models), no more than 2000m altitude of operation and Tma=60 Deg.C.
- As for the modes with PoE function, the function of the ITE being investigated to IEC 60950-1 standard is considered not likely to require connection to an Ethernet network with outside plant routing, including campus environment and the ITE is to be connected only to PoE networks without routing to the outside plant.
- Improper handling and/or installation could run the risk of fire or electrical shock.
- The product must be grounded to reduce the risk of electric shock.
- ⚠ Warning: Wear anti-static gloves or discharge static electricity before removing the bubble or cover of the camera.
- ⚠ Caution: Do not provide two power supply sources at the same time for the device unless otherwise specified; it may result in device damage!

Environment

- Heavy stress, violent vibration or exposure to water is not allowed during transportation, storage and installation.
- Avoid aiming the camera directly towards extremely bright objects, such as, sun, as this may damage the image sensor.
- Keep away from heat sources such as radiators, heat registers, stove, etc.
- Do not block any ventilation openings and ensure proper ventilation around the camera.
- Do not expose the product to the direct airflow from an air conditioner.
- Do not place the device in a damp, dusty extremely hot or cold environment, or the locations with strong electromagnetic radiation or unstable lighting.
- Make sure that no reflective surface (like shiny floors, mirrors, glass, lake surfaces and so on) is too close to the camera lens, resulting in image blur.

Operation and Daily Maintenance

- There are no user-serviceable parts inside. Please contact the nearest service center if the product does not work properly.
- Please shut down the device and then unplug the power cable before you begin any maintenance work.
- ⚠ Warning: All the examination and repair work should be done by qualified personnel.
- 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 cleaning (such as using cloth) may result in poor IR/illumination LEDs functionality and/or IR/illumination LEDs reflection.

- Dome cover is an optical device, please don't touch or wipe the cover surface directly during installation and use. For dust, use oil-free soft brush or hair dryer to remove it gently; for grease or finger print, use oil-free cotton cloth or paper soaked with detergent to wipe from the lens center outward. Change the cloth and wipe several times if it is not clean enough.

White Light Illuminator (if supported)

- DO NOT turn on the white light when you install or maintain the camera. Please wear appropriate eye protection when you want to test the white light.
- DO NOT stare at the operating light source. It will probably be harmful to your eyes.
- The white light illuminators and/or the IR LED's should at no time be covered when the camera is running to prevent overheating and the possible risk of fire.

Privacy Protection

- When installing cameras in public areas, a warning notice shall be given in a reasonable and effective manner and clarify the monitoring range.
- As the device user or data controller, you might collect the personal data of others, such as face, car plate number, etc. As a result, you shall implement reasonable and necessary measures to protect the legitimate rights and interests of other people, avoiding data leakage, improper use, including but not limited to, setting up access control, providing clear and visible notice to inform people of the existence of the surveillance area, providing required contact information and so on.

Disclaimer

- With regard to the product with internet access, the use of product shall be wholly at your own risks. Our company shall be irresponsible for abnormal operation, privacy leakage or other damages resulting from cyber attack, hacker attack, virus inspection, or other internet security risks; however, Our company will provide timely technical support if necessary.
- Surveillance laws vary from country to country. Check all laws in your local region before using this product for surveillance purposes. We shall not take the responsibility for any consequences resulting from illegal operations.

Cybersecurity Recommendations

- Use a strong password. At least 8 characters or a combination of characters, numbers, and upper and lower case letters should be used in your password.
- Regularly change the passwords of your devices to ensure that only authorized users can access the system (recommended time is 90 days).

- It is recommended to change the service default ports (like HTTP-80, HTTPS-443, etc.) to reduce the risk of outsiders being able to access.
- It is recommended to set the firewall of your router. But note that some important ports cannot be closed (like HTTP port, HTTPS port, Data Port).
- It is not recommended to expose the device to the public network. When it is necessary to be exposed to the public network, please set the external hardware firewall and the corresponding firewall policy.
- It is not recommended to use the v1 and v2 functions of SNMP.
- In order to enhance the security of WEB client access, please create a TLS certificate to enable HTTPS.
- Use black and white list to filter the IP address. This will prevent everyone, except those specified IP addresses from accessing the system.
- If you add multiple users, please limit functions of guest accounts.
- If you enable UPnP, it will automatically try to forward ports in your router or modem. It is really very convenient for users, but this will increase the risk of data leakage when the system automatically forwards ports. Disabling UPnP is recommended when the function is not used in real applications.
- Check the log. If you want to know whether your device has been accessed by unauthorized users or not, you can check the log. The system log will show you which IP addresses were used to log in your system and what was accessed.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

1. FCC compliance

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. 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.
- Consult the dealer or an experienced radio/TV technician for help.

2. FCC conditions:

- This device complies with part 15 of the FCC Rules. Operation of this product is subject the following two conditions:
- This device may not cause harmful interface.
- This device must accept any interference received, including interference that may cause undesired operation.

RoHS

The products have been designed and manufactured in accordance with Directive EU RoHS Directive 2011/65/EU and its amendment Directive EU 2015/863 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

2012/19/EU (WEEE directive): The Directive on waste electrical and electronic equipment (WEEE Directive). To improve the environmental management of WEEE, the improvement of collection, treatment and recycling of electronics at the end of their life is essential. Therefore, the product marked with this symbol must be disposed of in a responsible manner.

Directive 94/62/EC: The Directive aims at the management of packaging and packaging waste and environmental protection. The packaging and packaging waste of the product in this manual refers to must be disposed of at designated collection points for proper recycling and environmental protection.

REACH(EC1907/2006): REACH concerns the Registration, Evaluation, Authorization and Restriction of Chemicals, which aims to ensure a high level of protection of human health and the environment through better and earlier identification of the intrinsic properties of chemical substances. The product in this manual refers to conforms to the rules and regulations of REACH. For more information of REACH, please refer to DG GROWTH or ECHA websites.

Table of Contents

1 Network Connection

System Requirement

For proper operating the product, the following requirements should be met for your computer.

Operating System: Windows 7 Home basic or higher

CPU: 2.0GHz or higher

RAM: 1G or higher

Display: 1920*1080 resolution or higher (recommended)

Web browser: Chrome89.0+/Edge89.0+/Firefox87.0+/Safari 14.0+

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

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

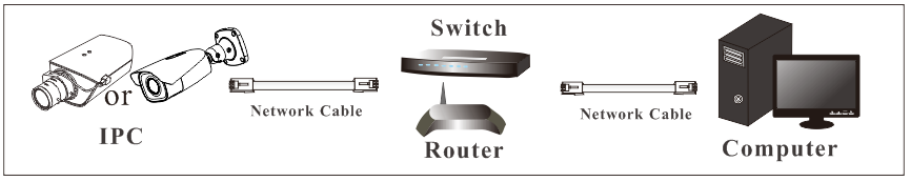
Connect IP camera via LAN or WAN. Here only take the plug-in required browser for example. The details are as follows:

1.1 LAN

In LAN, there are two ways to access IP Camera: 1. access through IP-Tool; 2. directly access via web browser.

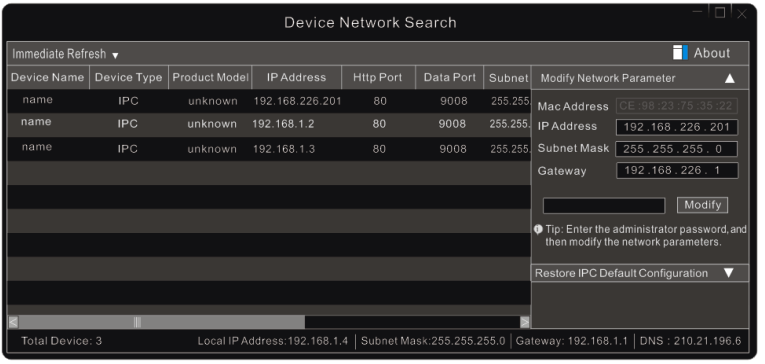
1.1.1 Access through IP-Tool

Network connection:



① Make sure the PC and IP Camera are connected to the LAN and the IP-Tool is installed in the PC.

② Double click the IP-Tool icon on the desktop to run this software as shown below:

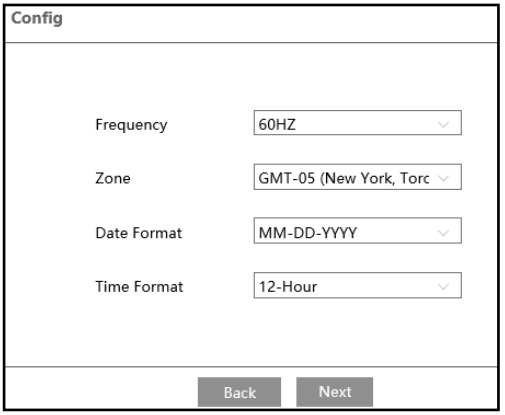


The default IP address of the camera is ***192.168.226.201*.**

③ Double click the IP address and then the system will open a web browser to connect the camera. After you read the privacy statement, check and click "Already Read". This will bring you to a configuration wizard interface.

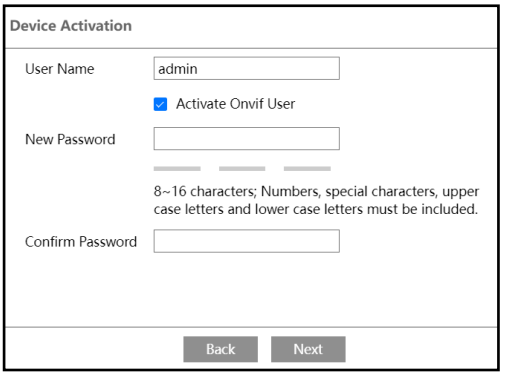
a. Select the location (eg. Britain). Then click [Next].

b. Set the zone, video format (frequency), date and time format.



c. Set security questions and answers as needed. After setting the questions and answers, click [Next] to continue. It is very important for you to reset your password. Please remember these answers.

d. Activate the device.



The default username is “admin”. Please self-define the password of admin according to the tip.

Note: It is highly recommended to use the strong password for your account security. If you want to change your password level, you can go to **Config→Security Management →Password Security** interface to change the level and then modify the admin password (Go to **Config→User**).

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→ Onvif**)

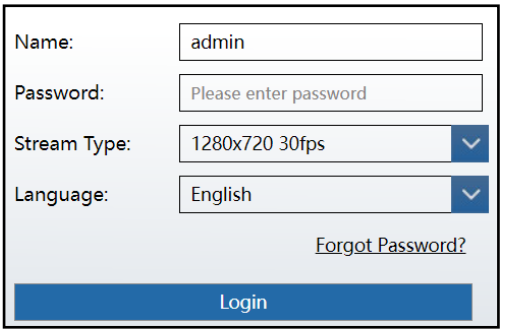
When you connect the camera through the ONVIF protocol in the third-party platform, you can use the username and the password set to connect.

e. Set the application scenarios. Face event or smart event is optional.

d. Click “Save” to save the settings.

Having set all above-mentioned items, the system will reboot. Read the privacy statement, check and click “Already Read”. Then the login interface will appear as shown below.

If it is the first time for you to log in, follow directions to download, install and run the Active X control if prompted.



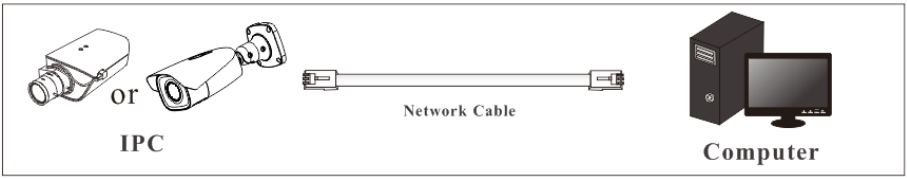
Please enter the user name (admin) and password. Then select the stream type and language as needed.
Stream Type: The plug-in free live view only supports 1080P or lower resolution.

If you forget the admin password, you can reset the password by clicking **Forget Password** on the login page. Then you can reset the password by the security questions and answers you set. You can set the account security question during the activation, or you can go to **Config→Security→User**, click **Safety Question**, select the security questions and input your answers.

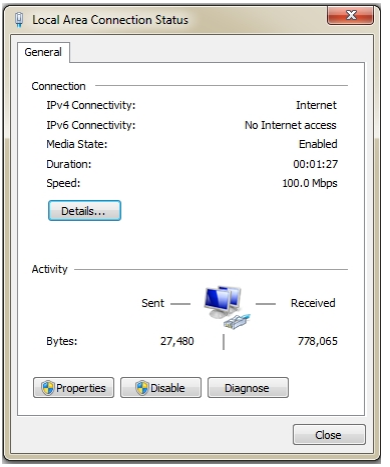
1.1.2 Directly Access via Web Browser

The default network settings are as shown below:
IP address: **192.168.226.201**
Subnet Mask: **255.255.255.0**
Gateway: **192.168.226.1**
HTTP: **80**
Data port: **9008**

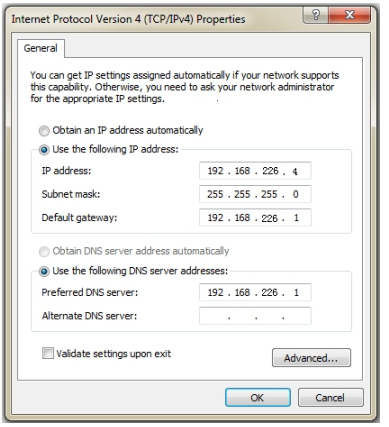
Use the above default settings when logging in the camera for the first time. Directly connect the camera to the computer through network cable.



① Manually set the IP address of the PC and the network segment should be as the same as the default settings of the IP camera. Open the network and share center. Click “Local Area Connection” to pop up the following window.



Select “Properties” and then select internet protocol according to the actual situation (for example: IPv4). Next, click the “Properties” button to set the network of the PC.



② Open a web browser and enter the default address of IP camera and confirm.

③ Follow directions to download and install the Active X control.

④ Enter the default username and password in the login window and then enter to view.

