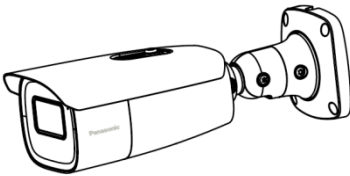

Panasonic[®]

Operating Instructions

Network Camera

Model No. PM-PB6ULVR-W/ PM-PD6ULVR-W/ PM-PX6NKBN-W



PM-PB6ULVR-W



PM-PD6ULVR-W

(The above pictures are for illustration purposes)

Before attempting to connect or operate this product, please read these instructions carefully and save this manual for future use

Safety Instruction

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 purposes, 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 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 DC12V/1.5 A or POE 48V/ 350mA or AC24V/1.0A (AC input for the model: PM-PX6NKBN-W), 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.

Environment

- Heavy stress, violent vibration or exposure to water is not allowed during transportation, storage and installation.
- Avoid aiming at 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 direct airflow from an air conditioner.
- Do not place the device in a damp, dusty extremely hot or cold environment, or the locations with strong electromagnetic radiation or unstable lighting.
- Make sure that no reflective surface (like shiny floors, mirrors, glass, lake surfaces and so on) is too close to the camera lens.

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, using cloth for 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 fingerprint, use oil-free 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 should 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 the 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 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 whitelist 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 the 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 care 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 the 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. The operation of this product is subject the following two conditions:
- This device may not cause harmful interface.
- This device must accept any interference received, including interference that may cause undesired operation.

RoHS

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



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

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

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

Table of Contents

1	Network Connection	1
1.1	LAN.....	1
1.2	WAN.....	4
2	Live View.....	7
3	Network Camera Configuration.....	10
3.1	System Configuration.....	10
3.1.1	Basic Information.....	10
3.1.2	Date and Time.....	10
3.1.3	Local Config	11
3.1.4	Storage	11
3.1.5	Serial Port Settings.....	15
3.2	Image Configuration	15
3.2.1	Display Configuration.....	15
3.2.2	Video / Audio Configuration	18
3.2.3	OSD Configuration	20
3.2.4	Video Mask.....	21
3.2.5	ROI Configuration	22
3.2.6	Lens Control.....	22
3.2.7	Smart Supplement Light Configuration.....	23
3.3	Alarm Configuration	24
3.3.1	Motion Detection	24
3.3.2	Exception Alarm	26
3.3.3	Alarm In	28
3.3.4	Alarm Out	30
3.3.5	Alarm Server	31
3.3.6	Audio Alarm	32
3.3.7	Light Alarm.....	33
3.3.8	Video Exception.....	34
3.3.9	Audio Exception	35
3.3.10	Disarming.....	36
3.4	Event Configuration	37
3.4.1	Object Abandoned/Missing.....	37
3.4.2	Line Crossing.....	39
3.4.3	Region Intrusion.....	44
3.4.4	Region Entrance.....	46
3.4.5	Region Exiting	46
3.4.6	Target Counting by Line	46
3.4.7	Target Counting by Area	50
3.4.8	Heat Map.....	52
3.4.9	Loitering Detection	53
3.4.10	Illegal Parking Detection	54

3.4.11	Video Metadata	56
3.4.12	People Gathering Detection	59
3.4.13	Face Detection	61
3.5	Network Configuration	63
3.5.1	TCP/IP.....	63
3.5.2	Port.....	65
3.5.3	Server Configuration.....	65
3.5.4	Onvif	66
3.5.5	DDNS.....	66
3.5.6	SNMP.....	67
3.5.7	802.1x.....	69
3.5.8	RTSP	69
3.5.9	RTMP	70
3.5.10	UPNP	71
3.5.11	Email	71
3.5.12	FTP.....	72
3.5.13	HTTP POST	73
3.5.14	HTTPS	75
3.5.15	Cloud Service.....	76
3.5.16	QoS	77
3.6	Security Configuration	77
3.6.1	User Configuration.....	77
3.6.2	Online User	79
3.6.3	Block and Allow Lists.....	80
3.6.4	Security Management	80
3.7	Maintenance Configuration.....	81
3.7.1	Backup and Restore	81
3.7.2	Reboot	82
3.7.3	Upgrade.....	83
3.7.4	Operation Log	84
3.7.5	Serial Output	84
3.7.6	Maintenance Information.....	84
4	Search.....	85
4.1	Image Search	85
4.2	Video Search	86
Appendix		89
Appendix 1 Troubleshooting		89

1 Network Connection

System Requirement

For proper operating the product, the following requirements are suggested for your computer.

Resolution	5MP or lower	6MP or higher
Operating System	Windows 7 or higher	Windows 10 professional version or higher
CPU	2.0GHz or higher	2.5GHz or higher
RAM	1G or higher	8G or above
Display	1920*1080 resolution or higher	

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

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

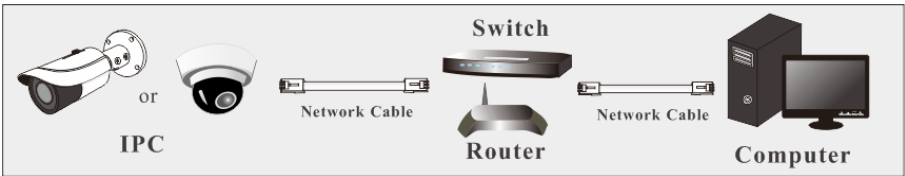
The menu display and operation of the camera may be slightly different by using the browser with plug-in or without plug-in. Installing the plug-in will display more functions of the camera.

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

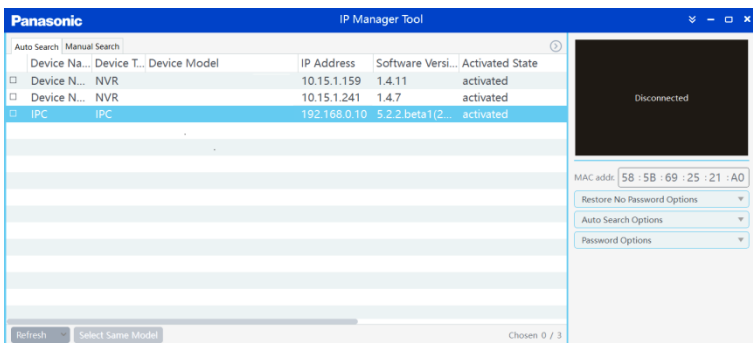
1.1 LAN

● Access through IP-Tool

Network connection:



- ① Make sure the PC and IP camera are connected to the LAN and the IP-Tool is installed in the PC.
- ② Double click the IP-Tool icon on the desktop to run this software as shown below:



The default IP address of the camera is **192.168.0.10**.

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

- a. Select the location (eg. Britain). Then click [Next].
- b. Set the zone, video format (frequency), date and time format.

Config

Frequency

60HZ

Zone

GMT-05 (New York, Torc

Date Format

MM-DD-YYYY

Time Format

12-Hour

Back

Next

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

d. Activate the device.

Device Activation

User Name

admin

☒ Activate Onvif User

New Password

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

Confirm Password

Back

Save

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

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

By default, the ONVIF password will match the admin password that you set. Should you wish to change the ONVIF password to a different password than your admin password, go to the ONVIF section to change the password (**Config→Network→ Onvif**)

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

e. Click “Save” to save the settings.

Read the privacy statement, check and click “Already Read”. Then the login interface will appear as shown below.

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

Panasonic

User Name

Password

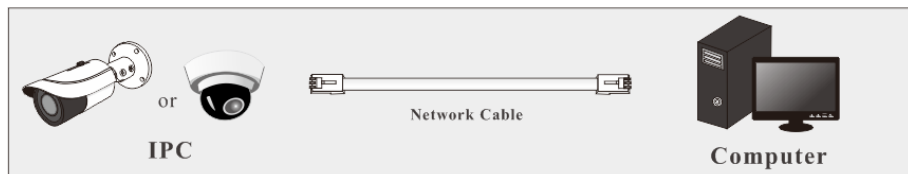
Login

Please enter the username (admin) and password. Then select the language as needed.

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.

In addition, you can also directly connect the camera to the computer through a network cable.



- ① Use a network cable to connect the IPC and the computer.
- ② Run the IP Tool to search the IPC. Double click the IP address and then the system will open a web browser to connect the IPC.
- ③ Follow directions to download and install the Active X control.
- ④ Enter the default username and password in the login window and then enter to view.

1.2 WAN

➤ Access via Cloud Service

Connect and activate the device according to the above-mentioned steps. Enable cloud service (click **Config**→**Network**→**Cloud Service**) and then enter the visit address in the address bar of a web browser to access remotely.

After you bind the camera to your APP account and enable the cloud service, a verification code will be required when logging onto the web client by using the above visit address (different areas and regions maybe have different visit addresses). Please enter the correct verification code that getting from the APP.

➤ 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** 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** to modify the IP address.

IPv4	IPv6	PPPoE Config	IP Change Notification Config
☐ Obtain an IP address automatically			
☒ 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 your web browser to forward the IP address and port of the camera in the "Virtual Server".

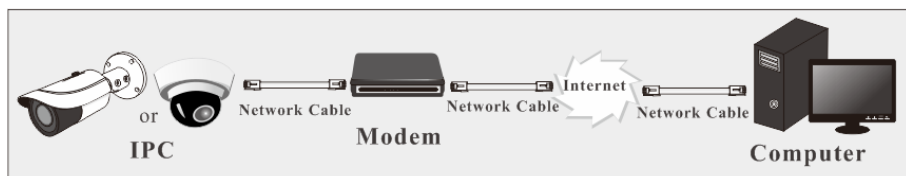
Port Range					
Application	Start	End	Protocol	IP Address	Enable
1	9007	to 9008	Both	192.168.1.201	☒
2	80	to 81	Both	192.168.1.201	☒
3	10000	to 10001	Both	192.168.1.166	☐
4	21000	to 21001	Both	192.168.1.166	☐

Router Setup

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

➤ **Access through PPPoE dial-up**

Network connection



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

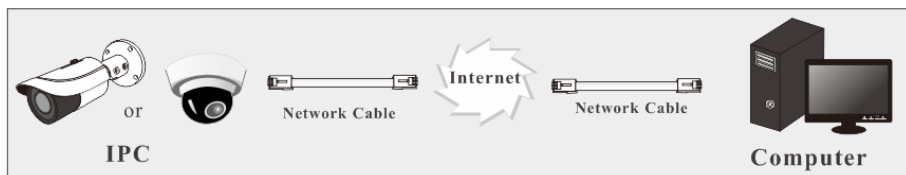
- ① Go to **Config** → **Network** → **Port** to set the port number.
- ② Go to **Config** → **Network** → **TCP/IP** → **PPPoE Config**. Enable PPPoE and then enter the username and password from your internet service provider.

IPv4	IPv6	PPPoE Config	IP Change Notification Config
☒ Enable			
User Name		xxxxxxx	
Password		•••••	
Save			

- ③ Go to **Config** → **Network** → **DDNS**. Before configuring the DDNS, please apply for a domain name first. Please refer to the DDNS configuration for detail information.
- ④ Open a web browser and enter the domain name and http port to access.

➤ Access through static IP

Network connection

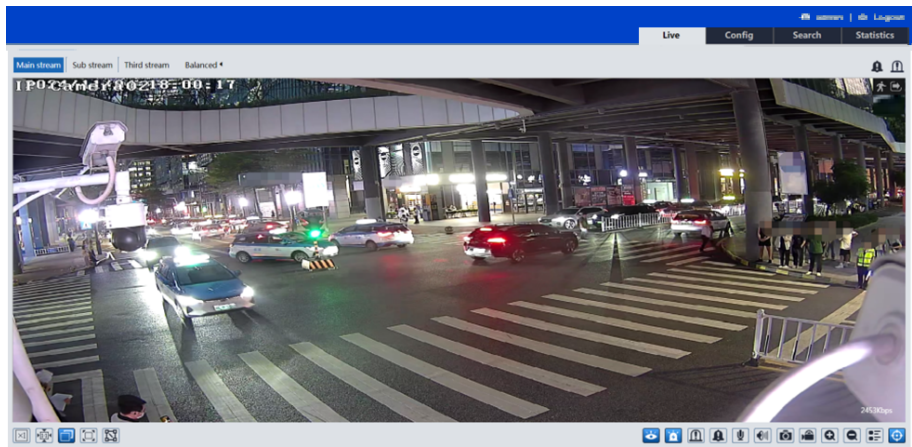


The setup steps are as follows:

- ① Go to **Config** → **Network** → **Port** to set the port number.
- ② Go to **Config** → **Network** → **TCP/IP** to set the IP address. Check “Use the following IP address” and then enter the static IP address and other parameters.
- ③ Open a web browser and enter its WAN IP and http port to access.

2 Live View

After logging in, the following window will be shown. The live view interface of different cameras may be slightly different. The following pictures and descriptions are for reference only.



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

Icon	Description	Icon	Description
	Original size		Light alarm indicator
	Fit correct scale		Audio exception indicator icon (sudden increase)
	Auto (fill the window)		Audio exception indicator icon (sudden decrease)
	Full screen		SD card recording indicator
	Measure Tool		Motion alarm indicator
	Start/stop live view		Color abnormal indicator
	Enable/disable alarm status display		Abnormal clarity indicator
	Enable/disable alarm output		Scene change indicator
	Enable or disable audio alarm (only some models support this function)		Line crossing indicator
	Enable/disable light alarm(only some models support this function)		Intrusion indicator

Icon	Description	Icon	Description
	Start/stop two-way audio (only available for the model with audio input connector)		Region entrance indicator
	Enable/disable audio		Region exiting indicator
	Snapshot		Target counting (by line) indicator
	Start/stop local recording		Target counting (by area) indicator
	Zoom in		Object detection indicator (object abandoned/missing)
	Zoom out		Heat map indicator
	AZ control (only available for the model with motorized zoom lens)		Loitering detection indicator
	Target detection (only available for face event or video metadata event)		Illegal parking detection indicator
	Rule information display		Video metadata indicator
	Alarm output indicator		People gathering indicator
	Sensor alarm indicator		Face detection indicator
	Audio alarm indicator		

*Measure Tool: get the height and width pixel of the selected region in the live view interface.

