GeoVision inc
The Vision of Security

GV-IP Camera

User's Manual

- GV-CBL2800
- GV-CEB2800

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

TVTCSERIES2MP-UM-A

© 2025 GeoVision, Inc. All rights reserved.
Under the copyright laws, this manual may not be copied, in whole or in part, without the written consent of GeoVision.

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

Trademarks used in this manual: *GeoVision*, the *GeoVision* logo and GV series products are trademarks of GeoVision, Inc. *Windows* is the registered trademark of Microsoft Corporation.

August 2025

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

[Warranty]

[Technical Support Policy]

Preface

GV-IP cameras have a variety of models designed to meet different needs. **The features described in the manual vary among camera models and versions. Some features may not be available in your camera.**

GV-CBL2800 and **GV-CEB2800** only support the following two Event configurations:

1. Line Crossing (Human detection only)
2. Region Intrusion (Human detection only)

Safety Instructions

About the Manual

- This manual is suitable for many models. All examples, screenshots, figures, charts, and illustrations used in the manual are for reference purpose, and actual products may be different with this Manual.
- Please read this user manual carefully to ensure that you can use the device correctly and safely.
- Within the maximum scope permitted by the law, the products described in this Manual (including hardware, software, firmware, etc.) are provided “AS IS”. The information in this document (including URL and other Internet site reference data) is subject to change without notice. This Manual may contain technical incorrect places or printing errors. This information will be periodically updated, and these changes will be added into the latest version of this Manual without prior notice.

Use of the Product

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

Electrical Safety

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

Environment

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

Operation and Daily Maintenance

- There are no user-serviceable parts inside. Please contact the nearest service center if the product does not work properly.
- Please shut down the device and then unplug the power cable before you begin any maintenance work.
- ⚠ Warning: All the examination and repair work should be done by qualified personnel.
- Do not touch the CMOS sensor optic component. You can use a blower to clean the dust on the lens surface.
- Always use the dry soft cloth to clean the device. If there is too much dust, use a cloth cleaning (such as using cloth) may result in poor IR functionality and/or IR reflection.
- Dome cover is an optical device, please don't touch or wipe the cover surface directly during installation and use. For dust, use oil-free soft brush or hair dryer to remove it gently; for grease or finger print, use oil-free cotton cloth or paper soaked with detergent to wipe from the lens center outward. Change the cloth and wipe several times if it is not clean enough.

White Light Illuminator (if supported)

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

Privacy Protection

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

Disclaimer

- 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 cyberattack, hacker attack, virus inspection, or other internet security risks; however, our company will provide timely technical support if necessary.
- Surveillance laws vary from country to country. Check all laws in your local region before using this product for surveillance purposes. We shall not take the responsibility for any consequences resulting from illegal operations.

Cybersecurity Recommendations

- Use a strong password. At least 8 characters or a combination of characters, numbers, and upper- and lower-case letters should be used in your password.
- Regularly change the passwords of your devices to ensure that only authorized users can access the system (recommended time is 90 days).
- It is recommended to change the service default ports (like HTTP-80, HTTPS-443, etc.) to reduce the risk of outsiders being able to access.
- It is recommended to set the firewall of your router. But note that some important ports cannot be closed (like HTTP port, HTTPS port, Data Port).
- It is not recommended to expose the device to the public network. When it is necessary to be exposed to the public network, please set the external hardware firewall and the corresponding firewall policy.
- It is not recommended to use the v1 and v2 functions of SNMP.
- In order to enhance the security of WEB client access, please create a TLS certificate to enable HTTPS.
- Use black and white list to filter the IP address. This will prevent everyone, except those specified IP addresses from accessing the system.
- If you add multiple users, please limit functions of guest accounts.

- If you enable UPnP, it will automatically try to forward ports in your router or modem. It is 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

CE Information

CE The products have been manufactured to comply with the following directives.

EMC Directive 2014/30/EU

RoHS Information

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

Chapter 1 Network Connection

System Requirement

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

Operating System: Windows 10 professional version or higher

CPU: i7-117000 2.5GHz or higher

GPU: AMD770+intel UHD Graphics 750

RAM: 8G or higher

Display: 1920*1080 resolution or higher

Web browser: Firefox / Edge / Safari / Google Chrome

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

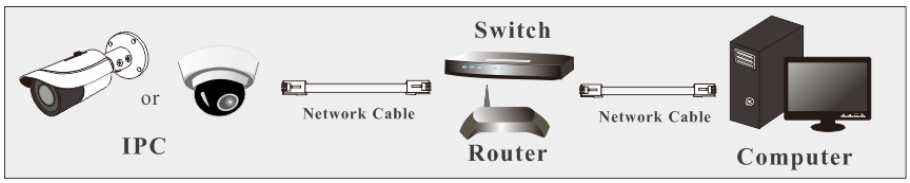
The menu display and operation of the camera may be slightly different by using the browser with plug-in or without plug-in. Installing the applicable plug-in will display more functions of the camera. Connect IP-Cam via LAN or WAN. Here only take plug-in browser for example. The details are as follows:

1.1 LAN

In LAN, there are two ways to access IP-Cam: 1. access through GV-IP Device Utility; 2. directly access through Web browser.

1.1.1 Access through GV-IP Device Utility

Network connection:

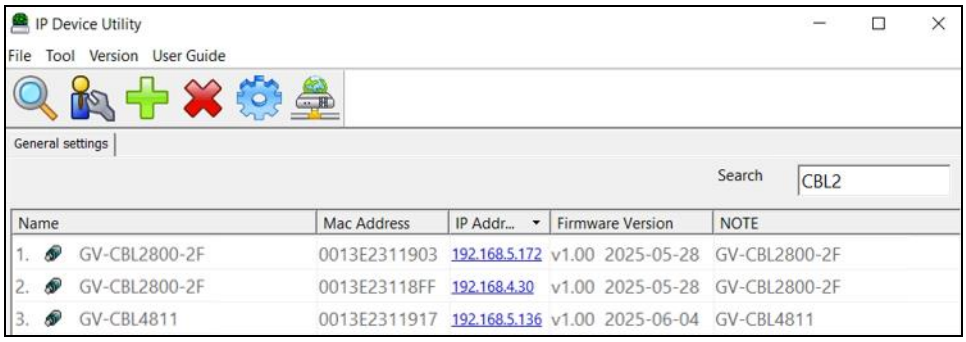


By default, when the camera is connected to LAN with DHCP server, it is automatically assigned with a dynamic IP address. Follow the steps below to look up its IP address, and use the accessed IP address to log in its Web interface.

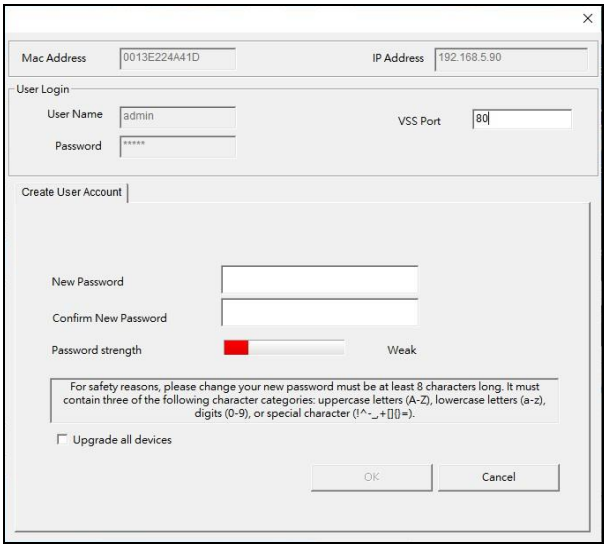
1. Make sure the PC and the camera are connected to the same LAN, and **GV-IP Device Utility** is installed on the PC from the GeoVision Website.

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, 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 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 *3.6 Security Configuration.*

1.1.2 Direct Access via Web Browser

The default network settings are as shown below:

IP address: **192.168.0.10**

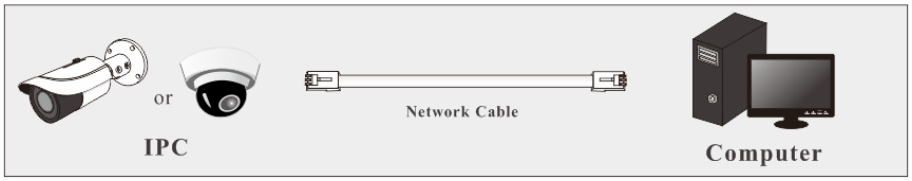
Subnet Mask: **255.255.255.0**

Gateway: **192.168.226.1**

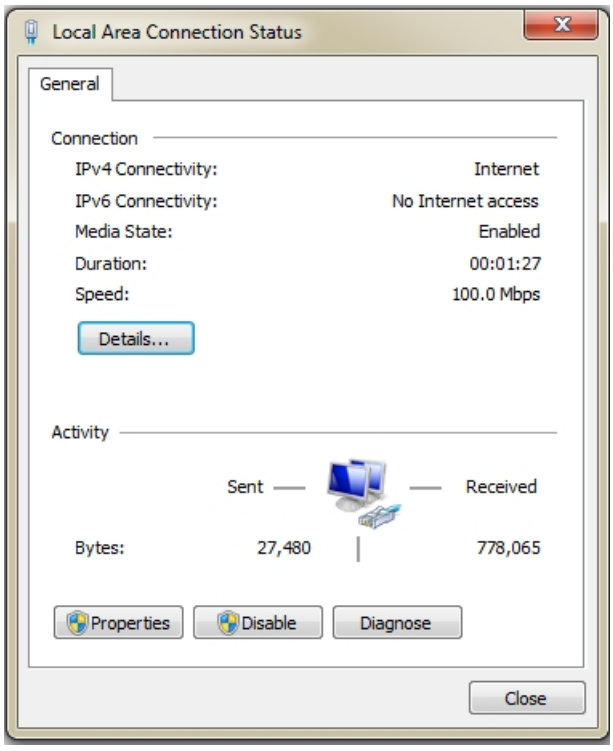
HTTP: **80**

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.