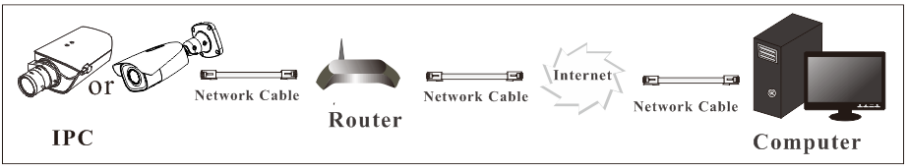
1.2 WAN

➢ **Access via P2P**

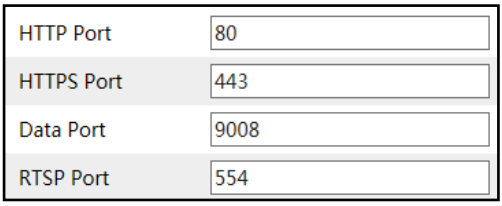
Connect and activate the device according to the above-mentioned steps (See 1.1.1). Enable P2P (click **Config→Network→P2P**) and then enter www.autonat.com to visit the web client remotely.

Note: Different regions may have different login addresses. Please contact your dealer for details.

➢ **Access through the router or virtual server**

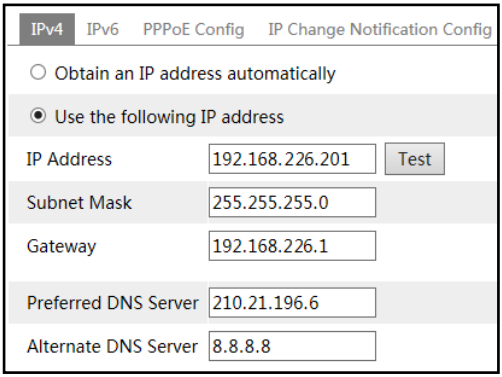


① Make sure the camera is connected to the local network and then log in the camera via LAN and go to **Config→Network→Port** menu to set the port number.



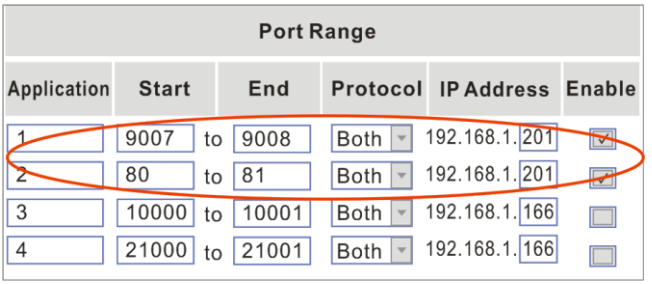
Port Setup

② Go to **Config →Network→TCP/IP** menu to modify the IP address.



IP Setup

③ Go to the router's management interface through your web browser to forward the IP address and port of the camera in the "Virtual Server".

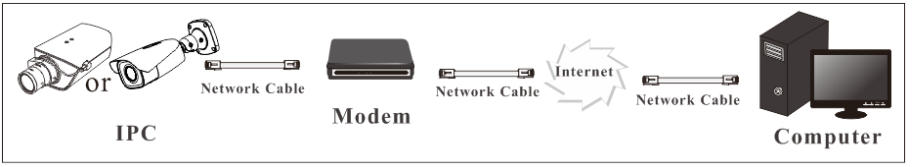


Router Setup

④ Open a web browser and enter its WAN IP and http port to access. (for example, if the http port is changed to 81, please enter "192.198.1.201:81" in the address bar of web browser to access).

➢ **Access through PPPoE dial-up**

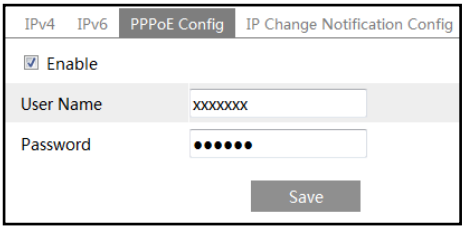
Network connection



Access the camera through PPPoE auto dial-up. The setup steps are as follow:

① Go to **Config→Network→Port** menu to set the port number.

② Go to **Config →Network→TCP/IP→PPPoE** Config menu. Enable PPPoE and then enter the user name and password from your internet service provider.

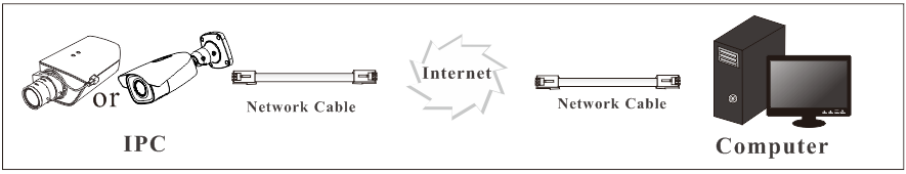


③ Go to **Config→Network→DDNS** menu. Before configuring the DDNS, please apply for a domain name first. Please refer to the DDNS configuration for detail information.

④ Open a web browser and enter the domain name and http port to access.

➢ **Access through static IP**

Network connection



The setup steps are as follow:

① Go to **Config→Network→Port** menu to set the port number.

② Go to **Config→Network→TCP/IP** menu to set the IP address. Check "Use the following IP address" and then enter the static IP address and other parameters.

③ Open a web browser and enter its WAN IP and http port to access.

2 License Plate Recognition

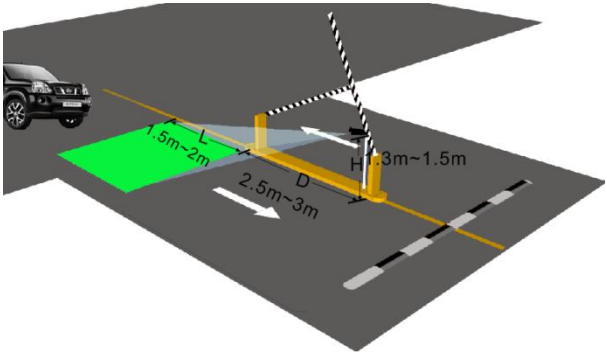
2.1 Configuration Requirements of Camera and Surrounding Area

The configuration of the camera will affect the accuracy of license plate recognition. To clearly capture the license plate, please refer to the following advices.

- The monitoring image should try to cover the lane, entering/exiting vehicles and these vehicles' plate number shall be always visible in the video.
- Avoid the scenes with the objects that will block the camera, such as pillars, obstacles, doors, etc.
- Avoid the scenes with many trees or other moving objects (such as people, non-motor vehicles) in the recognition area.
- The camera must be mounted in such a way that it can detect at least a 50 meters long of straight road.
- The capture angle of the camera should try to avoid the influence of the headlamps or rear lamps of cars, which will bring glare, ghosting and other bad effects to the image.
- The focus of the lens should be clear, and select an appropriate focal length according to the installation height (the license plate size in image should meet the requirement of the license plate capture setting).

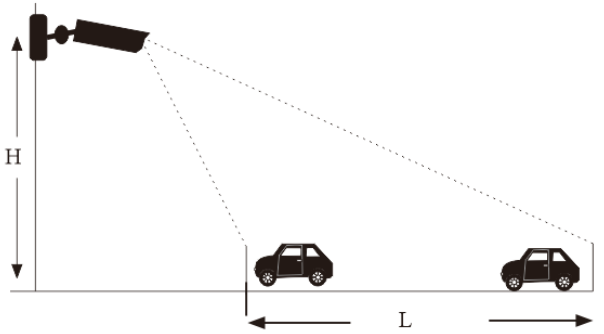
Entrance & Exit Monitoring

- The installation height (H) should range from 1.3 m to 1.5m.
- The distance D (between the location of the camera installation and the captured area) shall range 2.5m to 3m.
- The distance of the captured area (L) should be from 1.5m to 2m.



- The depression angle of the camera should range from 0 °to 5 °.
- The pan angle of the camera should range from 5 °to 20 °.

Road / Intersection Monitoring:



Lens: 2.8~12mm

- The installation height (H) should range from 1.2 m to 1.8m.
- The recommended recognition distance (L) should be 3~8m.
- The speed of vehicles should be within 80KM/H.
- The depression angle of the camera is suggested to be within 30 °.

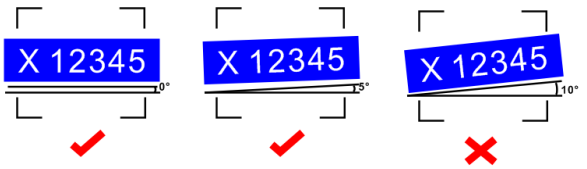
Lens: 8~32mm

- The installation height (H) should range from 4.5m to 8m.
- The recommended recognition distance (L) should be 16~48m.
- The speed of vehicles should be within 120KM/H.
- The depression angle of the camera is suggested to be within 15 °.

- If the camera is installed on the side of the road, the pan angle of the camera is suggested to be 0 °to 20 °.
- If the camera is installed right above the middle of the road, the pan angle of the camera is suggested to be -10 °to 10 °.
- The width of the license plate should be between 6% and 50% of the camera's field of view.

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 should range from -5 °to 5 °.

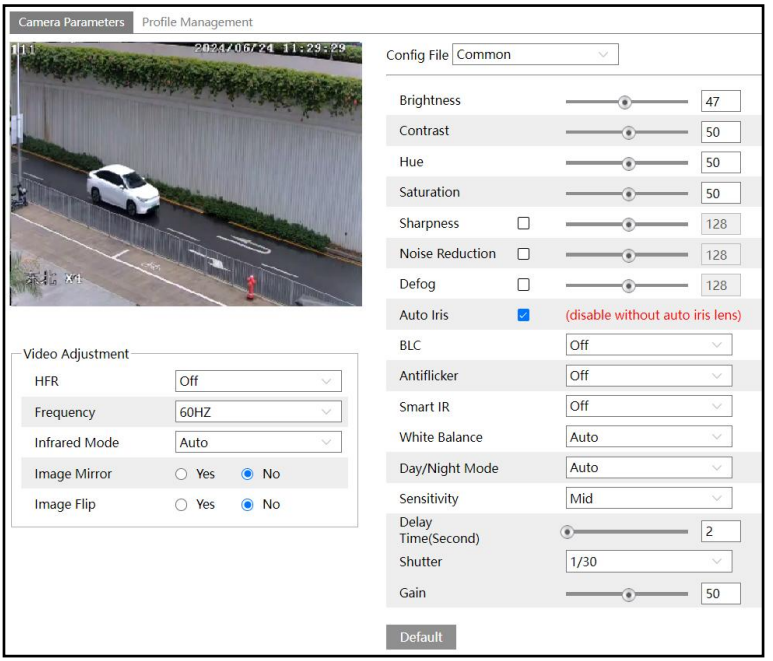


If the captured license plate doesn't meet the above requirement, you can adjust the pan angle of the camera to correct it.

2.2 Recommended Image Settings

In order to clearly capture the license plate, here are some suggestions about image settings.

- **IR models:**



Brightness: Set the brightness level of the camera's image. The brightness value can be kept around 50 in day mode, and in night mode it's suggested to be lower value to capture the license plate clearly.

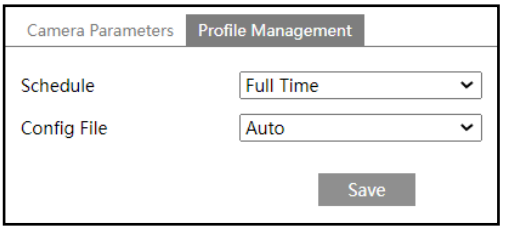
Gain: It is recommended not to exceed 20.

Shutter: When the vehicle speed is too fast and shutter time is too long, it'll cause a blur image. So it's recommended that the maximum shutter time should be adjusted to be shorter in this kind of situation.

Max. Shutter Speed: 1/500~1/1000; if the vehicle spped is lower than 40km/h, it can be extended approriately, but no more than 1/100.

Min. Shutter Speed: 1/100,000.

If the illumination is very low in the scene, in order to capture the license plate clearly, you need to reduce the gain and shutter time. It's recommened to set the schedule to "Full Time/Continuous" and set the config file to "Auto".

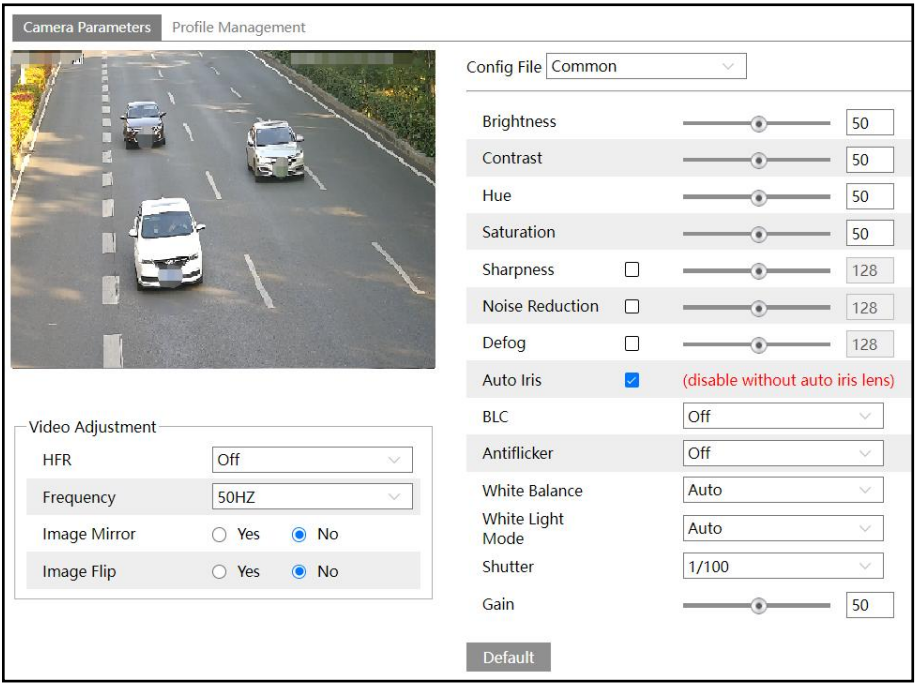


The recommended image parameter settings are as follows:

Image Parameter \ Config File	Common	Day	Night
Brightness	50	50	8
Contrast	50	50	50
Hue	50	50	50
Saturation	50	50	50
Sharpness	Unchecked	Unchecked	Unchecked
Noise Reduction	Unchecked	Unchecked	Unchecked
Defog	Unchecked	Unchecked	Unchecked
HFR	Off	Off	Off
BLC	Off	Off	Off
Antiflicker	Off	Off	Off
Smart IR	Off	Off	Off
White Balance	Auto	Auto	Auto
Day/night mode	Auto	Auto	Auto
Shutter	Normal Mode 50Hz: 1/100 60Hz: 1/120	Normal Mode 50Hz: 1/500 60Hz: 1/500	Normal Mode 50Hz: 1/500 60Hz: 1/500
	HWDR Mode 50Hz: 1/25 60Hz: 1/30	HWDR Mode 50Hz: 1/25 60Hz: 1/30	HWDR Mode 50Hz: 1/25 60Hz: 1/30
	HFR Mode 50Hz: 1/100 60Hz: 1/120	HFR Mode 50Hz: 1/500 60Hz: 1/500	HFR Mode 50Hz: 1/500 60Hz: 1/500
Gain	Normal Mode 10	Normal Mode 10	Normal Mode 10
	HWDR Mode 50	HWDR Mode	50
	HFR Mode 10	HFR Mode 10	HFR Mode 10
License Plate Detection —Detection Config— License Plate Exposure	Checked, set to “8” (see License Plate Exposure for details)		

Note: The above table is only for reference. You can slightly adjust according to the actual condition.

