

NYX IPB4-832ANPR

Automatic Number Plate Recognition Camera

User Manual



4MP

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.

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 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 is too close to the camera lens. The IR light from the camera may reflect back into the 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 the 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 functionality and/or IR 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.

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	Introduction	1
2	Network Connection.....	2
2.1	LAN	2
2.1.1	Access through IP-Tool.....	2
2.1.2	Directly Access through IE	4
2.2	WAN	6
3	License Plate Recognition	9
3.1	Configuration Requirements of Camera and Surrounding Area	9
3.2	Recommended Image Settings	10
3.3	License Plate Detection.....	12
4	Live View	18
5	Network Camera Configuration.....	20
5.1	System Configuration.....	20
5.1.1	Basic Information.....	20
5.1.2	Date and Time.....	20
5.1.3	Local Config	21
5.1.4	Storage	21
5.2	Image Configuration	24
5.2.1	Display Configuration.....	24
5.2.2	Video / Audio Configuration.....	27
5.2.3	OSD Configuration	28
5.2.4	Video Mask.....	29
5.2.5	ROI Configuration	30
5.2.6	Lens Control.....	31
5.3	Alarm Configuration	31
5.3.1	Motion Detection	31
5.3.2	Exception Alarm	33
5.3.3	Alarm In.....	35
5.3.4	Alarm Out	35
5.3.5	Alarm Server.....	37
5.4	Event Configuration.....	37
5.4.1	Video Exception Settings	37
5.5	Network Configuration.....	39
5.5.1	TCP/IP	39
5.5.2	Port.....	40
5.5.3	Server Configuration.....	40
5.5.4	Onvif.....	41
5.5.5	DDNS.....	42
5.5.6	SNMP.....	43

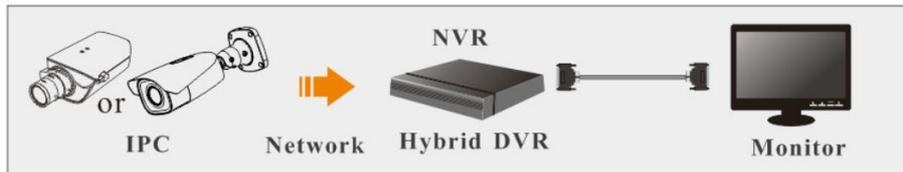
5.5.7	802.1x	44
5.5.8	RTSP	45
5.5.9	RTMP.....	46
5.5.10	UPNP	46
5.5.11	Email.....	46
5.5.12	FTP	47
5.5.13	HTTP POST.....	49
5.5.14	HTTPS	50
5.5.15	QoS	51
5.6	Security Configuration	52
5.6.1	User Configuration.....	52
5.6.2	Online User.....	53
5.6.3	Block and Allow Lists.....	54
5.6.4	Security Management.....	54
5.7	Maintenance Configuration.....	55
5.7.1	Backup and Restore	55
5.7.2	Reboot.....	56
5.7.3	Upgrade.....	56
5.7.4	Operation Log.....	56
6	Search	58
6.1	Image Search.....	58
6.2	Video Search	60
6.2.1	Local Video Search	60
6.2.2	SD Card Video Search.....	61
7	License Plate Recognition Result Search	63
	Appendix.....	65
	Appendix 1 Troubleshooting	65

1 Introduction

Main Features

- ICR auto switch, true day/night
- 3D DNR, WDR
- BLC, Defog, Anti-flicker, etc.
- ROI coding
- Abnormal video signal detection (scene change, video blur detection, video cast detection), license plate recognition
- Support mobile surveillance by smart phones with iOS and Android OS

Surveillance Application



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: IE (plug-in required)/ Firefox/Edge/Safari/Google Chrome

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

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

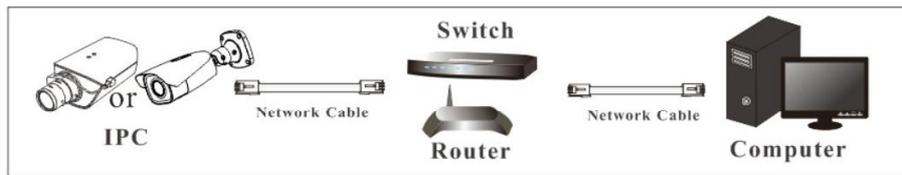
Connect IP-Cam via LAN or WAN. Here only take IE browser for example. The details are as follows:

2.1 LAN

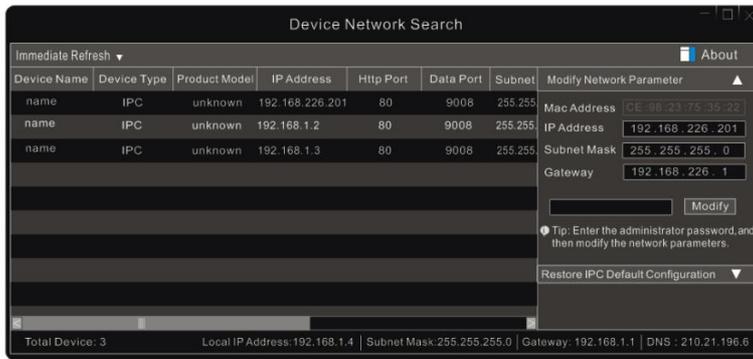
In LAN, there are two ways to access IP-Cam: 1. access through IP-Tool; 2. directly access through IE browser.

2.1.1 Access through IP-Tool

Network connection:



- ① Make sure the PC and IP-Cam are connected to the LAN and the IP-Tool is installed in the PC from the CD.
- 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 pop up the IE browser to connect IP-CAM. After you read the privacy statement, check and click “Already Read”. Then activate the device.

Device Activation

User Name

Activate Onvif User

New Password

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

Confirm Password

Please self-define the password of admin according to the tip.
 If “Activate Onvif User” is enabled, the ONVIF user can be activated simultaneously. When you connect the camera through the ONVIF protocol in the third-party platform, you can use the default username and the password set above to connect.
 After that, follow directions to download, install and run the Active X control if prompted.
 Re-connect your camera via IE browser and then a login box will appear.

Name:	<input type="text" value="Name"/>
Password:	<input type="password" value="Password"/>
Stream Type:	2592x1520 25fps <input type="button" value="v"/>
Language:	English <input type="button" value="v"/>
Forget Password?	
<input type="button" value="Login"/>	

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.

The safety questions should be set after you click “Login” button. It is very important for you to reset your password. Please remember these answers.

Safety Question	
Security Question1	<input type="button" value="v"/>
Answer	<input type="text"/>
Security Question2	<input type="button" value="v"/>
Answer	<input type="text"/>
Security Question3	<input type="button" value="v"/>
Answer	<input type="text"/>
<input type="button" value="OK"/>	

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.

2.1.2 Directly Access through IE

The default network settings are as shown below:

IP address: **192.168.226.201**

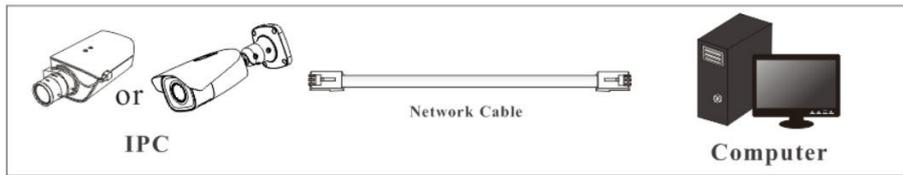
Subnet Mask: **255.255.255.0**

Gateway: **192.168.226.1**

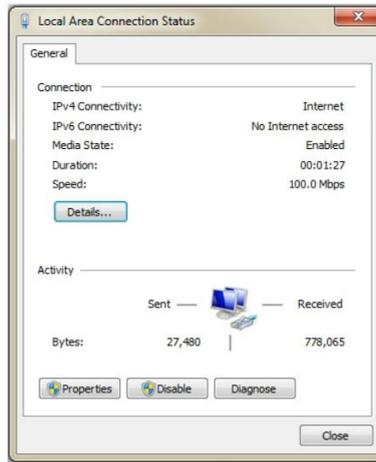
HTTP: **80**

Data port: **9008**

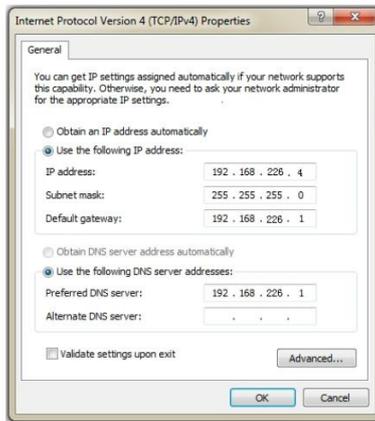
Use the above default settings when logging in the camera for the first time. Directly connect the camera to the computer through network cable.



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 the IE browser and enter the default address of IP-CAM 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.

2.2 WAN

➤ 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.

HTTP Port	80
HTTPS Port	443
Data Port	9008
RTSP Port	554

Port Setup

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

IPv4	IPv6	PPPoE Config	IP Change Notification Config
<input type="radio"/> Obtain an IP address automatically			
<input checked="" type="radio"/> Use the following IP address			
IP Address	192.168.226.201	Test	
Subnet Mask	255.255.255.0		
Gateway	192.168.226.1		
Preferred DNS Server	210.21.196.6		
Alternate DNS Server	8.8.8.8		

IP Setup

③ Go to the router’s management interface through IE browser to forward the IP address and port of the camera in the “Virtual Server”.

