GeoVision inc
The Vision of Security

GV-AI ISP Camera

User's Manual

- GV-GBLN4800
- GV-GDRN4800
- GV-GEBN4800

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

AIISP-UM-B

Every effort has been made to ensure that the information in this manual is accurate. GeoVision, Inc. makes no expressed or implied warranty of any kind and assumes no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages arising from the use of the information or products contained herein. Features and specifications are subject to change without notice.

GeoVision, Inc.
9F, No. 246, Sec. 1, Neihu Rd.,
Neihu District, Taipei, Taiwan
Tel: +886-2-8797-8377
Fax: +886-2-8797-8335
http://www.geovision.com.tw

January 2026

Scan the following QR codes for product warranty and technical support policy:

[Warranty]

[Technical Support Policy]

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

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

About the Manual

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

Use of the Product

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

attempt to use the product or the software, by hacking, stealing the password, or any other means.

Electrical Safety

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

Environment

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

Operation and Daily Maintenance

- There are no user-serviceable parts inside. Please contact the nearest service center if the product does not work properly.
- Please shut down the device and then unplug the power cable before you begin any maintenance work.
- ⚠ Warning: All the examination and repair work should be done by qualified personnel.
- Do not touch the CMOS sensor optic component. You can use a blower to clean the dust on the lens surface.

- Always use a dry soft cloth to clean the device. If there is too much dust, use a cloth cleaning (such as using cloth) may result in poor IR/illumination LEDs functionality and/or IR/illumination LEDs reflection.

- The dome cover is an optical device, please don't touch or wipe the cover surface directly during installation and use. For dust, use an oil-free soft brush or hair dryer to remove it gently; for grease or finger print, use oil-free cotton cloth or paper soaked with detergent to wipe from the lens center outward. Change the cloth and wipe it several times if it is not clean enough.
- The IR LEDs should at no time be covered when the camera is running to prevent overheating and the possible risk of fire.

Privacy Protection

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

Disclaimer

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

Cybersecurity Recommendations

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

- It is recommended to change the service default ports (like HTTP-80, HTTPS-443, etc.) to reduce the risk of outsiders being able to access.
- It is recommended to set the firewall of your router. But note that some important ports cannot be closed (like HTTP port, HTTPS port, Data Port).

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

Regulatory Information

FCC Information

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

1. FCC compliance

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

2. FCC conditions:

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

RoHS

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

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

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

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

Contents

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	i7-117000 2.5GHz or higher
GPU	/	AMD770+intel UHD Graphics 750
RAM	1G or higher	8G or above
Display	1920*1080 resolution or higher	

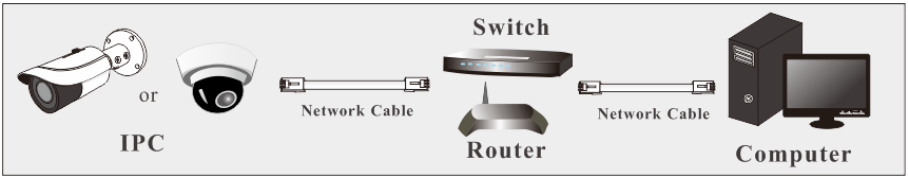
Web browser: Chrome89.0+/Edge89.0+/Firefox87.0+/Safari14.0+
It is recommended to use the latest version of these web browsers.
The menu display and operation of the camera may be slightly different by using the browser with plug-in or without plug-in. Installing the plug-in will display more functions of the camera.
Connect IP camera via LAN or WAN. Here only take the plug-in required browser for example. The details are as follows:

1.1 LAN

In LAN, there are two ways to access IP camera: 1. access through GV-IP Device Utility; 2. direct access through the Edge browser.

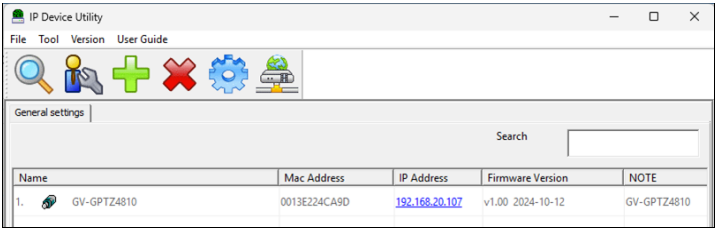
1.1.1 Access through GV-IP Device Utility

Network connection:

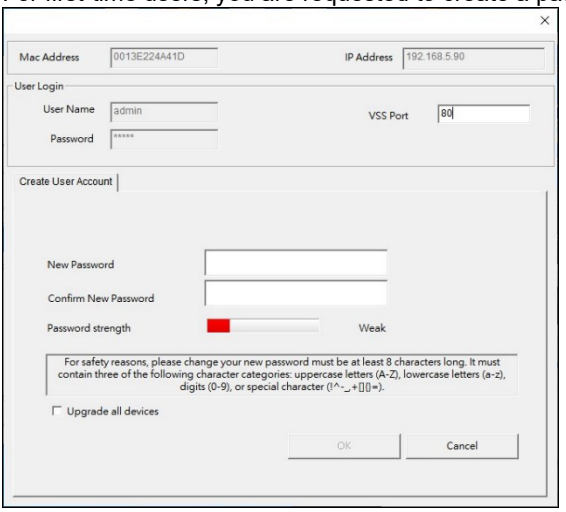


1. Make sure the PC and the camera are connected to the same LAN, and **GV-IP Device Utility** is installed on the PC from our website.
2. On the GV-IP Device Utility window, click the button to search for IP devices connected to the same LAN. To sort, click the **Name** or **Mac Address** column.

3. Find the camera with its Mac Address, and click on its IP address.



4. For first-time users, you are requested to create a password.



5. Type a new password and click **OK.**
6. Click its IP address on the Utility window again, and select **Web Page** to access its Web interface.
7. Type the set password on the login page, and click **Login**.

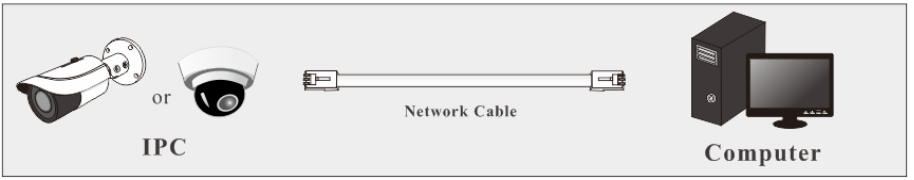
Note:

1. The Administrator's default username is **admin** and cannot be modified.
2. To change the password using the GV-IP Device Utility, click on the camera's IP address, and select **Configure** > **Change Password**. Alternatively, you can change the password on the camera's Web interface by clicking **Config** > **Security** > **User**; see "Modify User" in *3.7.1 Security Configuration*.

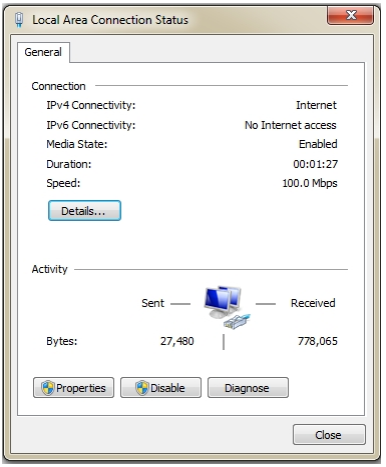
1.1.2 Directly Access via Web Browser

The default network settings are as shown below:
IP address: **192.168.0.10**
Subnet Mask: **255.255.255.0**
Gateway: **192.168.226.1**
HTTP: **80**
Data port: **9008**

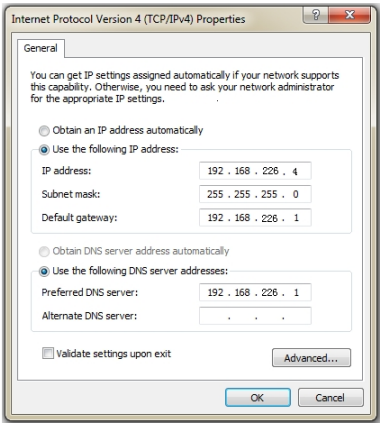
Use the above default settings when logging in the camera for the first time. Directly connect the camera to the computer through network cable.



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



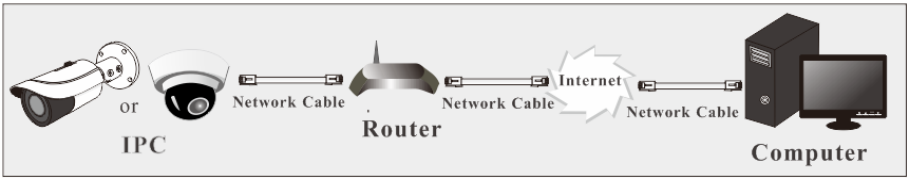
Select “Properties” and then select internet protocol according to the actual situation (for example: IPv4). Next, click the “Properties” button to set the network of the PC.



② Open a web browser and enter the default address of IP camera and confirm.
③ Follow directions to download and install the plug-in.
④ Enter the default username and password in the login window and then enter to view.

1.2 WAN

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

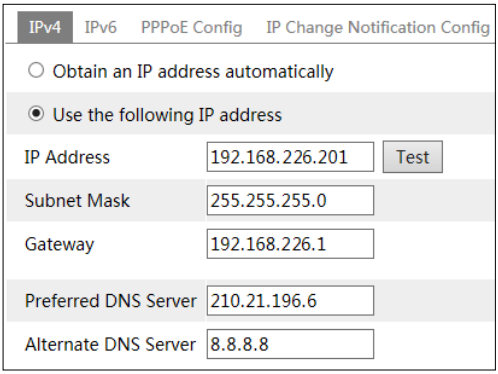


① Make sure the camera is connected to the local network and then log in the camera via LAN and go to **Config→Network→Port** to set the port number.

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

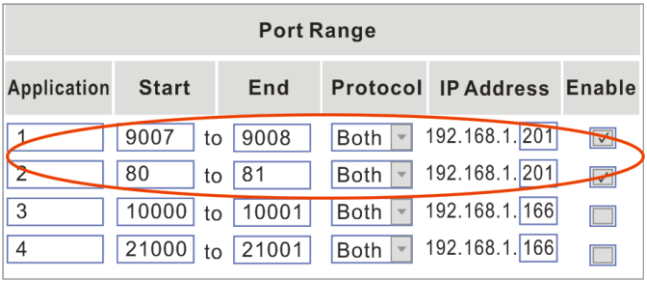
Port Setup

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



IP Setup

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

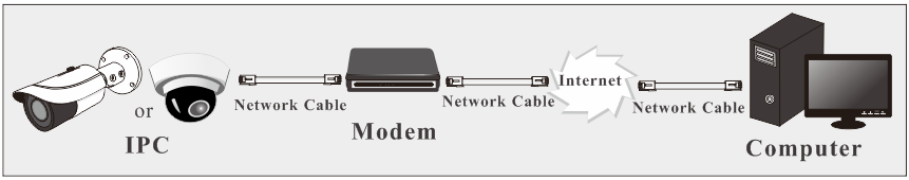


Router Setup

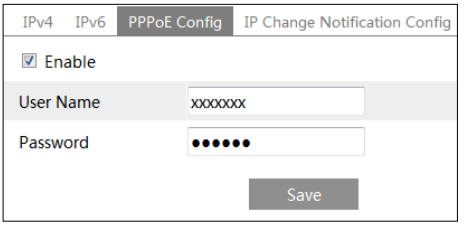
④ Open a web browser and enter its WAN IP and http port to access. (for example, if the http port is changed to 81, please enter "192.198.1.201:81" in the address bar of web browser to access).

➢ **Access through PPPoE dial-up**

Network connection



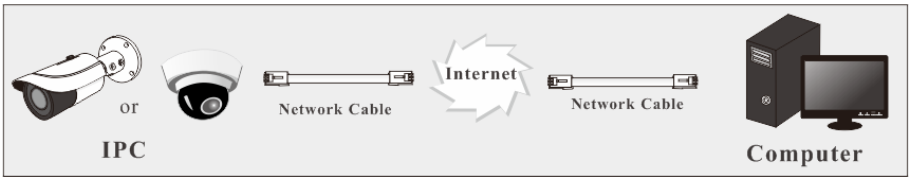
Access the camera through PPPoE auto dial-up. The setup steps are as follow:
① Go to **Config→Network→Port** to set the port number.
② Go to **Config →Network→TCP/IP→PPPoE Config**. Enable PPPoE and then enter the user name and password from your internet service provider.