- **White Light Models:**



Schedule: the default setting is “Full Time/Continous”.
Config File: the default setting is “Common”.

The recommended image parameter settings are as follows:

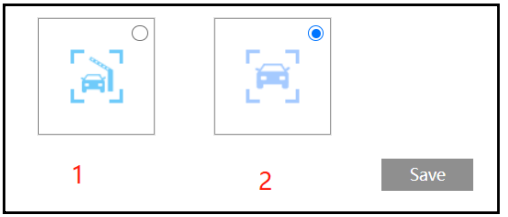
Config File / **Image Parameter**	Common
Brightness	50
Contrast	50
Hue	50
Saturation	50
Sharpness	Unchecked
Noise Reduction	Unchecked
Defog	Unchecked
Auto Iris	Checked
HFR	Off
BLC	Off
Antiflicker	Off
White Light Mode	Auto
White Balance	Auto

<table>
<tr><td rowspan="10">Shutter</td><td colspan="2">Normal Mode</td></tr>
<tr><td>Entrance & Exit</td><td>Low Speed Road</td></tr>
<tr><td>50Hz: 1/100
60Hz: 1/120</td><td>50Hz: 1/500
60Hz: 1/500</td></tr>
<tr><td colspan="2">HWDR Mode</td></tr>
<tr><td>Entrance & Exit</td><td>Low Speed Road</td></tr>
<tr><td>50Hz: 1/25
60Hz: 1/30</td><td>50Hz: 1/25
60Hz: 1/30</td></tr>
<tr><td colspan="2">HFR Mode</td></tr>
<tr><td>Entrance & Exit</td><td>Low Speed Road</td></tr>
<tr><td>50Hz: 1/100
60Hz: 1/120</td><td>50Hz: 1/500
60Hz: 1/500</td></tr>
<tr><td rowspan="9">Gain</td><td colspan="2">Normal Mode</td></tr>
<tr><td>Entrance & Exit</td><td>Low Speed Road</td></tr>
<tr><td>50</td><td>10</td></tr>
<tr><td colspan="2">HWDR Mode</td></tr>
<tr><td>Entrance & Exit</td><td>Low Speed Road</td></tr>
<tr><td>50</td><td>50</td></tr>
<tr><td colspan="2">HFR Mode</td></tr>
<tr><td>Entrance & Exit</td><td>Low Speed Road</td></tr>
<tr><td>50</td><td>10</td></tr>
<tr><td>License Plate Detection
—Detection Config—
License Plate Exposure</td><td colspan="2">Checked, set to “8” (see License Plate Exposure for details)</td></tr>
</table>

Note: The above table is only for reference. You can slightly adjust according to the actual condition.

2.3 Configuring Application Scenarios

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

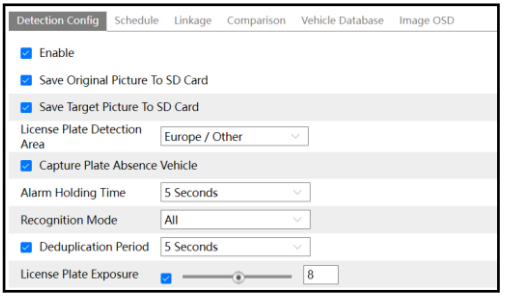


Event Type: 1- Entrance and Exit; 2- License Plate Detection.
If you want to switch the event type, please select it and then click “Save”. After successful reboot, the corresponding event type will be displayed. Select and set as needed.

2.4 License Plate Detection

License Plate Detection: This function is to detect and compare license plate numbers.

Alarms will be triggered when a license plate is detected.
Vehicle license plate detection and comparison settings:
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/latch time 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.

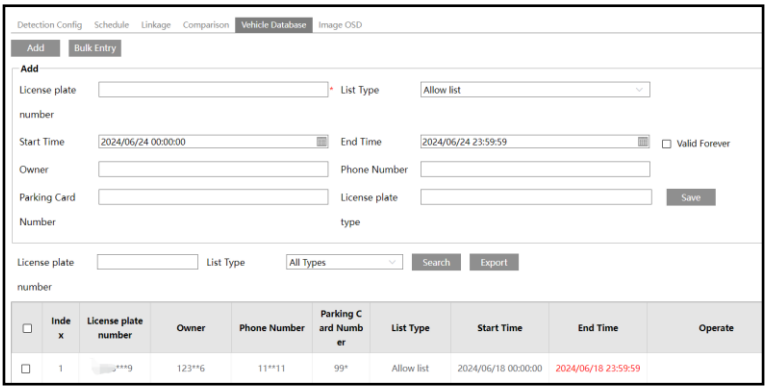
To set a blocked area:
Check “Blocked Area” and select the number. Then click “Draw Area” to draw a closed area. Up to 4 areas can be set up. After you set the blocked area, this area will not be detected.

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.

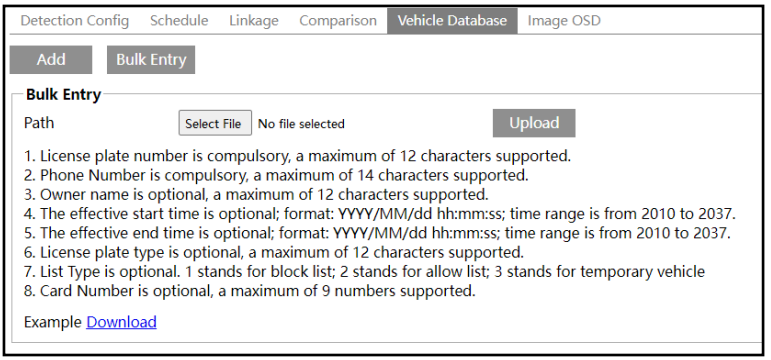
6.Set the schedule of license plate detection. The setup steps of the schedule are the same as schedule recording setup (See Schedule Recording).

7. Add vehicles to the vehicle Database. Click the vehicle database tab to go to the following interface.



- **Add vehicles**

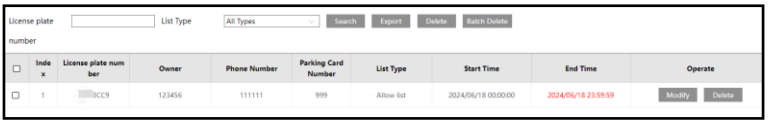
Click “Add” to extend a vehicle adding box as shown in the above figure. Enter the license plate number, select list type, start and end time, enter owner, license plate type, phone number, parking card number and so on. Then click “Save” to save the vehicle information.
List type: temporary vehicle, allow list and block list can be selected.
Click “Bulk Entry” to add multiple vehicles at one time as shown below.



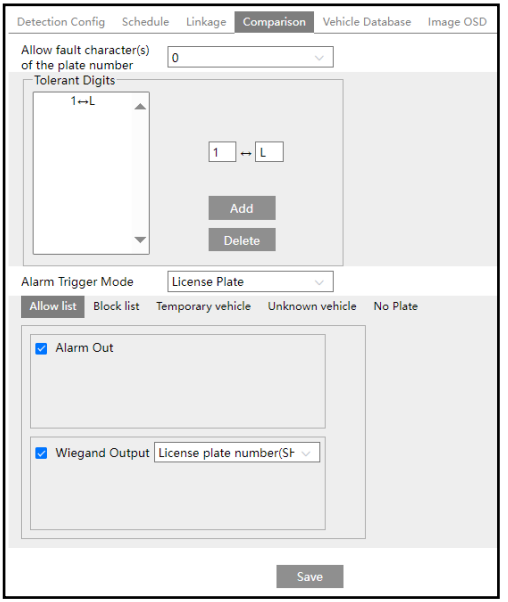
Please edit the vehicle information according to the requirements shown on the above interface. If you don’t know how to edit the file, please click “Download” to download an example file and then follow the example to edit. After that, click “Select File” to choose the vehicle information file and click “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. Note that the protocol of wiegand input only supports 26bit(8).

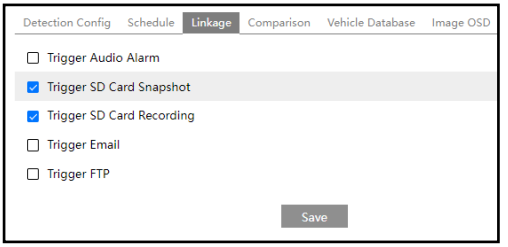
Alarm Out: Select the list type and then checkmark alarm out. Then the alarm output will be triggered when the captured plate number is matched successfully with the plate number of

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.

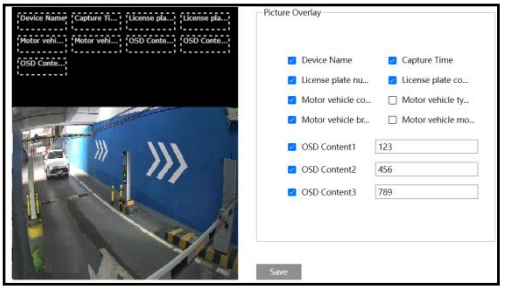
Wiegand Output: When the alarm trigger mode is “License Plate”, you can enable Wiegand Output. Select the list type and then checkmark wiegand output. Then the wiegand output will be triggered when the captured plate number is matched successfully with the plate number of the selected list. “License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

Note: The camera only supports 26bit(8) and 26bit (SHA1) wiegand output.

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 section for details.

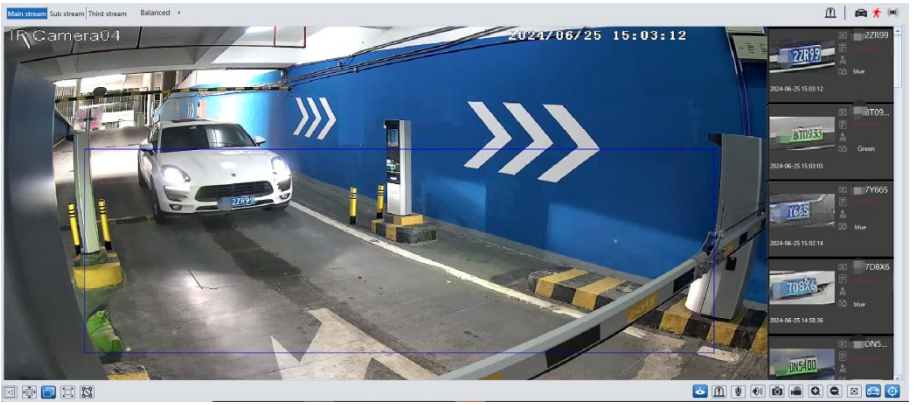


10. Select the attribute information of the target and set OSD contents as needed. Click “Image OSD” and then select the relevant attribute information.

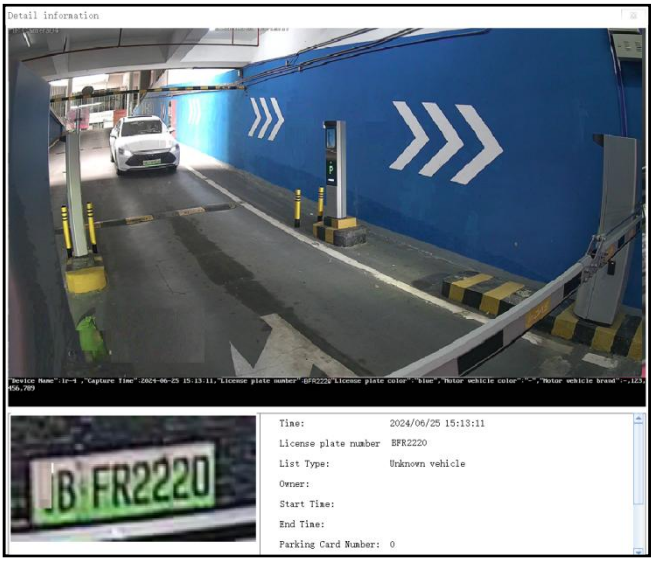


Additionally, you can enter some OSD contents as needed. When the target is detected, the information you select will be displayed under the original snapshot in the detail page of the snapshot.

After all above information 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.

