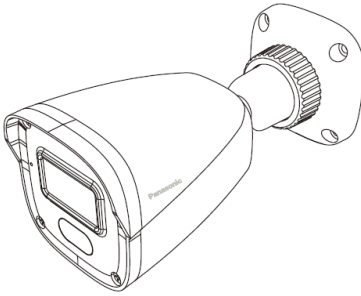


Panasonic[®]

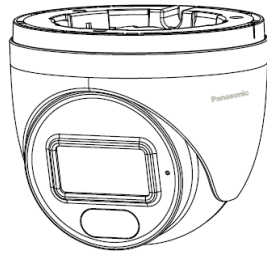
Operating Instructions

Network Camera

Model No. PM-EB2NLFR-W/PM-ED2NLFR-W



PM-EB2NLFR-W



PM-ED2NLFR-W

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

Safety Instruction

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

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

About the Manual

- This manual is suitable for many models. All examples, screenshots, figures, charts, and illustrations used in the manual are for reference 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 POE 48V/ 350mA, no more than 2000m altitude of operation and Tma=60 Deg.C.

- As for the modes with PoE function, the function of the ITE being investigated to IEC 60950-1 standard is considered not likely to require connection to an Ethernet network with outside plant routing, including campus environment and the ITE is to be connected only to PoE networks without routing to the outside plant.
- Improper handling and/or installation could run the risk of fire or electrical shock.
- The product must be grounded to reduce the risk of electric shock.
- **⚠ Warning:** Wear anti-static gloves or discharge static electricity before removing the bubble or cover of the camera.
- **⚠ Caution:** Do not provide two power supply sources at the same time for the device unless otherwise specified; it may result in device damage!

Environment

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

Operation and Daily Maintenance

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

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.

Privacy Protection

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

Disclaimer

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

Cybersecurity Recommendations

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

specified IP addresses from accessing the system.

- If you add multiple users, please limit functions of guest accounts.
- If you enable UPnP, it will automatically try to forward ports in your router or modem. It is really very convenient for users, but this will increase the risk of data leakage when the system automatically forwards ports. Disabling UPnP is recommended when the function is not used in real applications.
- Check the log. If you want to know whether your device has been accessed by unauthorized users or not, you can check the log. The system log will show you which IP addresses were used to log in your system and what was accessed.

Regulatory Information

FCC Information

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

1. FCC compliance

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

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

2. FCC conditions:

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

RoHS

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



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

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

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

Table of Contents

1	Network Connection	1
1.1	LAN	1
1.1.1	Access through Panasonic IP Manager Tool	1
1.1.2	Directly Access through IE	3
1.2	WAN	4
2	Live View	8
3	Network Camera Configuration	9
3.1	System Configuration	9
3.1.1	Basic Information	9
3.1.2	Date and Time	9
3.1.3	Local Config	10
3.2	Image Configuration	10
3.2.1	Display Configuration	10
3.2.2	Video / Audio Configuration	13
3.2.3	OSD Configuration	14
3.2.4	Video Mask	15
3.2.5	ROI Configuration	16
3.3	Alarm Configuration	16
3.3.1	Motion Detection	16
3.3.2	Alarm Server	18
3.4	Event Configuration	19
3.4.1	Video Exception	19
3.4.2	Line Crossing	20
3.4.3	Region Intrusion	22
3.5	Network Configuration	23
3.5.1	TCP/IP	23
3.5.2	Port	24
3.5.3	Server Configuration	24
3.5.4	Onvif	25
3.5.5	DDNS	26
3.5.6	SNMP	27
3.5.7	802.1x	29
3.5.8	RTSP	29
3.5.9	UPNP	30
3.5.10	Email	30
3.5.11	FTP	31
3.5.12	HTTPS	33
3.5.13	QoS	34
3.6	Security Configuration	35
3.6.1	User Configuration	35
3.6.2	Online User	36