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**

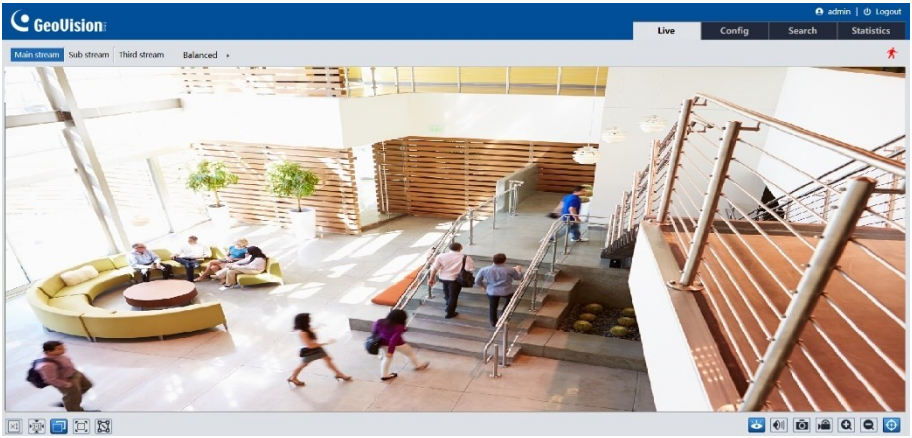
Network connection



The setup steps are as follow:
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. The Live View

After logging in, the live view window will be displayed as shown below.



Note: For plug-in free live view

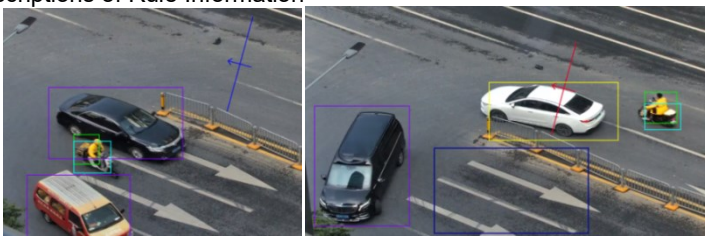
- When the main stream is set over 1080P, only the sub stream or third-stream tab can be displayed on the live view interface.
- Local recording is not supported and the preview mode switch (real-time/balanced/fluent mode) is not available too.

The descriptions of the icons on the live view interface are as follows:

Icon	Description	Icon	Description
	Original size		Motion alarm indicator
	Fit correct scale		Color abnormal indicator
	Auto (fill the window)		Abnormal clarity indicator
	Full screen		Scene Change indicator
	Measure Tool		Audio exception indicator
	Start/stop live view		Line crossing indicator
	Enable/disable audio		Intrusion indicator
	Snapshot		Region entrance indicator
	Start/stop local recording		Region exiting indicator

Icon	Description	Icon	Description
	Zoom in		Face detection indicator
	Zoom out		Target counting (by line) indicator
	Face Detection (when face event is selected)		Object detection indicator (object abandoned/missing)
	Rule information display		SD card recording indicator

- Measure Tool: get the height and width pixel of the selected region in the live view interface. (This function is only available for main stream). Click and drag the mouse on the image to draw a desired box. The width and height pixel will directly display in the box.
- In full screen mode, double click on the mouse to exit or press the ESC key on the keyboard.
- 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

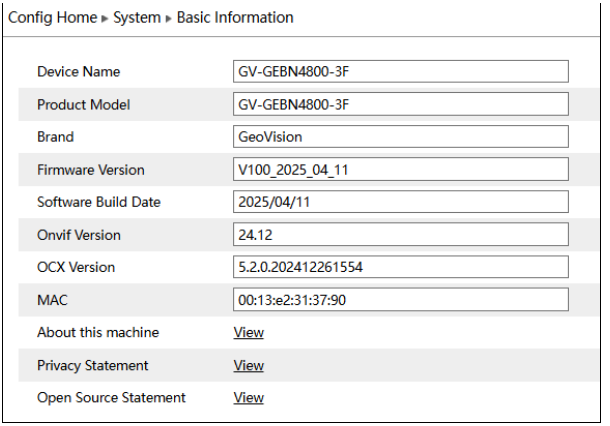
3. Network Camera Configuration

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

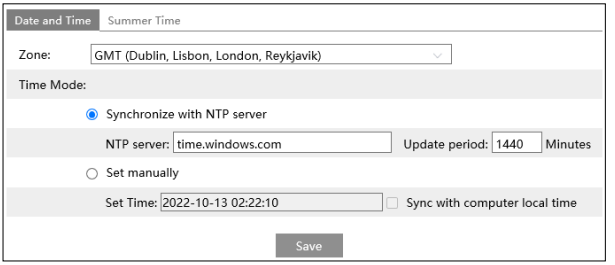
3.1.1 Basic Information

In the Basic Information interface, you can check the relative information of the device.



3.1.2 Date and Time

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



Select the time zone and time mode as needed.

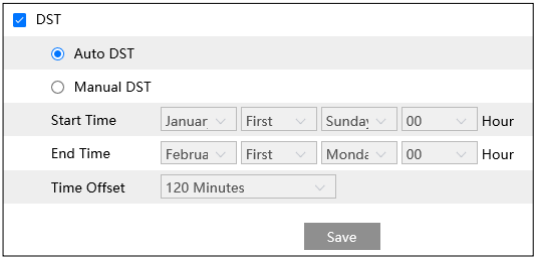
Note: The time zone of the camera and the computer must be the same. It is recommended to modify the time zone of the camera according to the time zone of the computer. If the time zone of the computer is modified, the current web client needs to be closed. Then re-open it and log in again.

Time Mode:

NTP: Specify an NTP server to synchronize the time.

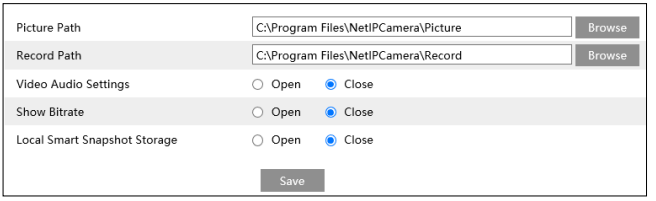
Manual: Set the system time manually or you can synchronize the time with the time of the local computer.

Click the "Summer Time" tab to set DST (Daylight Saving Time) as needed.



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.



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

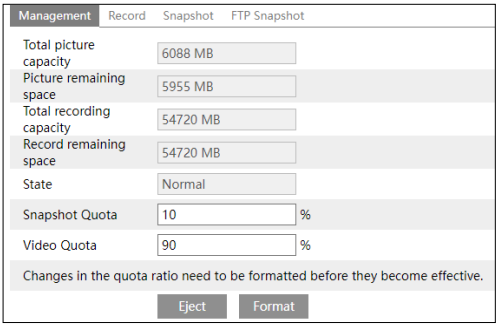
Additionally, "Local smart snapshot storage" can be enabled or disabled here. If enabled, the captured pictures triggered by smart events will be saved to the local PC.

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

Note: If your camera doesn't support the SD card storage function, please skip the following instructions.

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



- **SD Card Management**

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

Click the “Eject” button to stop writing data to the SD card. Then the SD card can be ejected safely.

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

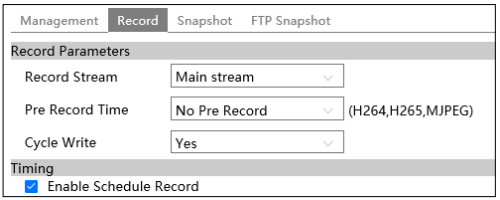
Video Quota: Set the capacity proportion of record files on the SD card.

Note: This series of products support ANR (Automatic Network Replenishment) function.

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

- **Schedule Recording Settings**

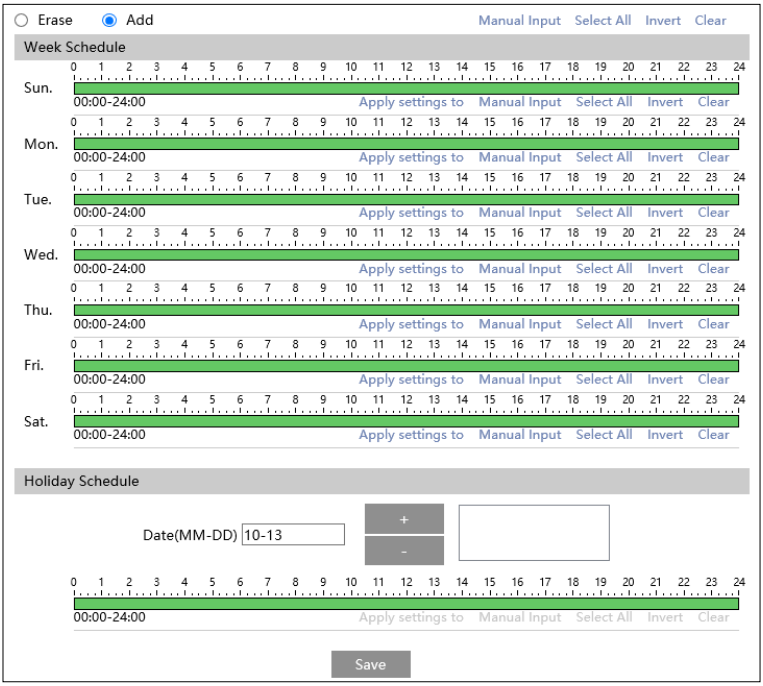
1. Go to **Config→System→Storage→Record** to go to the interface as shown below.



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

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

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

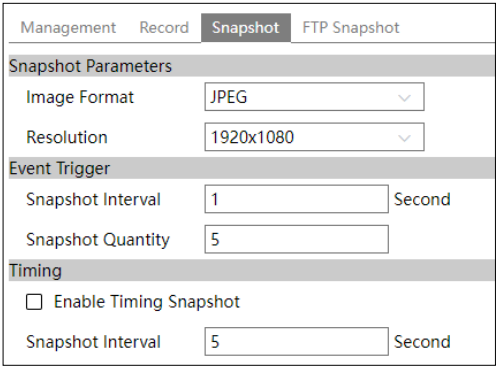


Weekly schedule
Set the alarm time from Monday to Sunday for a single week. Each day is divided into one- hour increments. Green means scheduled. Blank means unscheduled.
“Add”: Add the schedule for a special day. Drag the mouse to set the time on the timeline.
“Erase”: Delete the schedule. Drag the mouse to erase the time on the timeline.
Manual Input: Click it for a specific day to enter specific start and end times. This adds more granularities (minutes).

Day schedule
Set the alarm time for a special day, such as a holiday.
Note: Holiday schedule takes priority over weekly schedule.

- **Snapshot Settings**

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

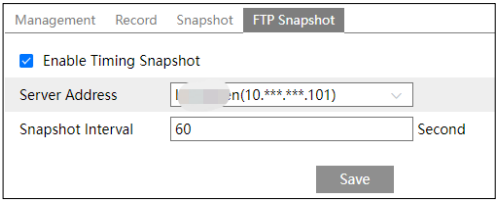


Set the format, resolution and quality of the image saved on the SD card and the snapshot interval and quantity and the timing snapshot here.
Snapshot Quantity: The number you set here is the maximum quantity of snapshots. The actual quantity of snapshots may be less than this number. Supposing the occurrence time of an alarm event is less than the time of capturing pictures, the actual quantity of snapshots is less than the set quantity of snapshots.