2.5 Entrance and Exit

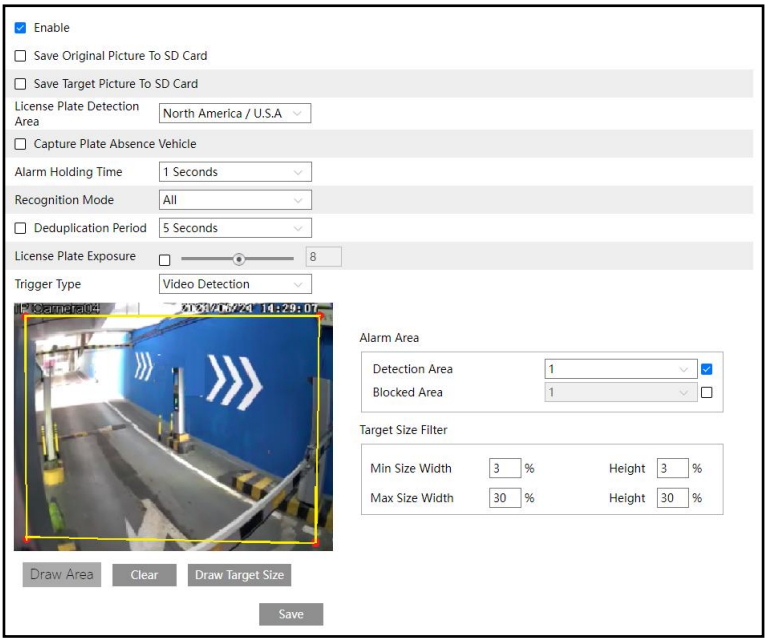
2.5.1 Real-time Image

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.

2.5.2 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.

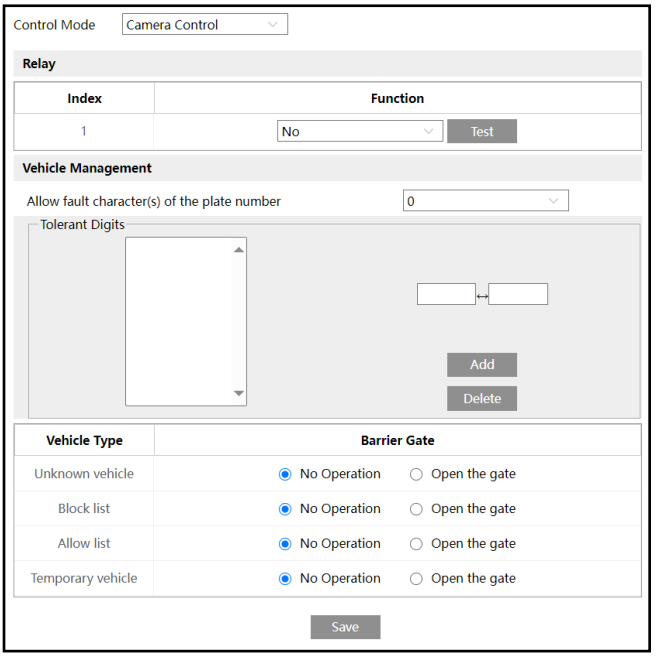


Trigger Type: video detection and IO coil.
Video Detection: Capture vehicle plates by video detection.
IO Coil: If the IO coil is connected to the camera, the trigger type could be set to "IO Coil" and then you can set the linked IO number and trigger status.

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-Point 1~6 for details).

2.5.3 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.

Camera Control

Relay Out: 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.

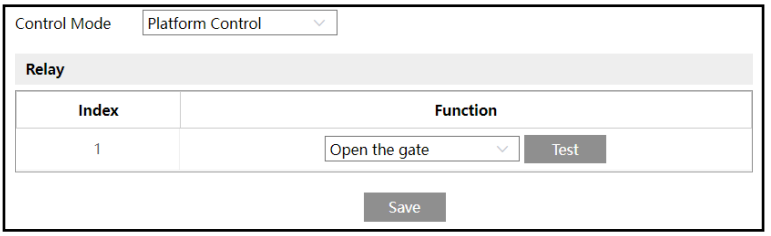
Vehicle Management

The fault tolerance setup here is the same as the fault tolerance setup of the license plate detection. (See License Plate Detection-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.

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.

2.5.4 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- Point 7 for details).

2.5.5 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- Point 10 for details).

2.5.6 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 section for details).

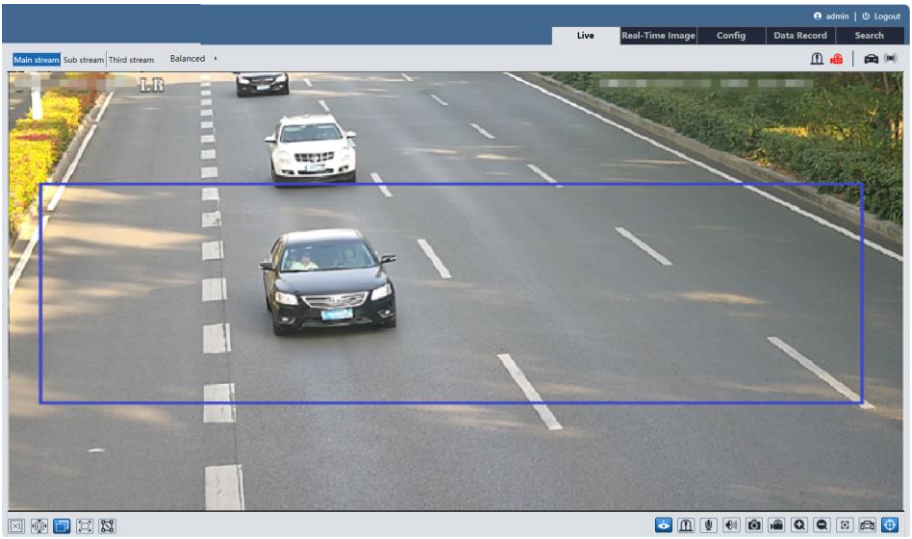
Note:

* 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.

3 Live View

After logging in, the following window will be shown.



The following table is the instructions of the icons on the live view interface.

Icon	Description	Icon	Description
	Original size		Start/stop local recording
	Fit correct scale		Zoom in
	Auto (fill the window)		Zoom out
	Full screen		Zoom/Focus control
	Measure Tool		License plate detection
	Start/stop live view		Rule information display
	Enable/disable alarm output		SD card recording indicator
	Start/stop two-way audio		Sensor alarm indicator
	Enable/disable audio		Motion alarm indicator
	Snapshot		Alarm output indicator

* Measure Tool: get the height and width pixel of the selected region in the live view interface. (This function is only available for main stream). Click  and drag the mouse on the image to draw a desired box. The width and height pixel will directly display in the box.
* Those smart alarm indicators will flash only when the camera supports those functions and the corresponding events are enabled.
* In full screen mode, double click on the mouse to exit or press the ESC key on the keyboard.
* Click AZ control button to show AZ 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		

In the Webcam client, choose “Config” to go to the configuration interface.
Note: Wherever applicable, click the “Save” button to save the settings.

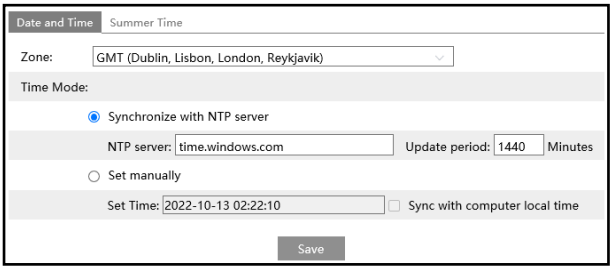
4.1 System Configuration

4.1.1 Basic Information

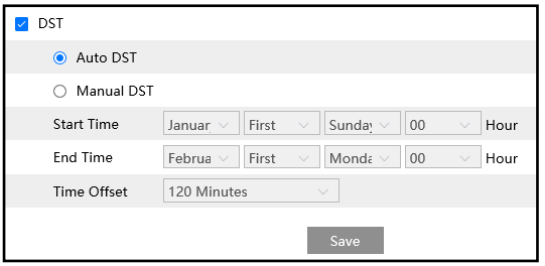
In the “Basic Information” interface, the system information of the device is listed, such as device name, product model, firmware version, device ID, QR code, etc.
After enabling the P2P function (**Config→Network→P2P**), you can use the mobile APP to scan this QRcode to quickly add this device.

4.1.2 Date and Time

Go to **Config→System→Date and Time**. Please refer to the following interface.

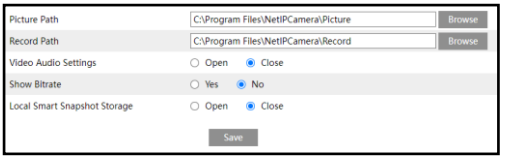


Select the time zone and time mode as needed.
Note: The time zone of the camera and the computer must be the same. It is recommended to modify the time zone of the camera according to the time zone of the computer. If the time zone of the computer is modified, the current web client needs to be closed.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



4.1.3 Local Config

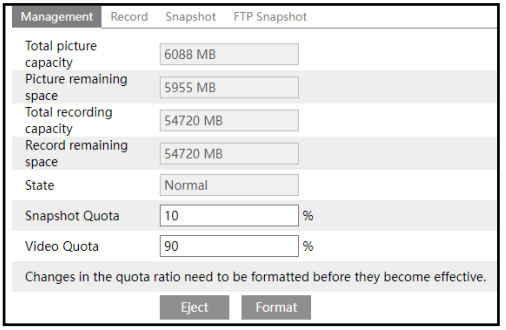
Go to **Config→System→Local Config** to set up the storage path of captured pictures and recorded videos on the local PC. There is also an option to enable or disable audio in the recorded files.



Show Bitrate: enable or disable bitrate display on the live video.
Additionally, "Local smart snapshot storage" can be enabled or disabled here. If enabled, the captured pictures triggered by smart events 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.

4.1.4 Storage

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



- **SD Card Management**

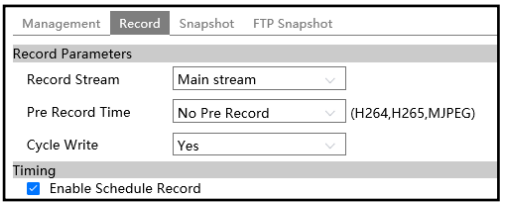
Click the "Format" button to format the SD card. All data will be cleared by clicking this button.

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.

- **Schedule Recording Settings**

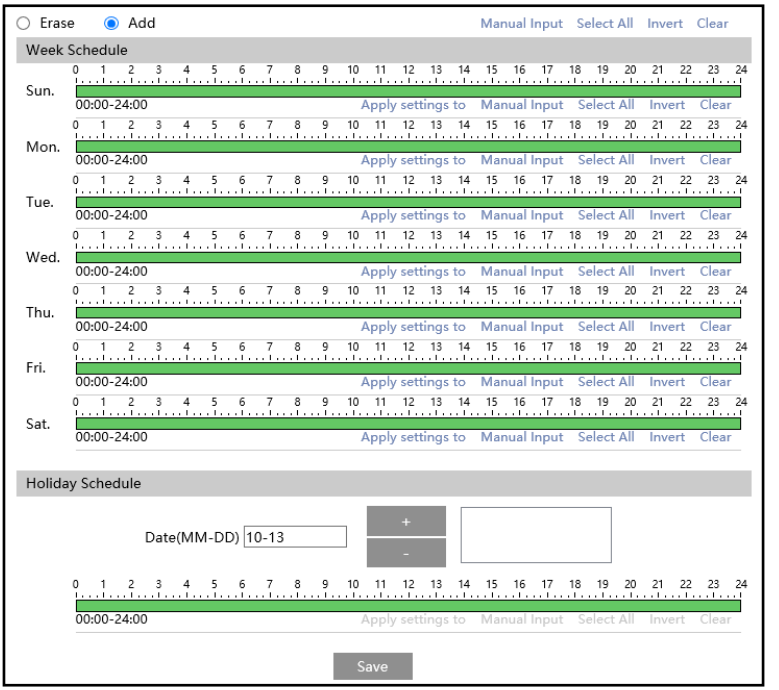
1. Go to **Config→System→Storage→Record** to go to the interface as shown below.



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

Pre Record Time: Set the time to record before the actual recording begins.
Overwrite (Cycle Write): the earliest record data will be replaced by the latest when the disks are full.

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



Weekly schedule

Set the alarm time from Monday to Sunday for a single week. Each day is divided 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).

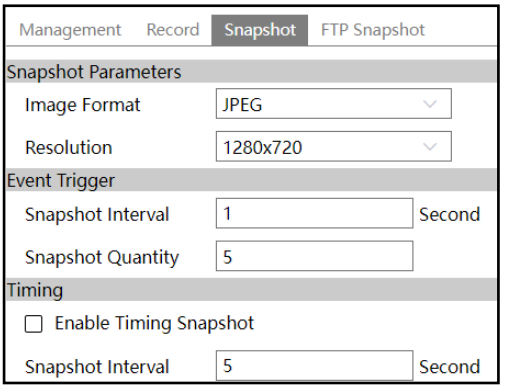
Day schedule

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

Note: Holiday schedule takes priority over weekly schedule.

- **Snapshot Settings**

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



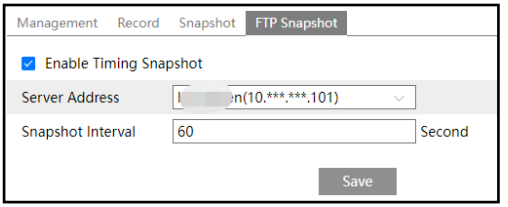
Set the format, resolution and quality of the image saved on the SD card and the snapshot interval and quantity and the timing snapshot here.

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 the schedule are the same as the schedule recording (See Schedule Recording).

- **FTP Snapshot**

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



Server Address: select the set FTP server. See FTP section for the FTP server setting.

4.1.5 Serial Port Settings

Go to **Config→System→Serial Port** interface 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.