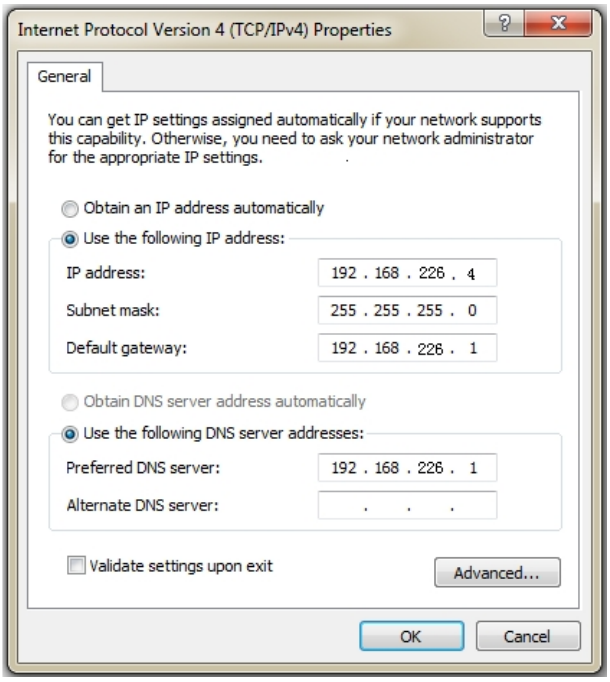


1. Manually set the IP address of the PC and the network segment should be the same as the default settings of the IP camera. Open the network and share center. Click “Local Area Connection” to pop up the following window.



2. Select “Properties” and then select internet protocol according to the actual situation (for example: IPv4).

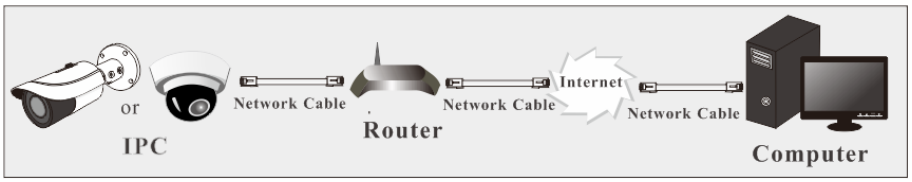
3. Click the “Properties” button to set the network of the PC.



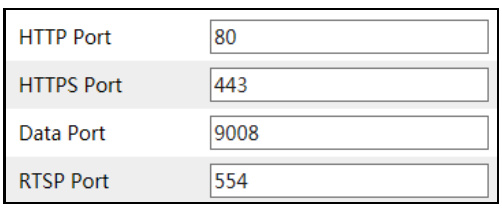
4. Open a Web browser and enter the default address of the IP-camera.
5. Follow directions to download and install the plug-in. After installation is complete, refresh the browser.
6. Enter the default username and password on the login page and click “Login”.

1.2 WAN

Access through a router or virtual server

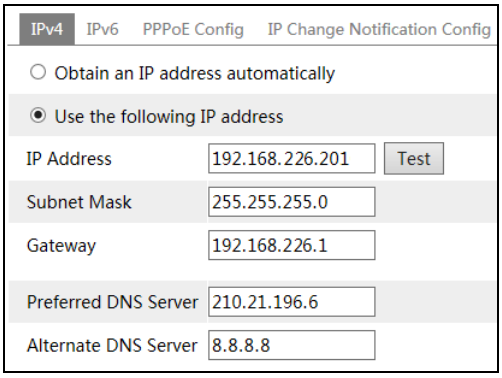


1. Make sure the camera is connected to the local network and then log in the camera via LAN and go to Config→Network→Port menu to set the port number.



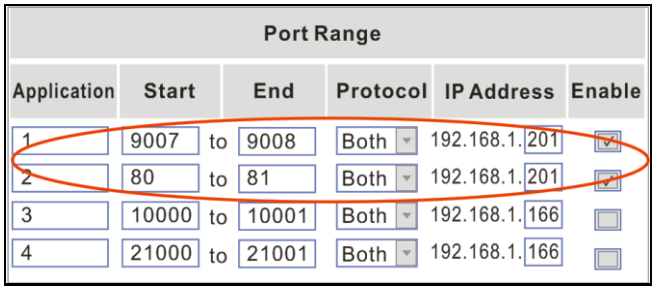
Port Setup

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



IP Setup

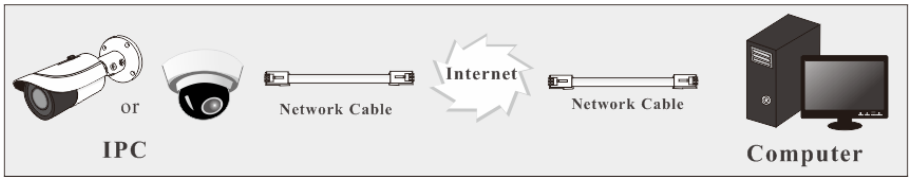
3. Go to the router's management interface through the Web browser to forward the IP address and port of the camera in the "Virtual Server".



Router Setup

4. Open the 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 static IP

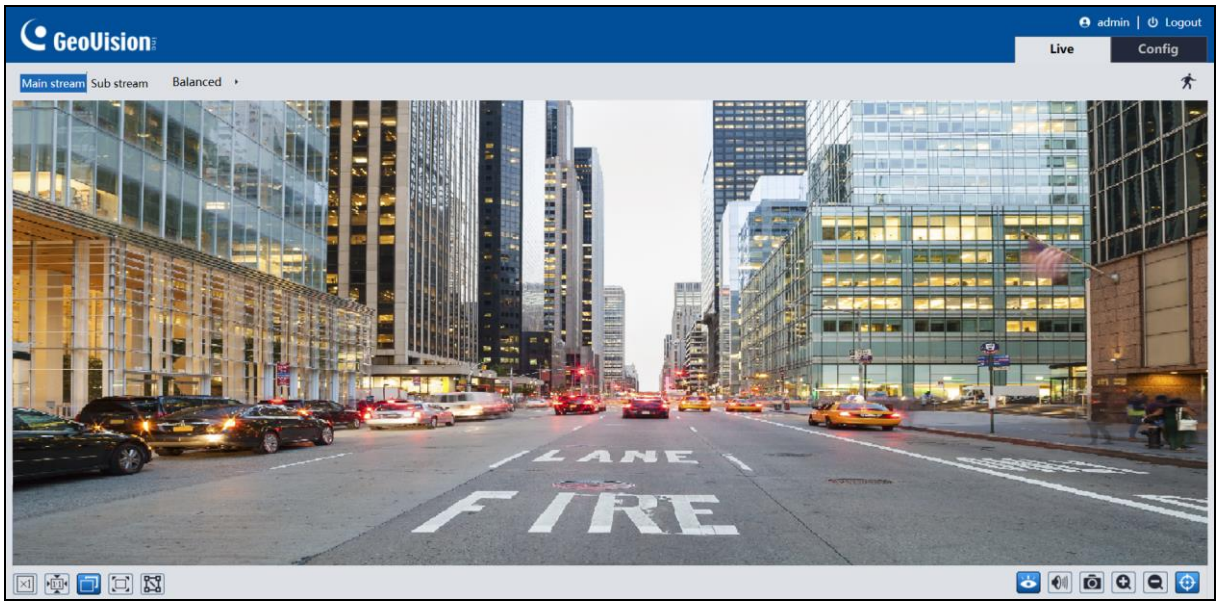


The setup steps are as follow:

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

Chapter 2 Live View

After logging in, the following window will be shown.



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

Icon	Description	Icon	Description
	Original size		Start/stop local recording
	Fit correct scale		Zoom in
	Auto (fill the window)		Zoom out
	Full screen		Rule information display
	Measure Tool		Motion alarm indicator
	Start/stop live view		Line crossing indicator
	Enable/disable light alarm		Light alarm indicator
	Enable/disable audio		Intrusion indicator
	Snapshot		

Note:

1. 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 under smart event scenarios. Click  and drag the mouse on the image to draw a desired box. The width and height pixel will directly display in the box.
2. Those smart alarm indicators will flash only when the camera supports those functions and the corresponding events are enabled.
3. After clicking the light alarm icon, the white light will flash according to the set flashing time (you can set the flashing time by clicking Config→Alarm→Light Alarm). Click this icon again to stop flashing. Only when the illumination mode in Display Settings is set to "Infrared light" can this function be displayed.
4. Local recording and the preview mode switch (real-time / balanced / fluent mode) are not supported in plug-in free live view.