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

- **FTP Snapshot**

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

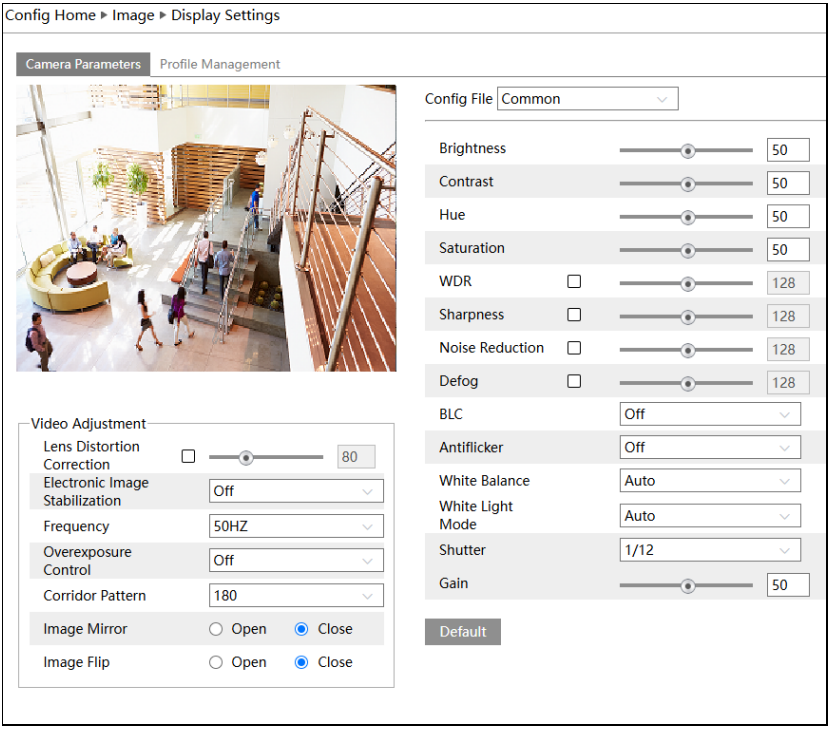


Server Address: select the set FTP server. See FTP for the FTP server setting.

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.



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.

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.

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. (Only some models support this function)

Image Mirror: Turn the current video image horizontally.
Image Flip: Turn the current video image vertically.

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 (only some models support this function) .
Backlight Compensation (BLC):

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

Antiflicker:

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

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

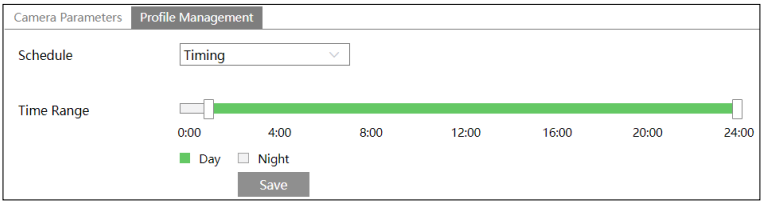
If "White light" is selected, overexposure control and white light mode can be set.
White light mode: Choose "Off", "Auto" or "Manual". Please select it as needed.

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

Note: For some items (like frequency), if selected/enabled, the camera will reboot automatically. After that, clicking "Default" button will not take effect.

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

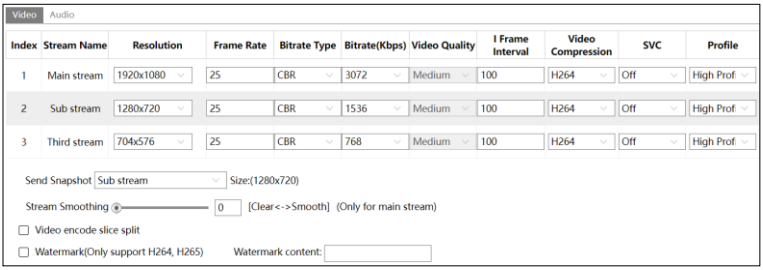
Set full time schedule for common, auto mode and specified time schedule for day and night.
Auto mode: in the daytime, it will automatically perform the day config file set above; at night, it will automatically perform the night config file set above.
Choose “Timing” in the drop-down box of schedule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



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

3.2.2 Video / Audio Configuration

Go to **Image→Video / Audio** interface as shown below. In this interface, set the resolution, frame rate, bitrate type, video quality, and so on subject to the actual network condition.
Note: the video stream parameters of different camera series may be different. The following pictures and descriptions are for reference only. The real camera interface shall prevail.



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 main stream. If H.265/H.265+is chosen, make sure the client system can 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.

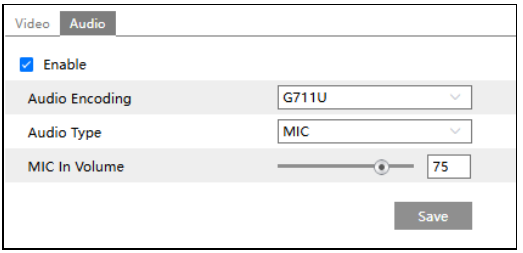
Note: Some models may support H264S (Smart H.264)/H265S(Smart H.265). Compared to H.265+/H.265, smart H.265 can spontaneously adjust the bitrate distribution according to the requirements of the actual scene. For example, when there is no human or vehicle detected, the bitrate will be automatically reduced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

SVC：Only some models support this function. Scalable Video Coding (SVC) is able to extract one or more subset bit streams with different frame rates from a bit stream.

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

Send Snapshot: Set the snapshot stream.
Stream Smoothing: Only some models support this function. Drag the progress bar or set the stream smoothing value as needed. The higher the value is, the better fluency of the stream is, but the video quality is reduced. The lower the value is, the clearer the image is.
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.

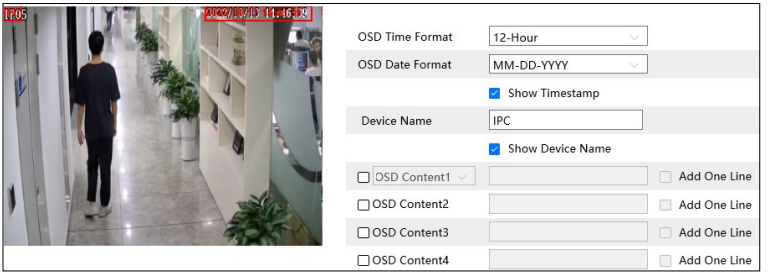
Click the “Audio” tab to go to the interface as shown below.



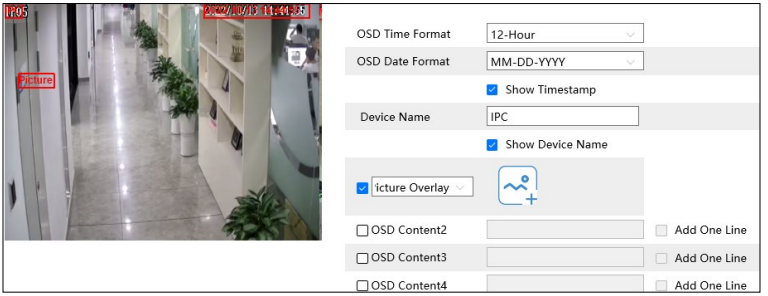
Audio Encoding: G711A and G711U are selectable.
Audio Type: MIC or LIN. (If the internal MIC is supported and used, choose “MIC”. If your camera supports audio input and an external line-level audio input device is also used, choose “LIN”.)
MIC IN Volume: Set the volume as needed.

3.2.3 OSD Configuration

Go to **Image→OSD** as shown below.



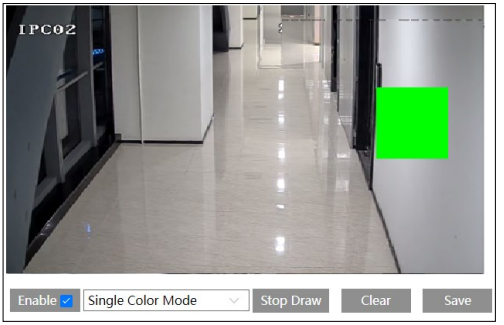
Set time stamp, device name, OSD content and picture overlap here. After enabling the corresponding display and entering the content, drag them to change their position. Then click the “Save” button to save the settings.
The quantities of the OSD items are different for different models.



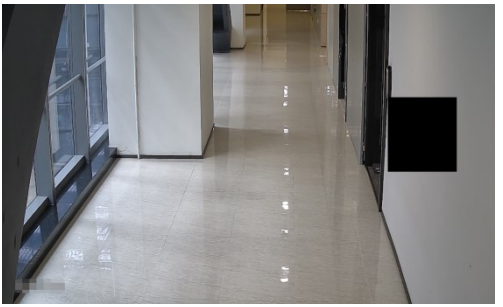
Picture Overlap Settings (This function is only available for some models):
Check “OSD Content1”, choose “Picture Overlay” and click to select the overlapping picture. Then click “Open” to upload the overlapping picture. The pixel of the image shall not exceed 200*200, or it cannot be uploaded.

3.2.4 Video Mask

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



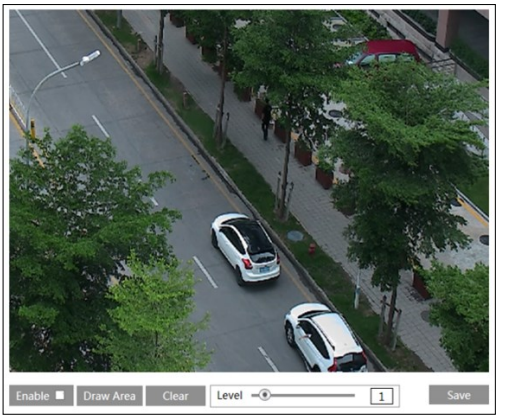
To set up a video mask:
1. Enable video mask.
2. Click the “Draw Area” button and then drag the mouse to draw the video mask area.
3. Click the “Save” button to save the settings.
4. Return to the live to verify that the area has been drawn as shown as blocked out in the image.



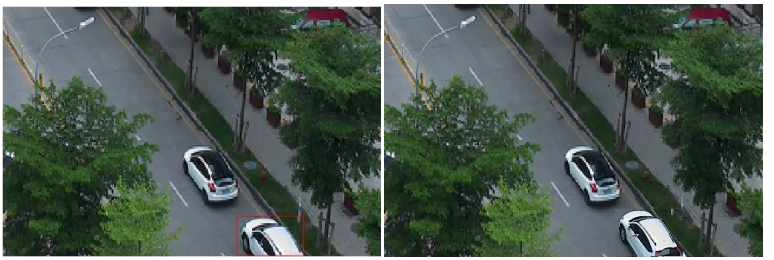
To clear the video mask:
Click the “Clear” button to delete the current video mask area.

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.



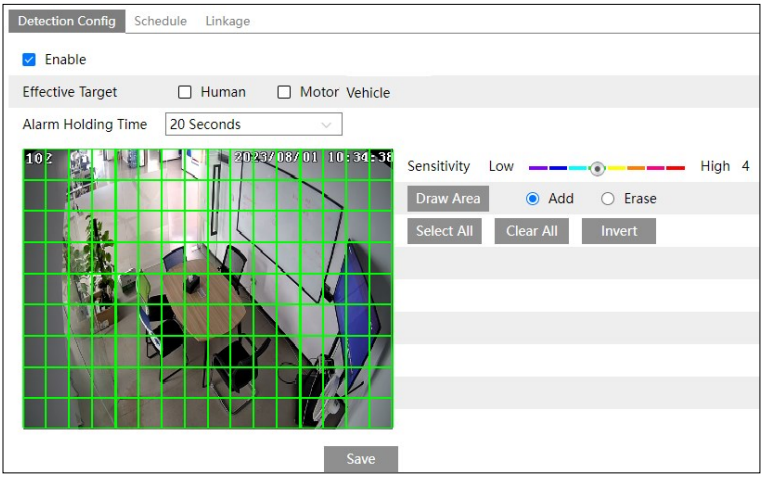
1. Check “Enable” and then click the “Draw Area” button.
2. Drag the mouse to set the ROI area.
3. Set the level.
4. Click the “Save” button to save the settings.