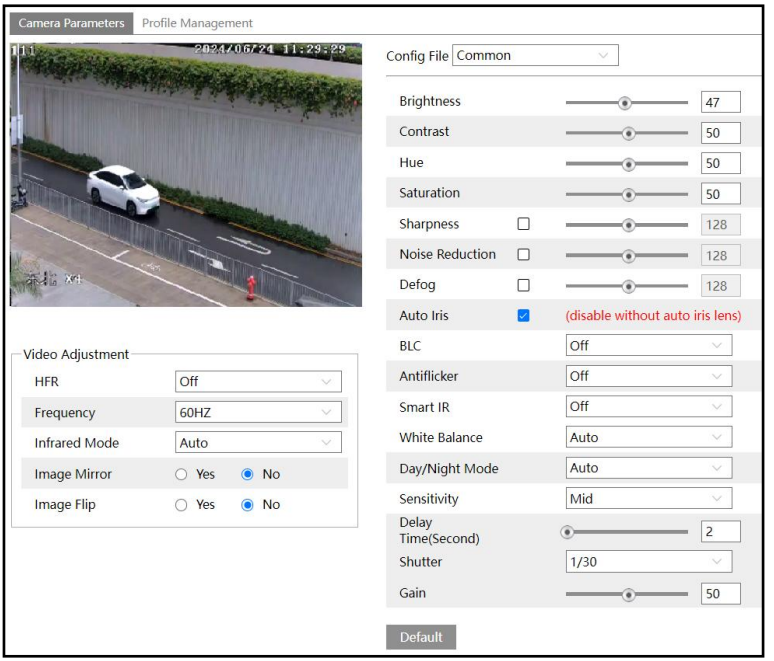
Note：Transparent mode should be enabled when you use RS232/RS485 to transmit the data between the camera and the computer or terminal.

4.2 Image Configuration

4.2.1 Display Configuration

Go to **Image→Display Settings** interface as shown below. The image's brightness, contrast, hue and saturation and so on for common, day and night mode can be set up separately. The image effect can be quickly seen by switching the configuration file.

Note: the camera parameters of different cameras may be slightly different. The following pictures and descriptions are for reference only. The real camera interface shall prevail.



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.

- 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.

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

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

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.

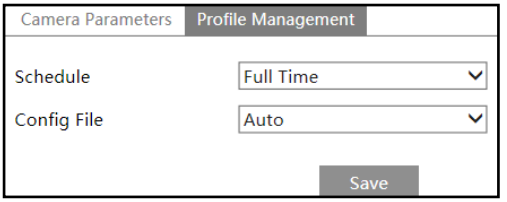
Image Flip/Flip Horizontally: Turn the current video image vertically.

Note: White light models support white light mode settings.

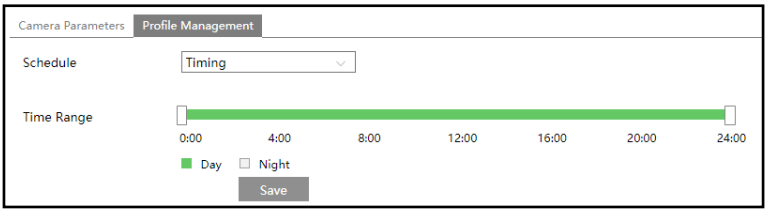
White light mode: Choose "Auto", "Manual" or "OFF" as needed.

Schedule Settings of Image Parameters:

Click the "Profile Management" tab as shown below.



Set full time/continuous schedule for common, day, night mode and specified time schedule for day and night. Choose "Timing/Timed" in the drop-down box of the schedule as shown below.

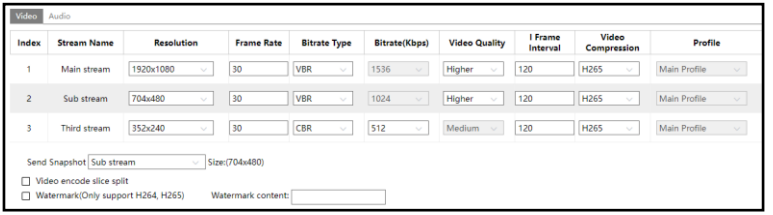


Drag " " icons to set the time of day and night. Blue means day time and blank means night time. If the current mode of camera parameters is set to schedule, the image configuration mode will automatically switch between day and night according to the schedule.

4.2.2 Video / Audio Configuration

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

Note: the video stream parameters of different camera series may be different. The following pictures and descriptions are for reference only. The real camera interface shall prevail.



Three video streams can be adjustable.

Resolution: The size of image.

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

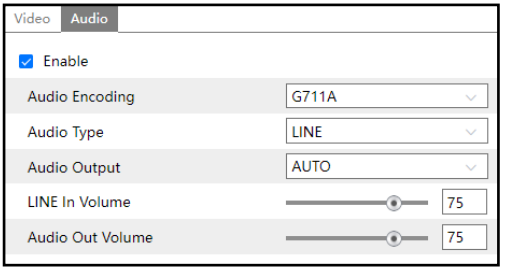
Bitrate type: CBR and VBR are optional. Bitrate is related to image quality. CBR means that no matter how much change is seen in the video scene, the compression bitrate will be kept constant. VBR means that the compression bitrate will be adjusted according to scene changes. For example, for scenes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

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

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

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

Video Compression: 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 thee 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.

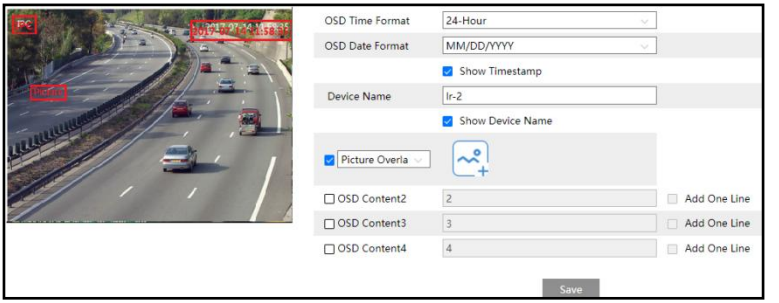


Audio Encoding: G711A and G711U are selectable.
Audio Type: LINE
Audio Output: Talkback, warning or auto can be optional. If "Talkback" is selected, the audio output will be used for two-way audio. If "Warning" is selected, the audio output will be used to play the pre-defined audio alarm. If "Auto" 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.
MIC IN/Audio Out Volume: Set the volume as needed.

4.2.3 OSD Configuration

Go to **Image→OSD** interface as shown below.

Set time stamp, device name, OSD content and picture overlap here. After enabling the corresponding display and entering the content, drag them to change their position. Then click the “Save” button to save the settings.



Picture Overlap Settings:

Check “OSD Content1”, choose “Picture Overlay” and click 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.

4.2.4 Video Mask

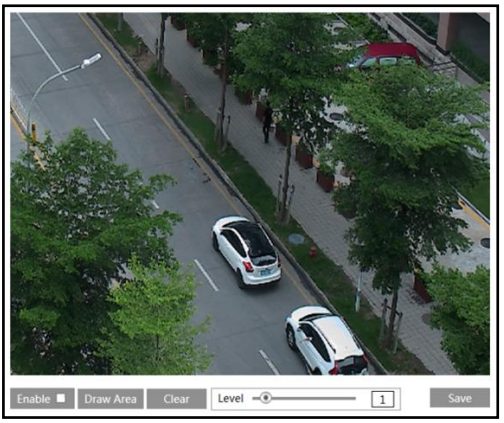
Go to **Image→Video Mask** interface as shown below. A maximum of 4 zones can be set up.

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

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

4.2.5 ROI Configuration

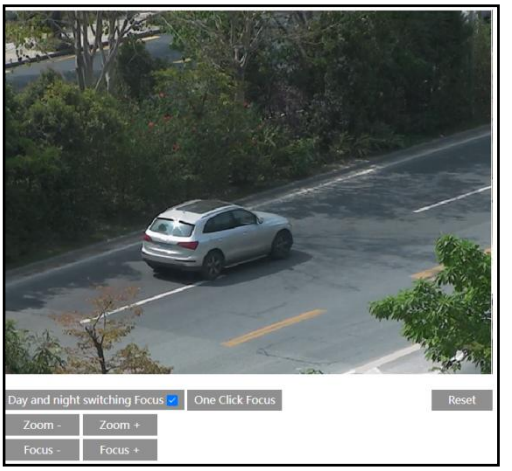
Go to **Image→ROI Config** interface as shown below. An area in the image can be set as a region of interest. This area will have a higher bitrate than the rest of the image, resulting in better image quality for the identified area.



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

4.2.6 Lens Control

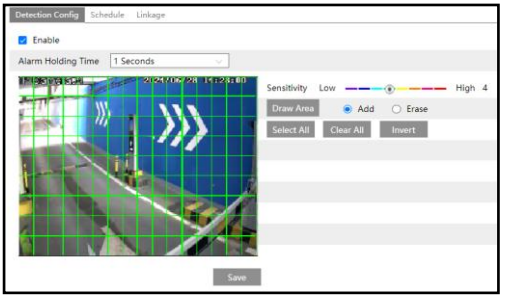
This function is only available for the model with a motorized zoom lens. Within this section, zoom and focus can be controlled. If the image is out of focus after a manual adjustment, one key focus can be used to set the focus automatically. Go to Config→Image→ Zoom/Focus interface to set.



4.3 Alarm Configuration

4.3.1 Motion Detection

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



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

Alarm Holding Time: it refers to the 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 would not detect any other motion in 20 seconds. If there is another motion detected during this period, it will be considered as continuous movement; otherwise it will be considered as a single motion.

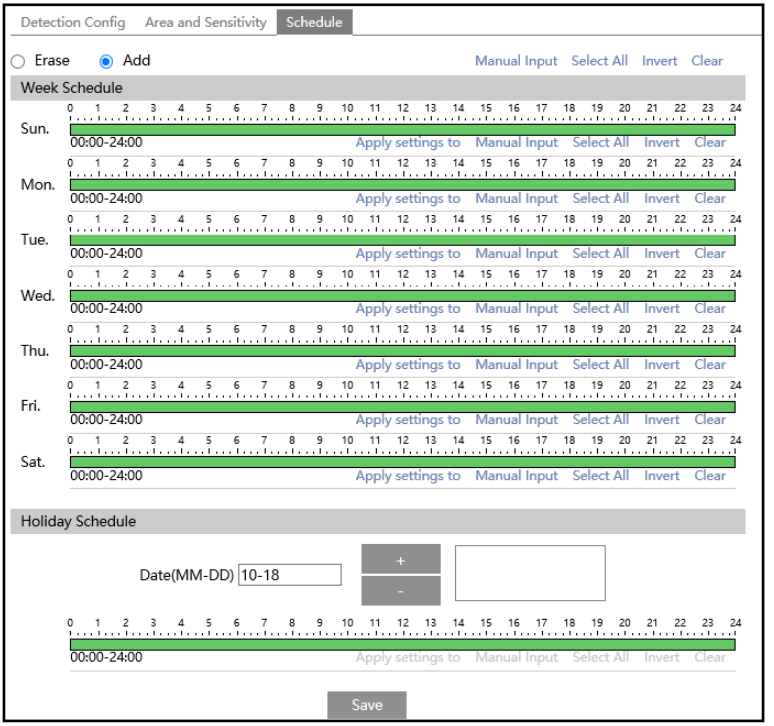
2. Set motion detection area and sensitivity.

Move the “Sensitivity” scroll bar to set the sensitivity. Higher sensitivity value means that motion will be triggered more easily.

Select “Add” and click “Draw”. Drag the mouse to draw the motion detection area; Select “Erase” and drag the mouse to clear motion detection area.

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

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.

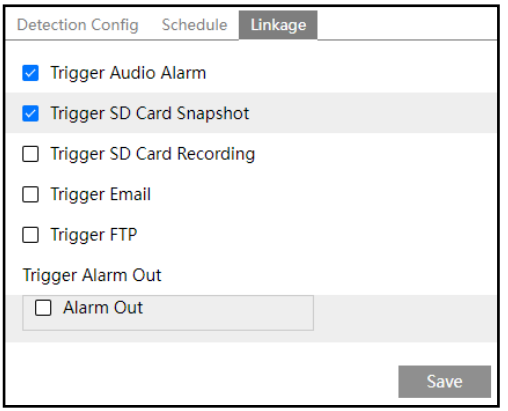
Manual Input: Click it for a specific day to enter specific start and end times. This adds more granularities (minutes).

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.

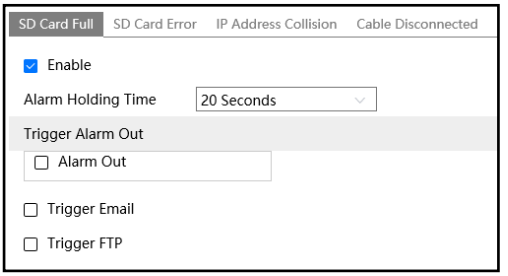


Trigger Audio Alarm: If selected, the warning voice will play automatically on detecting a motion based alarm. (Please set the warning voice first. See Audio Alarm for details). Only some models support this function.
Trigger SD Card Snapshot: If selected, the system will capture images on motion detection 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 FTP server address. Please refer to FTP configuration section 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 output can be selected)

4.3.2 Exception Alarm

- **SD Card Full**

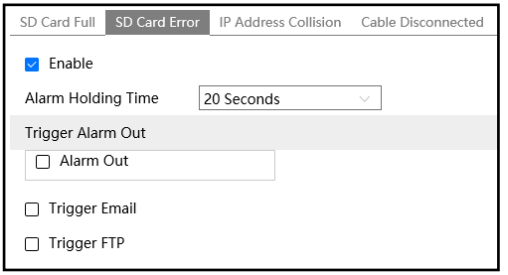
1. Go to **Config→Alarm→Exception Alarm→SD Card Full**.



2. Click “Enable”.
3. Set the alarm/latch holding time and alarm trigger options. The setup steps are the same as motion detection. Please refer to Motion Detection section 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 **Config→Alarm→ Exception Alarm →SD Card Error** as shown below.



2. Click “Enable”.
3. Set the alarm holding/latch time and alarm trigger options. Trigger alarm out, Email and FTP. The setup steps are the same as motion detection. Please refer to Motion Detection section for details.

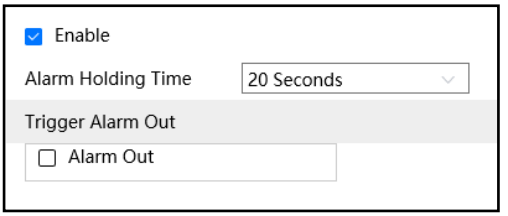
- **IP Address Conflict**

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

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

- **Cable Disconnection**

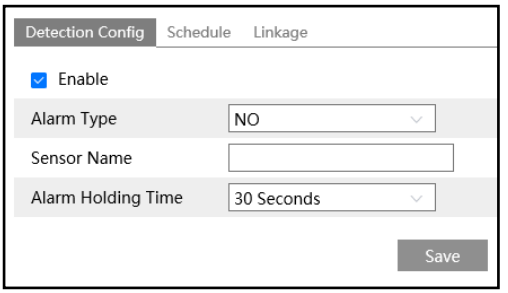
Go to **Config→Alarm→ Exception Alarm →Cable Disconnected** as shown below.