- 3.6.3 Block and Allow Lists 37
- 3.6.4 Security Management 37
- 3.7 Maintenance Configuration..... 38
 - 3.7.1 Backup and Restore 38
 - 3.7.2 Reboot 39
 - 3.7.3 Upgrade 39
 - 3.7.4 Operation Log..... 40
- 4 Search 41**
 - 4.1 Image Search 41
 - 4.2 Video Search..... 42
- Appendix..... 44**
- Appendix 1 Troubleshooting 44**

1 Network Connection

System Requirement

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

Operating System: Windows 7 Home basic or higher

CPU: 2.0GHz or higher

RAM: 1G or higher

Display: 1920*1080 resolution or higher (recommended)

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

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

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

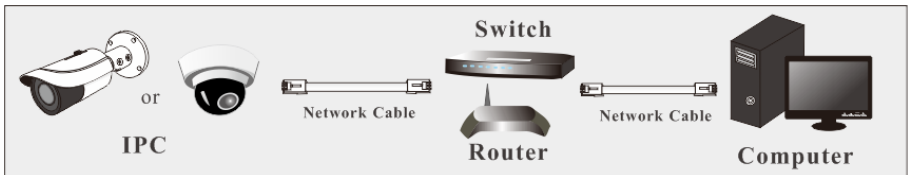
Connect IP Camera via LAN or WAN. Here only take IE browser for example. The details are as follows:

1.1 LAN

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

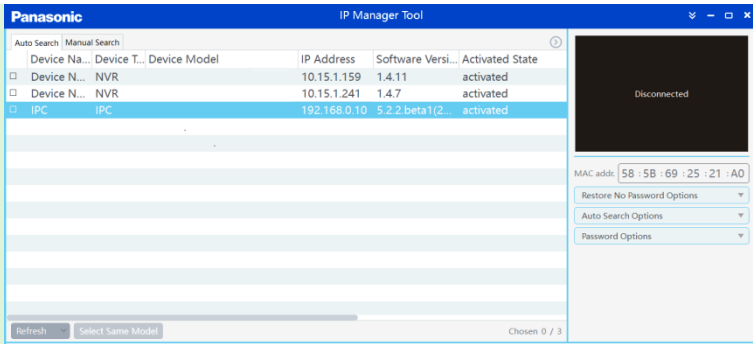
1.1.1 Access through Panasonic IP Manager Tool

Network connection:



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

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



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

③ Double click the IP address and then the system will pop up the IE browser to connect IP CAMERA. After you read the privacy statement, check and click “Already Read”. Then activate the device.

Device Activation

User Name

Activate Onvif User

New Password

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

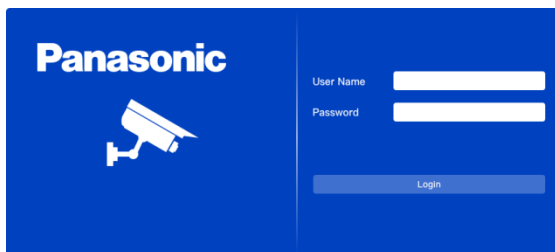
Confirm Password

Please self-define the password of admin according to the tip.

If “Activate Onvif User” is enabled, the ONVIF user can be activated simultaneously. When you connect the camera through the ONVIF protocol in the third-party platform, you can use the default username and the password set above to connect.

After that, follow directions to download, install and run the Active X control if prompted.

Re-connect your camera via IE browser and then a login box will appear.



Please enter the user name (admin) and password.

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

Safety Question	
Security Question1	<input type="text" value="Your father's name?"/>
Answer	<input type="text"/>
Security Question2	<input type="text" value="Your seniors school name?"/>
Answer	<input type="text"/>
Security Question3	<input type="text" value="Your favorite book?"/>
Answer	<input type="text"/>
<input type="button" value="OK"/>	

1.1.2 Directly Access through IE

The default network settings are as shown below:

IP address: **192.168.0.10**

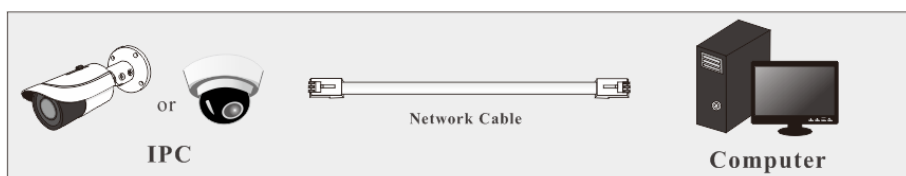
Subnet Mask: **255.255.255.0**

Gateway: **192.168.0.1**

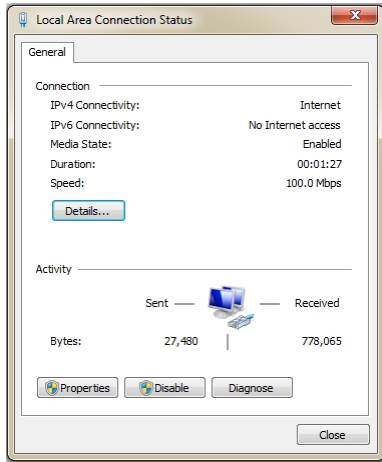
HTTP: **80**

Data port: **9008**

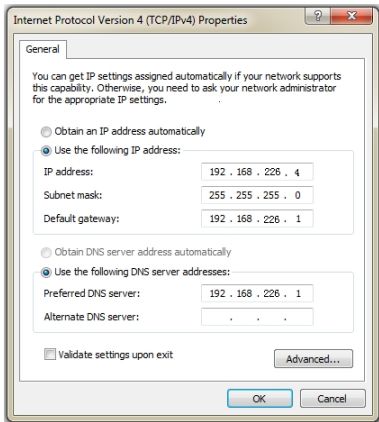
Use the above default settings when logging in the camera for the first time. Directly connect the camera to the computer through network cable.



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



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



- ② Open the IE browser and enter the default address of IP CAMERA and confirm.
- ③ Follow directions to download and install the Active X control.
- ④ Enter the default username and password in the login window and then enter to view.

1.2 WAN

➤ Access through the router or virtual server



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

HTTP Port	<input type="text" value="80"/>
HTTPS Port	<input type="text" value="443"/>
Data Port	<input type="text" value="9008"/>
RTSP Port	<input type="text" value="554"/>

Port Setup

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

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

IP Setup

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

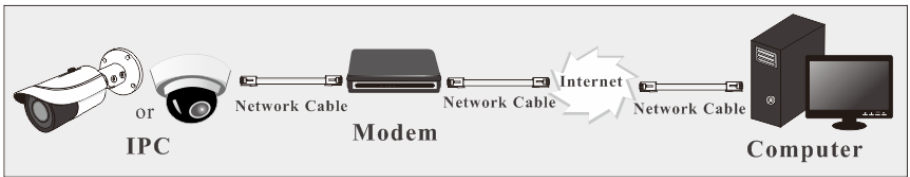
Port Range					
Application	Start	End	Protocol	IP Address	Enable
1	9007	to 9008	Both	192.168.1.201	<input checked="" type="checkbox"/>
2	80	to 81	Both	192.168.1.201	<input checked="" type="checkbox"/>
3	10000	to 10001	Both	192.168.1.166	<input type="checkbox"/>
4	21000	to 21001	Both	192.168.1.166	<input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

Router Setup

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

➤ Access through PPPoE dial-up

Network connection



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

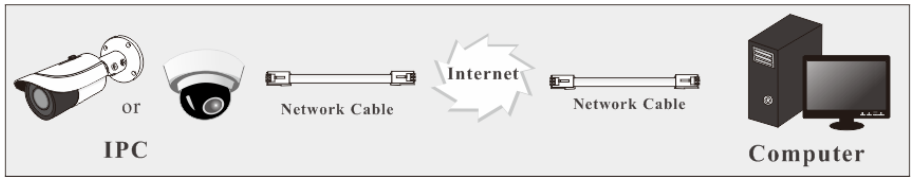
- ① Go to Config → Network → Port menu to set the port number.
- ② Go to Config → Network → TCP/IP → PPPoE Config menu. Enable PPPoE and then enter the user name and password from your internet service provider.