3.3 Alarm Configuration

3.3.1 Motion Detection

Go to **Alarm→Motion Detection** to set the 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”. For some models, you can only choose “Human”. 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 a moving object appears on the image, including human, vehicle or other moving objects. (Under face event mode, this function is not available)

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

2. Set motion detection area and sensitivity.

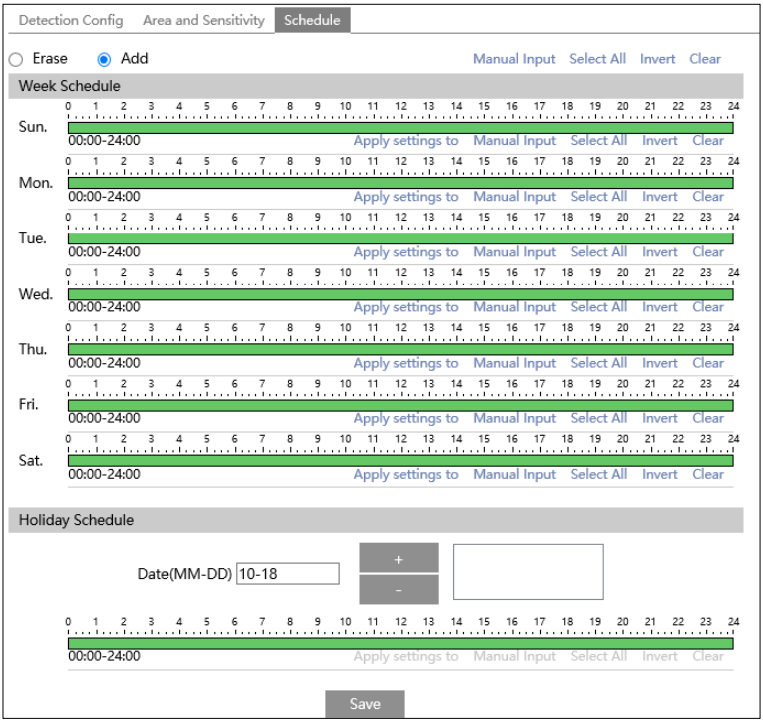
Move the “Sensitivity” scroll bar to set the sensitivity. A higher sensitivity value means that motion will be triggered more easily. The area without colored grids means the sensitivity value is 0, which will be considered as a blocked area.

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

Select “Erase” and drag the mouse to clear motion detection area.

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

3. Set the schedule for motion detection.



Weekly schedule

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

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

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

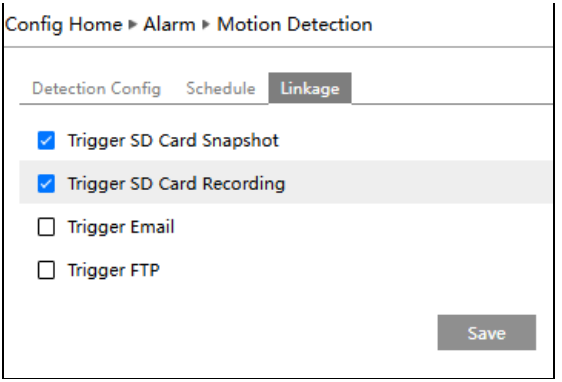
Manual Input: Click it for a specific day to enter specific start and end times. This adds more granularities (minutes).

Day schedule

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

Note: Holiday schedule takes priority over weekly schedule.

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



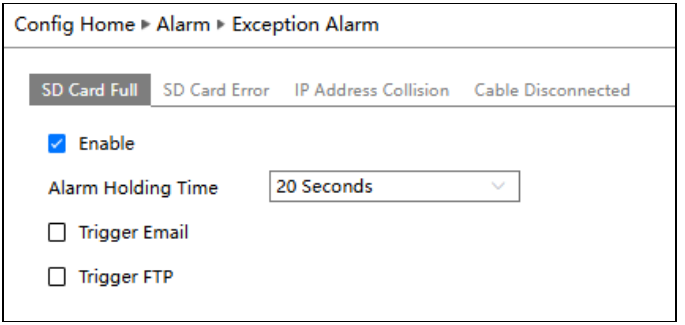
Trigger SD Card Snapshot: If selected, the system will capture images on motion detection and save the images on an SD card.
Trigger SD Card Recording: If selected, the video will be recorded on an SD card on motion detection.
Note: Only the camera with the SD card storage function supports “Trigger SD Card Snapshot/Recording”.
Trigger Email: If “Trigger Email” and “Attach Picture” are checked (email address must be set first in the Email configuration interface), the captured pictures and triggered event will be sent to those addresses. (Only some models support this function)
Trigger FTP: If “Trigger FTP” and “Attach Picture” are checked, the captured pictures will be sent to the FTP server address. Please refer to the FTP configuration section for more details. (Only some models support this function)

3.3.2 Exception Alarm

Note: Only the camera with the SD card storage function supports SD card full and SD card error alarms.

- **SD Card Full**

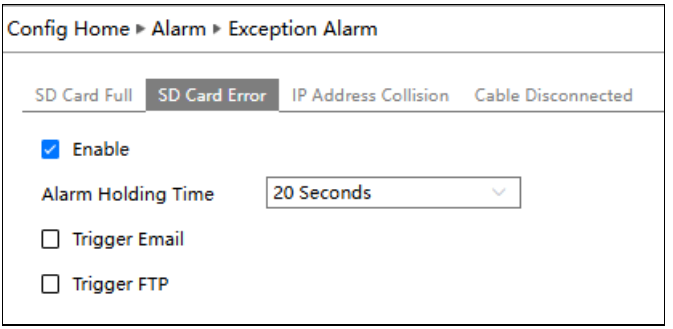
1. Go to **Config→Alarm→Exception Alarm→SD Card Full**.



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

- **SD Card Error**

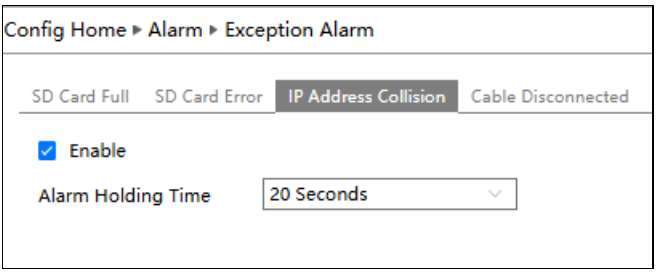
When there are some errors in writing to the SD card, the corresponding alarms will be triggered.
1. Go to **Config→Alarm→ Exception Alarm →SD Card Error** as shown below.



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

- **IP Address Conflict**

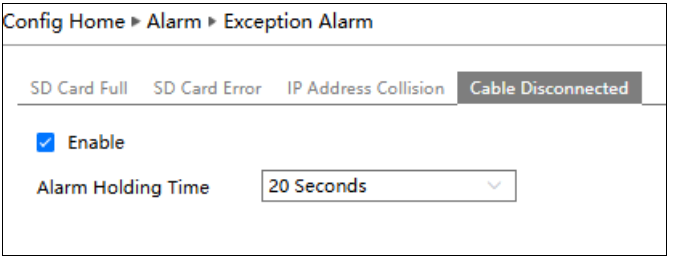
1. Go to **Config→Alarm→ Exception Alarm→IP Address Collision** as shown below.



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

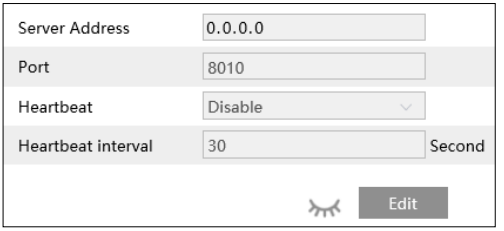
Go to **Config→Alarm→ Exception Alarm →Cable Disconnected** as shown below.



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 Server

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

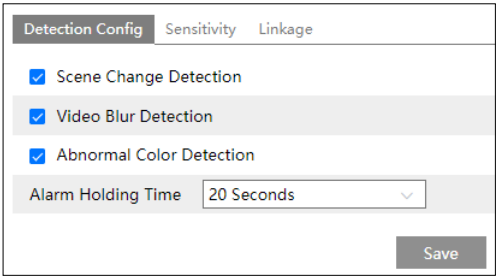


Click “Edit” to set the alarm server.
Set the server address, port, heartbeat and heartbeat interval. When an alarm occurs, the camera will transfer the alarm event to the alarm server. If an alarm server is not needed, there is no need to configure this section.

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

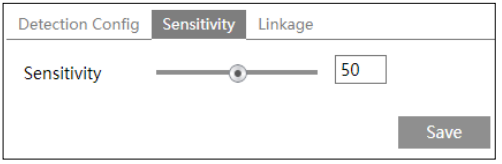
3.3.4 Video Exception

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



1. Enable the applicable detection that’s desired.
Scene Change Detection: Alarms will be triggered if the scene of the monitor video has changed.
Video Blur Detection: Alarms will be triggered if the video becomes blurry.
Abnormal Color Detection: Alarms will be triggered if the image is abnormal because of color deviation.
2. Set the alarm holding time.
3. Click “Save” button to save the settings.

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

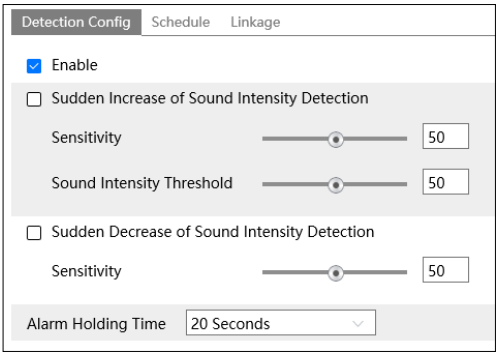


Drag the slider to set the sensitivity value or directly enter the sensitivity value in the textbox. Click “Save” button to save the settings.
The sensitivity value of Scene Change Detection: The higher the value is, the more sensitive the system responds to the amplitude of the scene change.
The sensitivity value of Video Blur Detection: The higher the value is, the more sensitive the system responds to the blurriness of the image.
The sensitivity value of Abnormal Color Detection: The higher the value is, the more sensitive the system responds to the color shift of the image.
5. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as those for 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 the 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.

3.3.5 Audio Exception

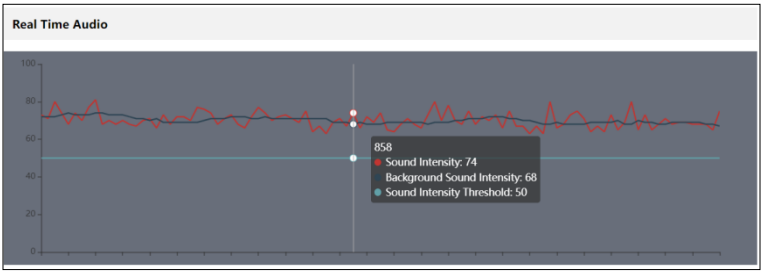
Only some models support this function.
Alarms will be triggered when the abnormal sound is detected in the surveillance scene, such as the sudden increase/decrease of the sound intensity.
To set audio exception detection:
1. Go to **Alarm→Audio Exception** as shown below.



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 sounds, 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.

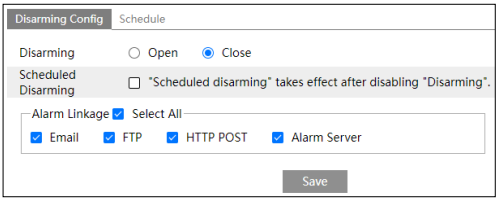


4. Set the alarm holding time and click “Save” to save the settings.
5. Set the schedule of audio exception detection. The setup steps of the schedule are the same as the schedule recording (See Schedule Recording).
6. Click “Linkage” to configure the alarm linkage items. The alarm linkage setup steps are the same as those for motion detection. Please refer to Motion Detection 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.

3.3.6 Disarming

Only some models support this function.
You can disarm alarm linkage actions quickly in this interface.



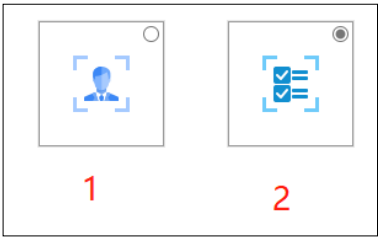
Disarming: If enabled, the system stops triggering alarm linkage actions immediately.
Scheduled Disarming: The system stops triggering alarm linkage actions in the selected period. Close disarming and check “Scheduled Disarming”. Then click “Schedule” to set the schedule. The setup steps of the schedule are the same as the motion detection schedule settings (See Motion Detection for details).