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.

4.3.3 Alarm In

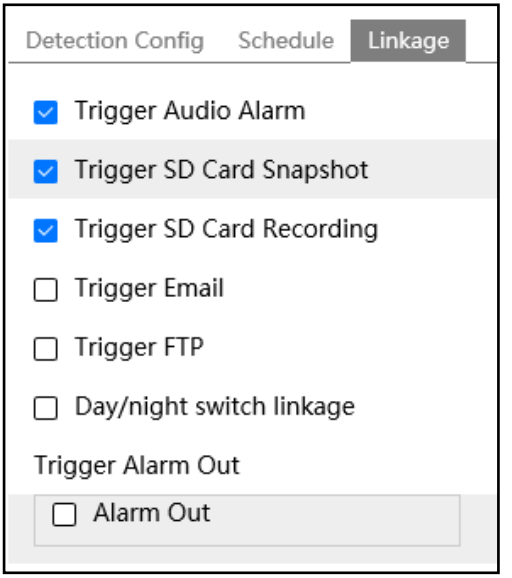
To set sensor alarm (alarm in):
Go to **Config→Alarm→Alarm In** interface as shown below.



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.

Trigger Audio Alarm: If selected, the camera will play the warning voice when the sensor alarm is triggered. Please set the warning voice first. See Audio Alarm for details.
Trigger SD Card Snapshot: If selected, the system will capture images when the sensor alarm is triggered and save the images on an SD card.
Trigger SD Card Recording: If selected, the video will be recorded on an SD card when the sensor alarm is triggered.
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 FTP server address. Please refer to the FTP configuration section for more details.
Day/night switch linkage: Day/night indicator (via Alarm In). If enabled, the system will switch to day or night mode upon the occurrence of the sensor alarm. (In white light mode, this function is not available)

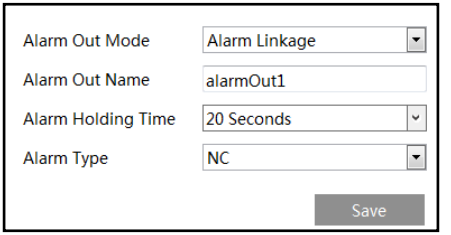
Trigger Alarm Out: If selected, this would trigger an external relay output that is connected to the camera when the sensor alarm is triggered (some models may support two alarm output interfaces).



If there are two sensors, please select the sensor ID and check alarm linkage options respectively.

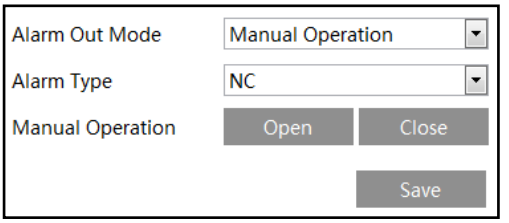
4.3.4 Alarm Out

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

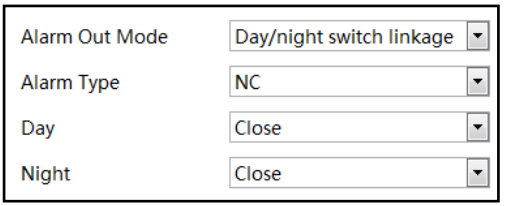


Alarm Out ID: Some models may support two alarm output interfaces. The alarm out can be set respectively by selecting alarm out ID.
Alarm Out Mode: Alarm linkage, manual operation, day/night switch linkage (day/night indicator via alarm in) and timing (schedule) are optional.
Note: In Entrance and Exit 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

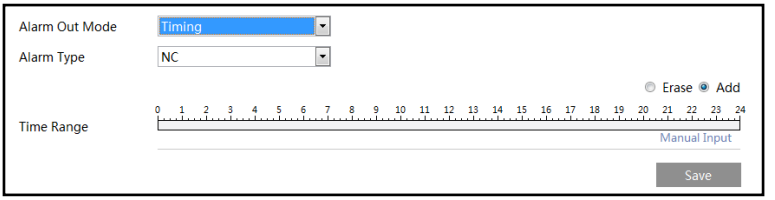
Control". If the alarm out mode is selected to other modes, the barrier gate switch will be ineffective. If "Access Control" is selected, alarm linkage actions will not take effect.
Alarm Linkage: Having selected this mode, select alarm out name, alarm holding time at the "Alarm Holding Time" pull down 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 (Day/Night indicator via alarm in): 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)

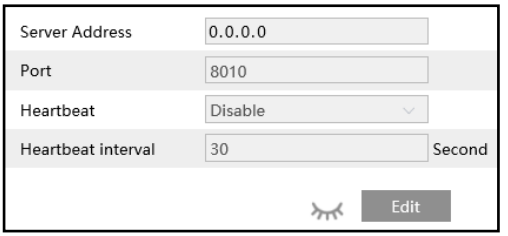


Timing (Schedule): Select the alarm type. Then click "Add" and drag the mouse on the timeline to set the schedule of alarm out; click "Erase" and drag the mouse on the timeline to erase the set time schedule. After this schedule is saved, the alarm out will be triggered in the specified time.



4.3.5 Alarm Server

Go to **Alarm→Alarm Server** interface as shown below.



Click “Edit” to set the alarm server.

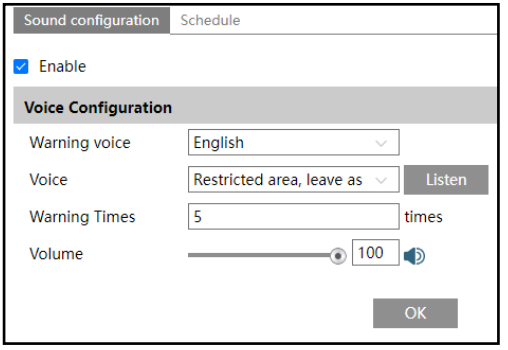
Set the server address, port, heartbeat and heartbeat interval. When an alarm occurs, the camera will transfer the alarm event to the alarm server. If an alarm server is not needed, there is no need to configure this section.

Click to view the entire server address; click to hide a part of sensitive data.

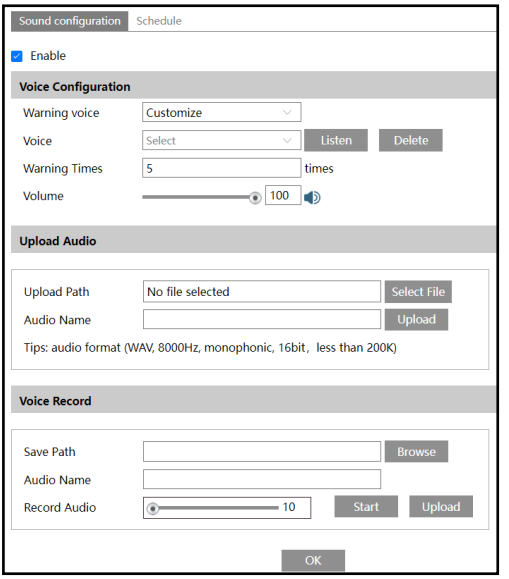
4.3.6 Audio Alarm

Go to **Alarm→Audio Alarm** interface 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.



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.

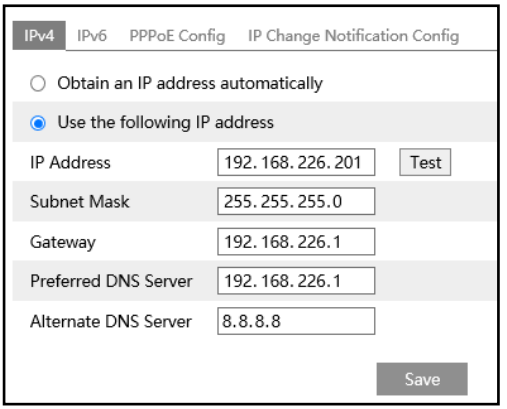
③ Set the schedule of audio alarm. The setup steps of the schedule are the same as the schedule recording setup. (See Schedule Recording).

④ Click “OK” to save the settings.

4.4 Network Configuration

4.4.1 TCP/IP

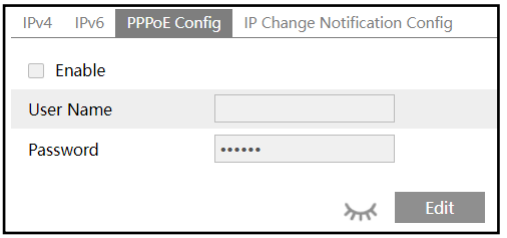
Go to **Config→Network→TCP/IP** interface as shown below. There are two ways for network connection.



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.

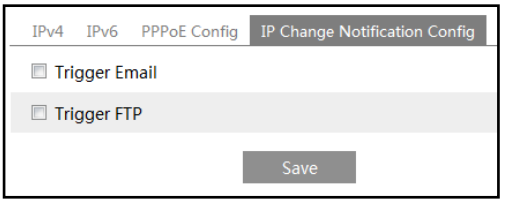
Test: Test the effectiveness of the IP address by clicking this button.

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.



Either method of network connection can be used. If PPPoE is used to connect internet, the camera will get a dynamic WAN IP address. This IP address will change frequently. To be notified, the IP change notification function can be used.

Click "IP Change Notification Config" to go to the interface as shown below.



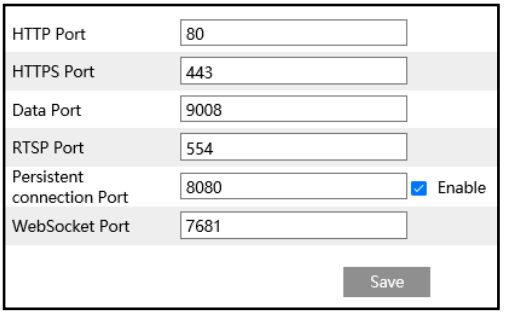
Trigger Email: when the IP address of the device is changed, the new IP address will be sent to the email address that has been set up.

Trigger FTP: when the IP address of the device is changed, the new IP address will be sent to

FTP server that has been set up.

4.4.2 Port

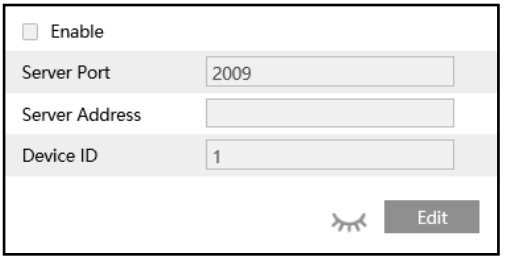
Go to **Config→Network→Port** interface as shown below. HTTP port, Data port and RTSP port can be set.



HTTP Port: The default HTTP port is 80. It can be changed to any port which is not occupied.
HTTPS Port: The default HTTPs port is 443. It can be changed to any port which is not occupied.
Data Port: The default data port is 9008. Please change it as necessary.
RTSP Port: The default port is 554. Please change it as necessary.
Persistent Connection Port: The port is used for a persistent connection of the third-party platform to push smart data, like face pictures.
WebSocket Port: Communication protocol port for plug-in free preview.

4.4.3 Server Configuration

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

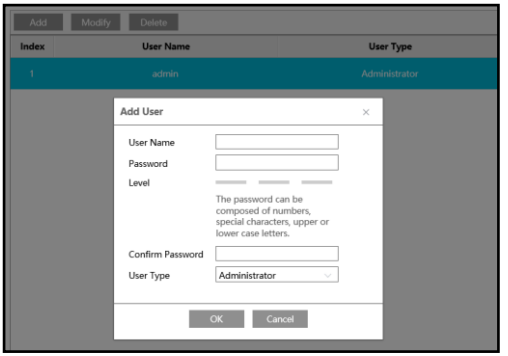


1. Click “Edit” and then check “Enable”.
2. Check the IP address and port of the transfer media server in the NVMS/NVR. Then enable the auto report in the NVMS/NVR when adding a new device. Next, enter the remaining information of the device in the NVMS/NVR. After that, the system will automatically allot a

device ID. Please check it in the NVMS/NVR.
3. Enter the above-mentioned server address, server port and device ID in the corresponding boxes. Click the “Save” button to save the settings. You can show or hide the sensitive data as needed.
3. Enter the above-mentioned server address, server port and device ID in the corresponding boxes. Click the “Save” button to save the settings.

4.4.4 Onvif

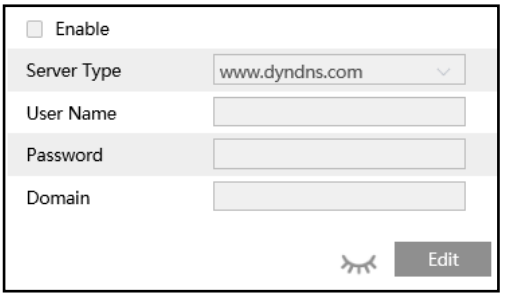
The camera can be searched and connected to the third-party platform via ONVIF/RTSP protocol.
If “Activate Onvif User” is enabled in the device activation interface, the password of ONVIF admin user can be modified simultanously. When you connect the camera through the ONVIF protocol in the third-party platform, you can use this onvif user to connect.
You can also modify the password of admin sperately in the following interface and add new users in the Onvif interface.



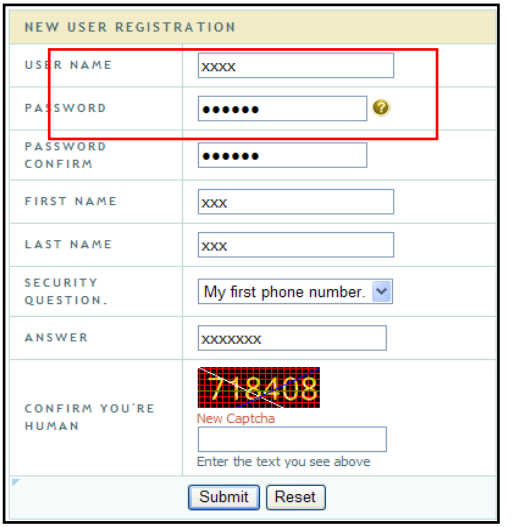
Note: when adding the device to the third-party platform with ONVIF/RTSP protocol, please use the onvif user in the above interface.