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

To set the stream profile, select the main stream and sub stream. Go to ***Configure→Video/Audio*** to set the resolution for each stream as needed.

Color Descriptions of Target Recognition Box and Rule Line

- Green box: detect human
- Target box after an event is triggered: turn yellow
- Rule line or area: blue
- Rule line or area after an event is triggered: turn from blue to red

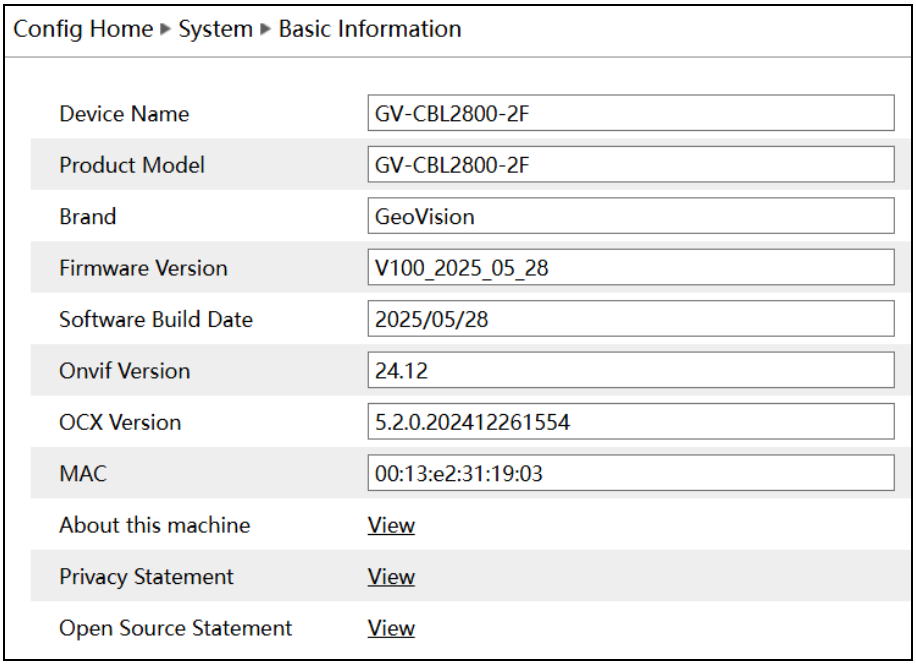
Chapter 3 Network Camera Configuration

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

3.1 System Configuration

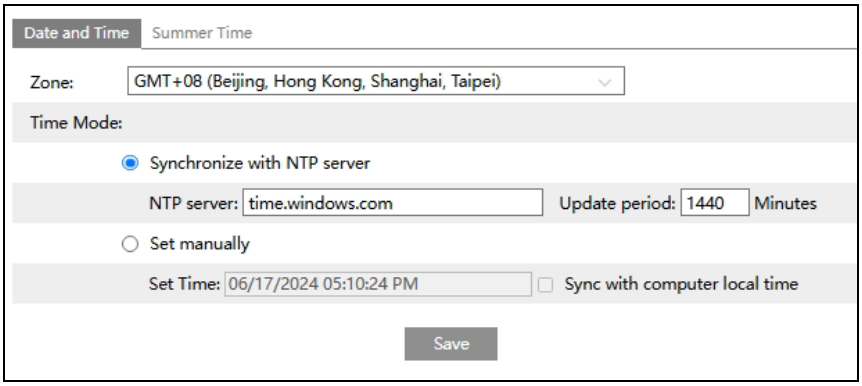
3.1.1 Basic Information

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



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 required.

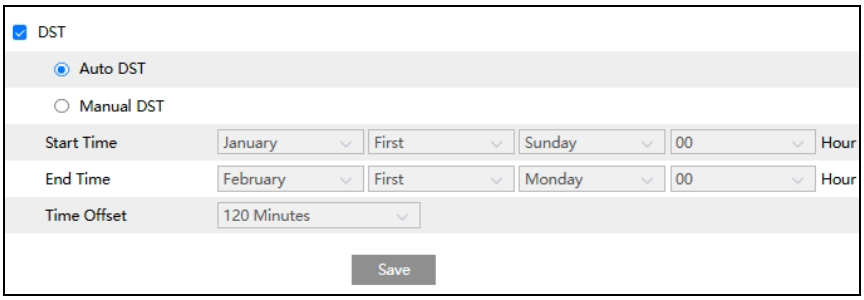
Note: The time zone of the camera and the computer must be the same. It is recommended to modify the time zone of the camera according to the time zone of the computer. If the time zone of the computer is modified, the current web client needs to be closed. Then re-open it and log in again.

Time Mode:

NTP: Specify an NTP server to synchronize the time.

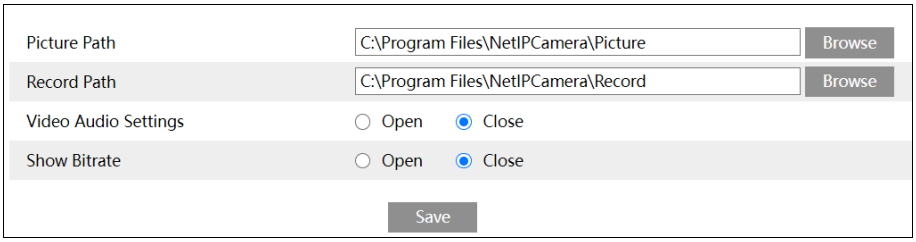
Manual: Set the system time manually or you can synchronize the time with the time of the local computer.

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 in the live video.

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

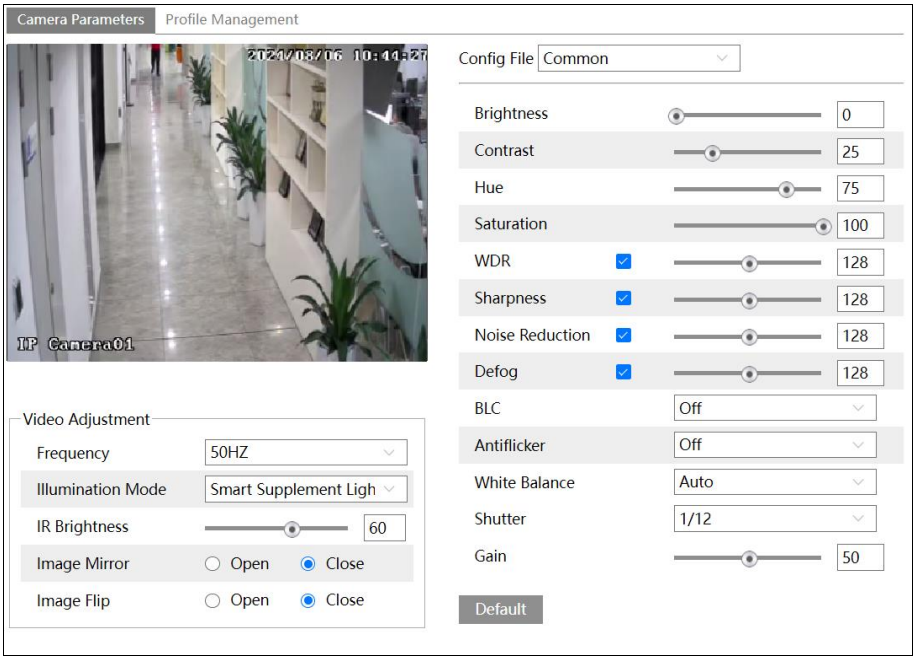
3.2 Image Configuration

3.2.1 Display Configuration

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

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

Dual-light models:



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.

WDR: Digital WDR. WDR can adjust the camera to provide a better image when there are both very bright and very dark areas simultaneously in the field of view by lowering the brightness of the bright area and increasing the brightness of the dark area.

Recording will be stopped for a few seconds while the mode is changing from non-WDR to WDR mode.

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

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

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

Auto Iris: If your camera is equipped with auto Iris lens, please enable it.

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.

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.

Frequency: 50Hz and 60Hz can be optional.

Image Mirror: Turn the current video image horizontally.

Image Flip: Turn the current video image vertically.

Illumination Mode: Choose "White light", "Infrared light" or "Smart supplement light" as needed.

If "Smart Supplement Light" is selected, in low ambient light, the system will automatically turn on the visible infrared light. Once there are people appearing in the detection area, it will automatically switch to full-brightness visible white light. When people leaving the detection area exceeds the set duration, it will resume to infrared light. See Smart Supplement Light Configuration for details.

IR Brightness: Set the IR brightness as needed.

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

White Light Mode: Choose "Off", "Auto" or "Manual". Please select it as needed.

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

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

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

IR Brightness: Set the IR brightness as needed.

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

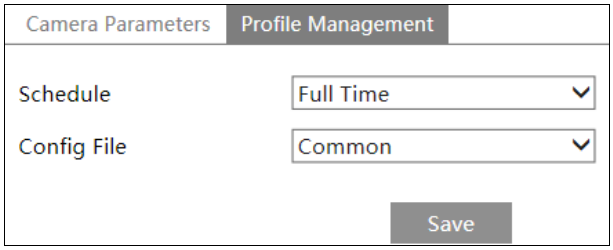
If “Timing” is selected, you need to set daytime and night time. For example: if “Daytime” is set to “7:00”, the camera will switch to Day mode at 7:00; if “Night time” is set to “17:00”, the camera will switch from Day mode to Night mode at 17:00.