(This function is only available for mainstream). Click  and drag the mouse onto the image to draw a desired box. The width and height pixel will directly display in the box.

*Those smart alarm indicators will flash only when the camera supports those functions and the corresponding events are enabled.

*After clicking the audio alarm icon, the sound warning will be triggered according to the set warning times (you can set the warning times by clicking **Config → Alarm → Audio Alarm**). Click this icon again. After the current warning voice is completely sounded, it will stop.

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

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

*Plug-in free live view: two-way audio and local recording are not supported, and the preview mode switch (real-time/balanced/fluent mode) is not available too.

* In full screen mode, double click on the mouse to exit or press the ESC key on the

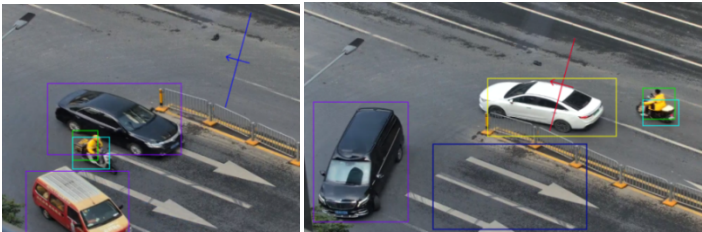
keyboard.

* 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)		

To set the stream profile, select Mainstream, Sub stream, Third stream and fourth/fifth stream (if supported). Go to **Configure**→**Video/Audio** to set the resolution for each stream as needed.

Descriptions of Rule Information



Color Descriptions of Target Recognition box:

Green box: detect human

Purple box: detect motor vehicle

Light blue box: detect non-motor vehicle (motorcycle/bicycle)

Target box after an event is triggered: turn yellow

Rule line or area color display:

Rule line or area: blue

Rule line or area after an event is triggered: turn from blue to red

3 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.

3.1 System Configuration

3.1.1 Basic Information

In the “Basic Information” interface, the system information of the device is listed, such as product model, brand, firmware version, ONVIF version, MAC address, device ID, etc. In addition, you can modify the device name as needed.

3.1.2 Date and Time

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

Date and TimeSummer Time

Zone: GMT (Dublin, Lisbon, London)⚠ The device time zone is different from the computer time zone, please select the correct time zone

Time Mode:

☒ Synchronize with NTP server

☐ Set manually

NTP server: time.windows.comUpdate period: 1440 Minutes

Set Time: 2025/4/15 17:54:35Sync with computer local time

Save

Select the time zone and time mode as needed.

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

Time Mode:

NTP: Specify an NTP server to synchronize the time.

Manual: Set the system time manually or you can synchronize the time with the time of the local computer.

Click the “Summertime” tab to set DST (Daylight Saving Time) as needed.

☒ DST					
☒ Auto DST					
☐ Manual DST					
Start Time	January	First	Sunday	00	Hour
End Time	Februa	First	Monday	00	Hour
Time Offset	120 Minutes				
Save					

3.1.3 Local Config

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

Picture Path	C:\Program Files\NetIPCamera\Picture	Browse
Record Path	C:\Program Files\NetIPCamera\Record	Browse
Video Audio Settings	☐ Open ☒ Close	
Show Bitrate	☐ Open ☒ Close	
Local Smart Snapshot Storage	☐ Open ☒ Close	
Save		

Show Bitrate: Enable or disable bitrate display on the live video.

Additionally, “Local smart snapshot storage” can be enabled or disabled here. If enabled, the captured pictures triggered by smart events will be saved to the local PC.

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

3.1.4 Storage

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

Management	Record Parameters	Schedule Record	Snapshot	FTP Snapshot
Total picture capacity	380 MB			
Picture remaining space	379 MB			
Total recording capacity	3328 MB			
Record remaining space	3200 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.

Note: This series of products support ANR (Automatic Network Replenishment) function. The offline video recorded files can be searched in the search interface.

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

● **Configuring Record Parameters**

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

Management	Record Parameters	Schedule Record	Snapshot	FTP Snapshot
Cycle Write		Yes		
		Save		

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

● **Schedule Recording Settings**

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

Management	Record Parameters	Schedule Record	Snapshot	FTP Snapshot
Parameter Settings				
Record Stream	Main stream			
Pre Record Time	6 Seconds (H.264,H.265,MJPEG)			
Timing				
☒ Enable Schedule Record				

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

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

☐ Erase
 ☒ Add
 Manual Input Select All Invert Clear

Week Schedule

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Sun.	00:00-24:00																								
	Apply settings to Manual Input Select All Invert Clear																								
Mon.	00:00-24:00																								
	Apply settings to Manual Input Select All Invert Clear																								
Tue.	00:00-24:00																								
	Apply settings to Manual Input Select All Invert Clear																								
Wed.	00:00-24:00																								
	Apply settings to Manual Input Select All Invert Clear																								
Thu.	00:00-24:00																								
	Apply settings to Manual Input Select All Invert Clear																								
Fri.	00:00-24:00																								
	Apply settings to Manual Input Select All Invert Clear																								
Sat.	00:00-24:00																								
	Apply settings to Manual Input Select All Invert Clear																								

Holiday Schedule

Date(MM-DD)

+

-

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	00:00-24:00																								
	Apply settings to Manual Input Select All Invert Clear																								

Save

Weekly schedule

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

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

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

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

Day schedule

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

Note: Holiday schedule takes priority over weekly schedule.

● Snapshot Settings

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

Management	Record Parameters	Schedule Record	Snapshot	FTP Snapshot
Snapshot Parameters				
Image Format		JPEG		
Resolution		2560x1440		
Event Trigger				
Snapshot Interval		1 Second		
Snapshot Quantity		5		
Timing				
☒ Enable Timing Snapshot				
Snapshot Interval		1 Second (0 Day 00 Hour 00 Minute 01 Second)		

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

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

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

● FTP Snapshot

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

Management	Record Parameters	Schedule Record	Snapshot	FTP Snapshot
☒ Enable Timing Snapshot				
Server Address		172.19.21.129(172.***.***.129)		
Snapshot Interval		60 Second (0 Day 00 Hour 01 Minute 00 Second)		
Sub Storage Path&Name		%a/FTP_TIMING_SNAP/%4y-%2m-%2d/%h/FTP_TIMING_SNAP_%4y%2m%2d%2h%2n%2s_%r.*		
		Reset Default Help		
Save				

Server Address: select the set FTP server. See [FTP section](#) for the FTP server setting.

Sub Storage Path& Name: Click “Help” to view the rule and then set it as needed.

Meanings of the default Path & Name Settings:

“%a/FTP_TIMING_SNAP/%4y-%2m-%2d/%h” stands for sub storage path

“FTP_TIMING_SNAP_%4y%2m%2d%2h%2n%2s_%r.* ” stands for file name

The entire default value means that a jpg file named “FTP_TIMING SNAP_Year Month Day Hour Minute Second_Random number” will be generated under FTP root directory> MAC address>FTP_TIMING SNAP>Year-Month-Day>Hour

“FTP_TIMING SNAP” refers to the event type. You can modify the event name as needed (for example: FTP Snapshot).

If the sub storage path and name box is empty, the snapshot will be uploaded and named according to the default settings.

If you only enter the file name rule, the snapshot will be uploaded to the root directory of the

FTP server.

3.1.5 Serial Port Settings

Only some models support this function. If your camera doesn't support RS485 interface, you can skip the following instructions.

You can use RS485 to transmit the data between the camera and the computer or terminal. Before using this function, please connect the camera and computer or terminal with RS485 cable. Please set the parameters of RS485 as needed. Note that you should keep the parameters of the camera and the computer or terminal all the same.

3.2 Image Configuration

3.2.1 Display Configuration

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

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

Section	Parameter	Value	
Video Adjustment	Lens Distortion Correction	☒	
	Electronic Image Stabilization	Off	
	Frequency	60HZ	
	Illumination Mode	Infrared light	
	Infrared Mode	Auto	
	Corridor Pattern	270	
	Image Mirror	☒ Open ☐ Close	
	Image Flip	☒ Open ☐ Close	
	Config File (Common)	Brightness	53
		Contrast	57
Hue		54	
Saturation		56	
Sharpness		204	
Noise Reduction		44	
Defog		208	
Auto Iris		(disable without auto iris lens)	
BLC		Off	
Antiflicker		50HZ	
Smart IR		Off	
White Balance		Auto	
IR Brightness		29	
Day/Night Mode		Auto	
Sensitivity		Mid	
Delay Time(Second)	2		
Shutter	1/30		
Gain Limit	50		

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 (only varifocal models support this function).

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 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.

Note: Only some models support HWDR (true WDR). If your camera doesn't support HWDR, you can set (digital) WDR as needed.

Antiflicker:

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

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

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

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

Lens Distortion Correction: When the image appears distortion to some extent, please enable this function and adjust the level according to the actual scene to correct the distortion (only some models support this function).

EIS: Electronic image stabilization; increase the stability of video image by using jitter compensation technology (only some models support this function).

Frequency: 50Hz and 60Hz can be optional.

Note: If the frequency is switched, the camera will reboot automatically.

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.

For dual-light models, you can set the illumination mode as shown in the picture above.

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

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

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

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

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

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

For IR models, “Smart IR”, “IR Brightness”, “Day/Night Mode” and “Infrared Mode” can be configured.

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

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

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

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

If “Alarm input linkage” is selected, the system will switch to day or night mode (according to your choice) upon the occurrence of the sensor alarm.

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

Schedule Settings of Image Parameters:

Click the “Profile Management” tab as shown below.

Camera Parameters	Profile Management
Schedule	Full Time
Config File	Common
Save	

Set full time schedule for common, auto mode and specified time schedule for day and night.

Auto mode: in the daytime, it will automatically perform the day config file set above; at night, it will automatically perform the night config file set above.
Choose “Timing” in the drop-down box of schedule as shown below.

Camera Parameters

Profile Management

Schedule

Timing

Time Range

0:00

4:00

8:00

12:00

16:00

20:00

24:00

Day

Night

Save

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

3.2.2 Video / Audio Configuration

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

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

Video

Audio

Index	Stream Name	Resolution	Frame Rate	Bitrate Type	Bitrate(Kbps)	Video Quality	I Frame Interval	Video Compression	Profile
1	Main stream	1920x1080	30	CBR	10240	Medium	120	H.264S	High Profile
2	Sub stream	704x480	18	CBR	5120	Medium	120	H.265+	Main Profile
3	Third stream	352x240	30	VBR	32	Medium	120	MJPEG	Main Profile

Send Snapshot

Sub stream

Size:(704x480)

☒ Video encode slice split
 ☒ Watermark(Only support H.264, H.265)
 Watermark content: 4562456425b2353

Save

Multiple video streams can be adjustable.

Resolution: The size of the 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 mainstream. 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.

Note: Some models may support H264S (Smart H.264)/H265S(Smart H.265). Compared to H.265+/H.265, smart H.265 can spontaneously adjust the bitrate distribution according to the requirements of the actual scene. For example, when there is no human or vehicle detected, the bitrate will be automatically reduced with no effect on image quality by using H.265S.

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

Send Snapshot: Set the snapshot stream.

Video encode slice split: If this function is enabled, a smooth image can be obtained even 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.

Video

Audio

☒ Enable

Audio Encoding

G711A

Audio Type

LIN

Audio Output

AUTO

LIN In Volume

75

Audio Out Volume

100

Audio Encoding: G711A and G711U are selectable.

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

Audio Output (if supported): Talkback, warning or auto can be optional. If “Talkback” is selected, the audio output will be used for two-way audio. If “Warning” is selected, the audio output will be used to play the pre-defined audio alarm. If “Auto” is selected, the system will output sound for two-way audio or warning voice as needed. But when it is warning and two-way audio is being enabled simultaneously, two-way audio will be output first.

Some models may support built-in speaker. You can set the audio output or speaker

separately.

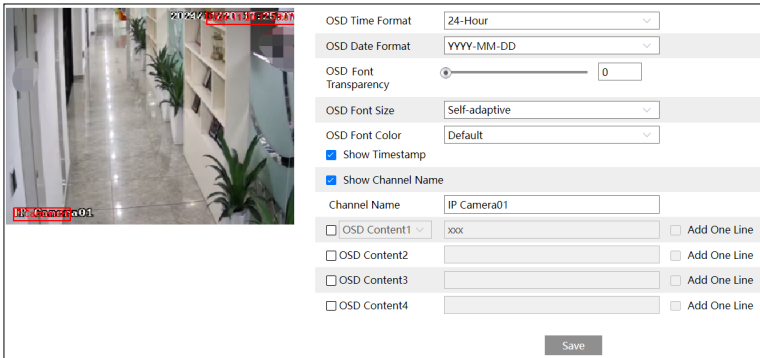
Speaker: Talkback, warning or auto can be optional. If “Talkback” is selected, the built-in speaker will be used for two-way audio. If “Warning” is selected, the built-in speaker will be used to play the pre-defined audio alarm. If “Auto” is selected, the system will output sound for two-way audio or warning voice as needed. But when it is warning and two-way audio is being enabled simultaneously, two-way audio will be output first.

Select audio output or speaker as needed. Only one of them can be effective.

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

3.2.3 OSD Configuration

Go to **Image→OSD** as shown below.



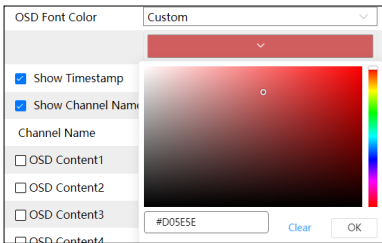
Set time format, date format, OSD content and OSD font transparency/size/color here. After enabling the corresponding display and entering the content, drag them to change their position. Then click the “Save” button to save the settings.