4.4.5 DDNS

If the camera is set up with a DHCP connection, DDNS should be set for the internet.
1. Go to **Config→Network→ DDNS**.

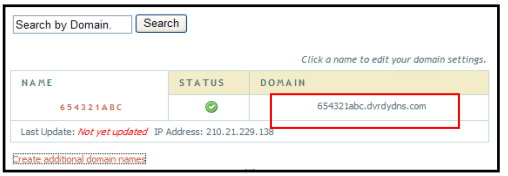


2. Apply for a domain name. Take www.dvrdyndns.com for example.
Enter www.dvrdydns.com in the web address bar to visit its website. Then Click the "Registration" button.



Create domain name.

After the domain name is successfully applied for, the domain name will be listed as below.



3. Click “Edit” and then enter the username, password, domain you apply for in the DDNS configuration interface.
4. Click the “Save” button to save the settings.

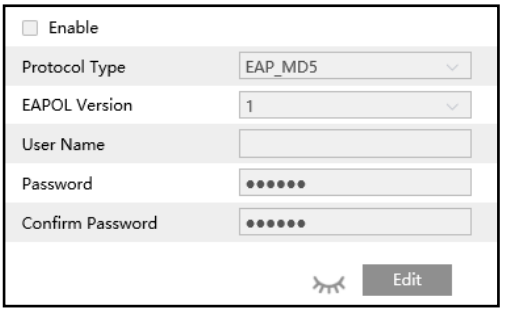
4.4.6 SNMP

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

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.

4.4.7 802.1x

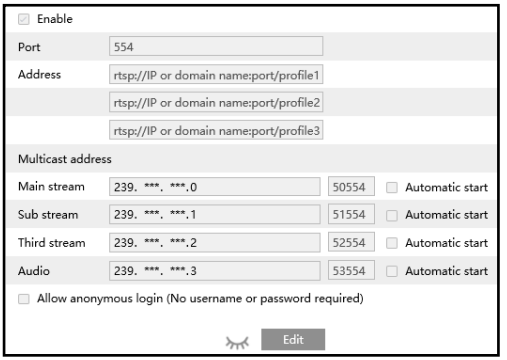
If it is enabled, the camera's data can be protected. When the camera is connected to the network protected by the IEE802.1x, user authentication is needed.



To use this function, the camera shall be connected to a switch supporting 802.1x protocol. The switch can be 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 certificate(s). 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 with the user name and password applied for and registered in the authentication server.

4.4.8 RTSP

Go to **Config→Network→RTSP**.



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

Multicast Address

Main stream: The address format is

"rtsp://IP address: rtsp port/profile1?transportmode=mcast".

Sub stream: The address format is

"rtsp://IP address: rtsp port/profile2?transportmode=mcast".

Third stream: The address format is

"rtsp://IP address: rtsp port/profile3?transportmode=mcast".

……

Note: Some models may support third stream, fourth stream or fifth stream.

Audio: Having entered the main/sub stream in a VLC player, 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.

Note:1. This camera supports local video preview through a VLC player. Enter the RTSP address (unicast or multicast, eg. rtsp://192.168.226.201:554/profile1?transportmode=mcast) in a VLC player to realize the simultaneous video preview with the web client.

2. The IP address mentioned above cannot be the address of IPv6.

3. Avoid the use of the same multicast address in the same local network.

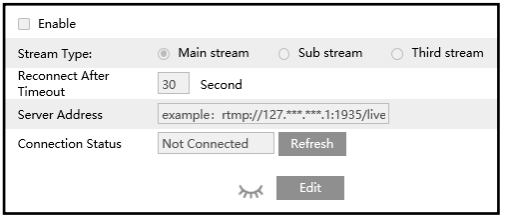
4. When playing the video through the multicast streams in a VLC player, please pay attention to the mode of the VLC player. If it is set to TCP mode, the video cannot be played.

5. If the coding format of the video of the main stream is MJPEG, the video may be disordered at some resolutions.

4.4.9 RTMP

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

Go to **Config→Network→RTMP**.



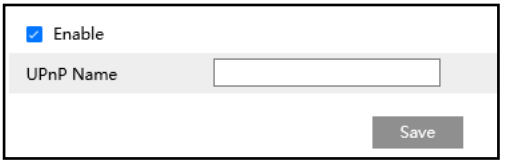
Click "Edit" and then check "Enable", select stream type and set the reconnection time after timeout and server address as needed.

Server address: Enter the server address allocated by the third party server.

After that, click "Save" to save the settings. Then click "Refresh" to view the connection status.

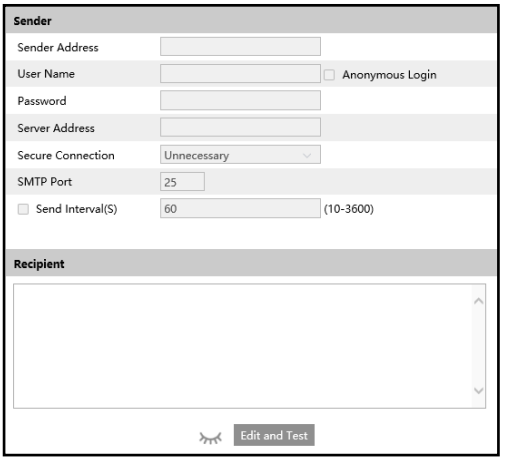
4.4.10 UPNP

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



4.4.11 Email

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



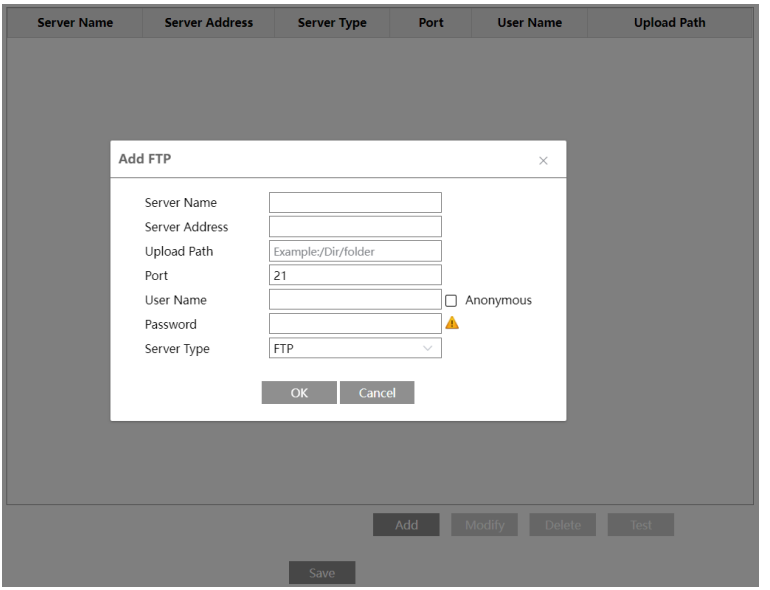
Click "Edit and Test" to set the sender and the recipient.
Sender Address: sender's e-mail address.
User name and password: sender's user name and password (you don't have to enter the username and password if "Anonymous Login" is enabled).
Server Address: The SMTP IP address or host name.
Select the 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.

4.4.12 FTP

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

1. Go to **Config→Network →FTP**.



2. 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.

3. In the event setting interface (like intrusion, line crossing, etc.), trigger FTP as shown below.

Please refer to Storage-Snapshot Setting for the parameter settings of the sending snapshots.

Rule of FTP storage path: /device MAC address/event type/date/time/
For example: a license plate detection alarm occurs
FTP file path：\00-18-ae-a8-da-2a\VEHICE\2021-01-09\14\
Event name table:

File Name	Event Type
IP	IP address change
MOTION	Motion Detection
SENSOR	Sensor Alarm
VEHICE	License Plate Detection
SDFULL	SD Full
SDERROR	SD Error

Jpg image naming rule:
Event type_Year(4digits)-Month(2digits)-Day(2 digits)-Hour(2 digits)-Minute(2 digits)-Second(2 digits)-Millisecond(3 digits)_index(3digits).jpg
Description:
1. Event type: refers to the above table.
2. Zero shall be added if the digits are insufficient.
For example: MOTION_2021-03-16-16-20-07-529_032.jpg

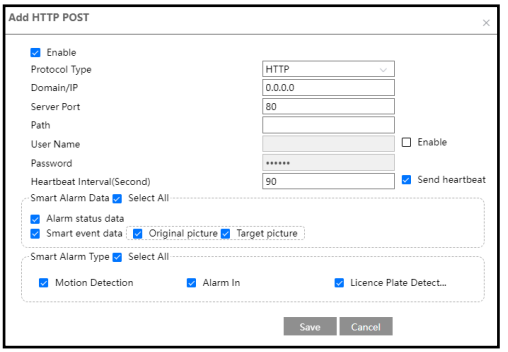
Txt file naming rule:
Event type_Year(4digits)-Month(2digits)-Day(2 digits)-Hour(2 digits)-Minute(2 digits)-Second(2 digits)-Millisecond(3 digits)_index(3digits).txt

TXT file content:
device name: xxx mac: device MAC address Event Type time:
For example: device name: IPC mac: 00-18-ae-a8-da-2a MOTION time: 2021-03-16 12:20:07

Correspondence between txt file and jpeg file: the index of the txt file and jpeg file will be named as the same when the event is triggered each time.

4.4.13 HTTP POST

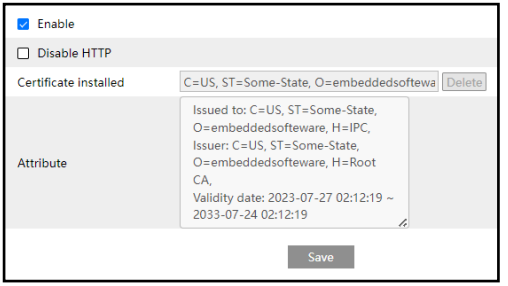
Go to **Config→Network →HTTP POST** interface.
1. Click “Edit”.
2. Click “Add” to add HTTP POST.



Protocol type: HTTP
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.
Enable "Send heartbeat" and set heartbeat interval as needed.
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 the third-party platform. The online state can be viewed in the above interface. After the camera is successfully connected, it will send the selected alarm data to the third-party platform once the selected smart alarm is triggered.

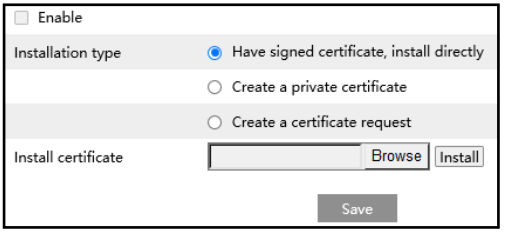
4.4.14 HTTPS

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

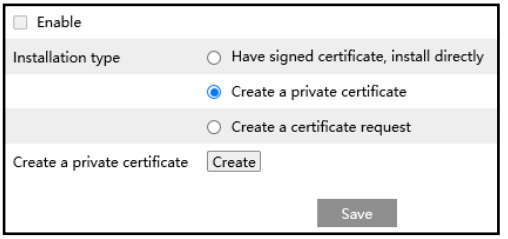


There is a certificate installed by default as shown above. Enable this function and save it. Then the camera can be accessed by entering https://IP: https port via the web browser (eg. https://192.168.226.201:443).
A private certificate can be created if users don't want to use the default one. Click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

to cancel the default certificate. Then the following interface will be displayed.



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



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

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

4.4.15 P2P

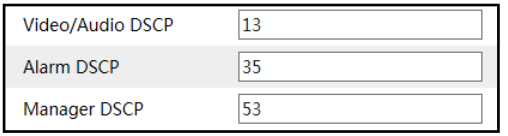
If this function is enabled, the network camera can be quickly accessed by scanning the QR Code in mobile surveillance client via WAN. Enable this function by going to **Config→Network→P2P** interface. After this function is enabled, you can view whether it is

online.

4.4.16 QoS

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

Go to **Config→Network→QoS**.



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

4.4.17 Cloud Upgrade

Note: Before you use cloud upgrade, please make sure P2P is enabled successfully.

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

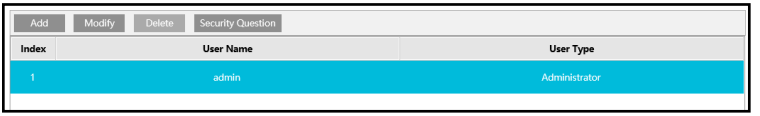
1. Go to **Settings→Network→Cloud Upgrade**.
2. Select "Notify Only" in the cloud upgrade options or click "Manual Check" to check whether the current version is the latest. If your software version is not the latest, click "Upgrade" to download and upgrade from the cloud server.

The cautions of the cloud upgrade are the same with the local upgrade (See Upgrade section for details.

4.5 Security Configuration

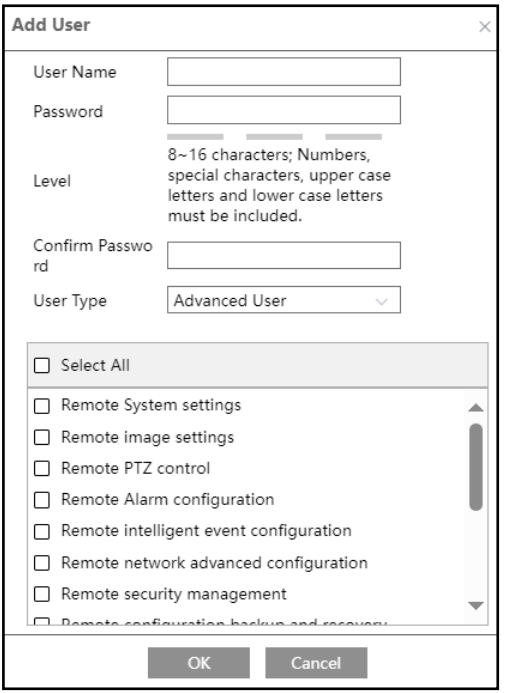
4.5.1 User Configuration

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



Add user:

1. Click the "Add" button to pop up the following textbox.



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

3. Enter the password in the “Password” and “Confirm Password” textbox. Please set the password according to the requirement of the password security level (Go to **Config→Security→Security Management→Password Security** interface to set the security level).