Infrared Mode: Choose “Auto”, “On” or “Off”.

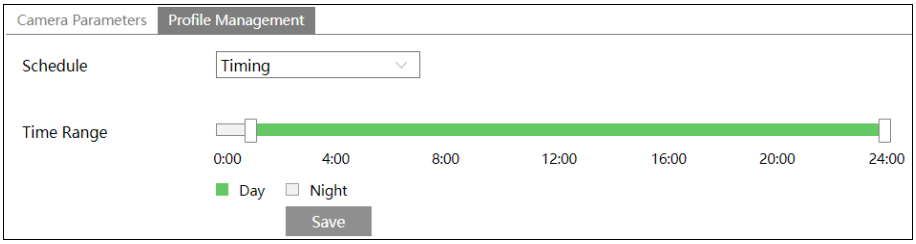
Note: For some items (like frequency), if selected/enabled, the camera will reboot automatically. After that, clicking “Default” button will not take effect.

Schedule Settings of Image Parameters

Click the “Profile Management” tab as shown below.



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

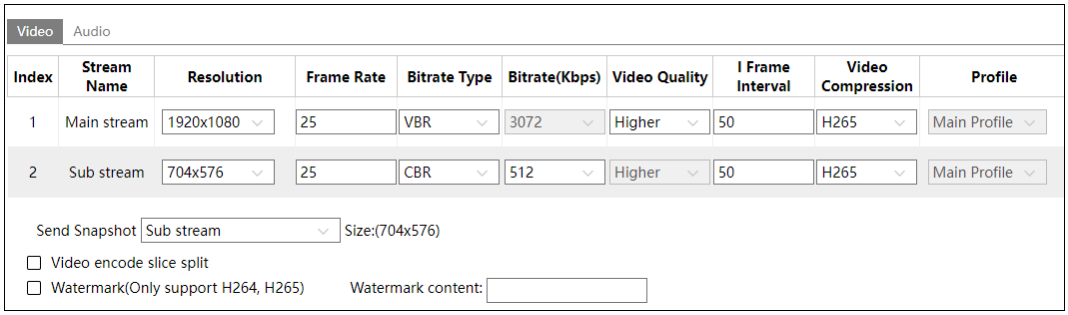


Drag “” icons to set the time of day and night. Blue means day time and blank means night time. If the current mode of camera parameters is set to schedule, the image configuration mode will automatically switch between day and night according to the schedule.

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



Two video streams can be adjustable.

Resolution: The size of the image.

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

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 bitrate type is set to CBR. The higher the bitrate, the better the image quality will be.

Video Quality: It can be adjusted when the bitrate type 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+ are applicable. MJPEG is not available for main stream. If H.265 / H.265+is chosen, make sure the client system is able to decode H.265 / H.265+. Compared to H.265, H.265+ saves more storage space with the same maximum bitrate in most scenes. Compared to H.264, H.265 reduces the transmission bitrate under the same resolution, frame rate and image quality.

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

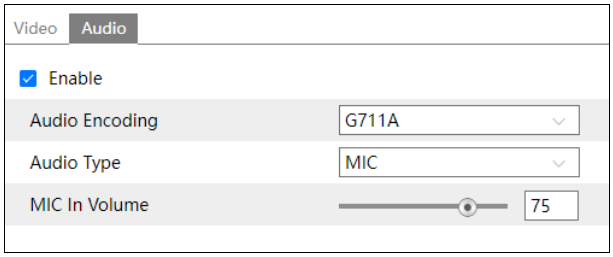
Send Snapshot: Set the snapshot stream.

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

Watermark: When playing back the local recorded video, 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.

Only the models with the built-in MIC support this function.



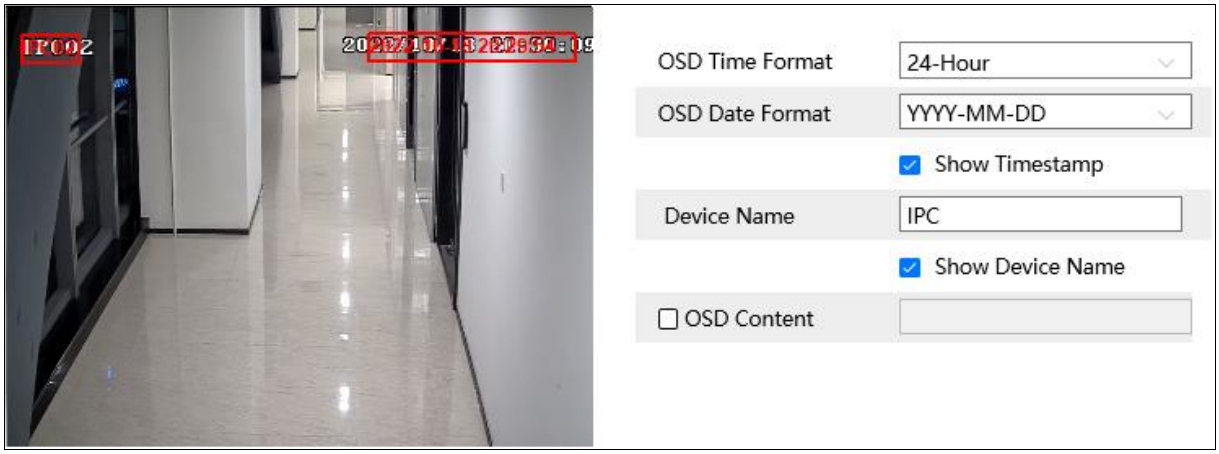
Audio Encoding: G711A and G711U are selectable.

Audio Type: MIC. (for supported internal MIC)

MIC IN Volume: If MIC is selected, MIC IN volume can be set.

3.2.3 OSD Configuration

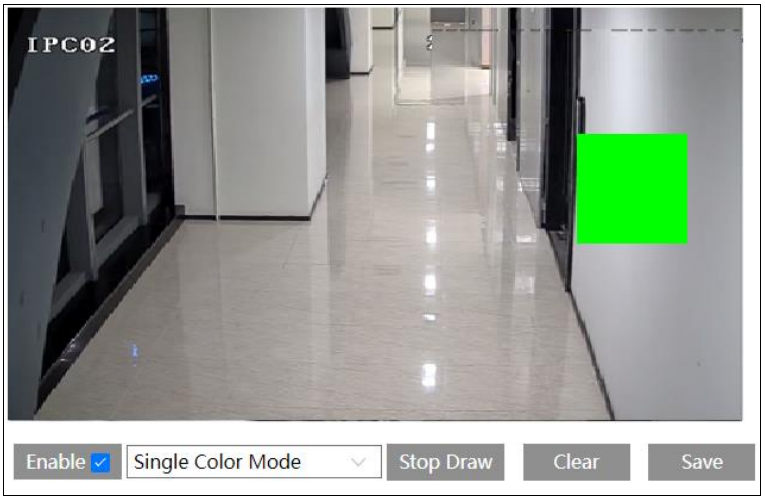
Go to **Image→OSD** interface as shown below.



Set time stamp, device name, OSD content 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.

3.2.4 Video Mask

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



To set up video mask:

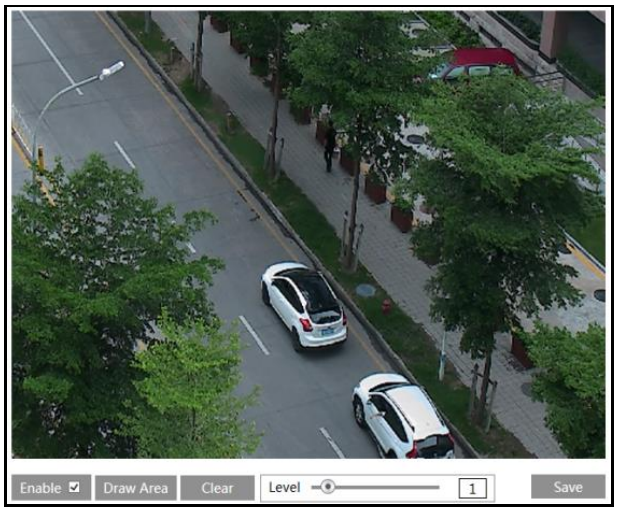
1. Enable video mask.
2. Click the “Draw Area” button and then drag the mouse to draw the video mask area.
3. Click the “Save” button to save the settings.
4. Return to the live to verify that the area has been drawn as shown as blocked out in the image.