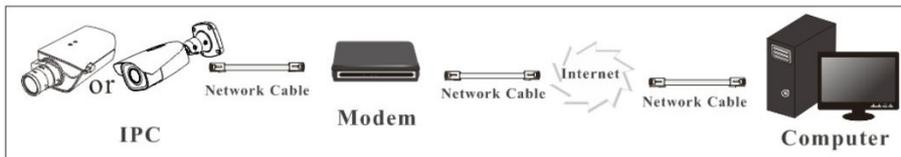
Port Range					
Application	Start	End	Protocol	IP Address	Enable
1	9007	to 9008	Both	192.168.1.201	<input checked="" type="checkbox"/>
2	80	to 81	Both	192.168.1.201	<input checked="" type="checkbox"/>
3	10000	to 10001	Both	192.168.1.166	<input type="checkbox"/>
4	21000	to 21001	Both	192.168.1.166	<input type="checkbox"/>

Router Setup

④ Open the IE 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.

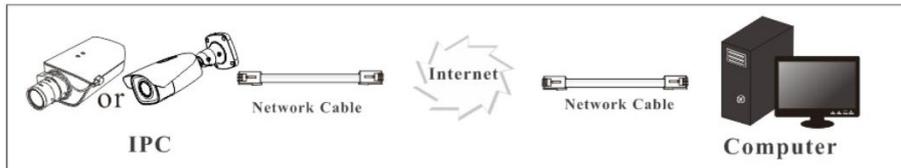
IPv4	IPv6	PPPoE Config	IP Change Notification Config
<input checked="" type="checkbox"/> Enable			
User Name	<input type="text" value="xxxxxxx"/>		
Password	<input type="password" value="•••••"/>		
<input type="button" value="Save"/>			

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

- ④ Open the IE 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 the IE browser and enter its WAN IP and http port to access.

3 License Plate Recognition

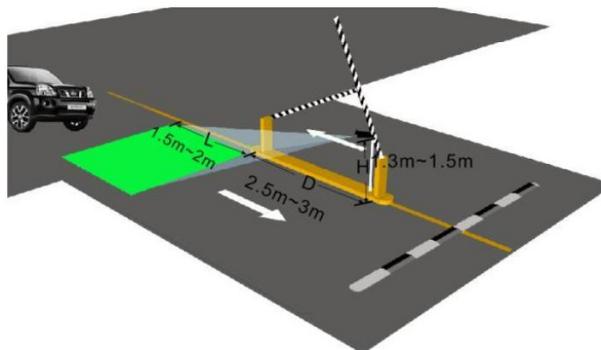
3.1 Configuration Requirements of Camera and Surrounding Area

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

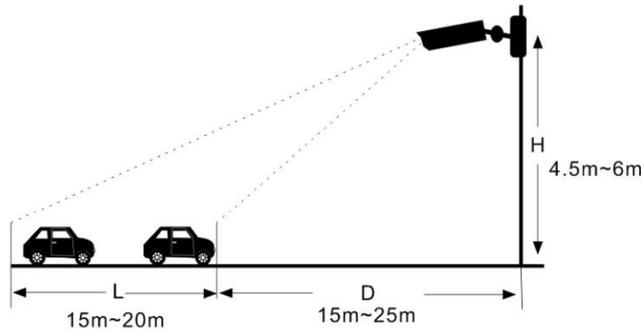
- The installation height (H) should range from 1.3 m to 1.5m.
- The distance D (between the location of the camera installation and the captured area) shall range 2.5m to 3m.
- The distance of the captured area (L) should be from 1.5m to 2m.



- 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:

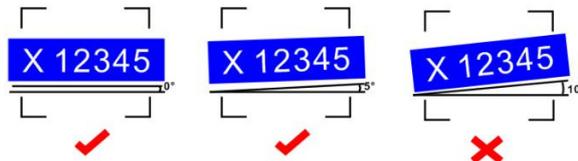
- The installation height (H) should range from 4.5 m to 6m.
- The distance D (between the location of the camera installation and the captured area) should range from 15m to 25m. This distance (D) depends on the installation height, usually 3 or 4 times the installation height (H).
- The distance of the captured area (L) should be from 15m to 20m.



- The depression angle of the camera should range from 10° to 15°.
- If the camera is installed on the side of the road, the pan angle of the camera should range from 0° to 20°.
- If the camera is installed right above the middle of the road, the pan angle of the camera should range from -10° to 10°.
- The speed of the vehicles should be less than 120km/h
- 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

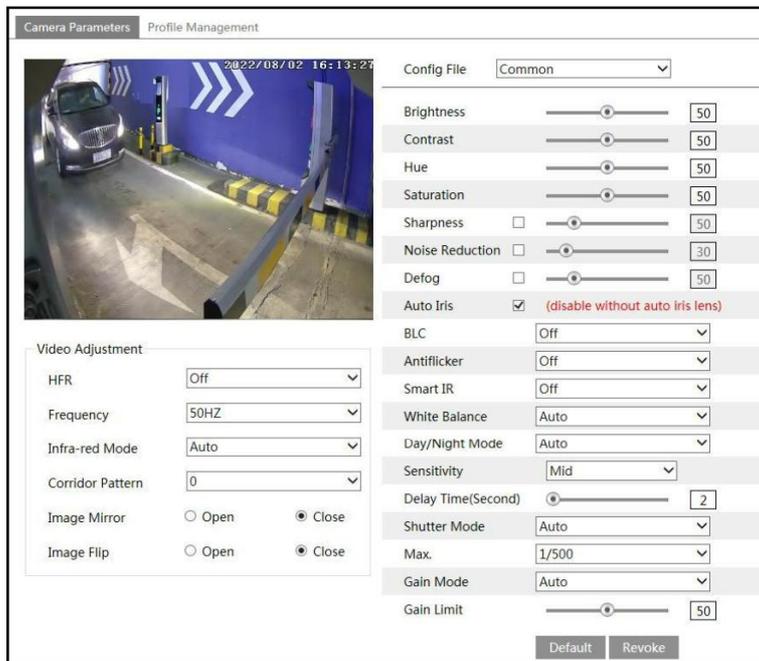
After the camera is installed, you can log in the web client and view whether the license plate tilts in the video. The tilt angle should range from -5° to 5°.



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

3.2 Recommended Image Settings

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



Brightness: Set the brightness level of the camera’s image. The brightness value can be kept around 25 in day mode, and in night mode it’s suggested to be lower value to capture the license plate clearly.

Gain Mode: “Auto” is suggested to set. The gain value will be automatically adjusted in Auto mode.

Gain Limit: It is recommended not to exceed 20.

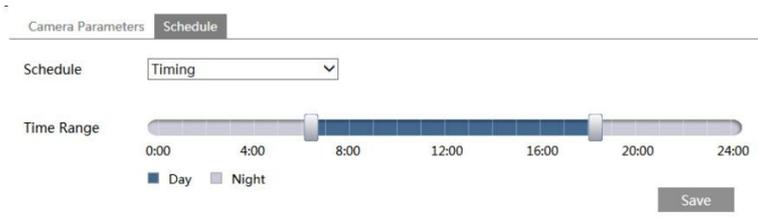
Shutter Mode: “Auto” or “Manual” can be selected. When the vehicle speed is too fast and shutter time is too long, it’ll cause a blur image. So it’s recommended that the maximum shutter time should be adjusted to be shorter in this kind of situation.

Max. Shutter Speed: 1/500~1/1000; if the vehicle speed is lower than 40km/h, it can be extended appropriately, 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 recommended to switch between day mode and night mode by schedule. Save the day mode parameters in the day config file (following left), save the night mode parameters in the night config file(following right), and then switch two sets of parameters through schedule.





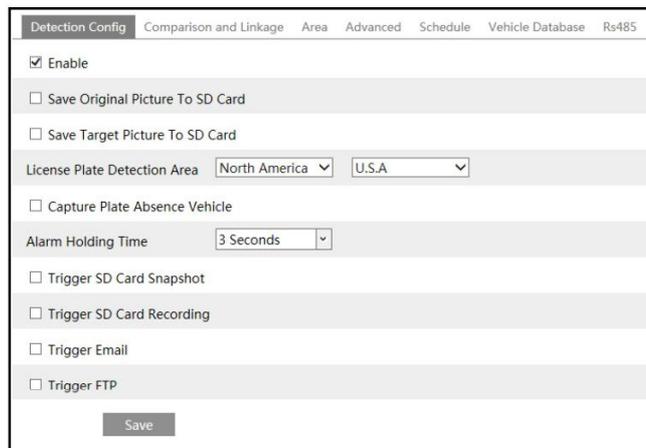
Click “Schedule” and then select “Timing”. Please Drag “” icons to set the time of day and night. Blue means day time and blank means night time. The image configuration mode will automatically switch between day and night according to the schedule.

3.3 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 as needed.

3.Set alarm holding time and alarm trigger options. The alarm trigger setup steps are the same as motion detection setup. Please refer to [motion detection](#) section for details.

4. Set the alarm detection area and the blocked area.



To set the detection area

Click “Draw Area” and drag the border lines of the rectangle to modify its size. Click “Stop Draw” to stop drawing the area. Click “Clear” to clear the area. Then set the detectable size by defining the maximum value and the minimum value (The default size range of a single number plate image occupies from 1% to 50% of the entire image).