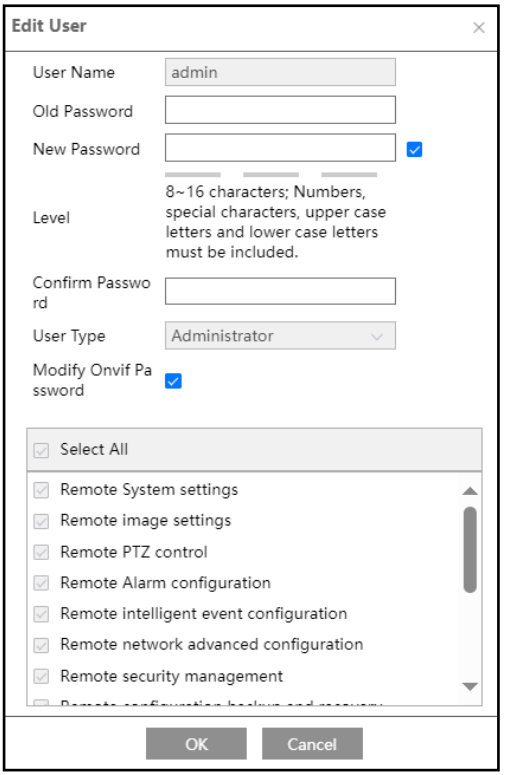
4. Choose the user type and select the desired user permissions.

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

Modify user:

1. Select a user to modify password in the user configuration list box.

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



Admin can modify its password and change the user type and permission of other users here. Other users only can modify their password in this interface.

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 default admin user.

4.5.2 Online User

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

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

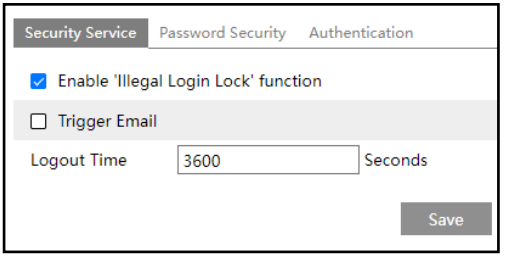
4.5.3 Block and Allow Lists

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

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

4.5.4 Security Management

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

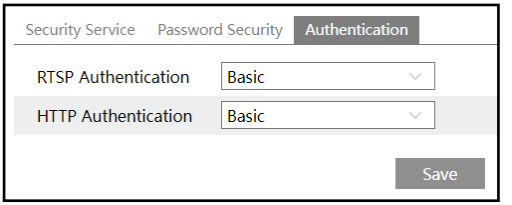


In order to prevent against malicious password unlocking, "Illegal Login Lock" function can be enabled here. If this function is enabled, login failure after trying five times will make the login interface locked. The camera can be logged in again after a half hour or after the camera reboots.
Trigger Email: if enabled, e-mail will be sent when logging in/out or illegal login lock occurs.
Logout/lockout 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 and lower case letters.
Strong Level: 8~16 characters. Numbers, special characters, upper case letters and lower case letters must be included.
For your account security, it is recommended to set a strong password and change your password regularly.

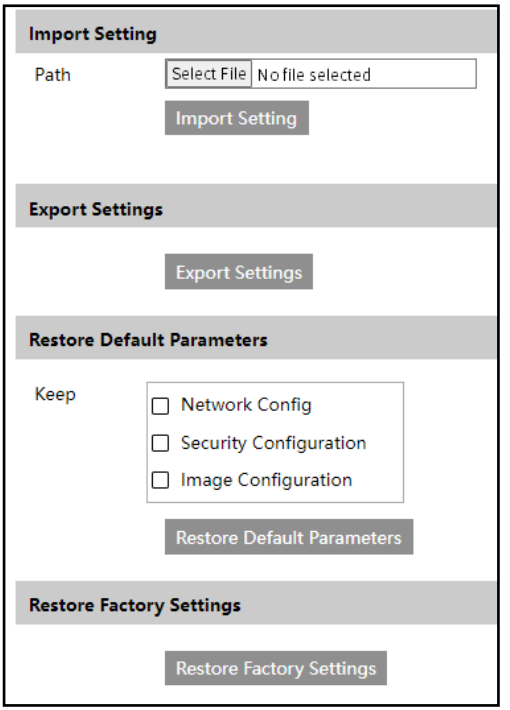
HTTP/RTSP Authentication: Basic or Token is selectable.



4.6 Maintenance Configuration

4.6.1 Backup and Restore

Go to **Config→Maintenance→Backup & Restore**.



- **Import & Export Settings**

Configuration settings of the camera can be exported form a camera into another camera.
1. Click "Browse" to select the save path for import or export information on the PC.
2. Click the "Import Setting" or "Export Setting" button.
Note: The login password needs to be entered after clicking the "Import Setting" button.

- **Restore Default Parameters**

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

- **Restore Factory Settings**

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

4.6.2 Reboot

Go to **Config→Maintenance→Reboot**.
Click the "Reboot" button and then enter the password to reboot the device.

Scheduled Reboot Setting:
If necessary, the camera can be set up to reboot on a time interval. Enable "Time

Settings/Schedule", set the date and time, click the "Save" button and then enter the password to save the settings.

4.6.3 Upgrade

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

1. Click the "Browse/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.

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.

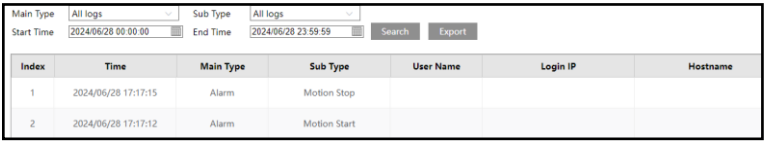
Note: To decrease the upgrade risk, this series of cameras adopts two systems. After one system is successfully upgraded, the other system will be synchronized. If one system fails caused by power failure or other reasons during the upgrade, the other system will not be affected and the camera still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

4.6.4 Operation Log

To query and export log:

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

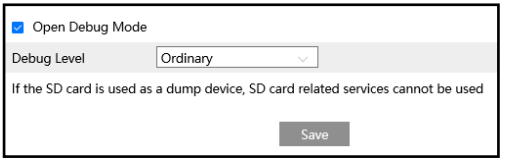


2. Select the main type, sub type, start and end time.
3. Click "Search" to view the operation log.
4. Click "Export" to export the operation log.

4.6.5 Debug Mode

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

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



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

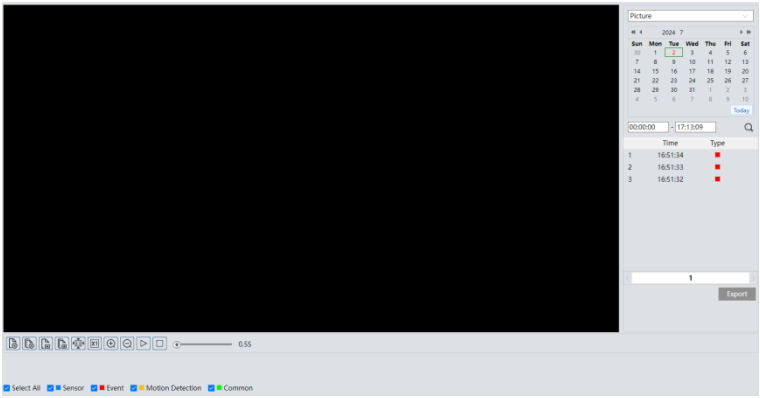
4.6.6 Maintenance Information

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.

5.1 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.

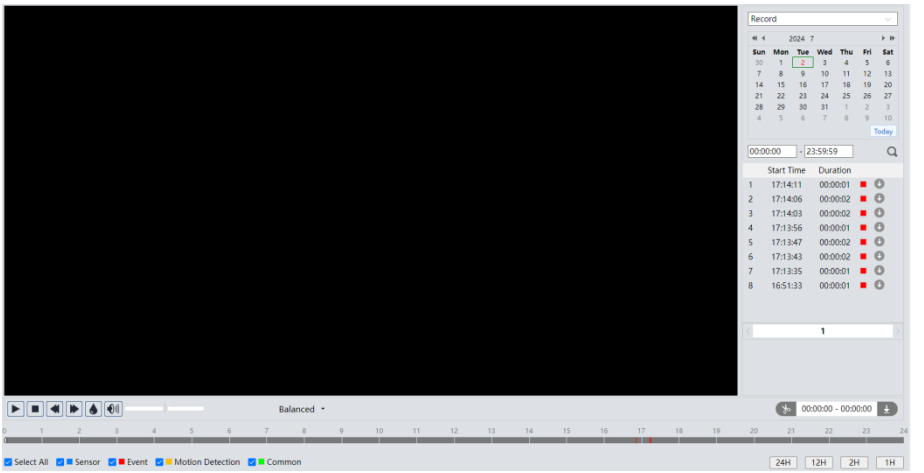
Icon	Description	Icon	Description
	Close: Select an image and click this button to close the image.		Close all: Click this button to close all images.
	Save: Click this button to select the path for saving the image on the PC.		Save all: Click this button to select the path for saving all pictures on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

Icon	Description	Icon	Description
	Play speed: Play speed of the slide show.		

5.2 Video Search

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

1. Choose “Record”.
2. Set search time: Select the date and choose the start and end time.
3. Select the alarm events at the bottom of the interface.
4. Click  to search the images.



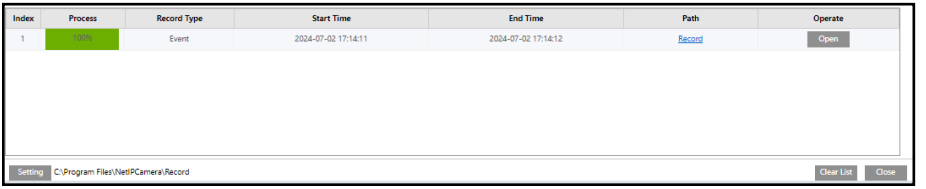
Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button
	Stop button		Speed down
	Speed up		Watermark display
	Enable / disable audio; drag the slider to adjust the volume after enabling audio.		

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

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

Video clip and downloading

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



Click “Setting” to set the storage directory of the video files.

Click “Open” to play the video.

Click “Clear List” to clear the downloading list.

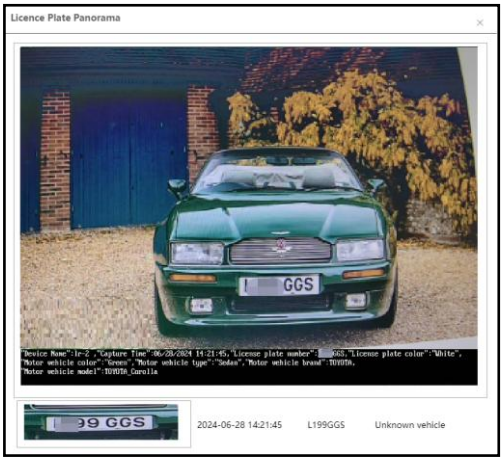
Click “Close” to close the downloading window.

6 License Plate Recognition Result Search

Click Data Record/Vehicle Log tab to go to the license plate recognition result 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 1 Troubleshooting

How to find the password?

A：Click “Forget Password” and then answer the security questions to reset the password.

Fail to connect devices through a web browser.

A: Network is not well connected. Check the connection and make sure it is connected well.

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

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

D: Exclude the above reasons. Restore to default setting by IP-Tool.

IP tool cannot search devices.

It may be caused by the anti-virus software in your computer. Please exit it and try to search device again.

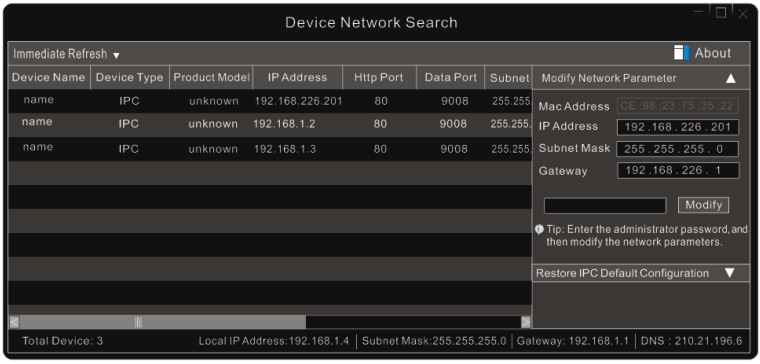
No sound can be heard.

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

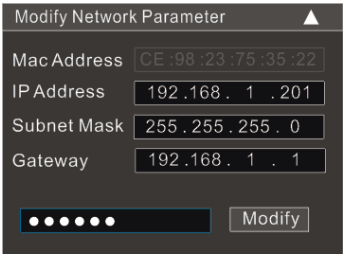
B: Audio function is not enabled at the corresponding channel. Please enable this function.

How to modify IP address through IP-Tool?

A: After you install the IP-Tool, run it as shown below.



The default IP address of this camera is 192.168.226.201. Click the information of the camera listed in the above table to show the network information on the right hand. Modify the IP address and gateway of the camera and make sure its network address is in the same local network segment as the computer’s. Please modify the IP address of your device according to the practical situation.



For example, the IP address of your computer is 192.168.1.4. So the IP address of the camera shall be changed to 192.168.1.X. After modification, please enter the password of "admin" which is set in the device activation interface in advance and then click the "Modify" button to change the network parameters.

How to restore to factory default setting through IP-Tool?

A： Drag the slider at the bottom of the device list to the right and then the MAC address of the searched devices will be viewed. Find the MAC address of the IPC you want to restore to the factory default setting, click ▼ next to "Restore IPC Default Configuration" to expand the menu, then enter the MAC address and click "OK". After that, manually reboot your camera within 30s. Then the camera will successfully restore to the factory default setting