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

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

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

To customize the font size color:



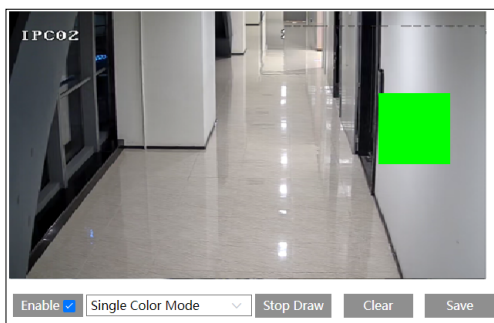
1. Select “Custom” and then click on the blank box under it.
2. Select a color on the colorful bar (right).
3. Click on the left color box to choose the desired color. Or you can directly enter the hexadecimal color code to set the color.
4. Click “OK” to save the OSD font color settings.

Picture Overlap Settings (This function is only available for some models):

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

3.2.4 Video Mask

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



To set up a video mask:

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

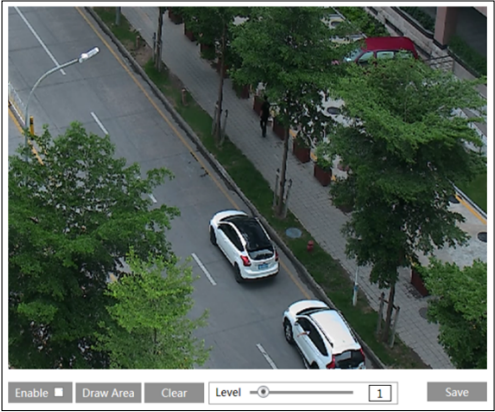


To clear the video mask:

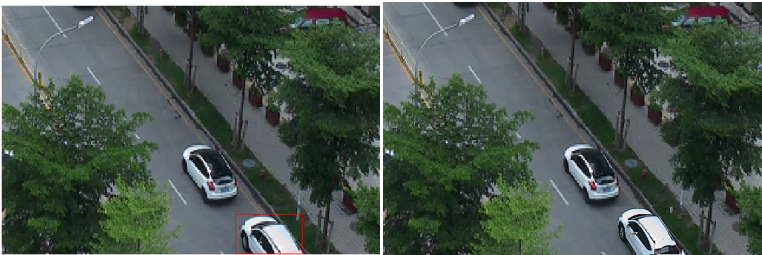
Click the “Clear” button to delete the current video mask area.

3.2.5 ROI Configuration

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

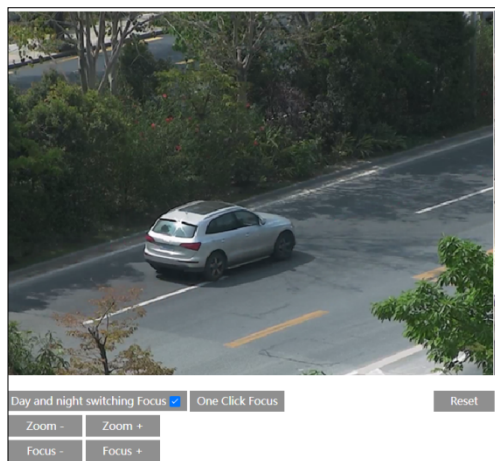


1. Check “Enable” and then click the “Draw Area” button.
2. Drag the mouse to set the ROI area.
3. Set the level.
4. Click the “Save” button to save the settings.



3.2.6 Lens Control

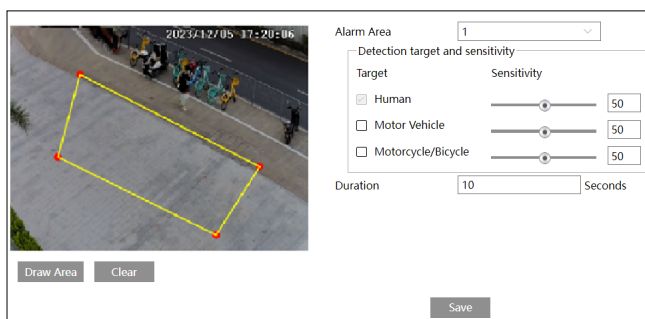
This function is only available for the model with a motorized zoom lens. Within this section, zoom and focus can be controlled. If the image is out of focus after a manual adjustment, one key focus can be used to set the focus automatically. Go to **Config→Image→Zoom/Focus** to set.



3.2.7 Smart Supplement Light Configuration

This function is only available for some models.

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



3. Set alarm areas. Select the alarm area number. Four alarm areas can be added. Click the “Draw Area” button and then click around the area where you want to set as the alarm area in the image (the alarm area should be a closed area). Click the “Stop Draw” button to stop drawing. Click the “Clear” button to delete the alarm area.
4. Set the detection target and sensitivity. “Human” is selected by default. You can also select “Motor Vehicle” or “Motorcycle/Bicycle” as needed.

Sensitivity: The higher the value is, the easier the white light will be triggered by targets.

5. Set the duration of the white light. In low ambient light, the system will automatically turn on the visible infrared light. Once there are people/vehicles appearing in the set alarm area, it will automatically switch to full-brightness visible white light. When people/vehicles leaving the alarm area exceed the set duration and no other persons/vehicles are detected during the period, it will resume to infrared light.

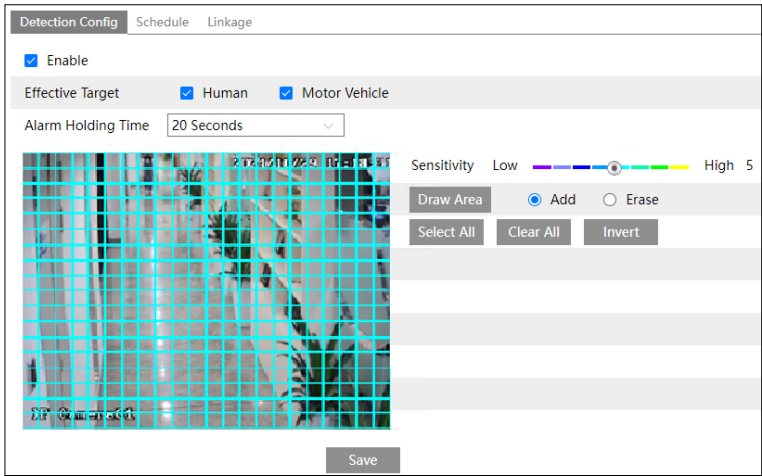
Note: If the people/vehicles staying and not moving in the detection area exceed the set duration, it will resume to infrared light too.

6. Click “Save” to save the settings.

3.3 Alarm Configuration

3.3.1 Motion Detection

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



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

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

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

2. Set motion detection area and sensitivity.

Clear all grids. Then move the “Sensitivity” scroll bar to set the sensitivity. A higher sensitivity value means that motion will be triggered more easily.

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

You can set different sensitivity levels for different areas.

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

Note:

- a) The area without colored grids means the sensitivity value is 0, which will be considered as a blocked area.
- b) After detecting a moving object in the area covered with grid lines, an alarm will be triggered when the number of the red grid lines exceeds the threshold of the sensitivity level.

3. Set the schedule for motion detection.

Detection Config
Schedule
Linkage

☐ Erase
☒ Add
Manual Input
Select All
Invert
Clear

Week Schedule

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Sun.	00:00-24:00 Apply settings to Manual Input Select All Invert Clear																								
Mon.	00:00-24:00 Apply settings to Manual Input Select All Invert Clear																								
Tue.	00:00-24:00 Apply settings to Manual Input Select All Invert Clear																								
Wed.	00:00-24:00 Apply settings to Manual Input Select All Invert Clear																								
Thu.	00:00-24:00 Apply settings to Manual Input Select All Invert Clear																								
Fri.	00:00-24:00 Apply settings to Manual Input Select All Invert Clear																								
Sat.	00:00-24:00 Apply settings to Manual Input Select All Invert Clear																								

Holiday Schedule

Date(MM-DD) 11-07
+
-

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
00:00-24:00 Apply settings to Manual Input Select All Invert Clear

Save

Weekly schedule

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

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

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

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

Day schedule

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

Note: Holiday schedule takes priority over weekly schedule.

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

The screenshot shows a configuration window with three tabs: 'Detection Config', 'Schedule', and 'Linkage'. The 'Linkage' tab is active. It contains several settings:

- ☒ Trigger Audio Alarm
 - Voice File Select Mode: Default (dropdown menu)
- ☒ Trigger SD Card Snapshot
- ☒ Trigger SD Card Recording
- ☐ Trigger Email
- ☐ Trigger FTP
- Trigger Alarm Out
 - ☐ Alarm Out

A 'Save' button is located at the bottom right of the configuration area.

Trigger Audio Alarm: If selected, the warning voice will be played on detecting a motion-based alarm. After checking it, you need to select the voice file as needed. If “Default” is selected, the voice file is the voice set in the audio alarm interface (see [Audio Alarm](#) for details). If “Specified” is selected, you can specify the warning voice and language for the motion alarm. (Only some models support this function)

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

Trigger SD Card Recording: If selected, 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 to the FTP server address. You can set the sub storage path and name as needed. Please refer to the [FTP](#) configuration for more details.

Trigger Alarm Out: If selected, this would trigger an external relay output that is connected to the camera on detecting a motion-based alarm. Only some models support this function. After that, click “Save” to save the settings.

3.3.2 Exception Alarm

● SD Card Full

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

SD Card Full SD Card Error IP Address Conflict Cable Disconnected

☒ Enable

Alarm Holding Time 20 Seconds

Trigger Alarm Out

☐ Alarm Out

☐ Trigger Email

☐ Trigger FTP

Save

2. Click “Enable”.

3. 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.

● SD Card Error

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

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

SD Card Full SD Card Error IP Address Conflict Cable Disconnected

☒ Enable

Alarm Holding Time 20 Seconds

Trigger Alarm Out

☐ Alarm Out

☐ Trigger Email

☐ Trigger FTP

Save

2. Click “Enable”.

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

● IP Address Conflict

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

SD Card Full	SD Card Error	IP Address Conflict	Cable Disconnected
--------------	---------------	----------------------------	--------------------

☒ Enable

Alarm Holding Time

Trigger Alarm Out

☐ Alarm Out

Save

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

3. Trigger alarm out. When the IP address of the camera conflicts with the IP address of other devices, the system will trigger the alarm out.

Note: if your camera doesn’t support alarm out, you can go to **Config → Maintenance → Operation Log** to check the relevant alarm information after enabling this function.

● Cable Disconnection

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

SD Card Full	SD Card Error	IP Address Conflict	Cable Disconnected
--------------	---------------	---------------------	---------------------------

☒ Enable

Alarm Holding Time

Trigger Alarm Out

☐ Alarm Out

Save

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.

Note: if your camera doesn’t support alarm out, you can go to **Config → Maintenance → Operation Log** to check the relevant alarm information after enabling this function.

3.3.3 Alarm In

This function is only available for some models. To set sensor alarm (alarm in):

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

Detection Config Schedule Linkage

☒ Enable

Alarm Type NO

Sensor Name

Alarm Holding Time 30 Seconds

Save

1. Click “Enable” and set the alarm type, alarm holding time and sensor name. If your camera supports two alarm input interfaces, please select the sensor ID first.
2. Set the schedule of the sensor alarm. The setup steps of the schedule are the same as the schedule recording setup. (See [Schedule Recording](#)).
3. Click “Linkage” to configure the alarm linkage items.

Detection Config Schedule Linkage

☐ Trigger Audio Alarm

☐ Trigger Light Alarm

☐ Trigger SD Card Snapshot

☐ Trigger SD Card Recording

☐ Trigger Email

☐ Trigger FTP

Trigger Alarm Out

☒ Alarm Out

Trigger Audio Alarm: If selected, the warning voice will be played when the sensor alarm is triggered. Select the voice file as needed. If “Default” is selected, the voice file is the voice set in the audio alarm interface (see [Audio Alarm](#) for details). If “Specified” is selected, you can specify the warning voice and language for the sensor alarm. (Only some models support this function)

Trigger Light Alarm: If selected, the light of the camera will flash when the sensor alarm is triggered. Please set the light flashing time and frequency first. See [Light Alarm](#) for details. (This function is only available for the red-blue light alert cameras and white light alert cameras; for the white light alert cameras, only when the illumination mode in Display

Settings is set to “Infrared light”, can this function be displayed.)

Trigger SD Card Snapshot: If selected, the system will capture images when the sensor alarm is triggered and save the images on an SD card.

Trigger SD Card Recording: If selected, video will be recorded on an SD card when the sensor alarm is triggered.

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

Trigger FTP: If “Trigger FTP” and “Attach Picture” are checked, the captured pictures will be sent in the FTP server address. You can set the sub storage path and name as needed. Please refer to the [FTP](#) configuration for more details.

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

3.3.4 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 ID: Some models may support two alarm output interfaces. The alarm out can be set respectively by selecting alarm out ID.

Alarm Out Mode: Alarm linkage, manual operation, day/night switch linkage 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. (In white light mode, this function is not available)

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	☐ Erase ☒ Add Manual Input
Save	

3.3.5 Alarm Server

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

Server Address	0.0.0.0
Port	8010
Heartbeat	Disable
Heartbeat interval	30 Second
Edit	

Click “Edit” to set the alarm server.

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

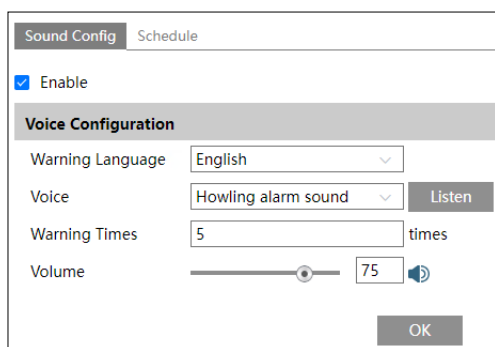
Click  to view the entire server address; click  to hide a part of sensitive data.

3.3.6 Audio Alarm

Only some models support this function.