To set the blocked area:

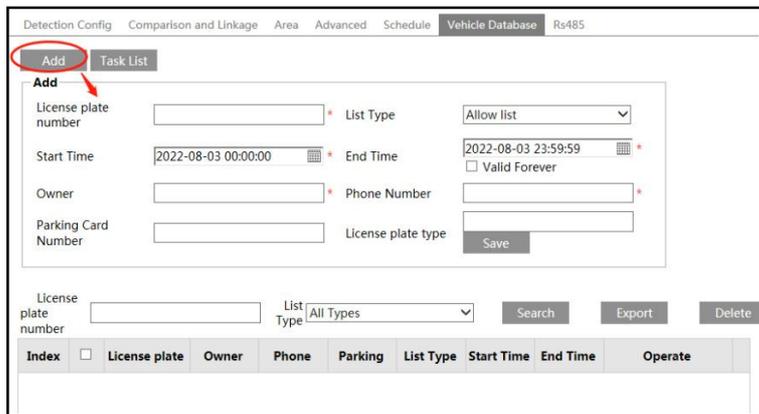
Select the number of the undetected area. Then click “Draw Area” to draw a closed area. Up to 4 areas can be set up. After you set the blocked area, this area will not be detected.



License Plate Exposure: When the brightness of the captured license plate is not enough, it can be enabled. Then check and set license plate exposure as needed.

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

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

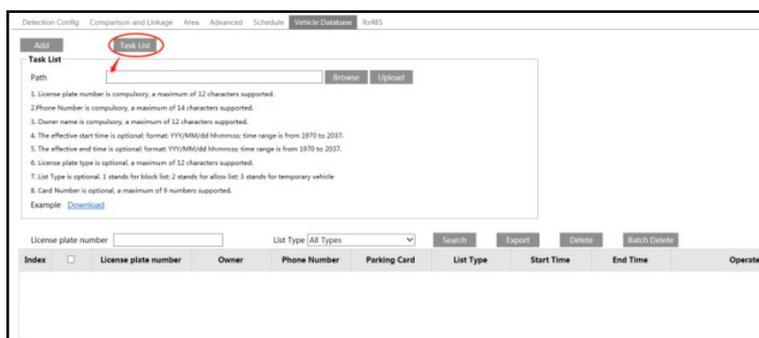


● **Add vehicles**

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 and so on. Then click “Save” to save the vehicle information.

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

Click “Task List” to add multiple vehicles at one time as shown below.



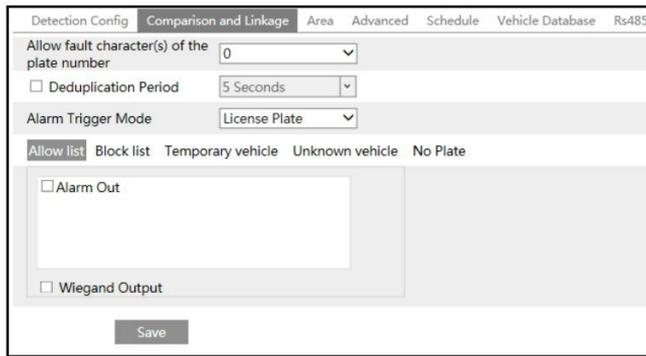
Please edit the vehicle information according to the requirements shown on the above interface. If you don’t know how to edit the file, please click “Download” to download an example file and then follow the example to edit. After that, click “Browse” to choose the vehicle information file and click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

● **Search vehicles**

After the vehicles are added, you can search them in the vehicle list. 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.

7. Set the license plate comparison and alarm linkage. Click the “Comparison and linkage”

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: 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.

Deduplication Period: In the set period, delete the repeated comparison results.

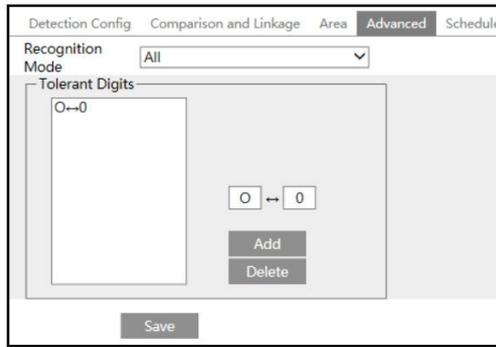
Alarm Trigger Mode: “License Plate” or “License Plate and Parking Card”.

Note: Only the model with the wiegand interface supports the “License Plate and Parking Card” mode and the wiegand interface has been connected to the card reader as wiegand input.

Alarm Output: 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: 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.

8. Advanced Settings. Click the “Advanced” tab to go to the following interface.



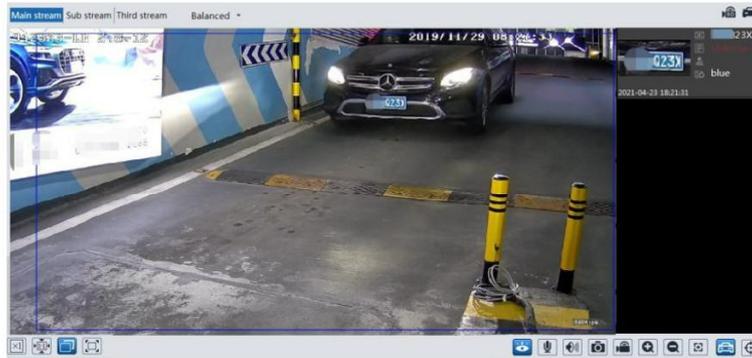
Recognition Mode: All, Recognizing when approaching, Recognizing when driving away.

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.

Multiple tolerant digital pairs can be set as needed.

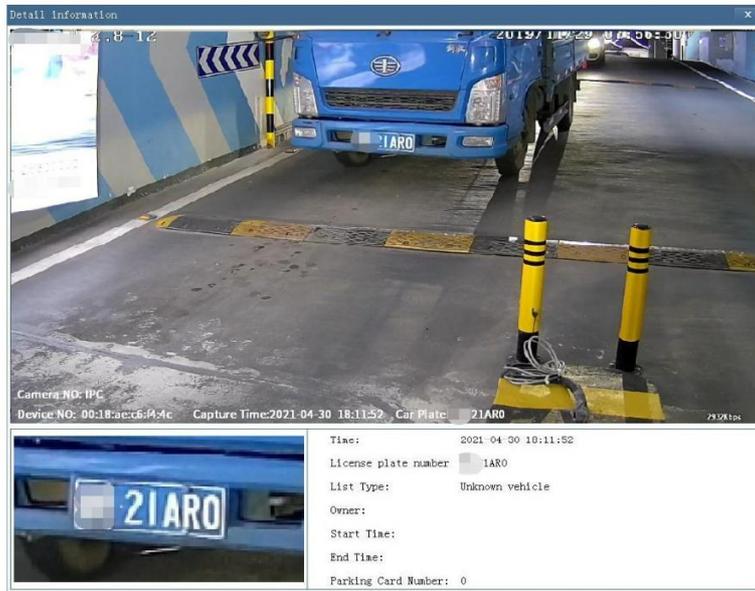
9. RS 485 settings. This function is used to connect the LED screen. Please set the relevant parameters according to the LED screen you connect.

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 matched license plate picture, and then the matched details will pop up as shown below.

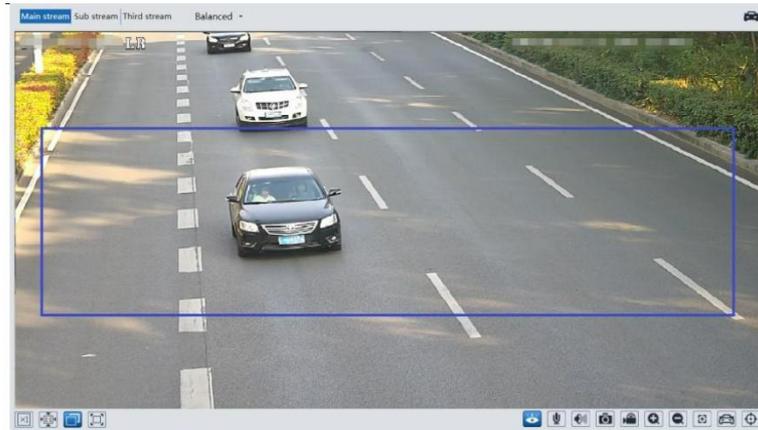
Detail information



Camera NO: IP-1
Device NO: 00:18:ae:c6:44c Capture Time:2021-04-30 18:11:52, Car Plate: 21ARO

Time:	2021-04-30 18:11:52
License plate number:	21ARO
List Type:	Unknown vehicle
Owner:	
Start Time:	
End Time:	
Parking Card Number:	0

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

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)		

5 Network Camera Configuration

In the Webcam client, choose “Config” to go to the configuration interface.