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

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

➤ **Access through static IP**

Network connection

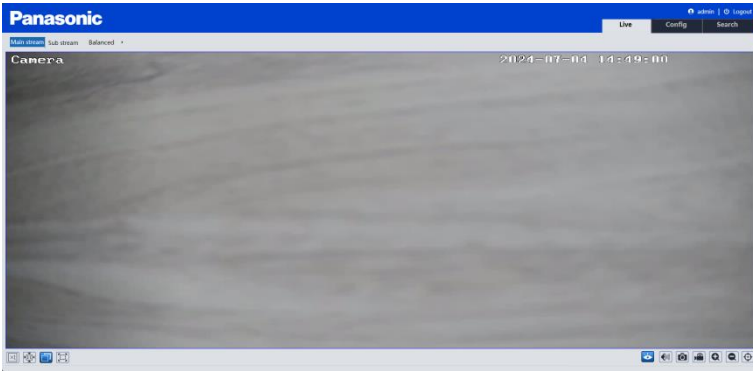


The setup steps are as follow:

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

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		Zoom out
	Fit correct scale		Rule information display
	Auto (fill the window)		Motion alarm indicator
	Full screen		Scene change indicator
	Start/stop live view		Color abnormal indicator
	Enable/disable audio		Abnormal clarity indicator
	Snapshot		Line crossing indicator
	Start/stop local recording		Intrusion indicator
	Zoom in		

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

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

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

3 Network Camera Configuration

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

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

3.1 System Configuration

3.1.1 Basic Information

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

Device Name	IPC
Product Model	IPC
Brand	Customer
Software Version	5.1.1.0(50769)
Software Build Date	2023-09-18
Onvif Version	22.12
MAC	00:18:ae:00:00:04
About this machine	View
Privacy Statement	View

3.1.2 Date and Time

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

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

Select the time zone and DST 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.

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

Zone	Date and Time
Time Mode:	
<input checked="" type="radio"/> Synchronize with NTP server	
NTP server:	<input type="text" value="time.windows.com"/>
Update period:	<input type="text" value="1440"/> Minutes
<input type="radio"/> Synchronize with computer time	
Date	<input type="text" value="2021-09-01"/>
Time	<input type="text" value="17:37:36"/>
<input type="radio"/> Set manually	
	<input type="text" value="2021-09-01 09:37:32"/> <input type="button" value="Calendar"/>
Time Format	<input type="text" value="24-Hour"/> <input type="button" value="v"/>
<input type="button" value="Save"/>	

3.1.3 Local Config

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

Picture Path	<input type="text" value="C:\Program Files\NetAllIPCamera"/>	<input type="button" value="Browse"/>
Record Path	<input type="text" value="C:\Program Files\NetAllIPCamera"/>	<input type="button" value="Browse"/>
Video Audio Settings	<input type="radio"/> Open	<input checked="" type="radio"/> Close
Show Bitrate	<input type="radio"/> Open	<input checked="" type="radio"/> Close
Local Smart Snapshot Storage	<input type="radio"/> Open	<input checked="" type="radio"/> Close
<input type="button" value="Save"/>		