Go to **Alarm** → **Audio Alarm** as shown below.

Enable audio alarm. If disabled, the camera will not play the desired warning voice even if an event triggers audio alarm. Additionally, you need to enable audio in the audio configuration interface and the speaker type (if supported) should be “Warning” or “Auto”, or the warning voice cannot play too.



Sound Config		Schedule	
☒ Enable			
Voice Configuration			
Warning Language	English		
Voice	Howling alarm sound	Listen	
Warning Times	5	times	
Volume	<input type="range" value="75"/> 75 Speaker		
OK			

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

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

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

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

- ② Select the voice and then set the warning times and volume as needed.

Warning times: it ranges from 1 to 50.

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

- ④ Click “OK” to save the settings.

3.3.7 Light Alarm

Note: This function is only available for the red-blue light alert cameras and white light alert cameras; for the white light alert cameras, only when the illumination mode in Display Settings is set to “Infrared light”, can this function be displayed.

Go to **Alarm → Light Alarm** as shown below.

- ① Enable light alarm as needed. Enable light alarm as needed. If it is disabled, the flashing light will not be turned on when the light alarm is triggered.
- ② Set the flashing time and frequency of the light.

Light Configuration	Schedule
☒ Enable	
Flashing Time	2 Second
Flashing Frequency	Low
OK	

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

Flashing Frequency: three options- low, middle and high

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

3.3.8 Video Exception

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

To set video exception detection:

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

Detection Config	Linkage
☒ Scene Change Detection	
☒ Video Blur Detection	
☒ Abnormal Color Detection	
Alarm Holding Time	20 Seconds
Sensitivity	51
Save	

1. Enable the applicable detection that's desired.

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

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

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

2. Set the alarm holding time.

3. Set the sensitivity of the exception detection.

Drag the slider to set the sensitivity value or directly enter the sensitivity value in the textbox.

The sensitivity value of Scene Change Detection: The higher the value is, the more sensitive the system responds to the amplitude of the scene change.

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

The sensitivity value of Abnormal Color Detection: The higher the value is, the more

sensitive the system responds to the color shift of the image.

4. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as motion detection. Please refer to [Motion Detection](#) for details.

After checking “Trigger SD Card Snapshot” and/or “Trigger SD Card Recording”, you can search the recorded files or snapshots of video exception by selecting the “Common” event.

※ The requirements of camera and surrounding area

1. Auto-focusing function should not been 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.

3.3.9 Audio Exception

Only some models support this function.

Alarms will be triggered when the abnormal sound is detected in the surveillance scene, such as the sudden increase/decrease of the sound intensity.

To set audio exception detection:

1. Go to **Alarm** → **Audio Exception** shown below.

The screenshot shows the 'Detection Config' tab with three sub-tabs: 'Detection Config', 'Schedule', and 'Linkage'. The 'Enable' checkbox is checked. Below it, there are two sections for sound intensity detection. The first section, 'Sudden Increase of Sound Intensity Detection', has an unchecked checkbox and two sliders: 'Sensitivity' and 'Sound Intensity Threshold', both set to 50. The second section, 'Sudden Decrease of Sound Intensity Detection', also has an unchecked checkbox and a 'Sensitivity' slider set to 50. At the bottom, the 'Alarm Holding Time' is set to 20 Seconds.

2. Enable audio exception.
3. Select the audio exception detection types.

Sudden Increase of Sound Intensity Detection: Detect sudden increase of sound intensity. If enabled, sensitivity and sound intensity threshold are configurable. Alarms will be triggered when the detected sound intensity exceeds the sound threshold.

Sensitivity: The higher the value is, the easier the alarm will be triggered.

Sound Intensity Threshold: It is the sound intensity reference for the detection. The lower the value is, the easier the alarm will be triggered. It is recommended to set the average sound intensity in the environment. The louder the environment sound, the higher the value should be. Please adjust it according to the actual environmental condition.

Sudden Decrease of Sound Intensity Detection: Detect sudden decrease of sound intensity. Please set the sensitivity as needed. The higher the value is, the easier the alarm will be triggered.

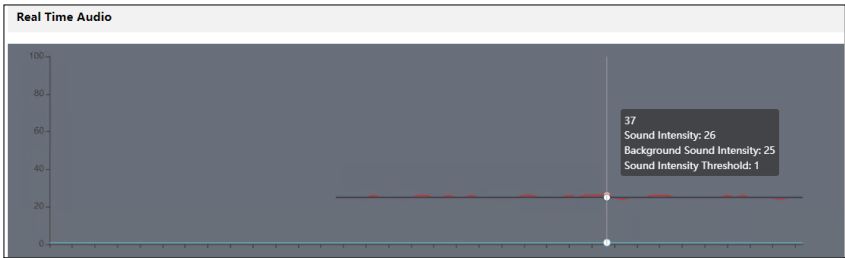
Real-time audio graphic:

Red wavy line stands for the current detected sound intensity.

Navy blue line stands for the environment (background) sound intensity.

Green line stands for the sound intensity threshold.

In order to reduce false alarms, it is recommended to set the sensitivity and sound intensity threshold according to the real-time audio graphic.



- 4. Set the alarm holding time and click “Save” to save the settings.
- 5. Set the schedule of the audio exception detection. The setup steps of schedule are the same as the schedule recording (See [Schedule Recording](#)).
- 6. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as sensor alarm. Please refer to [Alarm In](#) for details.

Note: The alarm recording type triggered by an audio exception event is “Common” . In the search interface, you can search the recorded files of audio exception by selecting the “Common” event.

3.3.10 Disarming

You can disarm alarm linkage actions quickly in this interface.

Disarming ConfigSchedule

Disarming

☒ Open☐ Close

Scheduled Disarming

☐ "Scheduled disarming" takes effect after disabling "Disarming".

Alarm Linkage

☒ Select All

☒ Email☒ FTP☒ HTTP POST☒ Alarm Server

☒ Alarm Out☒ Audio Alarm☒ Light Alarm

Save

Disarming: The system stops triggering alarm linkage actions immediately.

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

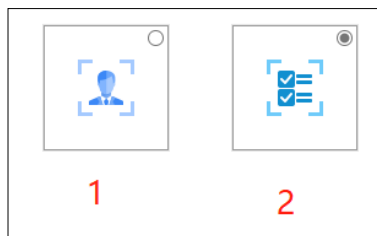
Note: After “Disarming” or “Scheduled Disarming” is enabled, the reported general alarms (the alarm start time and end time of alarm out and audio alarm) will probably not match the actual situation. You need to handle it manually.

3.4 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).
- Avoid places that are narrow or have too much shadowing.
- Avoid scenario where the object's color is similar to the background color.
- At any time of day or night, please make sure the image of the camera is clear and with adequate and even light, avoiding overexposure or too much darkness on both sides.

You can enable the event type for some models. Go to **Config** → **System** → **Application Scenarios** as shown below.



Event Type: 1- Face Event; 2- Smart Event

The default event type is smart event. If you want to switch to face event, please select face event and then click “Save”. After successful reboot, the corresponding event will be displayed. Select and set as needed.

Note:

* You can enable multiple smart detection events (such as line crossing detection, region intrusion detection, region exiting detection, etc.) simultaneously for some models, but detecting multiple smart events in the same time will cause a reduction in performance and affect the detection results. Please enable smart events according to the actual performance of your camera.

* Smart events may vary by model. If your camera doesn't support one or more of the following events, please skip the relevant instructions.

3.4.1 Object Abandoned/Missing

Alarms will be triggered when the objects are removed from or left at the pre-defined area.

To set abandoned/missing object detection:

Go to **Config** → **Event** → **Object Abandoned/Missing** as shown below.

Detection Config
Schedule
Linkage

☒ Enable

☒ Enable Abandoned Object Detection

☐ Enable Missing Object Detection

Time Threshold
10
Second

Alarm Holding Time
20 Seconds



Alarm Area
1

Draw Area
Clear

Save

1. Enable abandoned/missing object detection and then select the detection type.

Enable Abandoned Object Detection: Alarms will be triggered if there are items left in the pre-defined area.

Enable Missing Object Detection: Alarms will be triggered if items are missing in the pre-defined area.

Time Threshold: it is the alarm delay time of the object left in the region (ranging from 10~3600s) or the alarm delay time of the object removed from the region (ranging from 3~3600s). For example, if “Enable Abandoned Object Detection” is selected and the duration of delay is set as 10, alarms will be triggered after the object is left and stay in the region for 10s, but when someone takes away the object within 10s, alarms will not be triggered.

2. Set the alarm holding time.

3. Set the alarm area of the abandoned/missing object detection.

Set the alarm area number and then enter the desired alarm area name. Only one alarm area can be added. Click the “Draw Area” button and then click around the area where you want to set as the alarm area in the image (the alarm area should be a closed area). Click the “Stop Draw” button to stop drawing. Click the “Clear” button to delete the alarm area. Click the “Save” button to save the settings.

4. Click “Save” button to save the settings.

5. Set the schedule of the abandoned/missing object detection. The setup steps of the schedule are the same as the motion detection schedule settings (See [Motion Detection](#) for details).

6. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as sensor alarm. Please refer to [Alarm In](#) for details.

✖ The configuration requirements of camera and surrounding areas

1. The range of the detection object should occupy from 1/50 to 1/3 of the entire image.

2. The detection time of objects in the camera shall be from 3 to 5 seconds.
3. The defined area cannot be covered frequently and continuously (like people and traffic flow).
4. It is necessary for missing object detection that the drawn frame must be very close to the margin of the object in enhancing the sensitivity and accuracy of the detection.
5. Abandoned/missing object detection cannot determine the objects' ownership. For instance, there is an unattended package in the station. Abandoned object detection can detect the package itself but it cannot determine to whom it belongs to.
6. Try not to enable abandoned/missing object detection when light changes greatly in the scene.
7. Try not to enable abandoned/missing object if there are complex and dynamic environments in the scene.
8. Adequate light and clear scenery are very important to abandoned/missing object detection.

3.4.2 Line Crossing

Line Crossing: Alarms will be triggered if the target crosses the pre-defined alarm lines. Go to **Config**→**Event**→**Line Crossing** as shown below.

Detection Config
Schedule
Linkage

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

Alarm Holding Time
3 Seconds

Draw Area
Clear
Draw Target Size

Alarm Line
1
Direction
A->B

Alarm Line Parameters

Detection target and sensitivity

Target	Sensitivity
☒ Human	50
☒ Motor Vehicle	50
☒ Motorcycle/Bicycle	50

Target Size Filter

Target
Human

Min Size Width	1 %	Height	1 %
Max Size Width	90 %	Height	90 %

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

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

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

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

2. Set the alarm holding time.

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

Set the alarm line number and direction. Four lines can be added. Multiple lines cannot be added simultaneously.

Direction: A<->B, A->B and A<-B optional. This indicates the direction of the intruder who crosses over the alarm line that would trigger the alarm.

A<->B: The alarm will be triggered when the intruder crosses over the alarm line from B to A or from A to B.

A->B: The alarm will be triggered when the intruder crosses over the alarm line from A to B.

A<-B: The alarm will be triggered when the intruder crosses over the alarm line from B to A.

Click the “Draw Area” button and then drag the mouse to draw a line in the image. Click the “Stop Draw” button to stop drawing. Click the “Clear” button to delete the lines. Click the “Save” button to save the settings.

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

Detection Target:

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

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

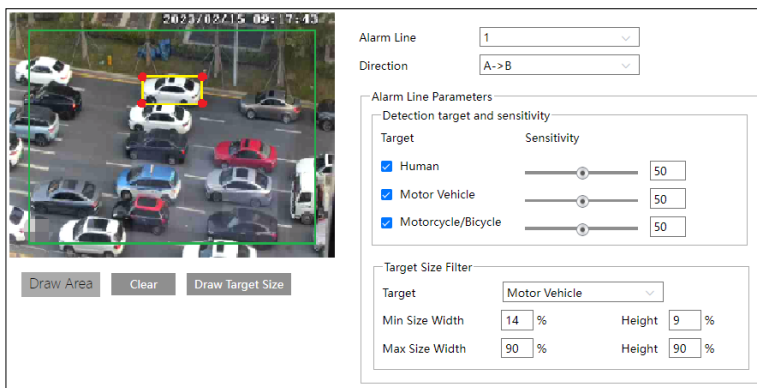
Motorcycle/Bicycle: Select it and then alarms will be triggered if a vehicle with two wheels (eg. a motorcycle or bicycle) crosses the pre-defined alarm lines.

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

Sensitivity: The higher the value is, the easier the alarm can be triggered.

To set target size filter:

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



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

The green box is the maximum target detection box; yellow box is the minimum target detection box.

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

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

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

Finally, click “Save” to save the settings.

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

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

4. Set the schedule of line crossing detection. The setup steps of the schedule are the same as the motion detection schedule settings (See [Motion Detection](#) for details).

6. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as sensor alarm. Please refer to [Alarm In](#) for details.

※ Configuration requirements of the camera and surrounding area

1. Auto-focusing function should not be enabled for line crossing detection.
2. Avoid the scenes with many trees or the scenes with various light changes (like many flashing headlights). The ambient brightness of the scenes shouldn't be too low.
3. Cameras should be mounted at a height of 2.8 meters or above.
4. The recommended depression angle of the camera is from 30° to 45° (See [Outdoor Mounting](#) example).

For pedestrians, their heads and main bodies should be clearly visible on a video.



For vehicles, the depression angle should not be more than the recommended value. The sideways or horizontal viewing angle is recommended on a video (see below).