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

5.1 System Configuration

5.1.1 Basic Information

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

Device Name	IPC
Product Model	
Brand	Customer
Software Version	5.1.1.0(35127)
Software Build Date	2022-07-23
Onvif Version	21.12
OCX Version	2.2.4.7
MAC	00:18:ae:00:9d:ea
About this machine	View
Privacy Statement	View

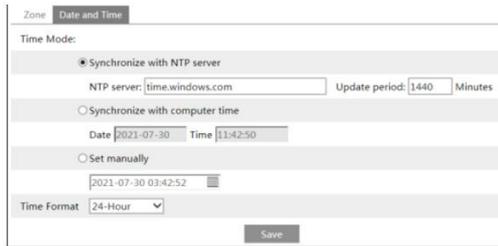
5.1.2 Date and Time

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

Zone Date and Time	
Zone	GMT (Dublin, Lisbon, London, Reykjavik)
<input checked="" type="checkbox"/> DST	
<input checked="" type="radio"/> Auto DST	
<input type="radio"/> Manual DST	
Start Time	January First Sunday 00 Hour
End Time	February First Monday 00 Hour
Time Offset	120 Minutes
<input type="button" value="Save"/>	

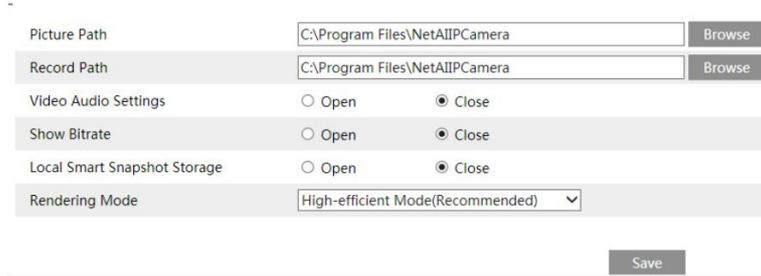
Select the time zone and DST as required.

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



5.1.3 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 the bitrate display in the recorded files.



Additionally, “Local smart snapshot storage” can be enabled or disabled here. If enabled, the captured pictures triggered by smart events (like line crossing detection, region intrusion, etc.) will be saved to the local PC.

Rendering Mode: High-efficient mode, compatible mode or low-efficient mode can be optional.

If the performance of your computer is not compatible with the web client or your computer has no graphics card, low-efficient mode is suggested.

Note: when you access your camera by the web browser without the plug-in, only Show Bitrate can be set in the above interface.

5.1.4 Storage

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

Management		Record	Snapshot
Total picture capacity	379 MB		
Picture remaining space	379 MB		
Total recording capacity	3329 MB		
Record remaining space	2048 MB		
State	Normal		
Snapshot Quota	10 %		
Video Quota	90 %		
Changes in the quota ratio need to be formatted before they become effective.			
		Eject	Format

● **SD Card Management**

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 SD card. Then the SD card can be ejected safely.

Snapshot Quota: Set the capacity proportion of captured pictures on the SD card.

Video Quota: Set the capacity proportion of record files on the SD card.

● **Schedule Recording Settings**

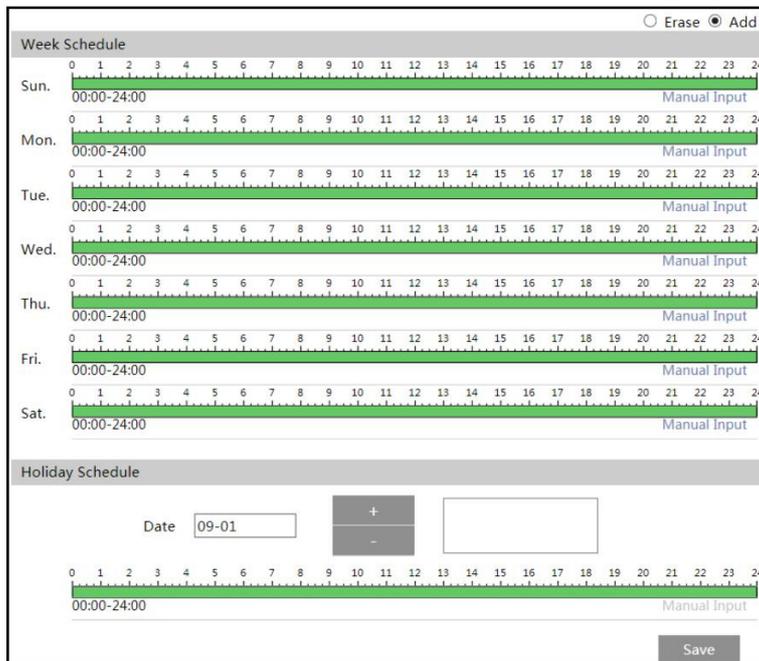
1. Go to Config→System→Storage→Record to go to the interface as shown below.

Management		Record	Snapshot
Record Parameters			
Record Stream	Main		
Pre Record Time	No Pre Record (H264,H265,MJPEG)		
Cycle Write	Yes		
Timing			
<input checked="" type="checkbox"/> Enable Schedule Record			

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

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

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



Weekly schedule

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

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

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

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

Day schedule

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

Note: Holiday schedule takes priority over weekly schedule.

● **Snapshot Settings**

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

Management	Record	Snapshot
Snapshot Parameters		
Image Format	JPEG	
Resolution	704x576	
Image Quality	Low	
Event Trigger		
Snapshot Interval	1	Second
Snapshot Quantity	5	
Timing		
<input checked="" type="checkbox"/> Enable Timing Snapshot		
Snapshot Interval	5	Second

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

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

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

- **USB disk**

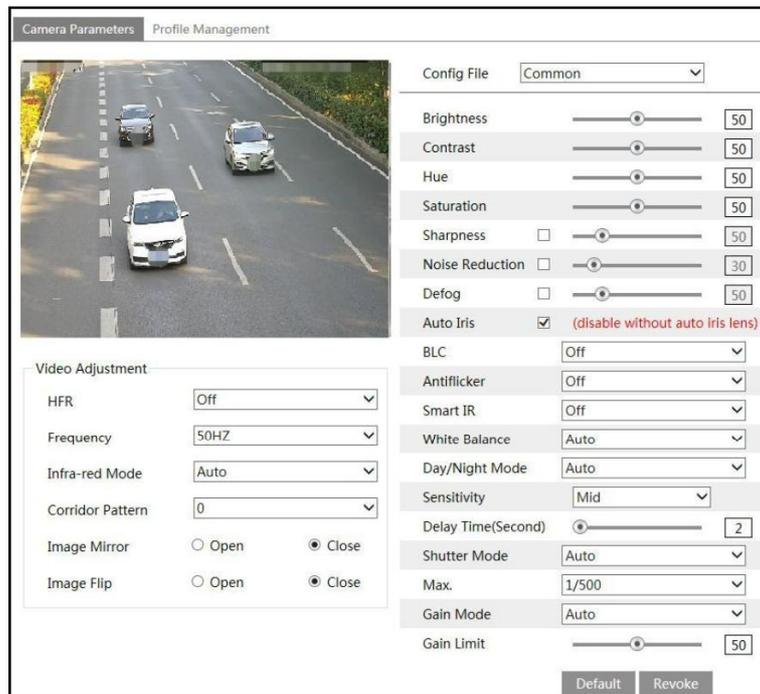
This function is only available for the model with USB interface. In this interface, you can view the state and capacity of the USB flash disk.

5.2 Image Configuration

Image Configuration includes Display, Video/Audio, OSD, Video Mask and ROI Config.

5.2.1 Display Configuration

Go to Image→Display 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.



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

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

Hue: Set the total color degree of the image.

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

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

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

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

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 so as to make the image more realistic. The higher the level is, the more overexposure compensation will be given.

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

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

Shutter Mode: Choose “Auto” or “Manual”. If manual is chosen, the digital shutter speed can be adjusted.

Gain Mode: Choose “Auto” or “Manual”. If “Auto” is selected, the gain value will be automatically adjusted (within the set gain limit value) according to the actual situation. If “Manual” is selected, the gain value shall be set manually. The higher the value is, the brighter the image is.

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 60 fps /50fps.

Frequency: 50Hz and 60Hz can be optional.

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

Corridor Pattern: Corridor viewing modes can be used for situations such as long hallways. 0, 90, 180 and 270 are available. The default value is 0.

Image Mirror: Turn the current video image horizontally.

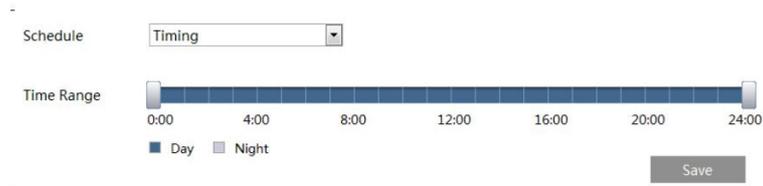
Image Flip: Turn the current video image vertically.

Schedule Settings of Image Parameters:

Click the “Profile Management” tab as shown below.



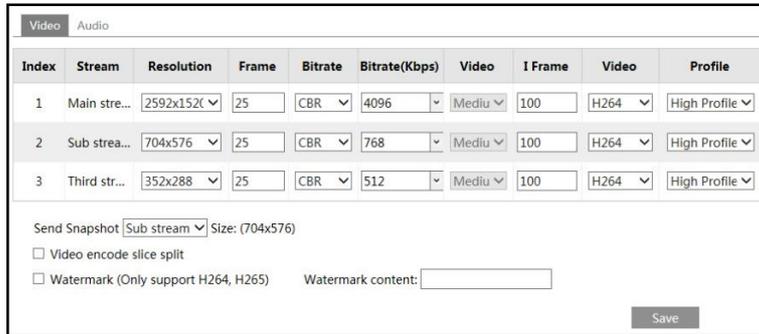
Set full time schedule for common, day, night mode and specified time schedule for day and night. Choose “Schedule” in the drop-down box of schedule as shown below.