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



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

3.2.6 Smart Supplement Light Configuration

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

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

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

4. Set the detection target and sensitivity. “Human” is selected by default.

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

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

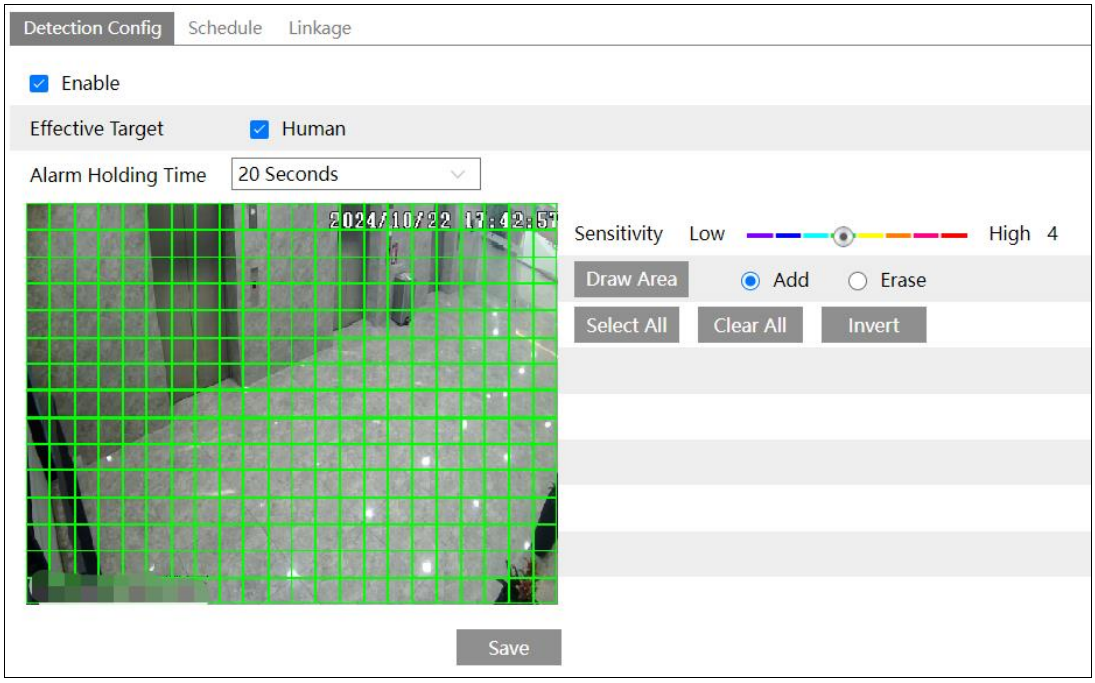
   Note：If the people staying and not moving in the detection area exceed the set duration, it will resume to infrared light too.

6. Click “Save” to save the settings.

3.3 Alarm Configuration

3.3.1 Motion Detection

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



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

Effective Target: If “Human” is enabled, the camera will only detect the movement of people. If no target is enabled, alarms will be triggered when the moving object appears on the image, including people or other moving objects.

Note: Enabling the Effective Target (for Human) helps detect specific objects and reduces false alarms. However, note that the accuracy of this feature may vary due to environmental factors. Adjust settings as needed for optimal performance.

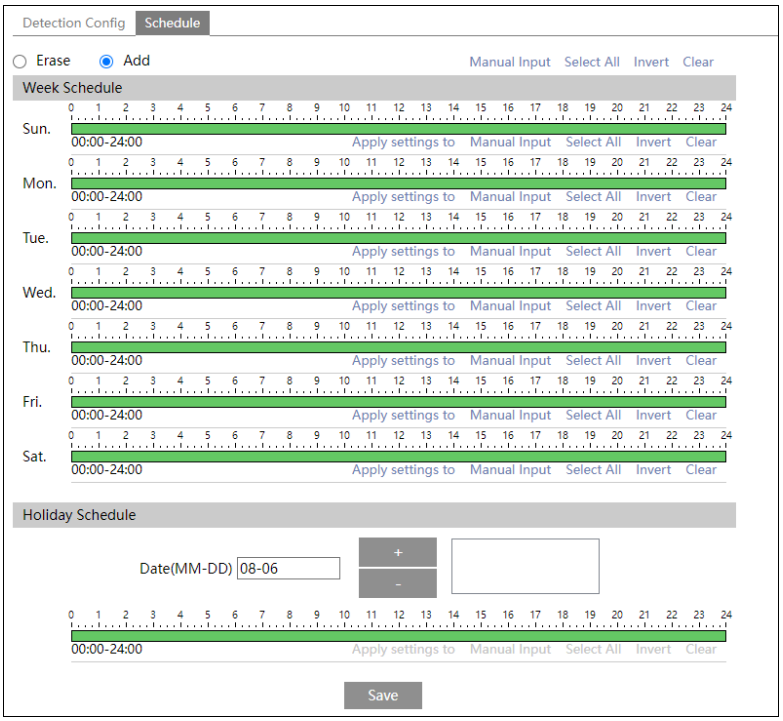
Alarm Holding Time: It refers to the interval time between the adjacent motion detections. For instance, if the alarm holding time is set to 20 seconds, once the camera detects a motion, it will go to alarm and would not detect any other motion in 20 seconds. If there is another motion detected during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

2. Set motion detection area and sensitivity.

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

Select “Add” and click “Draw”. Drag the mouse to draw the motion detection area; Select “Erase” and drag the mouse to clear motion detection area. After that, click the “Save” to save the settings.

3. Set the schedule for motion detection.



Weekly schedule

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

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

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

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

Day schedule

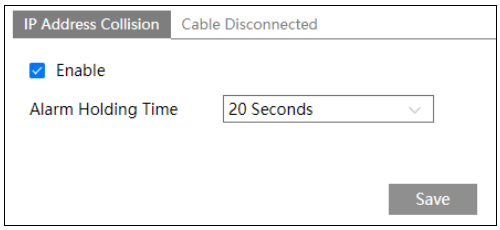
Set the alarm time for alarm a special day, such as a holiday.

Note: Holiday schedule takes priority over weekly schedule.

3.3.2 Exception Alarms

- **IP Address Conflict**

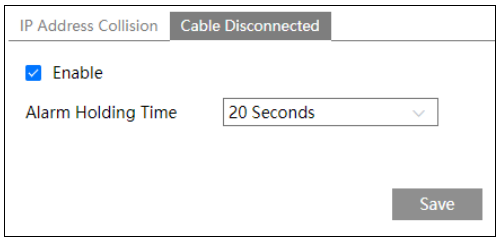
1. Go to **Config→Alarm→Exception Alarm→IP Address Collision** as shown below.



2. Click “Enable” and set the alarm holding time.
3. After this function is enabled and set the alarm holding time, you can go to **Config→Maintenance→ Operation Log** to check the relevant alarm information.

- **Cable Disconnection**

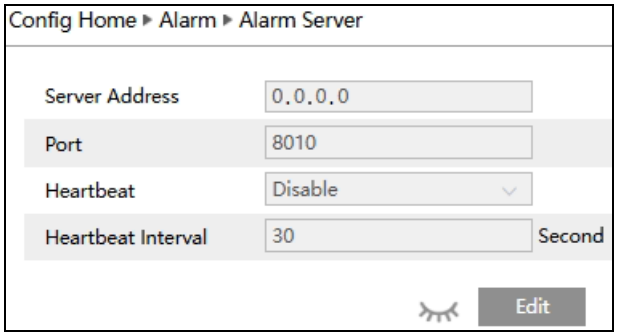
1. Go to **Config→Alarm→Exception Alarm→Cable Disconnected** as shown below.



2. Click “Enable” and set the alarm holding time.
3. After this function is enabled and set the alarm holding time, you can go to **Config→Maintenance→ Operation Log** to check the relevant alarm information.

3.3.3 Alarm Server

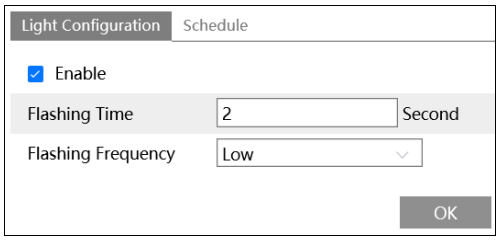
1. Go to **Alarm→Alarm Server** interface as shown below.



2. Click “Edit” to set the alarm server.
3. 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.
4. Click to view the entire server address; click to hide a part of sensitive data.

3.3.4 Light Alarm

1. Go to **Alarm→Light Alarm** as shown below. **Only when the illumination mode in Display Settings is set to "Infrared light" can this function be displayed.**



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

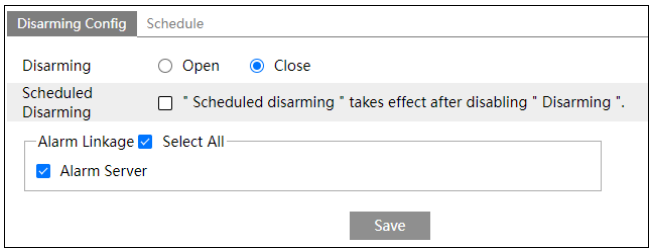
Flashing Time: the flashing time ranges from 1 second to 60 seconds.

Flashing Frequency: three options- low, middle and high.

Set the schedule of light alarm. The setup steps of schedule are the same as the motion detection schedule settings (See Motion Detection for details).

3.3.5 Disarming

You can disarm alarm linkage actions quickly in this interface.



Disarming: The system stops triggering alarm linkage actions immediately.

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

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

3.4 Event Configuration

For more accuracy, here are some recommendations for installation.