5. Make sure cameras can view objects for at least 2 seconds in the detected area for accurate detection.

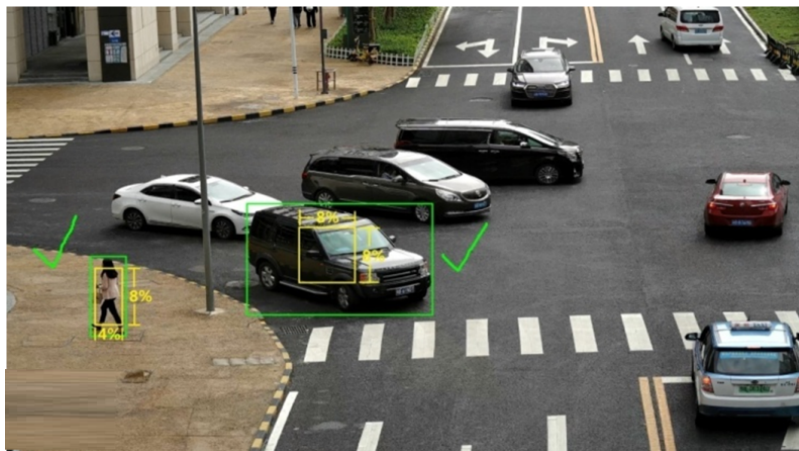
6. Adequate light and clear scenery are crucial for line crossing detection.

7. Please adjust the installation position or focus to meet the requirements of the target recognition size.

The recommended target recognition size:

Percentage	Human	Motor Vehicle	Motorcycle/Bicycle
Minimum (Width × Height)	$4\% \times 8\%$	$8\% \times 8\%$	$4\% \times 4\%$
Maximum (Width × Height)	$50\% \times 50\%$	$50\% \times 50\%$	$50\% \times 50\%$

Note: The percentage means that a target occupies the percentage of the entire image. For example: In a 1080P (1920×1080) video image, the minimum resolution of human is 80×160 (w = 1920×4%=80, h=1920×8%=160)



Correct example

The target recognition box meets the requirements of the minimum size. The yellow box stands for the minimum recognition size. The green box stands for the set target box.



Wrong example

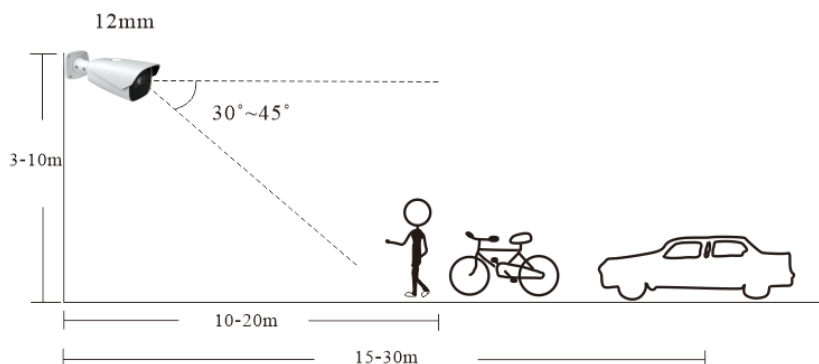
The yellow box stands for the minimum recognition size. The green box stands for the set target box. These two target recognition boxes don't meet the requirement of the minimum size. Therefore, you need to adjust the camera position or focus as needed.

8. Installation suggestion:

Outdoor mounting:

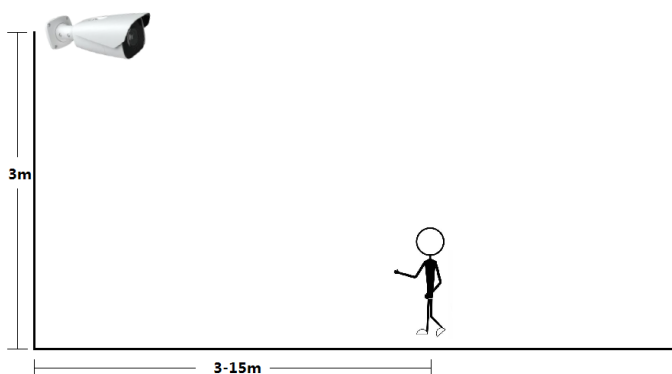
The optimal detection distance varies due to different focal length. Please refer to the following table.

Focal Length	Installation Height(m)	Human/Motorcycle/Bicycle		Motor Vehicle	
		Maximum Distance(m)	Optimal Distance(m)	Maximum Distance(m)	Optimal Distance(m)
2.8mm	3-10	8	4-8	15	10-15
3.6mm	3-10	10	5-10	20	15-20
12mm	3-10	25	10~20	35	15~30
22mm	3-10	45	30~40	70	20~50



Example of 12mm focal length

Indoor Mounting



3.4.3 Region Intrusion

Region Intrusion: Alarms will be triggered if the target intrudes into the pre-defined areas. This function can be applicable to important supervision places, danger areas and prohibited areas, like military administrative zones, high danger areas, no man's areas, etc.

Go to **Config**→**Event**→**Region Intrusion** as shown below.

Detection Config Schedule Linkage

☒ Enable

☒ Save Original Picture To SD Card

☒ Save Target Picture To SD Card

Alarm Holding Time 3 Seconds

Alarm Area 1

Alarm Area Parameters

Detection target and sensitivity

Target Sensitivity

☒ Human 50

☒ Motor Vehicle 50

☒ Motorcycle/Bicycle 50

Target Size Filter

Target Human

Min Size Width 1 % Height 1 %

Max Size Width 90 % Height 90 %

Draw Area Clear Draw Target Size

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

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

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

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

2. Set the alarm holding time.

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

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

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

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

Detection Target:

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

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

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

All of the three types of objects can be selected simultaneously. Please select the detection

objects as needed. If no object/target is selected, alarms will not be triggered even if intrusion detection is enabled.

Sensitivity: The higher the value is, the easier the alarm can be triggered.

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

4. Click “Save” button to save the settings.

5. Set the schedule of region intrusion detection. The setup steps of the schedule are the same as the motion detection schedule settings (See [Motion Detection](#) for details).

6. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as sensor alarm. Please refer to [Alarm In](#) for details.

※ Configuration requirements of the camera and surrounding area

The requirements are similar to line crossing detection. Please refer to [Configuration requirements of the camera and surrounding area](#) of line crossing detection for details.

3.4.4 Region Entrance

Only some models support this function.

Region Entrance: Alarms will be triggered if the target enters the pre-defined areas.

Go to **Config→Event→Region Entrance**.

1. Enable region entrance detection and select the snapshot type and the detection target.
2. Set the alarm holding time.
3. Set alarm areas, targets and target size filter for region entrance detection.
4. Set the schedule of region entrance detection.
5. Set the alarm linkage items.

The setup steps of the region entrance detection are the same as the region intrusion detection setup (See [Region Intrusion](#) for details).

3.4.5 Region Exiting

Only some models support this function.

Region Exiting: Alarms will be triggered if the target exists from the pre-defined areas.

Go to **Config→Event→Region Exiting**.

1. Enable region exiting detection and select the snapshot type and the detection target.
2. Set the alarm holding time.
3. Set alarm areas, targets and target size filter for region exiting detection.
4. Set the schedule of region exiting detection.
5. Set the alarm linkage items.

The setup steps of the region exiting detection are the same as the region intrusion detection setup (See [Region Intrusion](#) for details).

3.4.6 Target Counting by Line

Only some models support this function. If your camera doesn't support this function, please skip the following instructions.

This function is used to detect, track and count the number of people or vehicles crossing the set alarm line.

1. Go to **Config→Event→Target Counting by Line** as shown below.

The screenshot shows the 'Detection Config' window with three tabs: 'Detection Config', 'Schedule', and 'Linkage'. The 'Detection Config' tab is active. It contains the following settings:

- Enable:** Checked (blue square).
- Save Original Picture To SD Card:** Unchecked (white square).
- Save Target Picture To SD Card:** Unchecked (white square).
- Detection target and sensitivity:**
 - Target:** Human (checked), Motor Vehicle (checked), Motorcycle/Bicycle (checked).
 - Sensitivity:** Three sliders, each set to 50.
 - Staying Threshold:** Three input fields, each set to 0.
- Close Event Snapshot:** Unchecked (white square).
- Counting Reset:**
 - Timing:** Off (dropdown menu).
 - Manual:** A 'Reset' button.
- Time Threshold:** 0 (input field) Second (dropdown menu).
- Alarm Holding Time:** 20 Seconds (dropdown menu).

2. Enable target counting by line and select the snapshot type and the detection target.

Detection Target: Select the target to calculate. Human, motor vehicle and motorcycle/bicycle can be selected.

Staying Threshold: When the targets (human/vehicle) staying in the specified area exceed the threshold, alarms will be triggered.

Close Event Snapshot: if enabled, the captured pictures based on target counting by line will be neither saved to an SD card/local PC nor pushed to the NVR/APP/platform/....

Counting Reset: The current number of the target counting can be reset. You can choose to reset the counting daily, weekly or monthly. Click “Reset” to manually reset the current number of crossing line people/motor vehicle/non-motor vehicle counting.

Time Threshold: The duration time that the number of targets exceeds the staying threshold. Alarms will not be triggered even if the targets staying in the specified area exceed the threshold within the set delay alarm duration. But if you set it to “0”, alarms will be triggered immediately when the targets staying in the specified area exceed the threshold.

3. Set the alarm holding time.

Alarm Holding Time: it is the time that the alarm extends after an alarm ends.

4. Set alarm lines and target size filter.

Alarm Line

Alarm Line: 1
Direction: A->B

Target Size Filter

Target: Human
Min Size Width: 1 % Height: 1 %
Max Size Width: 90 % Height: 90 %

OSD

☒ Statistics
☒ Entrance: Entry
☒ Exit: Exit
☒ Stay: Stay
≤ Threshold: Welcome
> Threshold: Please wait

Save

Set the alarm line number and direction. Only one alarm line can be added.

Direction: A->B and A<-B can be optional. The direction of the arrow is entrance.

Click the “Draw Area” button and then drag the mouse to draw a line in the image. Click the “Clear” button to delete the lines.

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

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

Statistics: If enabled, you can see the statistical information in the live view interface. If disabled, the statistical information will not be displayed in the live view interface.

Check “Statistics” and then move the red box to change the position of the statistical information displayed on the screen.

The statistical OSD information can be customized as needed.

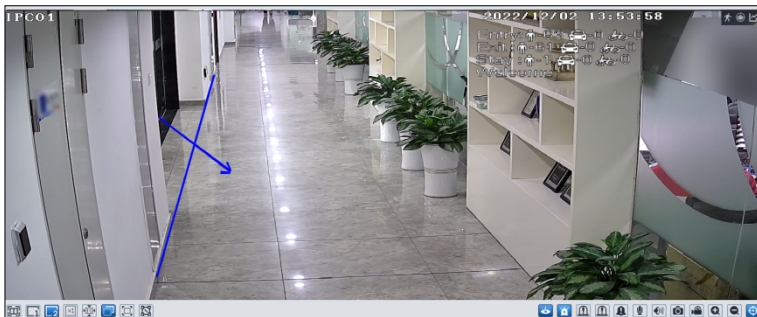
Note: When target counting by line and by area are enabled simultaneously, the OSD position shown in the image depends on the OSD position of target counting by area.

Click the “Save” button to save the settings.

5. Set the schedule of target counting by line. The setup steps of the schedule are the same as the schedule recording setup (See [Schedule Recording](#)).

6. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as sensor alarm. Please refer to [Alarm In](#) for details.

7. View the statistical information in the live view interface.



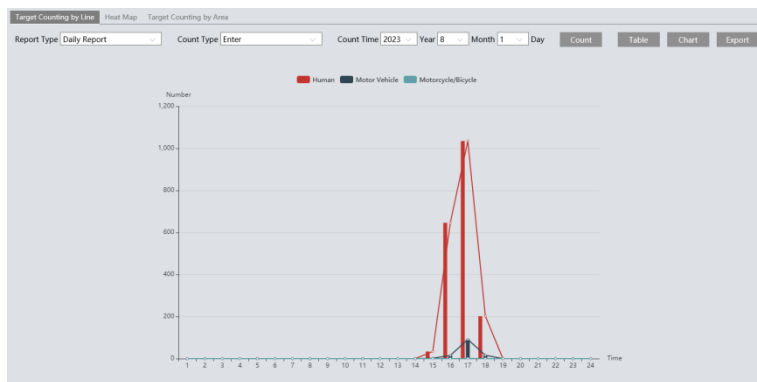
8. View the statistical information of target counting by line. Click “Statistics” to enter the following interface.

Target Counting by Line				
Heat Map Target Counting by Area				
Report Type: Daily Report Count Type: Enter Count Time: 2023 Year 12 Month 11 Day Count Table Chart Export				
Index	Count Time	Human	Motor Vehicle	Motorcycle/Bicycle
1	2023/12/11 00:00:00 - 2023/12/11 00:59:59	0	0	0
2	2023/12/11 01:00:00 - 2023/12/11 01:59:59	11	0	0
3	2023/12/11 02:00:00 - 2023/12/11 02:59:59	0	0	0

Select the report type. Daily report, weekly report, monthly report and annual report are selectable.

Select the count type. Enter or leave can be optional.

Select the start time and then click “Count”. Then the counting result will be displayed in the statistical result area. Click Table or Chart to display the result in different ways.



※ Configuration requirements of the camera and surrounding area

The requirements are similar to line crossing detection. Please refer to [Configuration requirements of the camera and surrounding area](#) of line crossing detection for details.

3.4.7 Target Counting by Area

Only some models support this function.

This function is used to detect, track and count the number of people or vehicles intruding into a pre-defined area.

1. Go to **Config**→**Event**→**Target Counting by Area** as shown below.

Detection Config

Schedule

Linkage

☒ Enable

☐ Save Original Picture To SD Card

☐ Save Target Picture To SD Card

Detection target and sensitivity

Target	Sensitivity	Staying Threshold
☒ Human	50	0
☒ Motor Vehicle	50	0
☒ Motorcycle/Bicycle	50	0

Counting Reset

Timing

Off

Manual

Reset

Time Threshold

0

 Second

 Alarm Holding Time

20 Seconds

2. Enable target counting by area, select the snapshot type, the detection target and counting reset. The setup steps are the same as the target counting by line.
3. Set the statistic area.