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

5.2.2 Video / Audio Configuration

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



Index	Stream	Resolution	Frame	Bitrate	Bitrate(Kbps)	Video	I Frame	Video	Profile
1	Main stre...	2592x1520	25	CBR	4096	Mediu	100	H264	High Profile
2	Sub strea...	704x576	25	CBR	768	Mediu	100	H264	High Profile
3	Third str...	352x288	25	CBR	512	Mediu	100	H264	High Profile

Send Snapshot Sub stream Size: (704x576)

Video encode slice split

Watermark (Only support H264, H265) Watermark content:

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 the snapshot stream.

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

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

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

Audio Encoding: G711A and G711U are selectable.

Audio Type: LIN

Please set the LIN IN volume and audio out volume as needed.

5.2.3 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 “Browse” to select the overlap picture. Then click “Upload” to upload the overlap picture. The pixel of the image shall not exceed 200*200, or it cannot be uploaded.

5.2.4 Video Mask

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



To set up video mask:

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

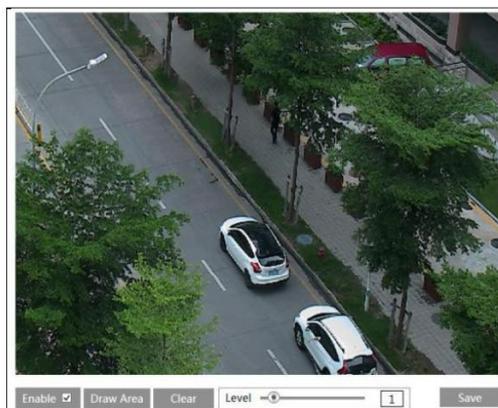


To clear the video mask:

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

5.2.5 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.

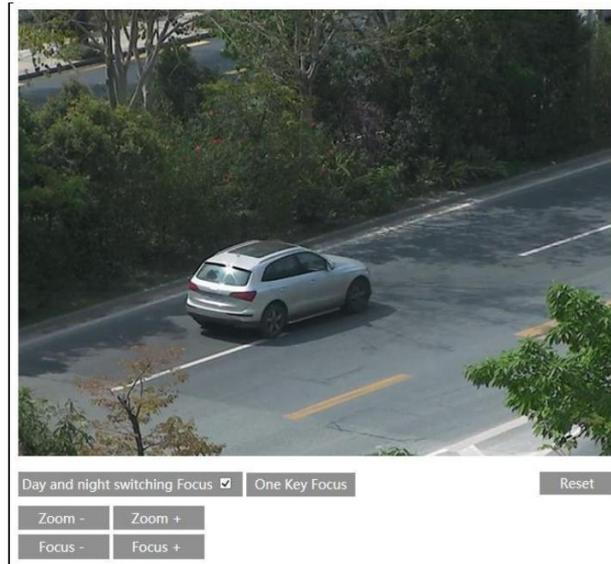


1. Check “Enable” and then click the “Draw Area” button.
2. Drag the mouse to set the ROI area.
3. Set the level.
4. Click the “Save” button to save the settings.



5.2.6 Lens Control

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



5.3 Alarm Configuration

5.3.1 Motion Detection

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

The screenshot shows the 'Detection Config' tab with the following settings:

- Enable
- Alarm Holding Time: 20 Seconds
- Trigger Alarm Out:
 - Alarm Out
 - Trigger SD Card Snapshot
 - Trigger SD Card Recording
 - Trigger Email
 - Trigger FTP
- Save button

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 interval time between the adjacent motion detections. 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.

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.)

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

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

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

Trigger FTP: If “Trigger FTP” and “Attach Picture” are checked, the captured pictures will be sent into FTP server address. Please refer to FTP configuration section for more details.

2. Set motion detection area and sensitivity. Click the “Area and Sensitivity” tab to go to the interface as shown below.



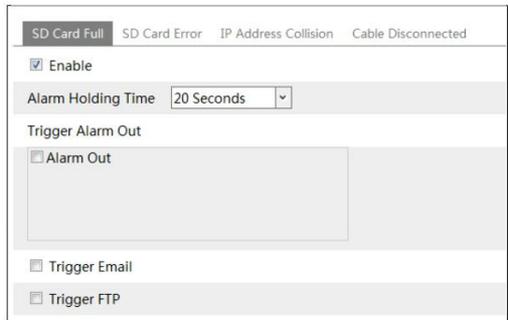
Move the “Sensitivity” scroll bar to set the sensitivity. Higher sensitivity value means that motion will be triggered more easily.
 Select “Add” and click “Draw”. Drag the mouse to draw the motion detection area; Select “Erase” and drag the mouse to clear motion detection area.
 After that, click the “Save” to save the settings.

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

5.3.2 Exception Alarm

● SD Card Full

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

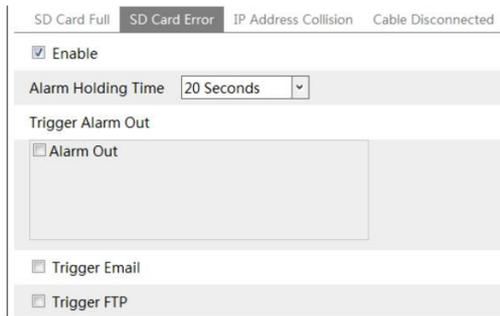


2. Click “Enable” and set the alarm holding time.
 3. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection section for details.

● SD Card Error

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

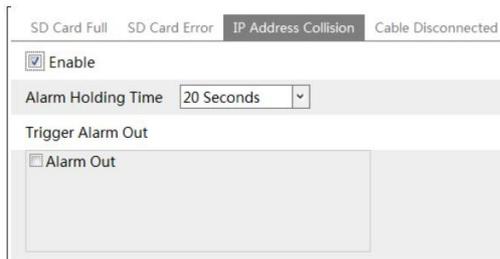
1. Go to Config→Alarm→ Exception Alarm →SD Card Error as shown below.



2. Click “Enable” and set the alarm holding time.
3. Set alarm trigger options. Trigger alarm out, Email and FTP. The setup steps are the same as motion detection. Please refer to [motion detection](#) section for details.

● **IP Address Conflict**

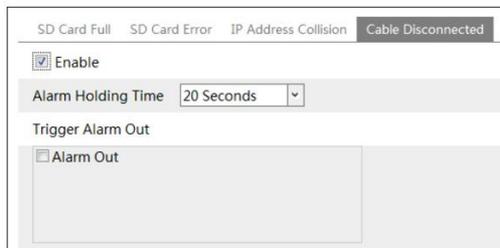
1. Go to Config→Alarm→ Exception Alarm→IP Address Collision as shown below.



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

● **Cable Disconnection**

1. 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.

5.3.3 Alarm In

To set sensor alarm (alarm in):

Go to Config→Alarm→Alarm In interface as shown below.

Detection Config Schedule

Enable

Alarm Type NO

Alarm Holding Time 20 Seconds

Sensor Name

Trigger Alarm Out

Alarm Out

Trigger SD Card Snapshot

Trigger SD Card Recording

Trigger Email

Trigger FTP

Day/night switch linkage

Save

1. Click “Enable” and set the alarm type, alarm holding time and sensor name.
 2. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to [motion detection](#) section for details.
 3. Click “Save” button to save the settings.
 4. Set the schedule of the sensor alarm. The setup steps of the schedule are the same as the schedule recording setup. (See [Schedule Recording](#)).
- Day/night switch linkage: if enabled, daytime mode or night mode can be triggered as needed

5.3.4 Alarm Out

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

Alarm Out Mode	Alarm Linkage
Alarm Out Name	alarmOut1
Alarm Holding Time	20 Seconds
Alarm Type	NC
Save	

Alarm Out Mode: Alarm linkage, manual operation, day/night switch linkage and timing are optional.

Alarm Linkage: Having selected this mode, select alarm out name, alarm holding time at the “Alarm Holding Time” pull down list box and alarm type.

Manual Operation: Having selected this mode, select the alarm type and click “Open” to trigger the alarm out immediately; click “Close” to stop alarm.

Alarm Out Mode	Manual Operation
Alarm Type	NC
Manual Operation	Open Close
Save	

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

Alarm Out Mode	Day/night switch linkage
Alarm Type	NC
Day	Close
Night	Close

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

Alarm Out Mode	Timing
Alarm Type	NC
Time Range	<div style="text-align: right;"> <input type="radio"/> Erase <input checked="" type="radio"/> Add </div>
Save	

5.3.5 Alarm Server

Go to Alarm→Alarm Server interface as shown below.

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

Server Address	<input type="text" value="0.0.0.0"/>
Port	<input type="text" value="8010"/>
Heartbeat	<input type="text" value="Disable"/> ▼
Heartbeat interval	<input type="text" value="30"/> Second

5.4 Event Configuration

For more accuracy, here are some recommendations for installation.