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:

*** Face events and smart events cannot be enabled at the same time.**

*** 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 the reduction in performance and affect the detection results. Please enable smart events according to the actual performance of your camera.**

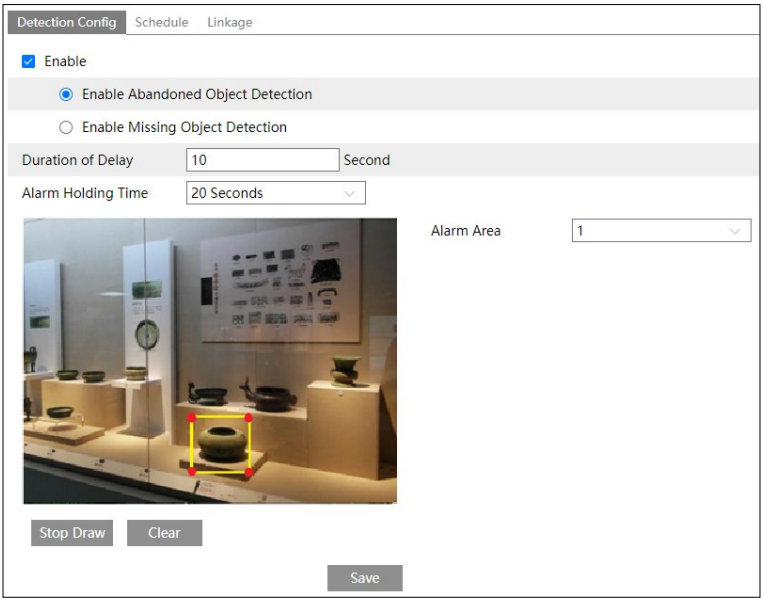
*** Smart events may vary by models. If your camera doesn't support one or more of the following events, please skip the relevant instructions.**

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.



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.

Duration of Delay: 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

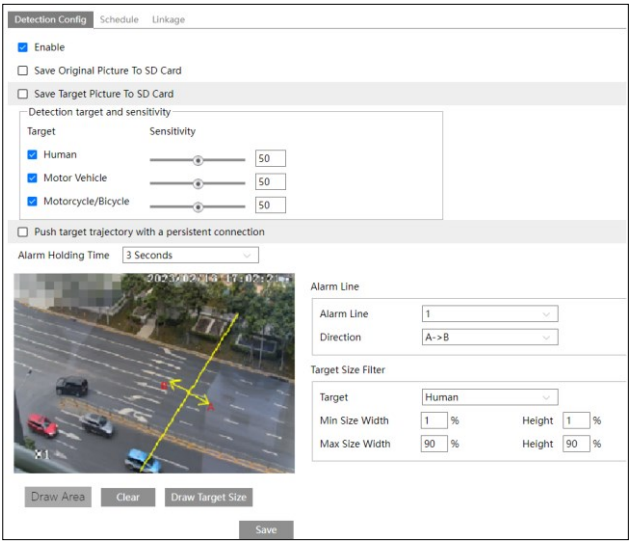
delete the alarm area. Click the “Save” button to save the settings.
4. Click the “Save” button to save the settings.
5. Set the schedule of abandoned/missing object detection. The setup steps of the schedule are the same as the motion detection schedule settings (See Motion Detection for details).
6. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as those for motion detection. Please refer to Motion Detection for details.

※ The Configuration requirements of the 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.



1. Enable line crossing 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 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.

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.

(For some models, only “Human” can be selected.)

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.

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 a line crossing alarm. (Only some models support this function)

2. Set the alarm holding time.
3. Set alarm lines 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.

To set target size filter:
Some models don’t support target size filter. If your camera doesn’t support it, please skip the following instructions.
Click “Draw Target Size” to draw the maximum and minimum size of a specific target as shown below.

Target: choose “Human”, “Motor Vehicle” or “Motorcycle/Bicycle” as needed.
Green box is the maximum target detection box; yellow box is the minimum target detection box.
Click the green box to edit the maximum target detection box; click the yellow box to edit the minimum target detection box.
Drag one of 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.
4. Click “Save” button to save the settings.
5. 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 alarm linkage setup steps are the same as those for motion detection. Please refer to Motion Detection 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.

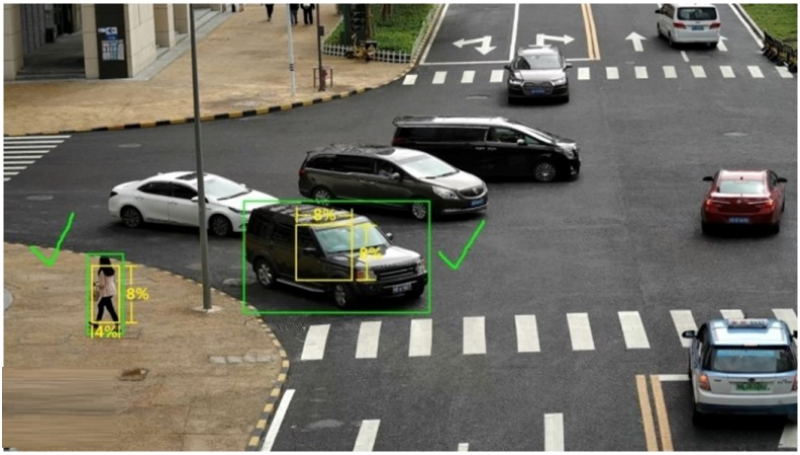
For vehicles, the depression angle should not be more than the recommended value. The sideways or horizontal viewing angle is recommended on a video (see below).

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% × 8%	8% × 8%	4% × 4%
Maximum (Width × Height)	50%× 50%	50%× 50%	50%× 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 =1920x4%=80, h=1920x8%=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.

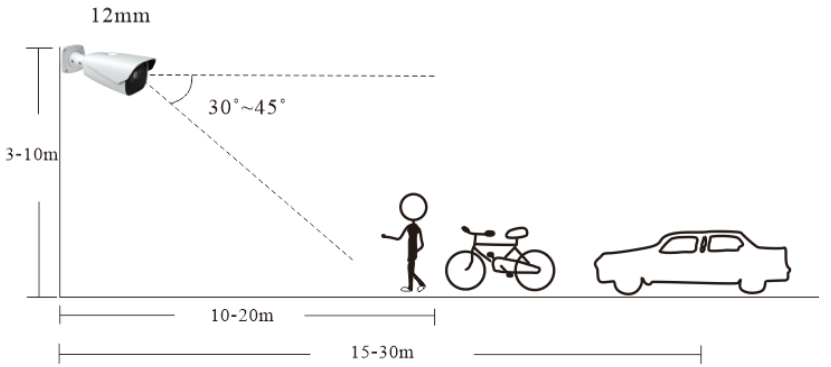
Wrong example

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:

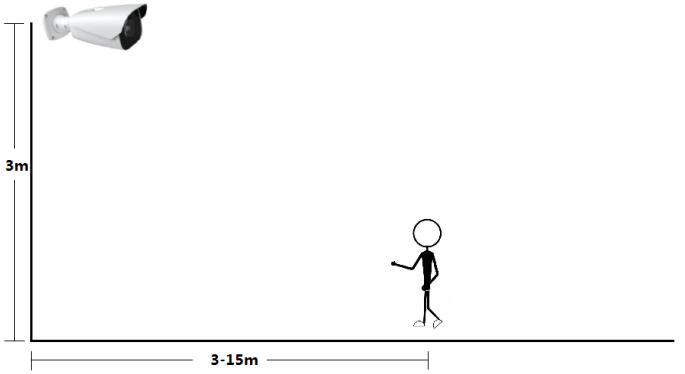
Outdoor mounting:
The optimal detection distance varies due to different focal length. Please refer to the following table.

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 for 12mm focal length

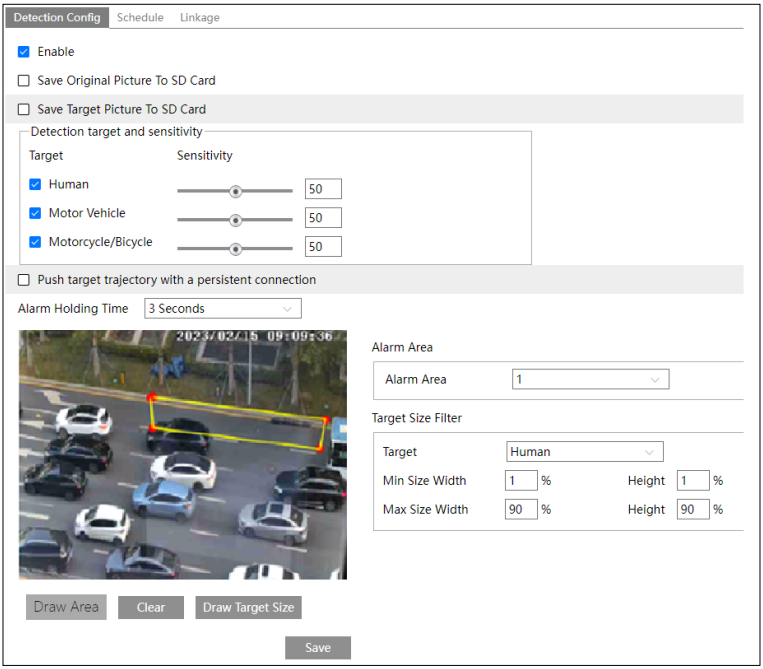
Indoor Mounting



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.



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.

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.

For some models, only “Human” can be selected.

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.
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 a region intrusion alarm.(Only some models support this function)
2. Set the alarm holding time.
3. Set alarm areas 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.

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 alarm linkage setup steps are the same as those for motion detection. Please refer to Motion Detection 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

Region Entrance: Alarms will be triggered if the target enters the pre-defined areas.
Go to **Config→Event→Region Entranc**e.
1. Enable region entrance detection and select the snapshot type and the detection target.
2. Set the alarm holding time.
3. Set alarm areas 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

Region Exiting: Alarms will be triggered if the target exits from the pre-defined areas. Go to **Config→Event→Region Exiting**.

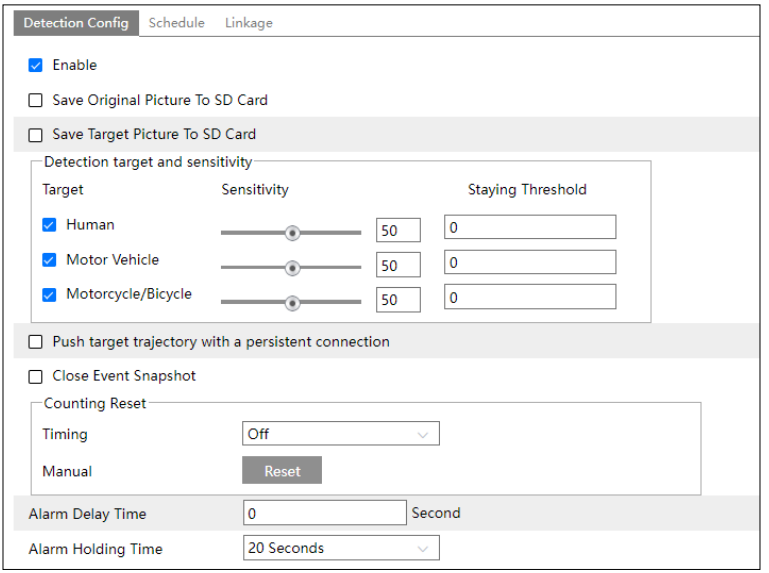
1. Enable region exiting detection and select the snapshot type and the detection target.
2. Set the alarm holding time.
3. Set alarm areas and target size filter for region exiting detection.
4. Set the schedule of region exiting detection.
5. Set the alarm linkage items.