Camera
10/15/2023 14:35:18



Exit # Entrance # Car # Zone #

EXIT: Entrance: Front # Zone: #

Start # Entrance # Car # Zone #

Draw Area
Clear
Draw Target Size

Alarm Area

Alarm Area	1
------------	---

Target Size Filter

Target	Human	
Min Size Width	1 %	Height 1 %
Max Size Width	90 %	Height 90 %

OSD

☒ Statistics	Iips
☒ Entrance	Entry
☒ Exit	Exit
☒ Stay	Stay
≤ Threshold	Welcome
> Threshold	Please wait

Save

Select the alarm area number. Only one alarm area can be added.

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

Note: If the set rule line is very close to the edge of the screen, it may be difficult for the

target to trigger the alarm. Please make sure that there is at least one full target-sized space between the rule line and the edge of the screen.

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

Statistics: If enabled, you can see the statistical information in the live view interface. If disabled, the statistical information will not be displayed in the live view interface.

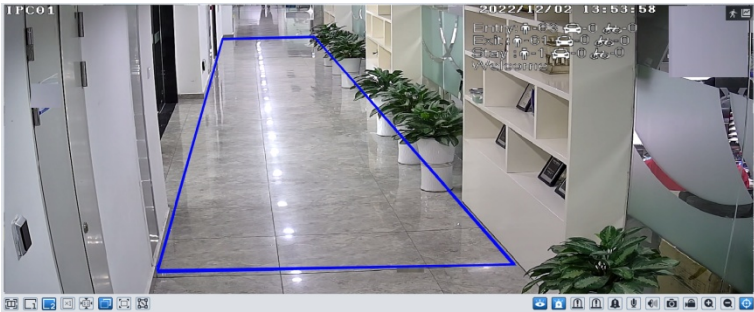
Check “Statistics” and then move the red box to change the position of the statistical information displayed on the screen.

The statistical OSD information can be customized as needed.

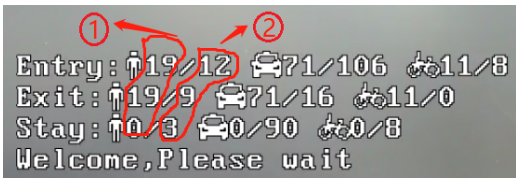
4. Set the schedule of target counting by area. The setup steps of the schedule are the same as the schedule recording setup (See [Schedule Recording](#)).

5. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as sensor alarm. Please refer to [Alarm In](#) for details.

6. View the statistical information in the live view interface.



Note: When target counting by line and by area are enabled simultaneously, the OSD position shown in the image depends on the OSD position of target counting by area.



① : the statistical number of target counting by area

② : the statistical number of target counting by line

Each line of the above OSD information (including OSD content, colon, slashes and images) cannot exceed 37 characters, or some data will not be displayed completely.

7. View the statistical information of target counting by area. Click **Statistics → Target Counting by Area** to enter the following interface.

Target Counting by Time		Heat Map		Target Counting by Area	
Report Type: Daily Report		Count Type: Enter		Count Time: 2023 - Year 12 - Month 11 - Day	
				Count Table Chart Export	
Index	Count Time	Human	Motor Vehicle	Motorcycle/Bicycle	
1	2023/12/11 00:00:00 - 2023/12/11 00:59:59	59	9	0	
2	2023/12/11 01:00:00 - 2023/12/11 01:59:59	0	0	0	

Please select report type, count type and start time as needed. Then click “Count” to search the statistic result. Click “Chart” to view the statistic result intuitively.

※ Configuration requirements of the camera and surrounding area

The requirements are similar to line crossing detection. Please refer to [Configuration requirements of the camera and surrounding area](#) of line crossing detection for details.

3.4.8 Heat Map

Only some models support this function.

Heat Map displays the flow distribution of people/vehicles in pre-defined areas by different colors.

- 1.Enable heat map, set snapshot type and detection target type as needed.
- 2.Set heat map display area and target size filter. Up to 4 areas can be set.

Detection Config

Schedule

☒ Enable

Draw Area

Clear

Draw Target Size

Alarm Area

1

Alarm area parameters

Detection target and sensitivity

Target

Human

Motor Vehicle

Motorcycle/Bicycle

Sensitivity

50

50

50

Target Size Filter

Target

Human

Min Size Width

1 %

Height

1 %

Max Size Width

90 %

Height

90 %

Save

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

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

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

4. View the heat map data (click **Statistics** → **Heat Map**). Set the start time and the end time. Click “Count” to view the heat map as shown below. The default heat map is people flow data

display. Click “Motor Vehicle” or “Motorcycle/bicycle” to view the corresponding data.



3.4.9 Loitering Detection

Only some models support this function.

Loitering Detection: when someone entering and loitering in a pre-defined area exceeds the threshold, alarms will be triggered until the object leaves this area.

Go to **Event**→**Loitering Detection** as shown below. The setting steps are as follows:

1. Enable loitering detection and select the snapshot type.

Detection ConfigScheduleLinkage

☒ Enable

☐ Save Original Picture To SD Card

☐ Save Target Picture To SD Card

Trigger mode

Moving object

Time Threshold

10

Second

Alarm Holding Time

20 Seconds

Draw Area

Clear

Draw Target Size

Alarm Area

1

Alarm area parameters

Sensitivity

50

Target Size Filter

Target

Human

Min Size Width

1

%

Height

1

%

Max Size Width

90

%

Height

90

%

Save

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

Trigger Mode: Choose “Moving object” or “All objects” as needed. If “Moving object” is selected, alarms will be triggered when a person staying and moving in the specified area exceeds the threshold. If “All objects” is selected, alarms will be triggered when a person keeping still or moving in the specified area exceeds the threshold.

Time Threshold: the time that a person is allowed to stay in the area. If a person staying and

moving in the specified area exceeds the threshold, alarms will be triggered until this person leaves.

For example: Set the threshold to “60seconds; when a person staying and moving in the specified area exceeds 60seconds, an alarm is triggered and continues unless the person leaves this area.

Alarm Holding Time: it is the time that the alarm extends after an alarm ends.

3. Set alarm areas, sensitivity and target size filter.

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

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

Sensitivity: The higher the value is, the easier the alarm can be triggered.

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

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

5. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as sensor alarm. Please refer to [Alarm In](#) for details.

※ Configuration requirements of the camera and surrounding area

1. Avoid enabling this function in complex scenes, such as a scene with a large flow of people and vehicles.

2. Other requirements are similar to line crossing detection. Please refer to [Configuration requirements of the camera and surrounding area](#) of line crossing detection for details.

3.4.10 Illegal Parking Detection

Only some models support this function.

Illegal Parking Detection: when a vehicle (like a car, truck, motorcycle, etc.) staying in a no-parking zone exceeds the threshold, alarms will be triggered until the vehicle is driven away.

Go to **Event→Illegal Parking Detection**. The setting steps are as follows:

1. Enable illegal parking detection and select the snapshot type.

Detection Config
Schedule
Linkage

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

Time Threshold
10
Second

Alarm Holding Time
20 Seconds



Draw Area
Clear
Draw Target Size

Alarm Area
1

Alarm area parameters

Detection target and sensitivity

Target
Sensitivity

☒ Motor Vehicle
50

☒ Motorcycle/Bicycle
50

Target Size Filter

Target
Motor Vehicle

Min Size Width
1
%
Height
1
%

Max Size Width
90
%
Height
90
%

Save

2. Set the time threshold and alarm holding time.

Time Threshold: the time that a vehicle is allowed to stay in the specified area. If a vehicle staying in the area exceeds the threshold, alarms will be triggered until they are driven away. For example, the time threshold is set to 30s. When the system detects a vehicle stopping in the set no-parking zone, it will start counting. Alarms will be triggered after it stays for more than 30s. And the illegal parking alarm will not stop until the vehicle is driven away from the non-parking zone.

Alarm Holding Time: This is the time that the alarm extends after the overstaying vehicle leaves.

3. Set alarm areas, target and target size filter.

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

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

Detection Target:

Motor Vehicle: a vehicle with four or more wheels

Motorcycle/Bicycle Vehicle: a vehicle with two wheels (eg. a motorcycle or bicycle)

Sensitivity: the higher the value is, the easier the alarm can be triggered.

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

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

5. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as sensor alarm. Please refer to [Alarm In](#) for details.

※ **Configuration requirements of the camera and surrounding area**

1. Avoid enabling this function in complex scenes, such as the scene with a large flow of people and vehicles.
2. Other requirements are similar to line crossing detection. Please refer to [Configuration requirements of the camera and surrounding area](#) of line crossing detection for details.

3.4.11 Video Metadata

Only some models support this function. If your camera doesn't support this function, please skip the following instructions.

Video Metadata: Human, motor vehicle and motorcycle/bicycle in the video can be classified and captured and the relevant features can be extracted and displayed on the live interface.

Go to *Config* → *Event* → *Video Metadata*. The setting steps are as follows:

Detection ConfigImage OSDScheduleLinkage

☒ Enable

☐ Save Original Picture To SD Card

☐ Save Target Picture To SD Card



Draw detection areaClearDraw Target Size

Detection Area

1

1

Detection area parameters

Detection target and sensitivity

TargetSensitivity

☒ Human50

☒ Motor Vehicle50

☒ Motorcycle/Bicycle50

Target Size Filter

Target

Human

Min Size Width

1

%

Height

1

%

Max Size Width

90

%

Height

90

%

1. Enable video metadata and select the snapshot type.

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

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

Detection target: Human, motor vehicle and motorcycle/bicycle. All of the three types of objects can be selected simultaneously.

Push target trajectory with a persistent connection: Push target trajectory (moving coordinate) to API test tool with a persistent connection. If enabled, the system will push the target trajectory upon detecting a target. If disabled, the system will push the target trajectory only when triggering video metadata alarm.

2. Set the detection area, blocked area, detection target and target size filter.

Detection Area: 4 detection areas can be set. Targets that enter the pre-defined detection area

56

will be captured.

Blocked Area: 4 blocked areas can be set. Targets that enter the pre-defined blocked area will not be captured.

You need to set the detection area and blocked area separately.

To set up a detection area:

Check the checkbox of the detection area and select the number and to set the detection area.

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

To set blocked area:

Check the checkbox of blocked area and select the number and set the blocked area. The setting steps are the same as detection area settings.

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

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

3. Select the attribute information of the target. Click “Image OSD” and then select the relevant attribute information. When the target is detected, the information you select will be displayed in the attribute display area. See [Video Metadata View](#) for details.

4. Set the schedule of the video metadata function. The setup steps of the schedule are the same as the schedule recording setup (See [Schedule Recording](#)).

5. Click “Linkage” to check “FTP” as needed. Please refer to the [FTP](#) configuration for more details.

After all settings above are configured, return to the live interface to view the captured pictures and features.

➤ **Video Metadata View**

In the live interface, click  to view the following smart snapshots.



Click the captured human picture to view the detailed information as shown below.

ID	87
Time	2024/11/7 16:58:33
Gender	Male
Age	Youth
Direction	Face
Hat	Yes
Glasses	-

Click the captured vehicle picture to view the detailed information as shown below.





ID	92
Time	2024/11/7 16:58:36
Type	Sedan
Color	black
Brand	TOYOTA
Model	TOYOTA_Corolla

Note: This function is not applicable to the scene with a large flow of people and vehicles.

3.4.12 People Gathering Detection

Only some models support this function. If your camera doesn't support this function, please skip the following functions.

People Gathering Detection: It detects the people density in a pre-defined area. If the people's density reaches the threshold of the set sensitivity level and exceeds the set time threshold, alarms will be triggered. This function can be applicable to the scenes with medium or long distance, such as outdoor plaza, government entrance, station entrance and exit.

The setting steps are as follows:

1. Go to **Config** → **Event** → **People Gathering Detection**.

Detection Config
Schedule
Linkage

☒ Enable

☐ Save Original Picture To SD Card

Time Threshold
10
Second

Alarm Holding Time
20 Seconds



Draw Area
Clear

Save

Alarm Area
1

Alarm area parameters

Sensitivity
50

2. Enable people gathering detection and select the snapshot type.

Save Original Picture to SD Card: If it is enabled, the detected original pictures will be captured and saved to the SD card when people gathering detection is triggered.

2. Set the alarm area and sensitivity.

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

Sensitivity: the sensitivity is related to the local density. The higher the value is, the easier the alarm can be triggered.

3. Set the time threshold and alarm holding time.

Time threshold: When the people density in the pre-defined area reaches the threshold of the sensitivity level and exceeds the set time threshold, alarms will be triggered.

Alarm Holding Time: it is the time that the alarm extends after an alarm ends.

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

5. Click “Linkage” to check “FTP” as needed. Please refer to the [FTP](#) configuration for more details.

✖ Configuration requirements of the camera and surrounding area

1. Low installation height is not allowed for this function.

2. Try to avoid the following situations: large percentage of a single person in the image, obvious target occlusion, continuous shaking of the camera, shaking of leaves and tree shade, or dense traffic or people flow.

3. Other requirements are similar to line crossing detection. Please refer to [Configuration requirements of the camera and surrounding area](#) of line crossing detection for details.

3.4.13 Face Detection

Only some models support this function. If your camera doesn't support this function, please skip the following instructions.

Face detection function is to detect face appearing in the surveillance scene. Alarms will be triggered when a face is detected.

Click **Config** → **System** → **Application Scenarios**. Select the face event and then save the setting. After the camera restarts successfully, you can view the face detection menu.

The setting steps are as follows:

1. Go to **Config** → **Event** → **Face Detection** as shown below.

Detection Config Advanced Schedule Linkage

State Working

☒ Enable

☐ Save Source Information To SD Card

☐ Save Face Information To SD Card

Trigger alarm condition All Alarm

Alarm Holding Time 20 Seconds

Camera33

12/11/2023 16:01:1

Draw Area Clear

☒ Min Size 5 %

☐ Max Size 50 %

Save

2. Enable the face detection function.

Save Source Information to SD Card: if checked, the whole picture will be saved to SD card when detecting a face.