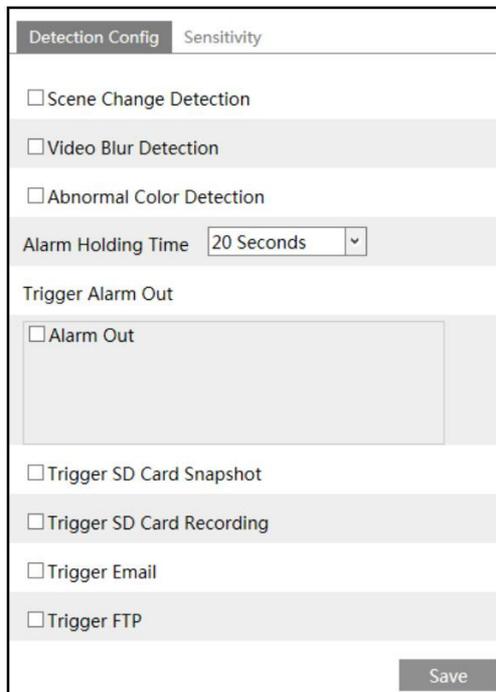
- Cameras should be installed on stable surfaces, as vibrations can affect the accuracy of detection.
- Avoid pointing the camera at the reflective surfaces (like shiny floors, mirrors, glass, lake surfaces and so on).
- Do not aim the camera at the sun, road lamp or headlights of the car.
- Avoid places that have too much shadowing.
- At any time of day or night, please make sure the image of the camera is clear and with adequate and even light, avoiding overexposure or too much darkness on both sides.

5.4.1 Video Exception Settings

This function can detect changes in the surveillance environment affected by the external factors.

To set exception detection:

Go to Config→Event→Video Exception interface as shown below.



1. Enable the applicable detection that's desired.

Scene Change Detection: Alarms will be triggered if the scene of the monitor video has changed.

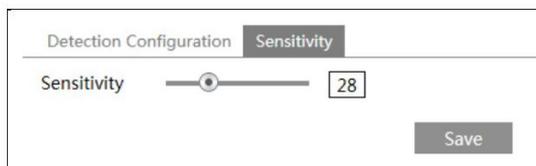
Video Blur Detection: Alarms will be triggered if the video becomes blurry.

Abnormal Color Detection: Alarms will be triggered if the image is abnormal caused by color deviation.

2. Set the alarm holding time and alarm trigger options. The setup steps are the same as motion detection. Please refer to [motion detection](#) section for details.

3. Click "Save" button to save the settings.

4. Set the sensitivity of the exception detection. Click "Sensitivity" tab to go to the interface as shown below.



Drag the slider to set the sensitivity value or directly enter the sensitivity value in the textbox. Click "Save" button to save the settings.

The sensitivity value of Scene Change Detection: The higher the value is, the more sensitive

the system responds to the amplitude of the scene change.

The sensitivity value of Video Blur Detection: The higher the value is, the more sensitive the system responds to the blurriness of the image.

The sensitivity value of Abnormal Color Detection: The higher the value is, the more sensitive the system responds to the color shift of the image.

※ **The requirements of camera and surrounding area**

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

5.5 Network Configuration

5.5.1 TCP/IP

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

The screenshot shows the 'IPv4' configuration tab. It has two radio buttons: 'Obtain an IP address automatically' (unselected) and 'Use the following IP address' (selected). Below these are input fields for 'IP Address' (192.168.226.201), 'Subnet Mask' (255.255.255.0), 'Gateway' (192.168.226.1), 'Preferred DNS Server' (210.21.196.6), and 'Alternate DNS Server' (8.8.8.8). A 'Test' button is next to the IP Address field.

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. Enable PPPoE and then enter the user name and password from your ISP.

The screenshot shows the 'PPPoE Config' tab. It has a checked checkbox for 'Enable'. Below are input fields for 'User Name' (xxxxxxx) and 'Password' (masked with dots). A 'Save' button is at the bottom.

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.

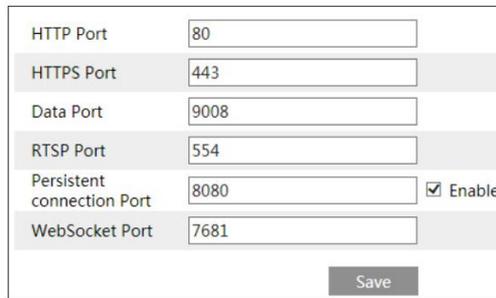


Trigger Email: when the IP address of the device is changed, the new IP address will be sent to the email address that has been set up.

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.

5.5.2 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.

5.5.3 Server Configuration

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

<input checked="" type="checkbox"/> Enable
Server Port <input type="text" value="2009"/>
Server Address <input type="text"/>
Device ID <input type="text" value="1"/>
<input type="button" value="Save"/>

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

5.5.4 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 ONVIF user can be activated simultaneously. 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 add new users in the Onvif interface.

Index	User Name	User Type
1	admin	Administrator

Add User [X]

User Name

Password

Level

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

Confirm Password

User Type

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

5.5.5 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.dvrddns.com for example.

Enter www.dvrddns.com in the IE 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.



Search by Domain:

Click a name to edit your domain settings.

NAME	STATUS	DOMAIN
654321ABC	✔	654321abc.dvndydns.com

Last Update: *Not yet updated!* IP Address: 210.21.229.138

[Create additional domain names](#)

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

5.5.6 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. 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.

SNMP v1/v2	
<input type="checkbox"/> Enable SNMPv1	
<input type="checkbox"/> Enable SNMPv2	
Read SNMP Community	<input type="text"/>
Write SNMP Community	<input type="text"/>
Trap Address	<input type="text"/>
Trap Port	<input type="text" value="0"/>
Trap community	<input type="text"/>
SNMP v3	
<input type="checkbox"/> Enable SNMPv3	
Read User Name	<input type="text"/>
Security Level	<input type="text" value="auth, priv"/>
Authentication Algorithm	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Authentication Password	<input type="text"/>
Private-key Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES
Private-key Algorithm	<input type="text"/>
Write User Name	<input type="text"/>
Security Level	<input type="text" value="auth, priv"/>
Authentication Algorithm	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Authentication Password	<input type="text"/>
Private-key Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES
Private-key Algorithm	<input type="text"/>
Other Settings	
SNMP Port	<input type="text" value="0"/>

5.5.7 802.1x

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

<input checked="" type="checkbox"/> Enable	
Protocol Type	<input type="text" value="EAP_MD5"/>
EAPOL Version	<input type="text" value="1"/>
User Name	<input type="text" value="test"/>
Password	<input type="text" value="•••••"/>
Confirm Password	<input type="text" value="•••••"/>

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

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

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

5.5.8 RTSP

Go to Config→Network→RTSP.

Select “Enable” to enable the RTSP function.

Port: Access port of the streaming media. The default number is 554.

RTSP Address: The RTSP address (unicast) format that can be used to play the stream in a media player.

Multicast Address

Main stream: The address format is

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

Sub stream: The address format is

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

Third stream: The address format is

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

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

5.5.9 RTMP

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

Go to Config→Network→RTMP.

Check “Enable”, select stream type, set the reconnection time after timeout and server address as needed.

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

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

5.5.10 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.

5.5.11 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.

Sender	
Sender Address	<input type="text" value="xxx@126.com"/>
User Name	<input type="text"/> <input checked="" type="checkbox"/> Anonymous Login
Password	<input type="password"/>
Server Address	<input type="text" value="smtp.126.com"/>
Secure Connection	<input type="text" value="Unnecessary"/> ▼
SMTP Port	<input type="text" value="25"/> <input type="button" value="Default"/>
<input type="checkbox"/> Send Interval(S)	<input type="text" value="60"/> (10-3600)
	<input type="button" value="Clear"/> <input type="button" value="Test"/>
Recipient	
	<input type="text" value="xxx@126.com"/>
	<input type="text"/>
Recipient Address	<input type="text"/>
	<input type="button" value="Add"/> <input type="button" value="Delete"/>
	<input type="button" value="Save"/>

Sender Address: sender's e-mail address.

User name and password: sender's user name and password (you don't have to enter the username and password if "Anonymous Login" is enabled).

Server Address: The SMTP IP address or host name.

Select the secure connection type at the "Secure Connection" pull-down list according to what's required.

SMTP Port: The SMTP port.

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

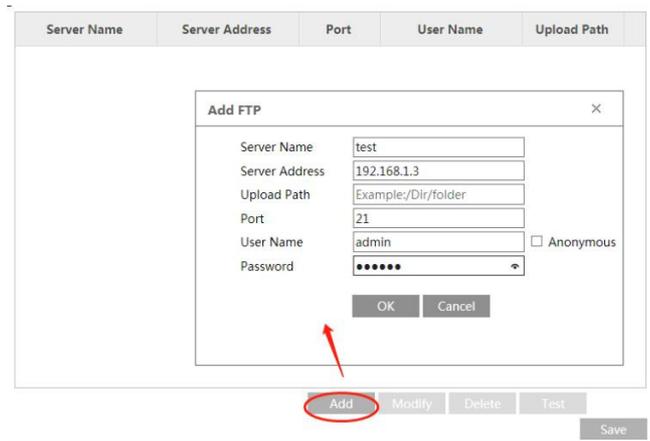
Click the "Test" button to test the connection of the account.

Recipient Address: receiver's e-mail address.

5.5.12 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.