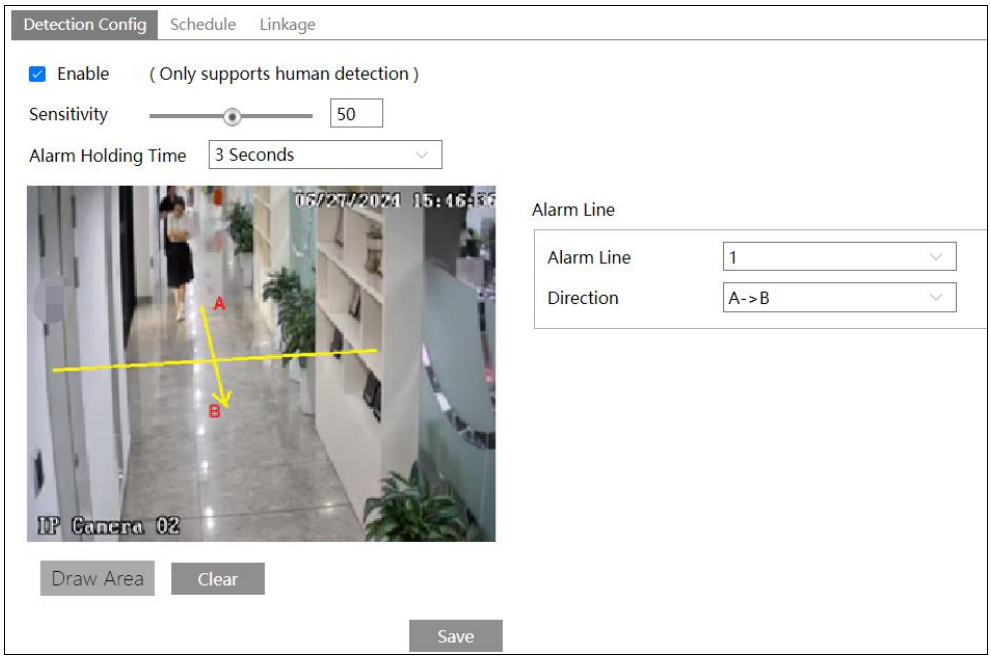
- Cameras should be installed on stable surfaces, as vibrations can affect the accuracy of detection.
- Avoid pointing the camera at the reflective surfaces (like shiny floors, mirrors, glass, lake surfaces and so on).
- Avoid places that are narrow or have too much shadowing.
- Avoid scenario where the object's color is similar to the background color.
- At any time of day or night, please make sure the image of the camera is clear and with adequate and even light, avoiding overexposure or too much darkness on both sides.

Note: GV-CBL2800 and GV-CEB2800 only support the following event configurations: Line Crossing and Region Intrusion (Human detection only). The two functions can only be enabled one at a time.

3.4.1 Line Crossing

Line Crossing: Alarms will be triggered if the target crosses the pre-defined alarm lines.

Go to Config→Event→Line Crossing interface as shown below.



1. Enable line crossing alarm and set the sensitivity.
2. Set the alarm holding time.
3. Set alarm lines 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.

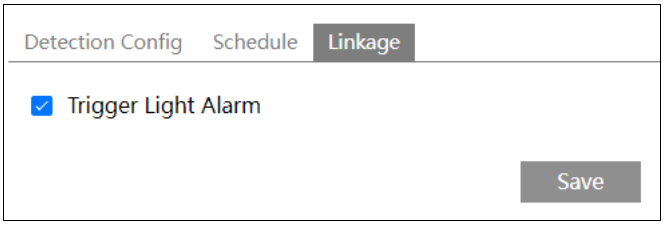
A<-B: The alarm will be triggered when the intruder crosses over the alarm line from B to A. Click the “Draw Area” button and then drag the mouse to draw a line in the image. Click the “Stop Draw” button to stop drawing. Click the “Clear” button to delete the lines. Click the “Save” button to save the 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.

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 section for details).
6. Click “Linkage” to trigger light alarm. Only when the illumination mode in Display Settings is set to “Infrared light”, can you trigger light alarm.

Trigger Light Alarm: If selected, the light of the camera will flash when a target cross the alarm line. (Please set the light flashing time and frequency first. See Light Alarm for details).



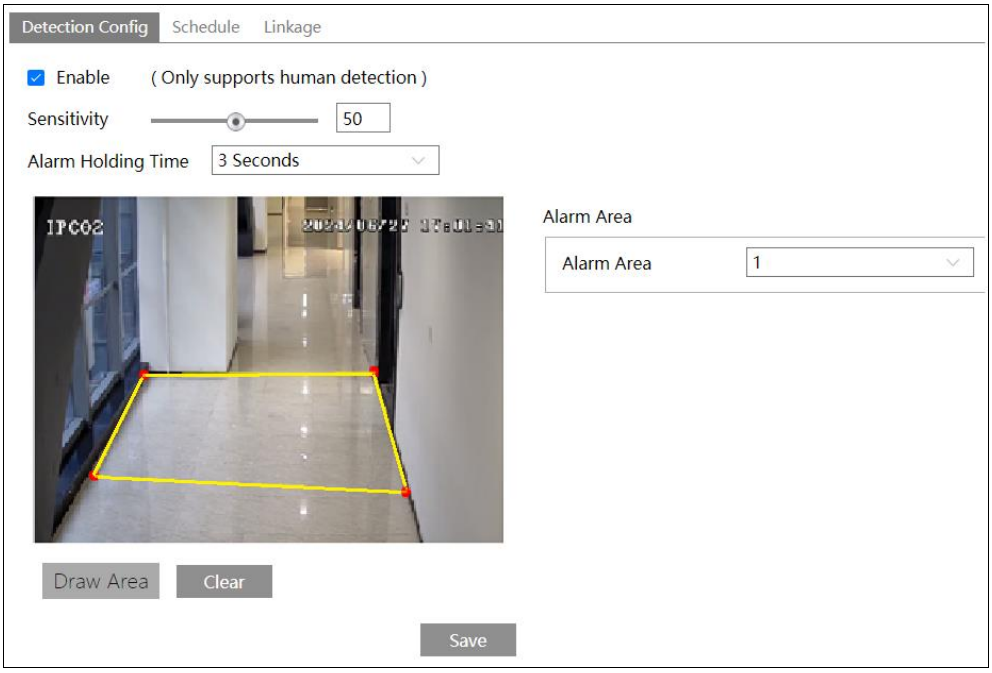
※ Configuration requirements of the camera and surrounding area

See Appendix 2 for details.

3.4.2 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** interface as shown below.



1. Enable region intrusion alarm and set the sensitivity.
2. Set the alarm holding time.
3. Set alarm lines 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.

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 section for details).
6. Click "Linkage" to trigger light alarm. Only when the illumination mode in Display Settings is set to "Infrared light", can you trigger light alarm.

Trigger Light Alarm: If selected, the light of the camera will flash when a target cross the alarm line. (Please set the light flashing time and frequency first. See Light Alarm for details).

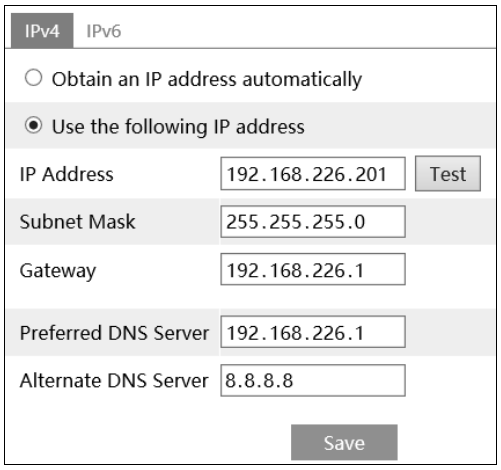
※ Configuration requirements of the camera and surrounding area

See Appendix 2 for details.

3.5 Network Configuration

3.5.1 TCP/IP

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

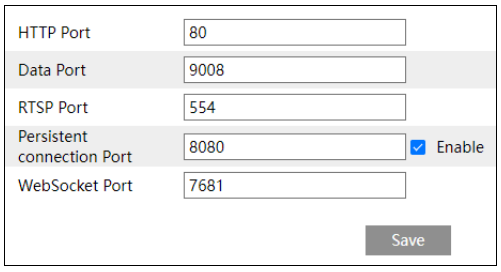


Use IP address (take IPv4 for example): There are two options for IP setup: obtain an IP address automatically by DHCP and use the following IP address. Please choose one of the options as needed.

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

3.5.2 Port

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



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

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.

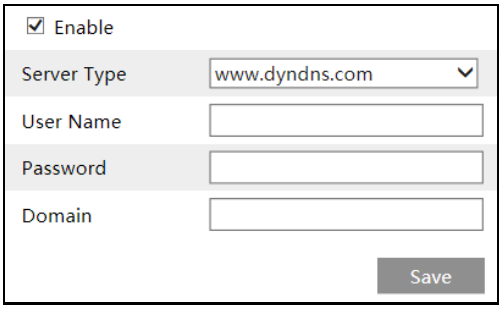
Persistent Connection Port: The port is used for a persistent connection of the third-party platform to push smart data, like face pictures.

WebSocket Port: Communication protocol port for plug-in free preview.

3.5.3 DDNS

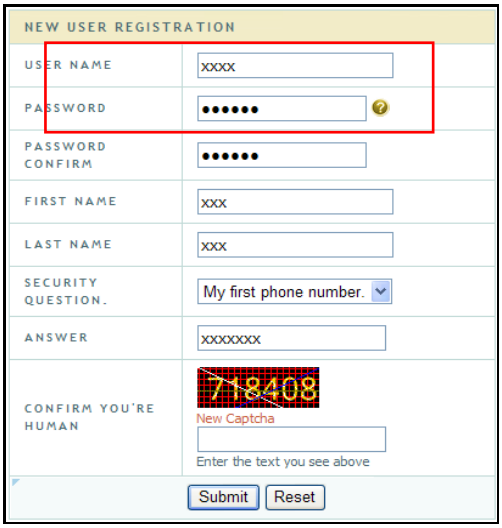
If the camera is set up with a DHCP connection, DDNS should be set for the internet.