Save Face Information to SD Card: if checked, the captured face picture will be saved to SD card when detecting a face.

Note: To save images to the local PC, please enable the local smart snapshot storage first (**Config** → **System** → **Local Config**). To save images to the SD card, please install an SD card first.

3. Set alarm condition and the alarm holding time.

Trigger alarm condition: all or mask off can be selectable.

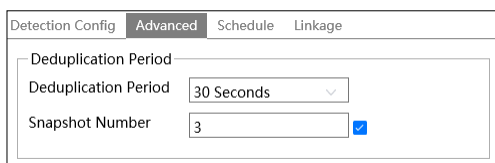
All: Alarms will be triggered when the camera detects a face (with/without a mask).

Mask off: Alarms will be triggered when the detected person is not wearing a mask on the face.

4. Set alarm detection area.

Click “Draw Area” and drag the border lines of the rectangle to modify its size. Move the rectangle to change its position. Click “Stop Draw” to stop drawing the area. Click “Clear” to clear the area. Then set the detectable face size by defining the maximum value and the minimum value (The default size range of a single face image occupies from 3% to 50% of the entire image).

5. Advanced settings. Choose the snapshot interval and number as needed to avoid capturing multiple similar pictures in a very short period of time.



The screenshot shows a configuration window titled "Detection Config" with three tabs: "Detection Config", "Advanced", and "Linkage". The "Advanced" tab is selected. Inside the "Advanced" tab, there is a section titled "Deduplication Period". Below this title, there are two settings: "Deduplication Period" is set to "30 Seconds" with a dropdown arrow, and "Snapshot Number" is set to "3" with a checked checkbox.

Deduplication Period: If 30 seconds is selected, the camera will capture the same target once every 30 seconds during its continuous tracking period.

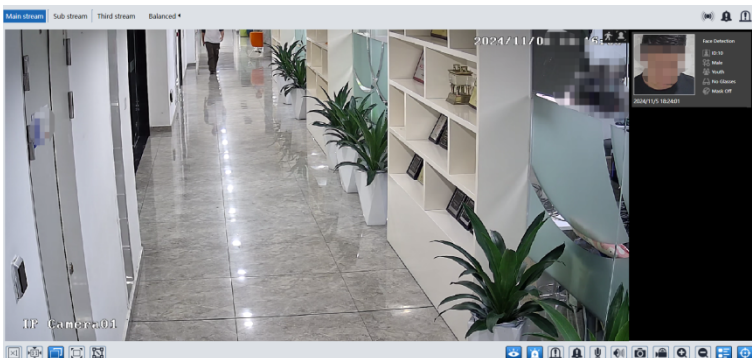
Snapshot Number: If the snapshot number is enabled and set (eg. 3), the camera will capture the same target once every 30 seconds and it will capture this target 3 times at most during its continuous tracking period. If the snapshot number is disabled, the camera will capture the same target once every 30 seconds until the target disappears in the detected area.

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

7. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as sensor alarm. Please refer to [Alarm In](#) section for details.

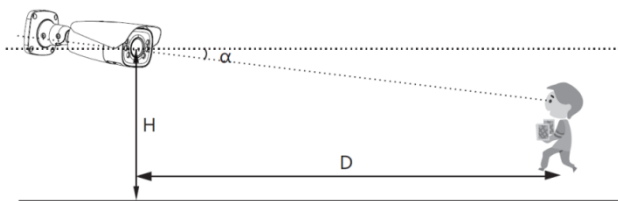
Face Capture View

After enabling face detection function, return to the live view interface. Click  to go to the following interface. When there are faces detected, the face pictures will be listed on the right. The features of captured faces also can be displayed, such as gender, whether to wear a mask, whether to wear glasses, age group, etc.



※ Configuration requirements of camera and surrounding area

1. Cameras must be installed in the area with stable and adequate light sources.
2. The installation height ranges from 2.0m to 3.5m, adjustable according to the focal length of different lenses and object distances.
3. The depression angle of the camera should be less than or equal to 15° .



4. The object distance depends on the focal-length of the lens mounted in the camera.
5. In order to guarantee the captured face recognition rate, the requirement for face capture are: left or right turn angle is less than about 30° ; pitching angle is less than 20° .
6. Face illumination must be uniform, if the brightness is low or there is a large area of shadow, need to do the light filling.
7. When dealing with backlight scenarios, enabling BLC, HLC, or WDR can help improve video quality and visibility. These features compensate for extreme lighting conditions and ensure better surveillance results.
8. The following scenes are not applicable, like crowded scenes (airport, railway station, square, etc), and so on.

3.5 Network Configuration

3.5.1 TCP/IP

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

IPv4	IPv6	PPPoE Config	IP Change Notification Config
☐ Obtain an IP address automatically			
☒ 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	192.168.226.1		
Alternate DNS Server	8.8.8.8		
			Save

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 needed.

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

Use PPPoE-Click the “PPPoE Config” tab to go to the interface as shown below. Click “Edit”, enable PPPoE and then enter the username and password from your ISP.

IPv4	IPv6	PPPoE Config	IP Change Notification Config
☐ Enable			
User Name			
Password			
			Edit

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

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

IPv4	IPv6	PPPoE Config	IP Change Notification Config
☐ Trigger Email			
☐ Trigger FTP			
			Save

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

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

the FTP server that has been set up.

3.5.2 Port

Go to *Config* → *Network* → *Port* as shown below.

HTTP Port	80
HTTPS Port	443
Data Port	9008
RTSP Port	554
RTSP over TLS	332
Subscription Listening Port	8080 ☒ Enable

Save

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

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

Data Port: The default data port is 9008. Please change it as necessary.

RTSP Port: The default port is 554. Please change it as necessary.

RTSP over TLS: Supports media stream transmission based on TLS channel encryption protection.

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

3.5.3 Server Configuration

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

☐ Enable

Server Port	2009
Server Address	
Device ID	1



Edit

1. Click “Edit” and then check “Enable”.
2. Check the IP address and port of the transfer media server in the NVMS. Then enable the auto report in the NVMS when adding a new device. Next, enter the remaining information of the device in the NVMS. After that, the system will automatically allot a device ID. Please check it in the 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. You can show or hide the sensitive data as needed.

3.5.4 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 password of ONVIF admin user can be modified 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 modify the password of admin separately in the following interface and add new users in the Onvif interface.

Index	User Name	User Type
1	admin	Administrator

Add User

User Name:

Password:

Level:

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

Confirm Password:

User Type:

OK Cancel

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

3.5.5 DDNS

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

1. Go to *Config* → *Network* → *DDNS*.

☐ Enable

Server Type:

User Name:

Password:

Domain:

Edit

2. Apply for a domain name. Take www.dvrddns.com for example.

Enter `www.dvrdydns.com` in the web address bar to visit its website. Then Click the “Registration” button.

NEW USER REGISTRATION

USER NAME	XXXX
PASSWORD	•••••
PASSWORD CONFIRM	•••••
FIRST NAME	xxx
LAST NAME	xxx
SECURITY QUESTION.	My first phone number. ▾
ANSWER	xxxxxxxx
CONFIRM YOU'RE HUMAN	718408 New Captcha Enter the text you see above
Submit Reset	

Create domain name.

You must create a domain name to continue.

Domain name must start with (a-z, 0-9). Cannot end or start, but may contain a hyphen and is not case-sensitive.

dvrdydns.com ▾

Request Domain

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.dvrdydns.com
Last Update: <i>Not yet updated</i> IP Address: 210.21.229.138		
Create additional domain names		

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

3.5.6 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**.

SNMP v1/v2	
☐ Enable SNMPv1	
☐ Enable SNMPv2	
Read SNMP Community	public
Write SNMP Community	private
Trap Address	192. ***. ***. 201
Trap Port	162
Trap community	public

SNMP v3	
☐ Enable SNMPv3	
Read User Name	public
Security Level	auth, priv
Authentication Algorithm	☒ MD5 ☐ SHA
Authentication Password	••••••••
Private-key Algorithm	☒ DES ☐ AES
Private-key Algorithm	••••••••
Write User Name	private
Security Level	auth, priv
Authentication Algorithm	☒ MD5 ☐ SHA
Authentication Password	••••••••
Private-key Algorithm	☒ DES ☐ AES
Private-key Algorithm	••••••••

Other Settings	
SNMP Port	161

 [Edit](#)

2. Click “Edit” and then check the corresponding version checkbox (Enable SNMPv1, Enable SNMPv2, Enable SNMPv3) according to the version of the SNMP software that will be used.
3. Set the values for “Read SNMP Community”, “Write SNMP Community”, “Trap Address”, “Trap Port” and so on. Please make sure the settings are the same as that of the SNMP software.

Note: Please use the different version in accordance with the security level you required. The higher the version is, the higher the level of security is.

3.5.7 802.1x

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.

☐ Enable

Protocol Type

EAP_MD5

EAPOL Version

1

User Name

Password

••••••

Confirm Password

••••••



Edit

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

Click “Edit” to start the setup.

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

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

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

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

3.5.8 RTSP

Go to *Config*→*Network*→*RTSP*.

☒ Enable	
Port	554
Address	rtsp://IP or domain name:port/profile1
	rtsp://IP or domain name:port/profile2
	rtsp://IP or domain name:port/profile3
Multicast address	
Main stream	239. *. *. *. 0 50554 ☐ Automatic start
Sub stream	239. *. *. *. 1 51554 ☐ Automatic start
Third stream	239. *. *. *. 2 52554 ☐ Automatic start
Audio	239. *. *. *. 3 53554 ☐ Automatic start
☐ Allow anonymous login (No username or password required)	
RTSP over TLS	
☐ Enable	
Port	332
Address	rtsp://IP or domain name:port/profile2
☐ Allow anonymous login (No username or password required)	
 Edit	

Click “Edit” and then select “Enable” to enable the RTSP function.

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

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

Multicast Address

Mainstream: 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.

RTSP over TLS: Enable RTSP stream encryption by using TLS.

Note: 1. The IP address mentioned above cannot be the address of IPv6.

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

3. 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.

3.5.9 RTMP

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

Go to **Config** → **Network** → **RTMP**.

☐ Enable (Please note: Some RTMP streaming services require audio to be enabled to work properly)	
Stream Type:	☒ Main stream ☐ Sub stream ☐ Third stream
Reconnect After Timeout	30 Second
Server Address	example: rtmp://127.***.***.1:1935/live
Connection Status	Not Connected Refresh
 Edit	

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

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

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

3.5.10 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.

☒ Enable
UPnP Name
Save

3.5.11 Email

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

Go to **Config** → **Network** → **Email**.

Sender	
Sender Address	
User Name	☐ Anonymous Login
Password	
Server Address	
Secure Connection	Unnecessary
SMTP Port	25
☐ Send Interval(S)	60 (10-3600)
Recipient	
 Edit and Test	

Click “Edit and Test” to set the sender and the recipient.

Sender Address: sender’s e-mail address.

Username and password: sender’s username 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 an 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.

3.5.12 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*.

Server Name	Server Address	Server Type	Port	User Name	Upload Path
FTP	10.15.239	FTP	21	anonymous	/

Add FTP

Server Name

Server Address

Upload Path

Port

User Name

Password

Server Type

Example/Dir/folder

21

FTPS

OK

Cancel

Add

Modify

Delete

Test

Save

2. Click “Edit and Test” and then click “Add” to add the information of the FTP. After that, click “Save” to save the settings.

- Server Name:** The name of the FTP server.
 - Server Address:** The IP address or domain name of the FTP.
 - Upload Path:** The directory where files will be uploaded to.
 - Port:** The port of the FTP server.
 - Username and Password:** The username and password that are used to login to the FTP server.
 - Server Type:** FTP or FTPS
3. In the event setting interface (like motion detection, region intrusion, line crossing, etc.), trigger FTP as shown below.

☒ Trigger FTP

Server Name

Server Address

Sub storage path&name

%a/MOTION/%4y-%2m-%2d/%4h/MOTION_%4y-%2m-%2d-%2h-%2n-%2s-%3u-%3i.*

Reset Default

Help

Trigger Alarm Out

☒ Alarm Out

Save

If “Trigger FTP” and “Attach Picture” are checked, the captured pictures will be sent to the FTP server address.

Sub Storage Path& Name: Click “Help” to view the rule and then set it as needed.

Meanings of the default Path & Name Settings (taking motion detection as an example):

“%0a/MOTION/%4y-%2m-%2d/%h” stands for sub storage path

“MOTION_%4y-%2m-%2d-%2h-%2n-%2s-%3u-%3i.*” stands for file name

When a motion alarm is triggered and “Trigger FTP” and “Attach Picture” are checked, a jpg file named “MOTION_Year Month Day Hour Minute Second_Event number” and a txt file named “MOTION_Year Month Day Hour Minute Second_Event number” will be generated under FTP root directory> MAC address>MOTION>Year-Month-Day>Hour

“MOTION” refers to the event type. You can modify the event name as needed (for example: Motion). You can also change the display order and contents of the sub storage path and file name.

If the sub storage path and name box is empty, the snapshot will be uploaded and named according to the default settings.

If you only enter the file name rule, the snapshot will be uploaded to the root directory of the FTP server.

3.5.13 HTTP POST

Go to *Config* → *Network* → *HTTP POST*.

Click “Edit” and then check “Enable” to enable push by subscription.

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

Push by Subscription: Push target trajectory (moving coordinate) to API test tool with a persistent connection. If enabled, the system will push the target trajectory upon detecting a

target. If disabled, the system will push the target trajectory only when triggering a smart event (such as line crossing detection, region intrusion detection, etc.)

Push By Subscription

☒ Enable

Subscription Listening Port 5080

Save

Actively Push

Add

Modify

Delete

Test

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

Actively Push: Click “Add” to add HTTP POST.