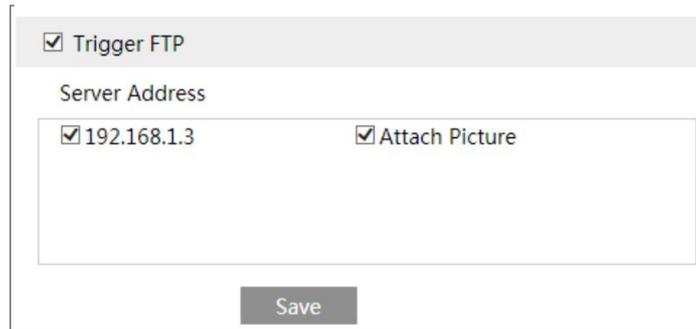
Server Address: The IP address or domain name of the FTP.

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\VEHICLE\2021-01-09\14\

Event name table:

File Name	Event Type
IP	IP address change
MOTION	Motion Detection
SENSOR	Sensor Alarm
AVD	Video Exception
VEHICLE	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.

5.5.13 HTTP POST

Go to Config→Network →HTTP POST interface.

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

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

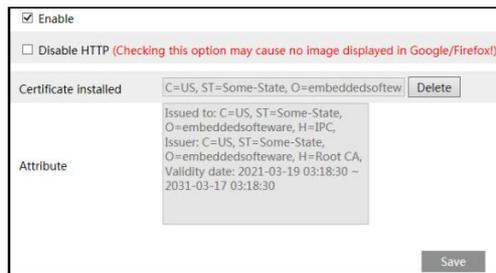
Server port: the server port of the third-party platform.

After the above parameters are set, click “Save” to save the settings. Then the camera will automatically connect the third-party platform. The online state can be viewed in the above interface. After the camera is successfully connected, it will send the alarm information (HTTP format) to the third-party platform once the smart alarm is triggered. The alarm information includes target tracing coordinates, target features, the captured original/target image (like the captured license plate picture) and so on.

5.5.14 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.

Enable
 Installation type: Have signed certificate, install directly
 Create a private certificate
 Create a certificate request
 Create a private certificate

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

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

Enable
 Installation type: Have signed certificate, install directly
 Create a private certificate
 Create a certificate request
 Create a certificate request

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

5.5.15 QoS

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

Go to Config→Network→QoS.

Video/Audio DSCP	<input type="text" value="13"/>
Alarm DSCP	<input type="text" value="35"/>
Manager DSCP	<input type="text" value="53"/>

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

Alarm DSCP: The range is from 0 to 63.

Manager DSCP: The range is from 0 to 63.

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

5.6 Security Configuration

5.6.1 User Configuration

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

Add Modify Delete			
Index	User Name	User Type	Binding MAC
1	admin	Administrator	

Add user:

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

Add User
×

User Name

Password

Level

Confirm Password

User Type

Select All

- Remote storage settings
- Remote image settings
- Remote PTZ control
- Remote alarm server configuration
- Remote intelligent event configuration
- Remote network advanced configuration
- Remote security management

OK
Cancel

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).

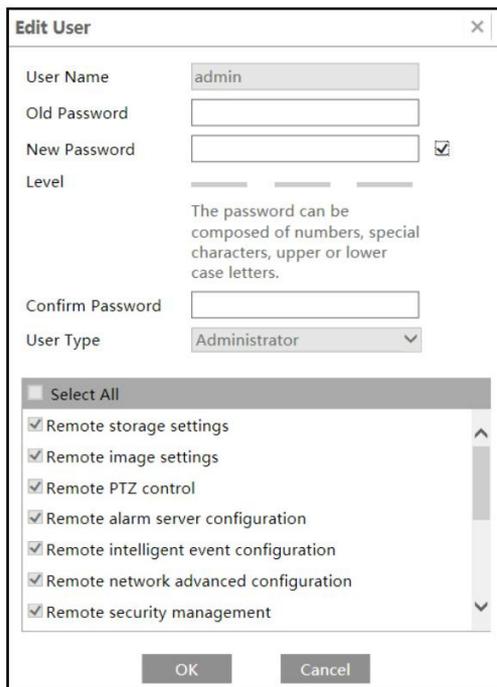
4. Choose the user type and select the desired user permissions.

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.

5.6.2 Online User

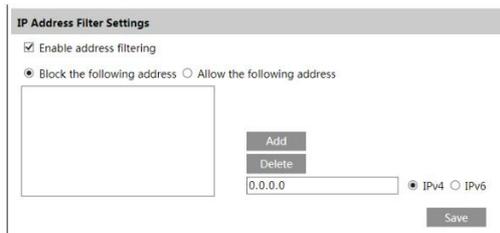
Go to Config→Security→Online User to view the user who is viewing the live video.

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

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

5.6.3 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.

5.6.4 Security Management

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



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

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

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

- **Password Security**



Please set the password level and expiration time as needed.

Password Level: Weak, Medium or Strong.

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

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

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

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

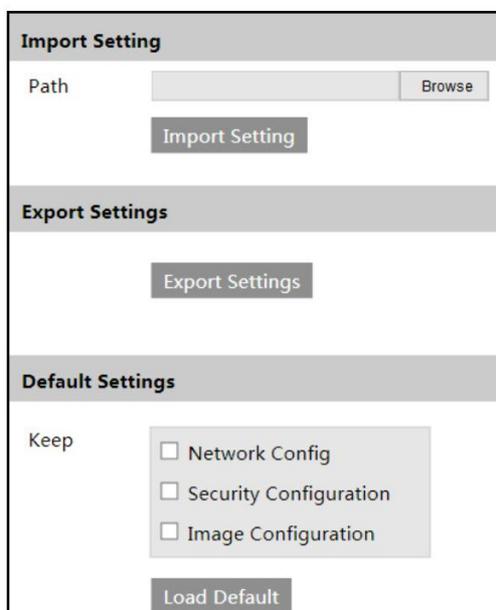
HTTP Authentication: Basic or Token is selectable.



5.7 Maintenance Configuration

5.7.1 Backup and Restore

Go to Config→Maintenance→Backup & Restore.



- Import & Export Settings

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

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

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

- **Running Log Settings**

After enabling it, select the log level and file size and click “Save”. Then the system will collect logs accordingly. When the device error occurs, you can export these logs and send them to the technician to find out the problem.

Log Level: it is recommended to select “INFO” or “Debug”.

- **Default Settings**

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

5.7.2 Reboot

Go to Config→Maintenance→Reboot.

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

Timed Reboot Setting:

If necessary, the camera can be set up to reboot on a time interval. Enable “Time Settings”, set the date and time, click the “Save” button and then enter the password to save the settings.

5.7.3 Upgrade

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

The screenshot shows a web interface titled "Local upgrade". It contains a text input field labeled "Path" with a "Browse" button to its right. Below the input field and buttons is an "Upgrade" button.

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

Caution! Do not close the browser or disconnect the camera from the network during the upgrade.

5.7.4 Operation Log

To query and export log:

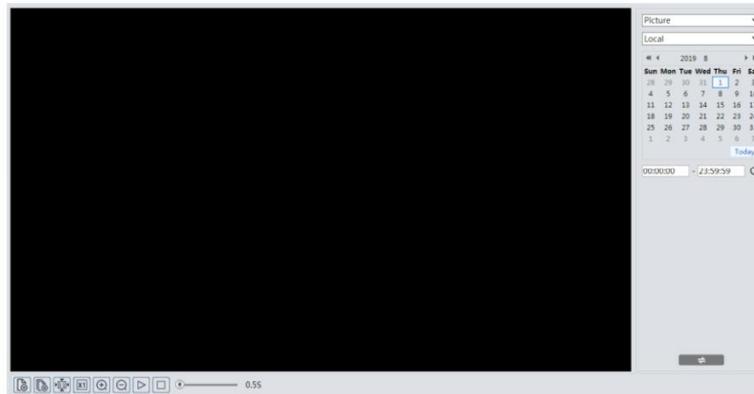
1. Go to Config→Maintenance→Operation Log.

Main Type	Operation	Sub Type	Log in			
Start Time	2021-09-06 00:00:00	End Time	2021-09-06 23:59:59	Search	Export	
Index	Time	Main Type	Sub Type	User Name	Login IP	Hostname
1	2021-09-06 03:1...	Operation	Log in	admin	10.20.52.7	
2	2021-09-06 03:1...	Operation	Log in	admin	10.20.52.7	

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.

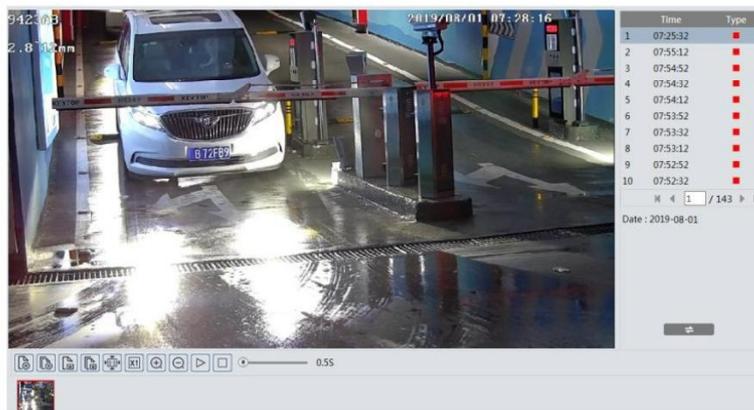
6.1 Image Search

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



● Local Image Search

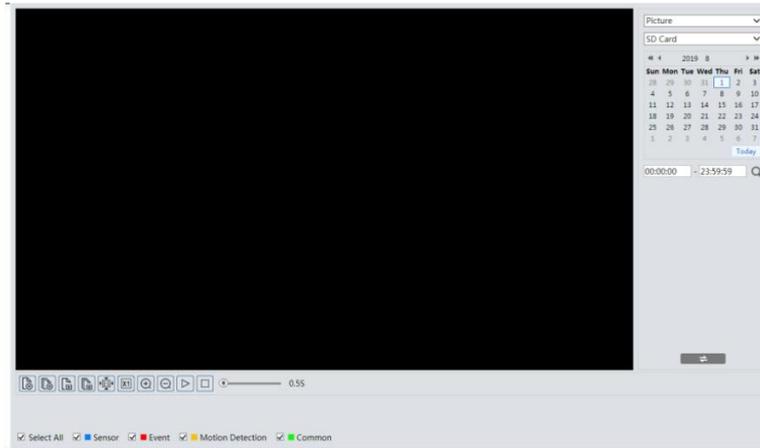
1. Choose “Picture”—“Local”.
2. Set time: Select date and choose the start and end time.
3. Click  to search the images.
4. Double click a file name in the list to view the captured photos as shown below.