1. Go to **Config→Network→ DDNS**.



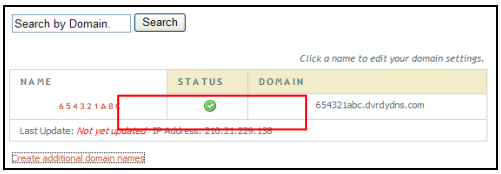
2. Apply for a domain name. Take www.dvrdyndns.com for example.

Enter www.dvrdydns.com in the Web browser address bar to visit its website. Then Click the "Registration" button.



Create domain name.

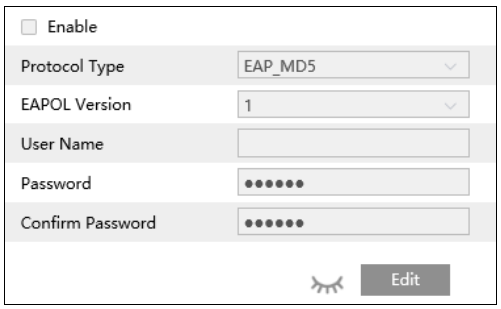
After the domain name is successfully applied for, the domain name will be listed as below.



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

3.5.4 802.1x

If it is enabled, the camera’s data can be protected. When the camera is connected to the network protected by the IEEE 802.1x, user authentication is needed.



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

Click “Edit” to start the setup.

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

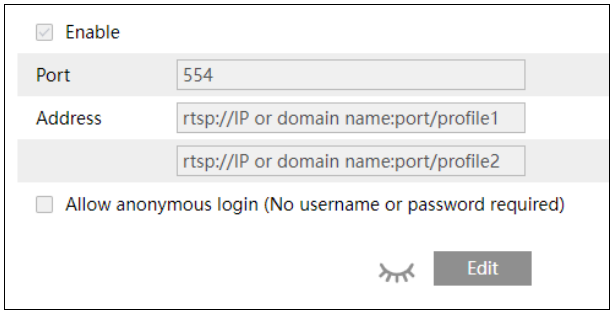
Select EAP-TLS as the EAP method. Enter your ID issued by the CA, and then upload related certificate(s). Before connecting the camera to the protected network with 802.1x, apply a digital certificate from a Certificate Authority (i.e., your network administrator) which can be validated by a RADIUS server.

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

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

3.5.5 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.

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

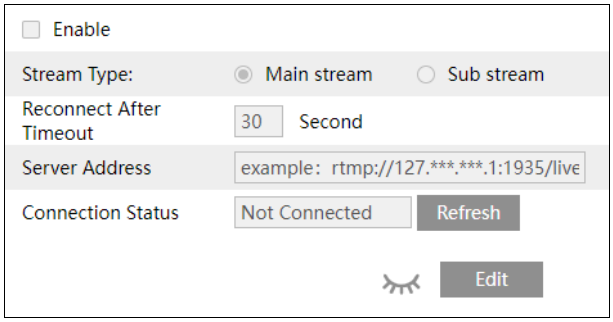
Note:

1. This camera supports local video preview through a VLC player. Enter the RTSP address 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.

3.5.6 RTMP

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

Go to **Config→Network→RTMP**.



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

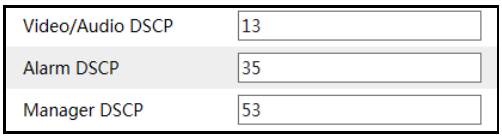
Server address: Enter the server address allocated by the third-party server.

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

3.5.7 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.

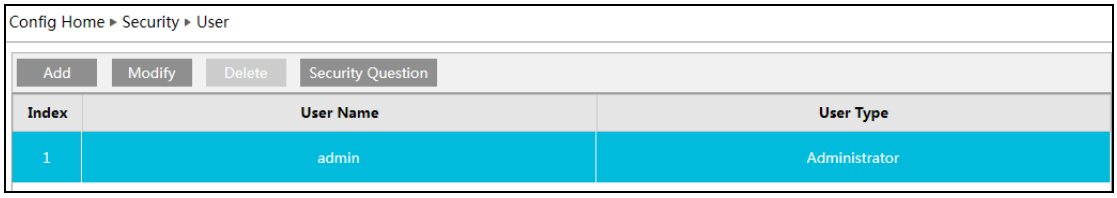
Manager DSCP: The range is from 0 to 63.

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

3.6 Security Configuration

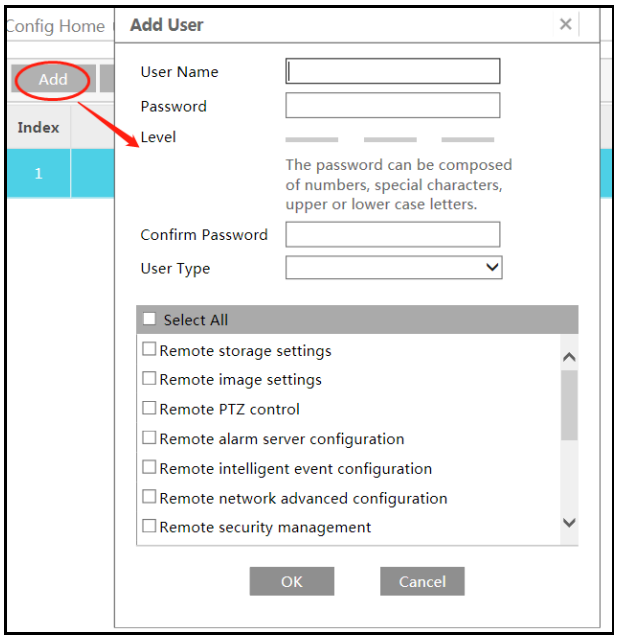
3.6.1 User Configuration

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



Add user:

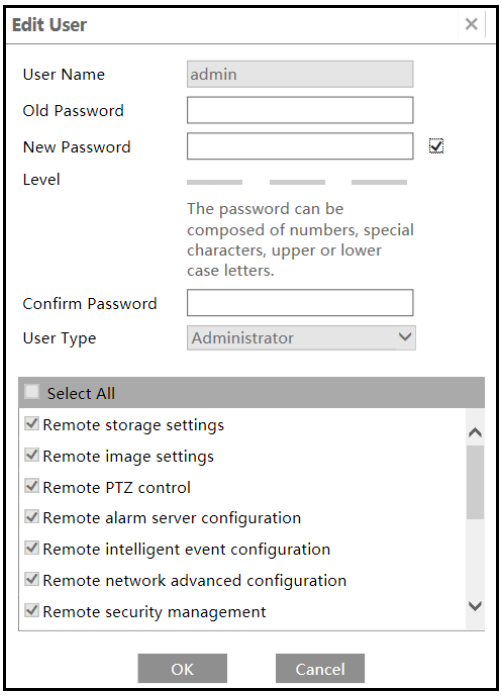
1. Click the “Add” button to pop up the following textbox.



2. Enter user name in 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 interface to set the security level).
4. Choose the user type and select the desired user permissions.
5. Click the “OK” button and then the newly added user will be displayed in the user list.

Modify user:

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



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.

Note: When the password level is set to “Strong”, the password cannot be set the same as the previous five.

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.

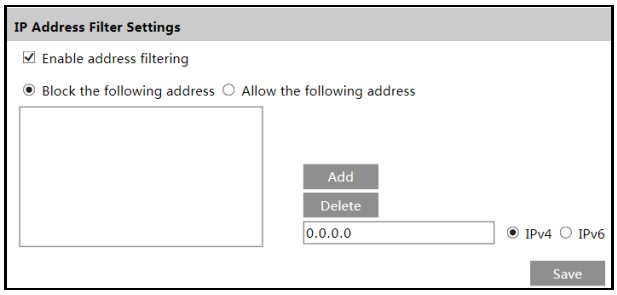
3.6.2 Online User

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.



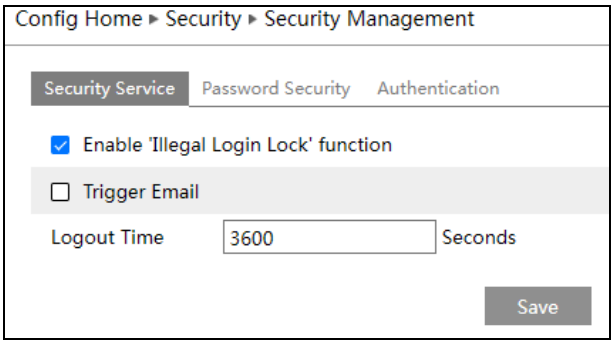
The setup steps are as follows:

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, “locking once illegal login” function can be enabled here. If this function is enabled, login failure after trying six 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: 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: 8~16 characters, including at least two of the following categories: numbers, special characters, upper case letters and lower case letters.
- Strong: 8~16 characters. Numbers, special characters, upper case letters and lower case letters must be included.