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

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

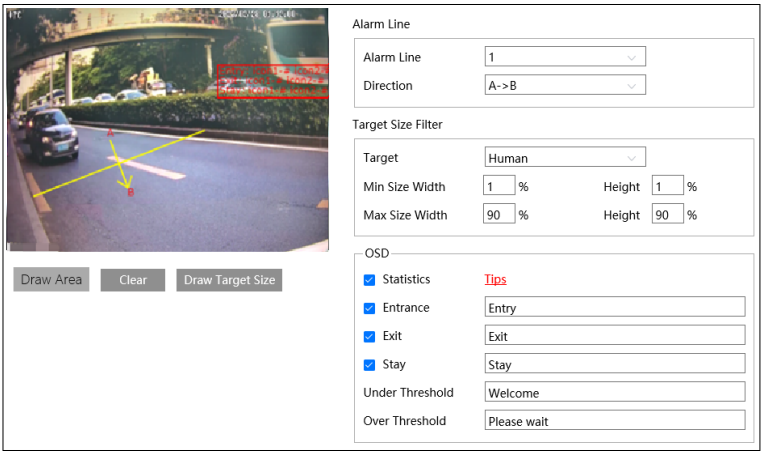
1. Go to **Config→Event→Target Counting by Line** as shown below.



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.

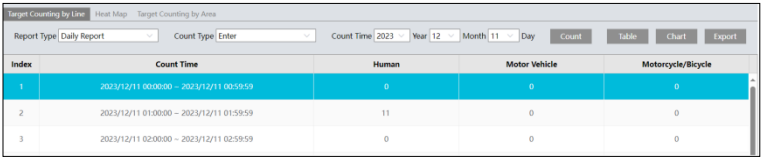
Staying Threshold: When the targets (human/vehicle) staying in the specified area exceed the threshold, alarms will be triggered.
Push target trajectory with a persistent connection: Push target trajectory (moving coordinate) to API test tool with a persistent connection. If enabled, the system will push the target trajectory upon detecting a target. If disabled, the system will push the target trajectory only when triggering target counting by line.
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.
Alarm Delay Time: 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.



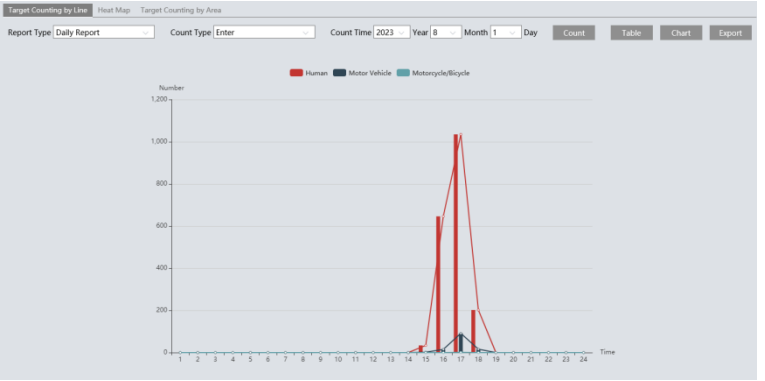
Set the alarm line number and direction. Only one alarm line can be added.
Direction：A->B and A<-B can be optional. The direction of the arrow is entrance.
Click the "Draw Area" button and then drag the mouse to draw a line in the image.
Click the "Clear" button to delete the lines.
Note: If the set 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 the 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 alarm linkage setup steps are the same as those for motion detection. Please refer to Motion Detection for details.
7. View the statistical information in the live view interface.

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



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 statistic result area. Click Table or Chart to display the result in different way.



※ Configuration requirements of the camera and surrounding area

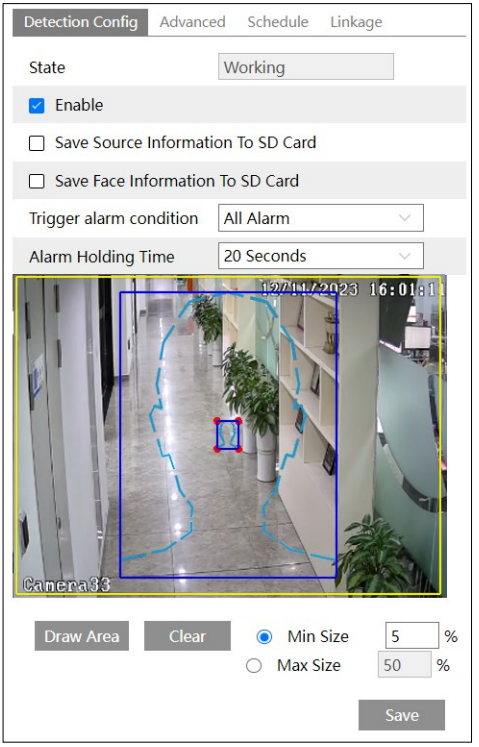
The requirements are similar to line crossing detection. Please refer to Configuration requirements of the camera and surrounding area of line crossing detection for details.

3.4.7 Face Detection

Face detection function is to detect the 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.



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.

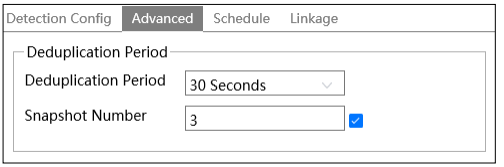
All: Alarms will be triggered when the camera detects a face (with/without a mask).

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.



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

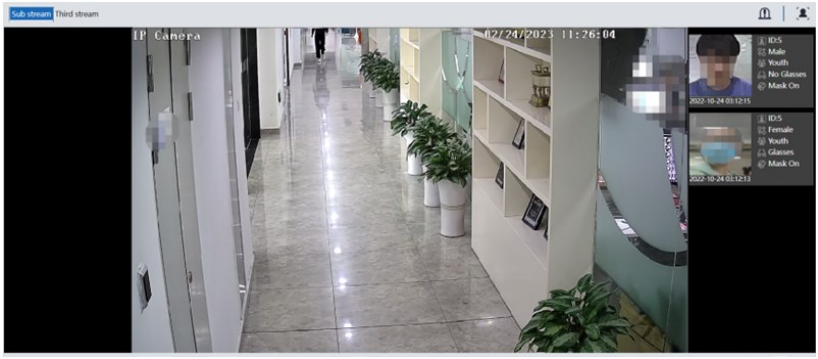
Snapshot Number: If the snapshot number is enabled and set (eg. 3), the camera will capture the same target once every 30 seconds and it will capture this target 3 times at most during its continuous tracking period. If the snapshot number is disabled, the camera will capture the same target once every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

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

Click “Linkage” to configure the alarm linkage items. The alarm linkage setup steps are the same as those for motion detection. Please refer to Motion Detection for details.

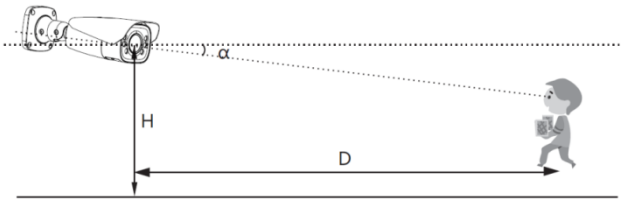
Face Capture View

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 the 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 shall be less than or equal to 15°.

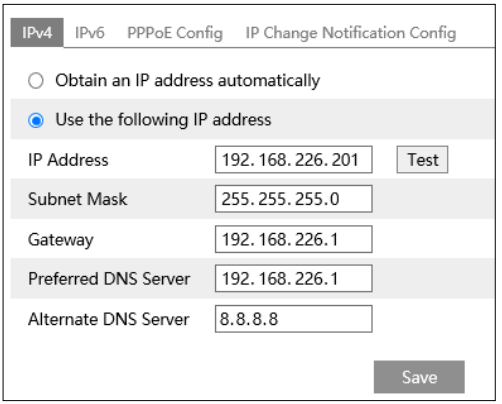


4. The object distance depends on the focal-length of the lens mounted in the camera.
5. In order to guarantee the captured face recognition rate, the requirement for face capture are: left or right turn angle is less than about 30°; pitching angle is less than 20°.
6. Face illumination must be uniform, 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

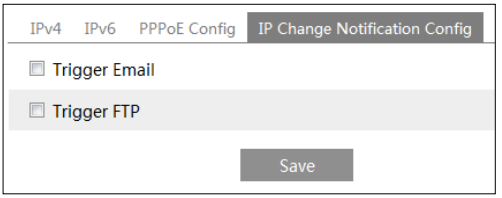
3.5.1 TCP/IP

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



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

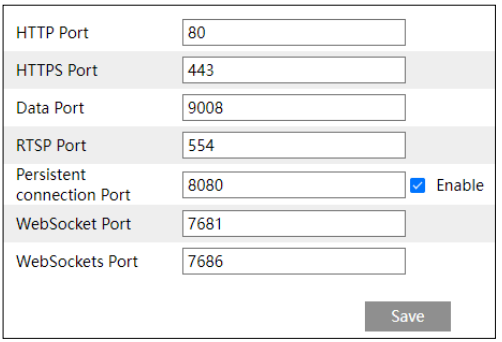
Either of these two network connection methods can be used. If PPPoE is used to connect internet, the camera will get a dynamic WAN IP address. This IP address will change frequently. To be notified, the IP change notification function can be used.
Click “IP Change Notification Config” to go to the interface as shown below. (Only some models support IP change notification).



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

3.5.2 Port

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

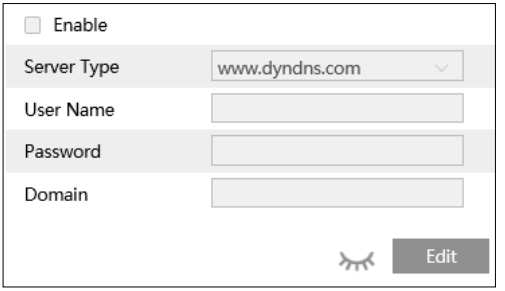


HTTP Port: The default HTTP port is 80. It can be changed to any port which is not occupied.
HTTPS Port: The default HTTPs port is 443. It can be changed to any port which is not occupied. (only some models support this port)
Data Port: The default data port is 9008. Please change it as necessary.
RTSP Port: The default port is 554. Please change it as necessary.
Persistent Connection Port: The port is used for a persistent connection of the third-party platform to push smart data, like face pictures.
WebSocket Port: Communication protocol port for plug-in free preview.
WebSockets Port: Communication protocol port for plug-in free preview. After the HTTPS protocol is enabled and used, WebSockets port will be shown here. Certificate verification is required to ensure the secure access. (only some models support this port)

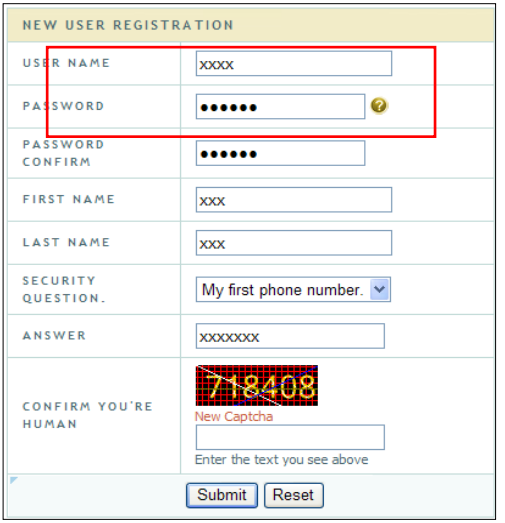
3.5.3 DDNS

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

1. Go to **Config→Network→ DDNS**.

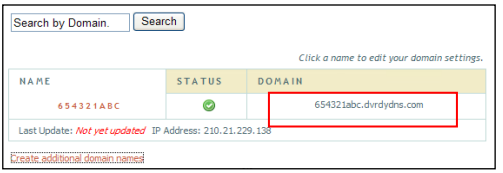


2. Apply for a domain name. Take www.dvrdyndns.com for example.
Enter www.dvrdydns.com in the web address bar to visit its website. Then Click the "Registration" button.



Create domain name.

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



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

3.5.4 SNMP

Only some models support this function.

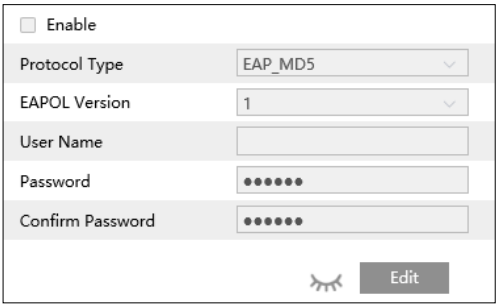
To get camera status, parameters and alarm information and remotely manage the camera, the SNMP function can be used. Before using SNMP, please install an SNMP management tool and set the parameters of the SNMP, such as SNMP port, trap address.