Click  to return to the previous interface.

● SD Card Image Search

1. Choose “Picture”—“SD Card”.



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

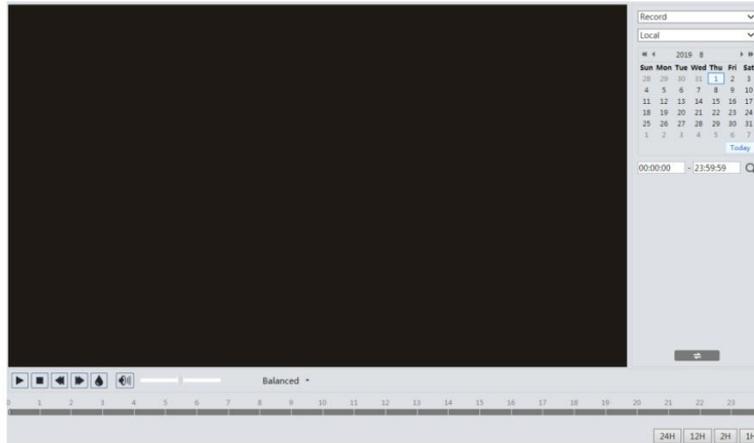
The descriptions of the buttons are shown as follows.

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

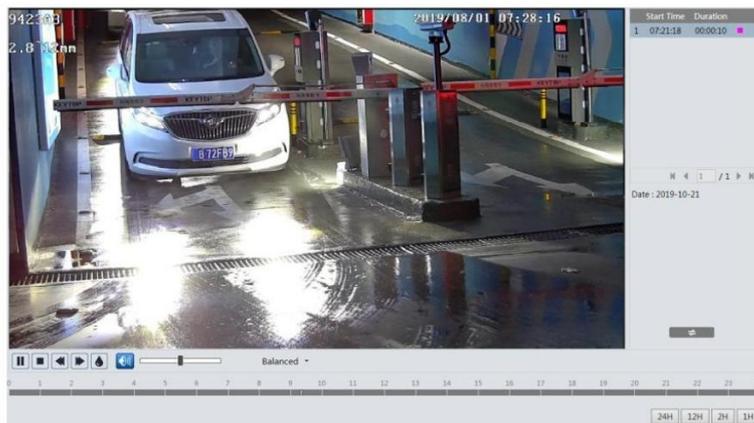
6.2 Video Search

6.2.1 Local Video Search

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



1. Choose “Record”—“Local”.
2. Set search time: Select the date and choose the start and end time.
3. Click  to search the images.
4. Double click on a file name in the list to start playback.

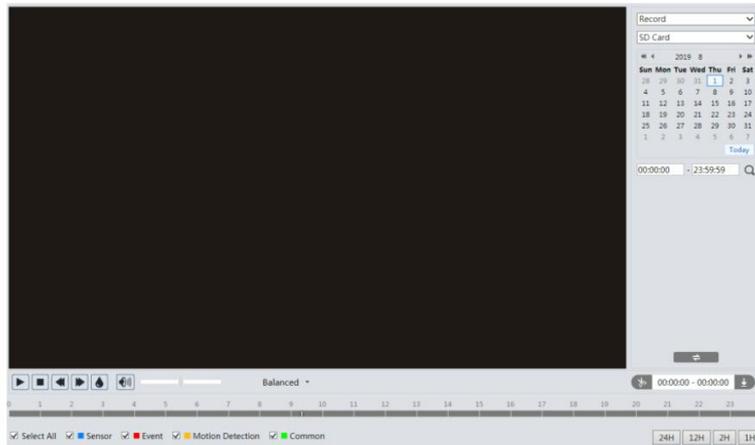


Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button
	Stop button		Speed down
	Speed up		Watermark display
	Enable / disable audio; drag the slider to adjust the volume after enabling audio.		

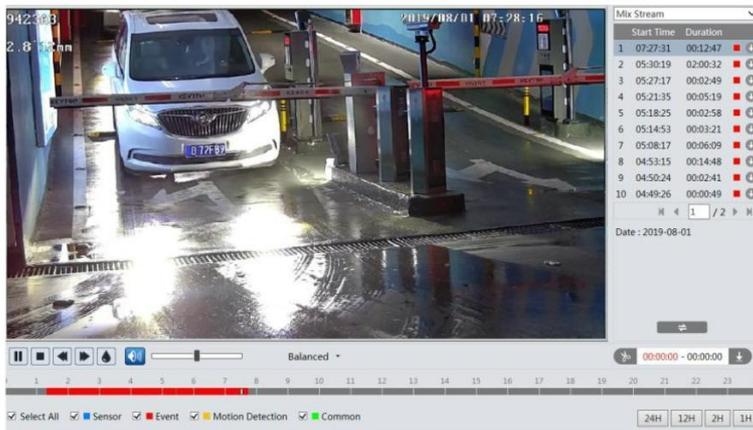
6.2.2 SD Card Video Search

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

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



4. Select the alarm events at the bottom of the interface.
5. Select mix stream (video and audio stream) or video stream as needed.
6. 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.

Index	Process	Record	Start Time	End Time	Path	Operate
1	100%	Cut	2019-08-01 01:1...	2019-08-01 01:1...	Favorites	Open

Set up D:\Favorites Clear List Close

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

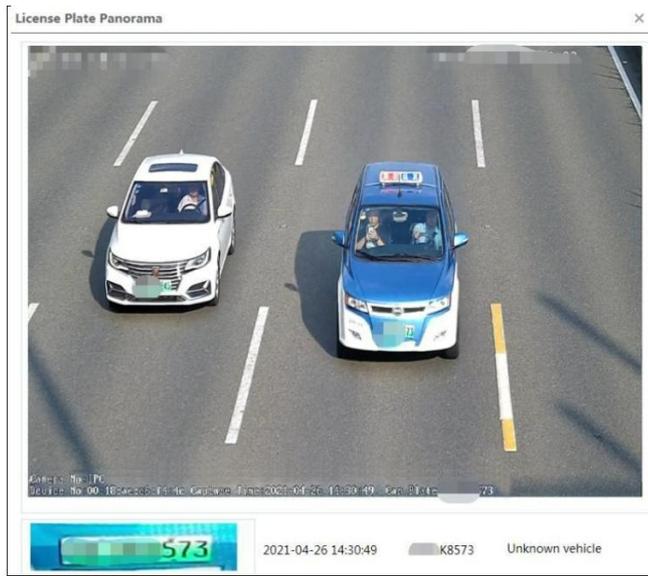
7 License Plate Recognition Result Search

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 IE 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.

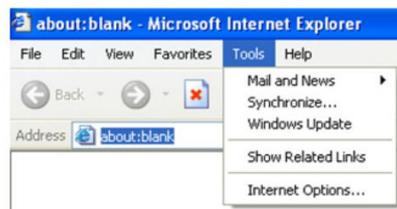
IP tool cannot search devices.

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

IE cannot download ActiveX control.

A. IE browser may be set up to block ActiveX. Follow the steps below.

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



② Select Security-----Custom Level....

③ Enable all the options under “ActiveX controls and plug-ins”.

④ Click OK to finish setup.

B. Other plug-ins or anti-virus blocks ActiveX. Please uninstall or close them.



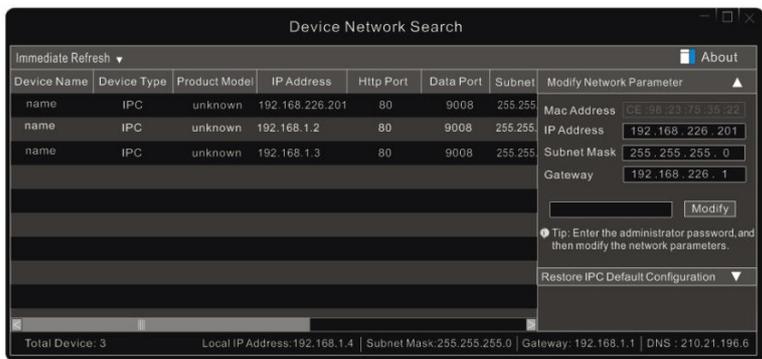
No sound can be heard.

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.

Modify Network Parameter ▲

Mac Address CE:98:23:75:35:22

IP Address 192.168.1.201

Subnet Mask 255.255.255.0

Gateway 192.168.1.1

••••• Modify

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.