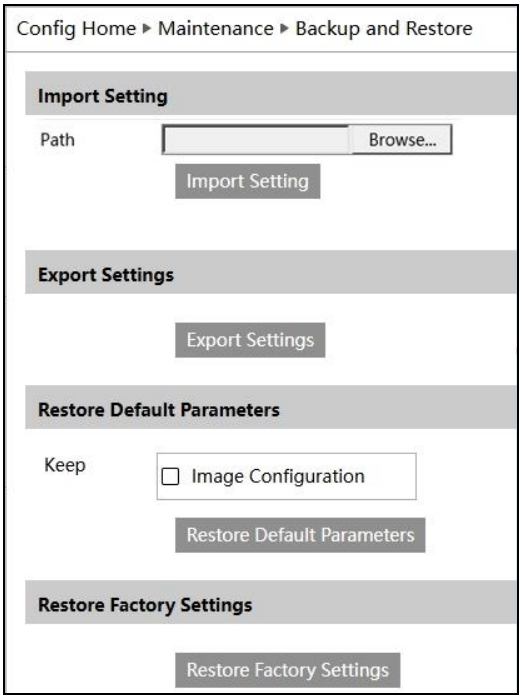
For your account security, it is recommended to set a strong password and change your password regularly.

HTTP Authentication: Basic or Token is selectable.

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.

- **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.

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

- **Restore Factory Settings**

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

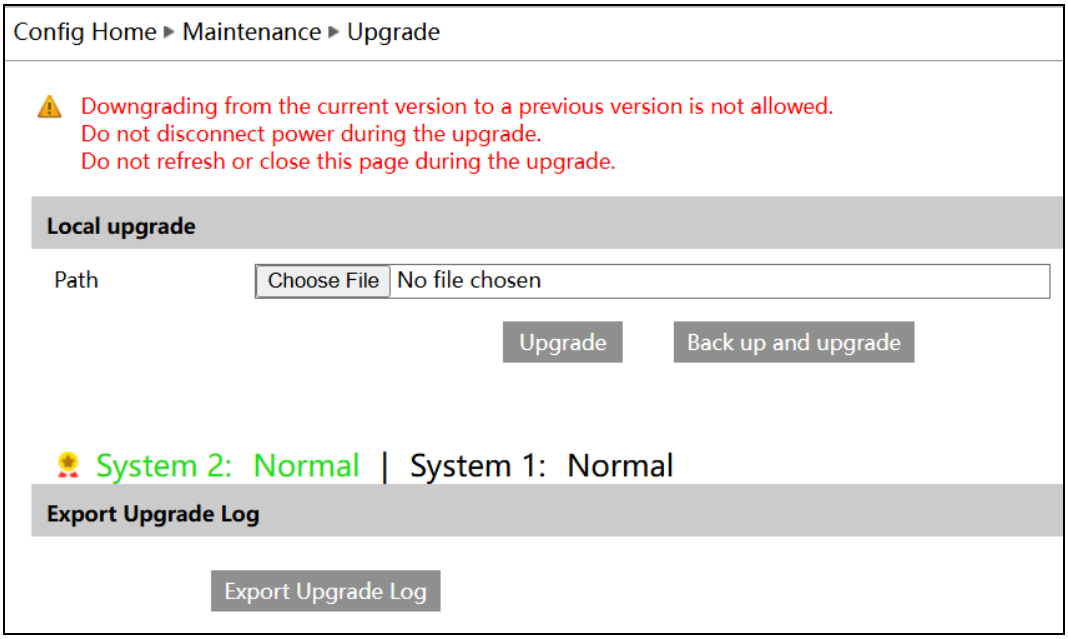
3.7.2 Reboot

Go to **Config→Maintenance→Reboot**.

Click the “Reboot” button to reboot the device.

3.7.3 Upgrade

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



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

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

Caution:

1. Do not allow downgrading from the current version to the 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.

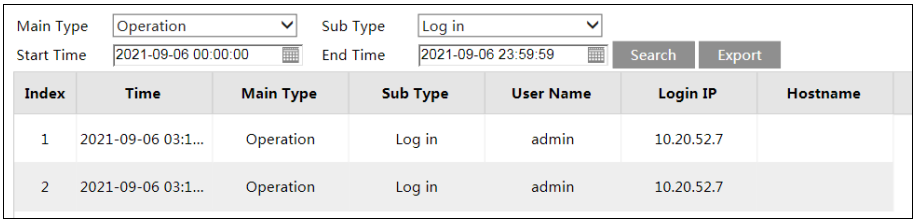
Note: To decrease the upgrade risk, this series of cameras adopts two systems. After one system is successfully upgraded, the other system will be synchronized. If one system fails caused by power failure or other reasons during the upgrade, the other system will not be affected and the camera still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

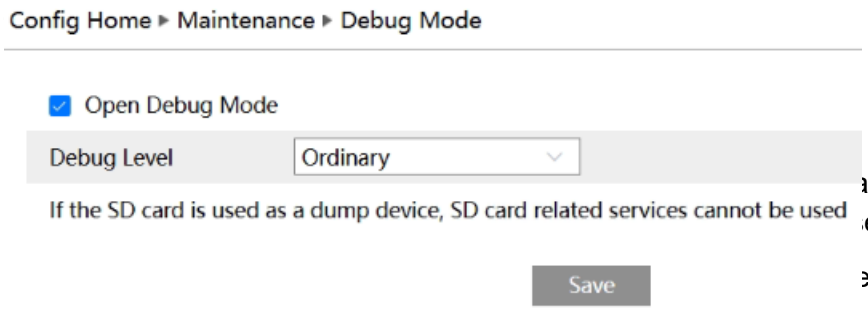
3.7.4 Operation Log

To query and export log:

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

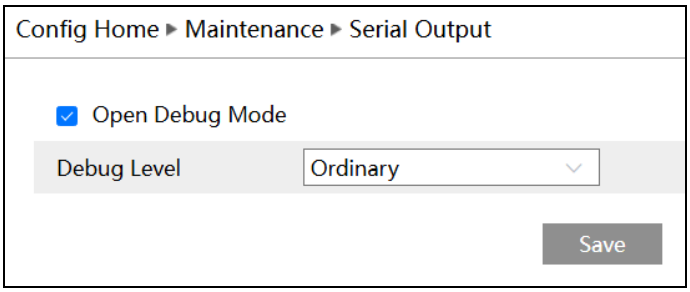


2. Select the main type, sub type, start and end time.
3. Click “Search” to view the operation log.



, so that the technician can
ervice.

echnical support.



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.

Appendix

Appendix 1 Troubleshooting

How to find the password?

A: The password for ***admin*** can be reset through “Edit Safety Question” function.

Click “Forget Password?” on the login page and 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 through a 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

No sound can be heard.

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

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

Appendix 2 Configuration Requirements and Surrounding Area

1. Try to avoid excessive obstruction from trees, while also avoiding excessive variations in lighting conditions in the scene, such as frequent and excessive car headlights, etc., to improve the accuracy of intelligent functions. The brightness of the scene should not be too low, as excessively dim scenes will reduce the accuracy of alarms. Adequate lighting and clear scenery are important conditions.
2. The optimal overhead angle for the camera is between 30 degrees and 45 degrees (see outdoor installation diagram for 12mm lens).

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

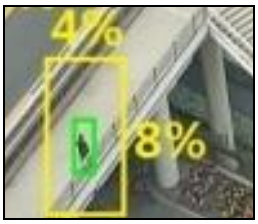
3. When the camera is detecting, the target should spend at least about 2 seconds passing through the detection area.
4. Not suitable for scenes with significant changes in lighting.
5. Adjust the camera so that the area needing protection is positioned as centrally as possible within the field of view. There should be no obstructions in the main thoroughfare areas. Try to exclude swaying obstructions such as trees, bushes, flags, etc., from the detection area.

6. Please adjust the camera's installation position or focal length so that the targets of interest in the frame meet certain size requirements. Optimal target recognition sizes:

Percentage	Human
Minimum (Width × Height)	4% × 8%
Maximum (Width × Height)	50%× 50%

The percentage here refers to the ratio of the target's width to the width of the frame. For example, in a resolution of 1920×1080, the minimum resolution for a person would be 80×160 (w=1920×4%=80, h=1920×8%=160).

Correct example: The target meets the minimum size requirements. The yellow box in the image represents the minimum detection box.

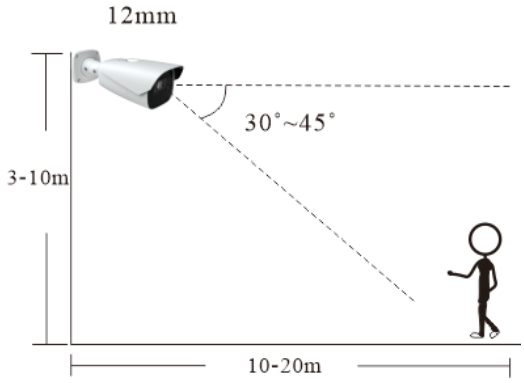


Incorrect example: The target does not meet the minimum size requirements. The yellow box in the image represents the minimum detection box.

7. Installation suggestion:

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

Focal Length	Installation Height(m)	Human Maximum Distance(m)	Optimal Distance(m)
2.8 mm	3-10	8	4-8
3.6 mm	3-10	10	5-10
12 mm	3-10	25	10~20
22 mm	3-10	45	30~40



Example for 12mm focal length

Indoor Mounting