1. Go to **Config→Network→SNMP**.

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

3.5.5 802.1x

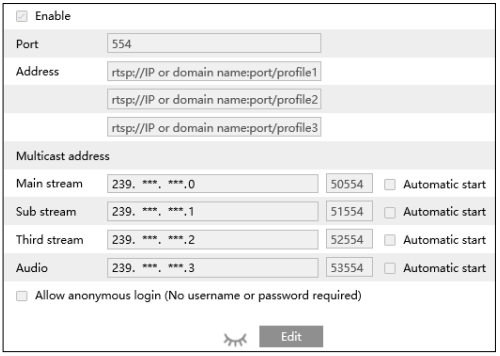
If it is enabled, the camera’s data can be protected. When the camera is connected to the network protected by the IEE802.1x, user authentication is needed.



To use this function, the camera shall be connected to a switch supporting 802.1x protocol. The switch can be regarded as an authentication system to identify the device in a local network. If the camera connected to the network interface of the switch has passed the authentication of the switch, it can be accessed via the local network.
Click “Edit” to start the setup.
Protocol type: Choose “EAP_MD5” or “EAP_TLS” as needed.
Select EAP-TLS as the EAP method. Enter your ID issued by the CA, and then upload related certificate(s). Before connecting the camera to the protected network with 802.1x, apply a digital certificate from a Certificate Authority (i.e., your network administrator) which can be validated by a RADIUS server.
Select EAP_MD5 as the EAP method. You need to enter the username and password.
User name and password: The user name and password must be the same as the user name and password applied for and registered in the authentication server.

3.5.6 RTSP

Go to **Config→Network→RTSP**.



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

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

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

Multicast Address

Main stream: The address format is

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

Sub stream: The address format is

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

Third stream: The address format is

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

……

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

Audio: Having entered the main/sub stream in a VLC player, the video and audio will play automatically.

If “Allow anonymous login…” is checked, there is no need to enter the username and password to view the video.

If “auto start” is enabled, the multicast received data should be added into a VLC player to play the video.

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

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

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

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

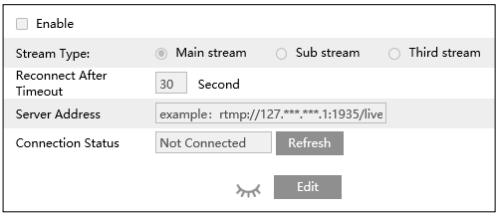
5. If the coding format of the video of the main stream is MJPEG, the video may be disordered at some resolutions.

3.5.7 RTMP

Only some models support this function.

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

Go to **Config→Network→RTMP**.



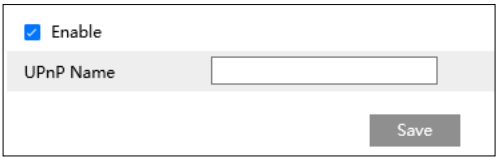
Click “Edit” and then check “Enable”, select stream type and set the reconnection time after timeout and server address as needed.

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

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

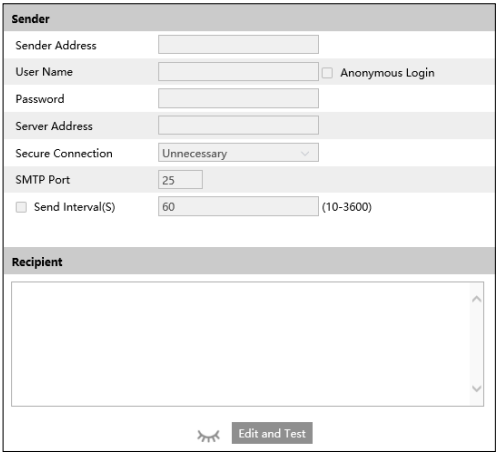
3.5.8 UPNP

Only some models support this function.
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.



3.5.9 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**.

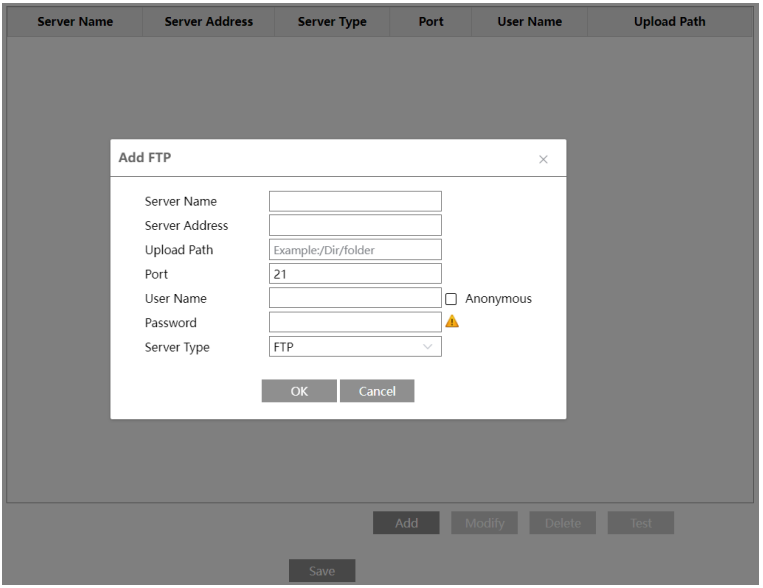


Click “Edit and Test” to set the sender and the recipient.
Sender Address: sender’s e-mail address.
User name and password: sender’s user name and password (you don’t have to enter the username and password if “Anonymous Login” is enabled).
Server Address: The SMTP IP address or host name.
Select the secure connection type at the “Secure Connection” pull-down list according to what’s required.
SMTP Port: The SMTP port.

Send Interval(S): The time interval of sending 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.

3.5.10 FTP

Only some models support this function.
After an FTP server is set up, captured pictures from events will be uploaded to the FTP server.
1. Go to **Config→Network →FTP**.



2. Click "Edit and Test" and then click "Add" to add the information of the FTP. After that, click "Save" to save the settings.
Server Name: The name of the FTP server.
Server Address: The IP address or domain name of the FTP.
Upload Path: The directory where files will be uploaded to.
Port: The port of the FTP server.
User Name and Password: The username and password that are used to login to the FTP server.

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

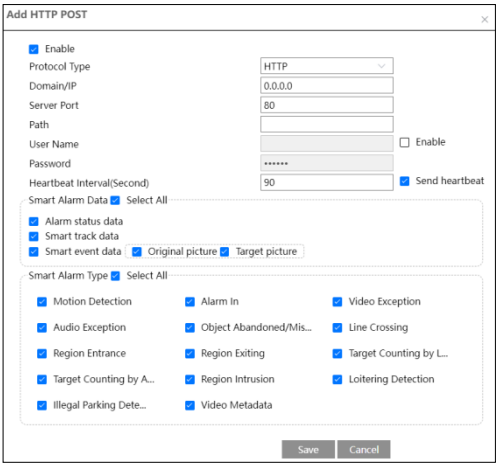
Rule of FTP storage path: /device MAC address/event type/date/time/
For example: a motion alarm occurs
FTP file path：\00-18-ae-a8-da-2a\MOTION\2021-01-09\14\
Event name table:

File Name	Event Type
IP	IP address change
MOTION	Motion Detection
SENSOR	Sensor Alarm
TRIPWIRE	Line Crossing Detection
PERIMETER	Region Intrusion Detection
OSC	Object Abandoned/Missing
AVD	Video Exception
ASD	Audio Exception
VFD	Face Detection
AOIENTRY	Region Entering
AOILEAVE	Region Exiting
PASSLINECOUNT	Target Counting by Line
SDFULL	SD Full
SDERROR	SD Error
VSD	Video Metadata

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

3.5.11 HTTP POST

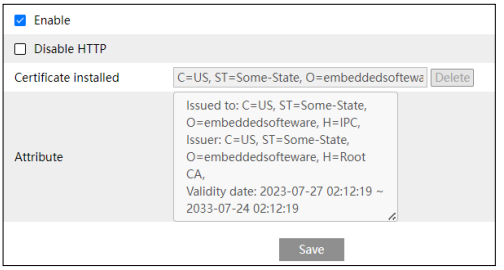
Only some models support this function.
Go to **Config→Network →HTTP POST**.
1. Click “Edit”.
2. Click “Add” to add HTTP POST.



Protocol type: HTTP
Domain/IP: the IP address/domain name of the third-party platform.
Server port: the server port of the third-party platform.
Path: enter the subdomain of the above server, for example, the URL of alarm information push: “/SendAlarmStatus”.
Username and password: Please enable and enter as needed.
Enable “Send heartbeat” and set heartbeat interval as needed.
After the above parameters are set, click “Save” to save the settings. Select one URL and click “Test” to test the connection of the URL. Then the camera will automatically connect to the third-party platform. The online state can be viewed in the above interface. After the camera is successfully connected, it will send the selected alarm data to the third-party platform once the selected smart alarm is triggered.

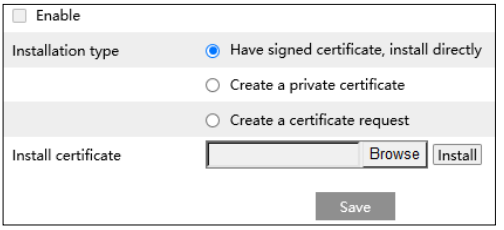
3.5.12 HTTPS

Only some models support this function.
HTTPS provides authentication of the web site and protects user privacy.
Go to **Config →Network→HTTPS** as shown below.



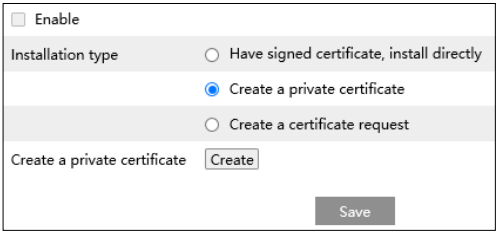
There is a certificate installed by default as shown above. Enable this function and save it. Then the camera can be accessed by entering https://IP: https port via a web browser (eg. https://192.168.226.201:443).

A private certificate can be created if users don't want to use the default one. Click "Delete" to cancel the default certificate. Then the following interface will be displayed.



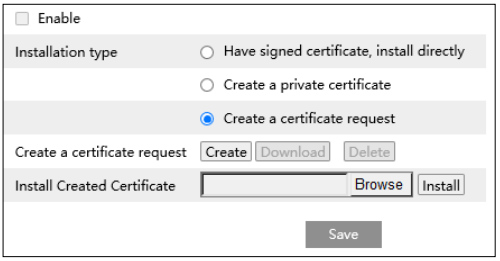
* If there is a signed certificate, click "Browse" to select it and then click "Install" to install it.

* Click "Create a private certificate" to enter the following creation interface.



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

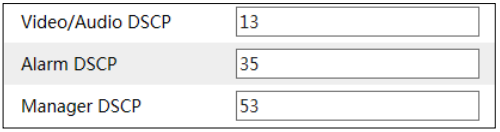
* Click "Create a certificate request" to enter the following interface.



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

3.5.13 QoS

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

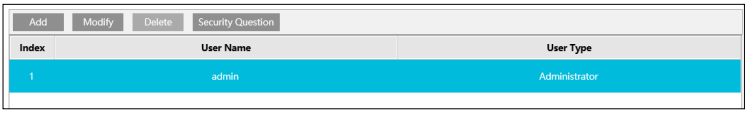


Video/Audio DSCP: The range is from 0 to 63.
Alarm DSCP: The range is from 0 to 63.
Manager DSCP: The range is from 0 to 63.
Generally speaking, the larger the number is, the higher the priority is.