Add HTTP POST

☒ Enable

Protocol Type HTTP

Domain/IP 0.0.0.0

Server Port 80

Path

User Name

Password

Connection Type Persistent connection

Heartbeat Interval(Second) 90

Smart Alarm Data

☐ Select All

☒ Alarm status data

☐ Smart track data

☒ Smart event data

☒ Original picture

☒ Target picture

Smart Alarm Type

☒ Select All

☒ Motion Detection

☒ Alarm In

☒ Region Entrance

☒ Region Exiting

☒ Audio Exception

☒ Video Exception

☒ People Gathering Det...

☒ Loitering Detection

☒ Object Abandoned/Mis...

☒ Target Counting by L...

☒ Region Intrusion

☒ Illegal Parking Dete...

☒ Target Counting by A...

☒ Line Crossing

☒ Video Metadata

Enable

Enable

Send heartbeat

Save

Cancel

Protocol type: HTTP

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

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

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

Username and password: Please enable and enter as needed.

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

3.5.14 HTTPS

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

The screenshot shows the HTTPS configuration window. At the top, there are two checkboxes: "Enable" (checked) and "Disable HTTP" (unchecked). Below these, a section titled "Certificate installed" shows a default certificate with the text "C=US, ST=Some-State, O=embeddedsoftwar". To the right of this text is a button labeled "Replace Certificate". Below the certificate information, there is a table with two columns: "Attribute" and "Value". The "Attribute" column is empty, and the "Value" column contains the following text: "Issued to: C=US, ST=Some-State, O=embeddedsoftware, H=IPC, Issuer: C=US, ST=Some-State, O=embeddedsoftware, H=IPC, Validity date: 2024/10/21 16:38:58 ~ 2034/10/19 16:38:58". At the bottom of the window is a "Save" button.

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 a web browser (eg. https://192.168.226.201:443).

A private certificate can be created if users don’t want to use the default one. Click “Replace Certificate” to cancel the default certificate. Then the following interface will be displayed.

The screenshot shows the HTTPS configuration window after clicking "Replace Certificate". At the top, there are two checkboxes: "Enable" (checked) and "Disable HTTP" (unchecked). Below these, there is a section titled "Installation type" with three radio button options: "Have signed certificate, install directly" (selected), "Create a private certificate", and "Create a certificate request". Below this section, there is a section titled "Install certificate" with a text input field containing "Select File" and "No file selected", and a button labeled "Install". At the bottom of the window is a "Save" button.

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

This screenshot shows the 'Enable' settings interface. At the top, there is a checkbox labeled 'Enable'. Below it, the 'Installation type' section contains three radio button options: 'Have signed certificate, install directly', 'Create a private certificate' (which is selected), and 'Create a certificate request'. Under the 'Create a private certificate' option, there is a 'Create' button. At the bottom right of the interface is a 'Save' button.

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.

This screenshot shows the 'Enable' settings interface with 'Create a certificate request' selected. The 'Installation type' section has three radio button options: 'Have signed certificate, install directly', 'Create a private certificate', and 'Create a certificate request' (which is selected). Below this, the 'Create a certificate request' section has three buttons: 'Create', 'Download', and 'Delete'. The 'Install Created Certificate' section features a 'Select File' button, a text field showing 'No file selected', and an 'Install' button. A 'Save' button is located at the bottom right.

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.

3.5.15 Cloud Service

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

This screenshot shows the 'Cloud Service' settings interface. At the top, there is a checkbox labeled 'Enable' which is checked. Below it, the 'Visit Address' field contains the text 'https://www.autonat.com'. The 'Online State' is 'Offline', and there is a 'Refresh' button. Below these are 'Push Test' and 'Save' buttons. A message states 'Please use the mobile client to scan the code to add a device' above a QR code. Below the QR code is the 'Security Code' section, which includes the text 'Required when adding to Account/Cloud device list' and a row of ten input fields for the code. At the bottom left, there is a text field with '192.4872' and a 'Net bound' button.

After the device is successfully bound, you can unbind it via APP (go to the server list of the

APP and delete the device).

Note that after you bind the camera to your APP account, a verification code will be required when logging onto the web client by using the above-mentioned visit address.

3.5.16 QoS

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

Go to *Config* → *Network* → *QoS*.

Video/Audio DSCP	13
Alarm DSCP	35
Manager DSCP	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.

3.6 Security Configuration

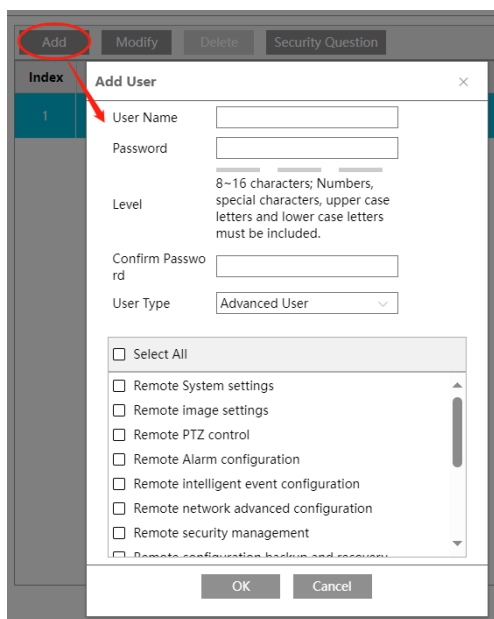
3.6.1 User Configuration

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

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

Add user:

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



2. Enter username in the “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** 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 if necessary, in the user configuration list box.
2. The “Edit user” dialog box pops up by clicking the “Modify” button.

×

Edit User

User Name

Old Password

New Password

✓

Level

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

Confirm Password

User Type

Administrator ▾

Modify Onvif Password

✓

☒ Select All

☒ Remote System settings

☒ Remote image settings

☒ Remote PTZ control

☒ Remote Alarm configuration

☒ Remote intelligent event configuration

☒ Remote network advanced configuration

☒ Remote security management

☐ Remote configuration backup and recovery

OK

Cancel

3. Enter the old password of the user in the “Old Password” text box.
4. Enter the new password in the “New password” and “Confirm Password” text box.
5. Select the user permissions for advanced or normal users.
6. Click the “OK” button to save the settings.

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 Settings: set the questions and answers for admin to reset the password after you forget the password.

3.6.2 Online User

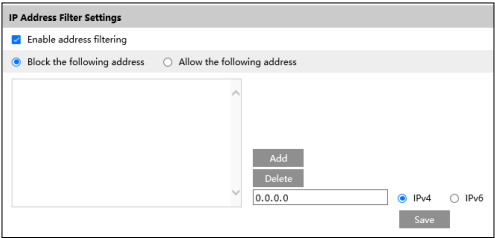
Go to **Config** → **Security** → **Online User** to view the user who is viewing the live video.

Index	Client Address	Port	User Name	User Type	Video Stream	
1	10.15.1.155	61588	admin	Administrator	1	<button>Kick Out</button>

In addition, you can also view the number of video streams, IP address, user type, etc. An administrator user can kick out all the other users (including other administrators).

3.6.3 Block and Allow Lists

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



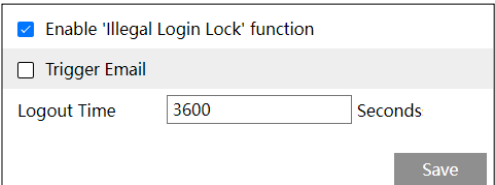
The setup steps are as follows:

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.

3.6.4 Security Management

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



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

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

- Password Security

Security Service	Password Security	Authentication
Password Level	Weak	
Expiration Time	Never	
		Save

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.

Authentication: you can set RTSP/HTTP authentication as needed.

Security Service	Password Security	Authentication
RTSP		
Authentication	Basic	
API Services		
☒ Enable		
Authentication	Basic	
Subscribe to push services		
Authentication	Basic	
		Save

RTSP Authentication: Digest or basic can be selected.

API Service Authentication: Digest or basic can be selected.

Push Subscription Authentication: Digest or basic can be selected.

3.7 Maintenance Configuration

3.7.1 Backup and Restore

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

The screenshot displays a web-based configuration interface for a camera. It is divided into four main sections, each with a title bar and a corresponding button:

- Import Setting:** Contains a 'Path' label, a text input field with 'Select File' and 'No file selected' buttons, and an 'Import Setting' button.
- Export Settings:** Contains an 'Export Settings' button.
- Restore Default Parameters:** Contains a 'Keep' label, a list of three checkboxes ('Network Config', 'Security Configuration', 'Image Configuration'), and a 'Restore Default Parameters' button.
- Restore Factory Settings:** Contains a 'Restore Factory Settings' button.

● Import & Export Settings

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

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

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

* The customized audio files are not supported by exporting or importing.

● Restore Default Parameters

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

● Restore Factory Settings

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

3.7.2 Reboot

Go to **Config** → **Maintenance** → **Reboot**.

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

Scheduled Reboot Setting:

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

3.7.3 Upgrade

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

⚠ Downgrading from the current version to a previous version is not allowed.
Do not disconnect power during the upgrade.
Do not refresh or close this page during the upgrade.

Local upgrade

Path No file selected

🔥 System 2: Normal | System 1: Normal

Cloud Upgrade

Upgrade Options

Current Version 5.3.0.5808B240930.JF3.U1(13A11).beta

Export Upgrade Log

● Local Upgrade

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

Note: If “Back up and upgrade” is selected, the configuration file will be exported to your local PC before starting upgrading.

● Cloud Upgrade

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

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

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

Caution:

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

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

affected, and the camera still can work normally. You can also upgrade your camera through the normal system.

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

3.7.4 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.

3.7.5 Serial Output

Serial output mode is used to record and collect the required system data, so that the technician can quickly find out and analyze the problem and help us to improve service. Before enabling the mode, you are advised to consult our technical support.

☒ Enable	
Debug Level	RUN/WARN/ERROR
Save	

3.7.6 Maintenance Information

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

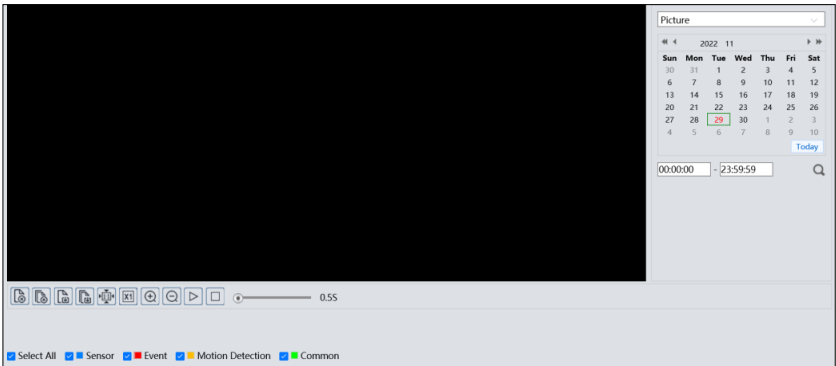
4 Search

4.1 Image Search

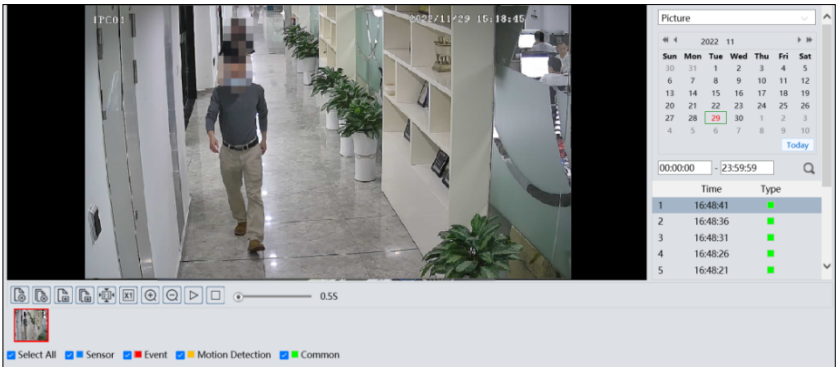
Click Search to go to the interface as shown below. Images that are saved on the SD card can be found here.

● SD Card Image Search

1. Choose “Picture”.



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



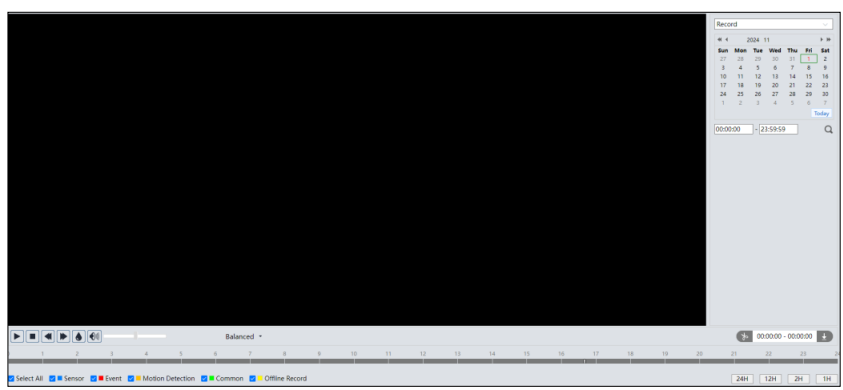
The descriptions of the buttons are shown as follows.

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.		

4.2 Video Search

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

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



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



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

Note: *1.  and  cannot be displayed in the above interface via the plug-in free browser.

*2. For plug-in free playback, playback mode switch (balanced/real-time/fluent mode) and downloading functions are not supported too.

*3. For the fluent playback, it is recommended to use the plug-in required browser to play the recorded video with 2MP or above resolution.

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

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

Appendix

Appendix 1 Troubleshooting

How to find the password?

A: The password for *admin* can be reset through “Edit Safety Question” function. Click “Forget Password” in the login window and then enter the corresponding answer of the selected question in the popup window. After you correctly answer all questions, you can reset the password for *admin*. If you forget the answer of the question, this way will be invalid, please contact your dealer for help.

B: The passwords of other users can be reset by *admin*.

Fail to connect devices via a web browser.

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

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

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

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

IP tool cannot search devices.

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

No sound can be heard.

A: Audio input devices are not connected. Please connect and try again.

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