3.6 Security Configuration

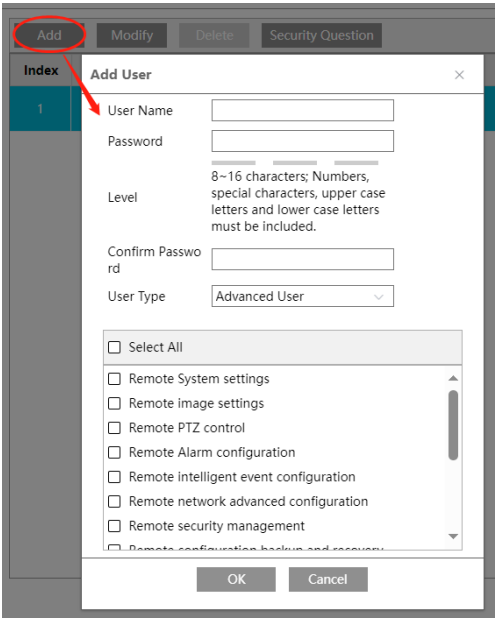
3.6.1 User Configuration

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



Add user:

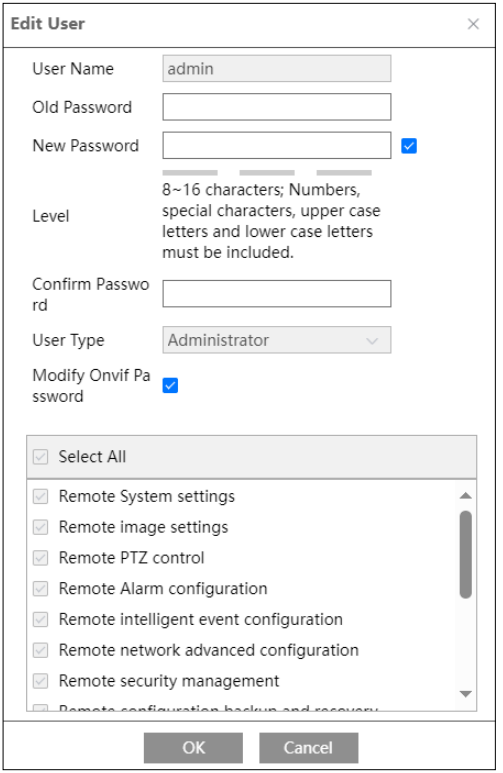
1. Click the “Add” button to pop up the following textbox.



2. Enter user name 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.



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 user.
6. Click the “OK” button to save the settings.

Delete user:

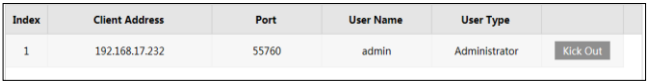
1. Select the user to be deleted in the user configuration list box.
2. Click the “Delete” button to delete the user.

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

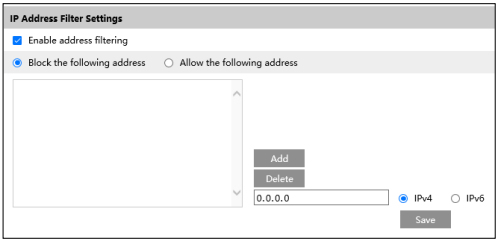
Go to **Config→Security→Online User** to view the user who is viewing the live video.



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

3.6.3 Block and Allow Lists

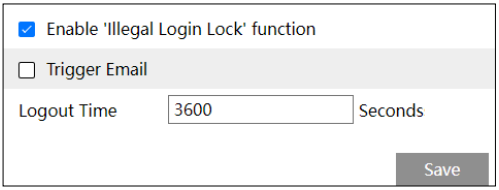
Go to **Config→Security→Block and Allow Lists** as shown below.



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.

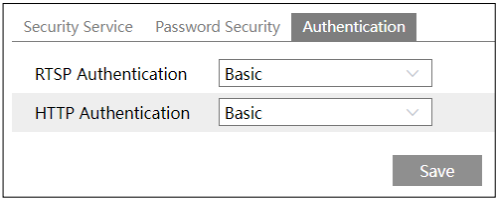


In order to prevent against malicious password unlocking, “Illegal Login Lock” function can be enabled here. If this function is enabled, login failure after trying five times will make the login interface locked. The camera can be logged in again after a half hour or after the camera reboots.
Trigger Email: if enabled, e-mail will be sent when logging in/out or illegal login lock occurs.

- **Password Security**

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.

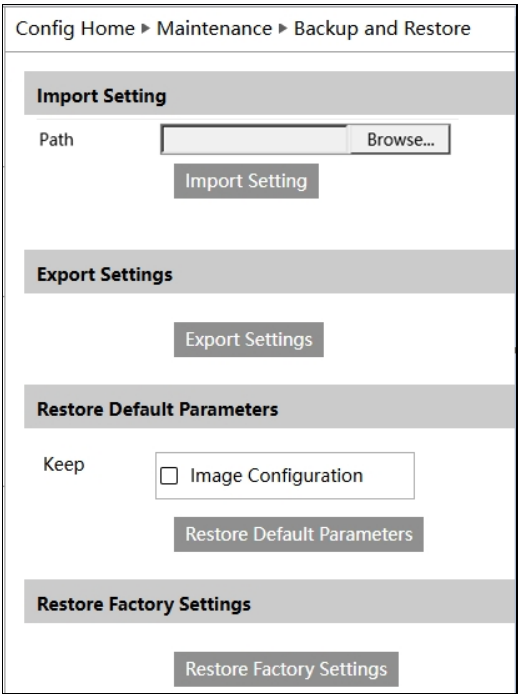
Authentication: you can set RTSP/HTTP authentication as needed.



3.7 Maintenance Configuration

3.7.1 Backup and Restore

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



- **Import & Export Settings**

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

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

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

- **Restore Default Parameters**

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

- **Restore Factory Settings**

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

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

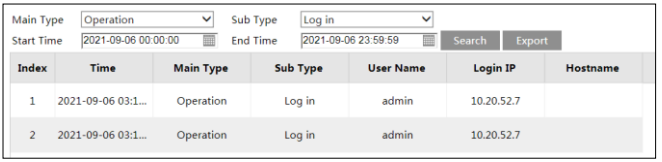
Go to **Config→Maintenance→Upgrade**. In this interface, the camera firmware can be updated.
1. Click the “Browse” button to select the save path of the upgrade file
2. Click the “Upgrade” or “Back up and upgrade” button to start upgrading the firmware.
3. Enter the correct password and then the device will restart automatically.
Note: If “Back up and upgrade” is selected, the configuration file will be exported to your local PC before starting upgrading.

Caution:
1. You cannot downgrade to a lower version.
2. Do not refresh/close the browser or disconnect the camera from the network during the upgrade, or it will cause system failure. After the device is successfully upgraded, there are ten minutes of observation. During this observation period, do not upgrade the device again.
Note: To decrease the upgrade risk, this series of cameras adopts two systems. After one system is successfully upgraded, the other system will be synchronized. If one system fails caused by power failure or other reasons during the upgrade, the other system will not be affected and the camera still can work normally. You can also upgrade your camera through the normal system.

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

3.7.4 Operation Log

To query and export log:
1. Go to **Config→Maintenance→Operation Log**.

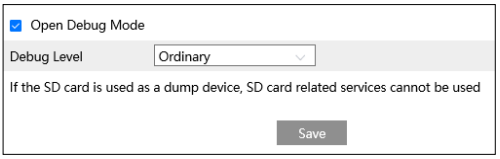


2. Select the main type, sub type, start and end time.
3. Click “Search” to view the operation log.

4. Click “Export” to export the operation log.

3.7.5 Debug Mode

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



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

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.

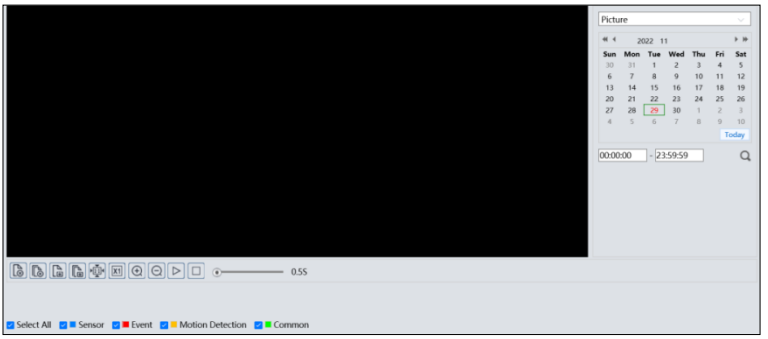
4. Search

4.1 Image Search

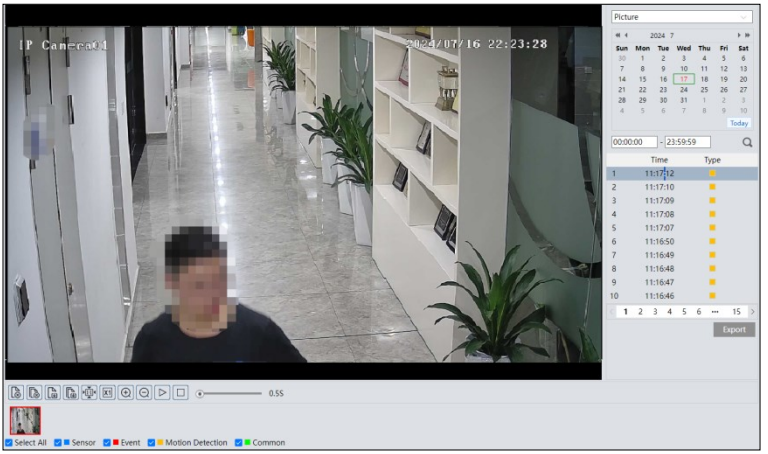
Click Search to go to the interface as shown below. Images that are saved on the SD card can be found here.

- **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.



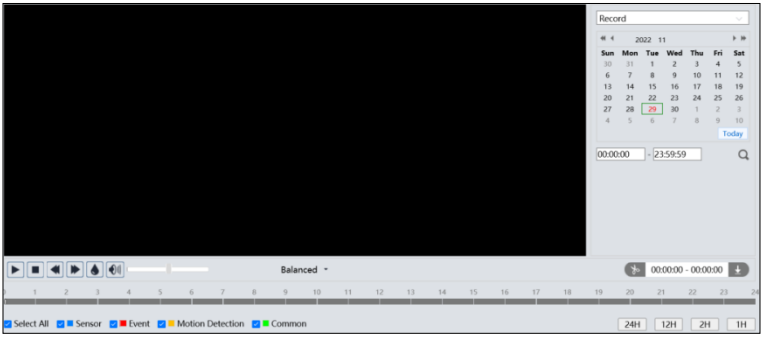
Click “Export” to export all searched pictures.
The descriptions of the buttons are shown as follows.

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

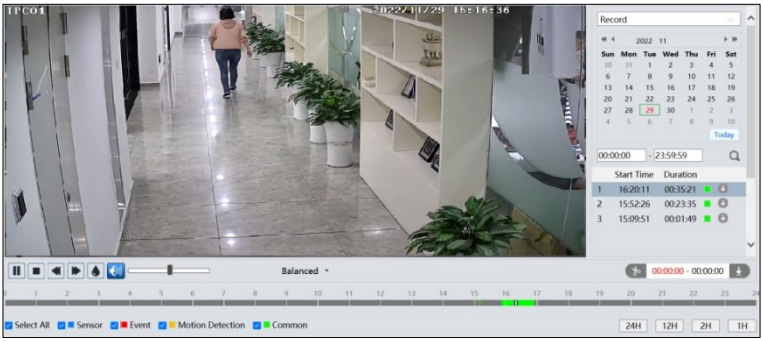
4.2 Video Search

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.

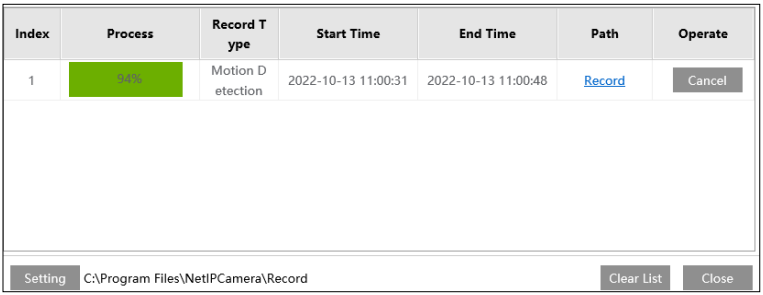
*2. For plug-in free playback, playback mode switch (balanced/real-time/fluent mode) and downloading functions are not supported too.

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

Video clip and downloading

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



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

5. Appendix

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 to default setting by GV-IP Device Utility.

Note: The default IP: 192.168.0.10，mask number: 255.255.255.0