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

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

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

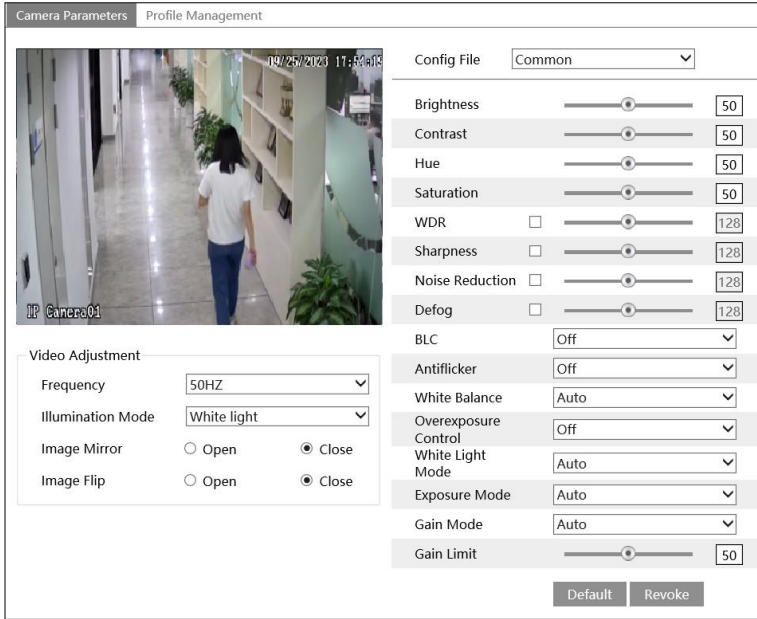
3.2 Image Configuration

3.2.1 Display Configuration

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

Note: the camera parameters of different cameras may be slightly different. The following

pictures and descriptions are for reference only. The real camera interface shall prevail.



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

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

Hue: Set the total color degree of the image.

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

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 the view by lowering the brightness of the bright area and increasing the brightness of the dark area.

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

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.

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.

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

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

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” or “Infrared light” 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” and “Infra-red Mode” can be configured.

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

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

Infra-red Mode: Choose “Auto”, “On” or “Off”.

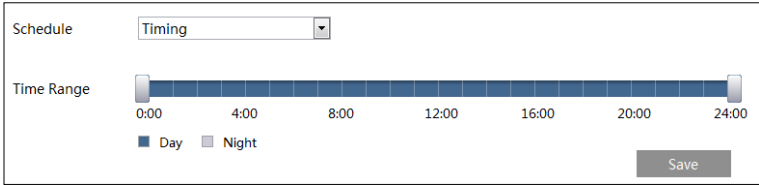
Note: For some items, if selected/enabled, the camera will reboot automatically. After that, clicking “Default” button will not take effect.

Schedule Settings of Image Parameters:

Click the “Profile Management” tab as shown below.

Camera Parameters	Profile Management
Schedule	Full Time
Config File	Common
Save	

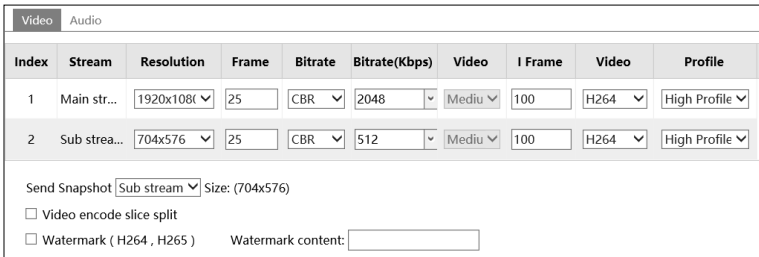
Set full time schedule for common, auto mode and specified time schedule for day and night. Choose “Timing” in the drop-down box of schedule as shown below.



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.



Two video streams can be adjustable.

Resolution: The size of image.

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

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

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

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

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

usage. However, if the value is set too high, and there is a high frequency of movement in the video, there is a risk of frame skipping.

Video Compression: H264+, H264, H265 or H265+ can be optional. If H.265/H.265+ is chosen, make sure the client system is able to decode H.265/H.265+. Compared to H.265, H.265+ saves more storage space with the same maximum bitrate in most scenes. Compared to H.264, H.265 reduces the transmission bitrate under the same resolution, frame rate and image quality.

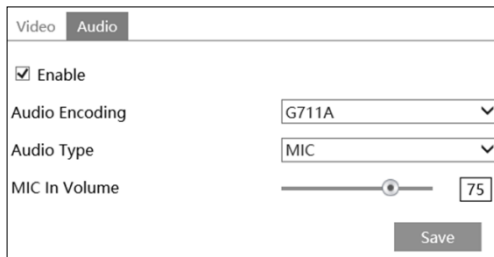
Profile: For H.264. Baseline, main and high profiles are selectable.

Send Snapshot: Set the snapshot stream.

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

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

Click the “Audio” tab to go to the interface as shown below.
Only the models with the built-in MIC support this function.



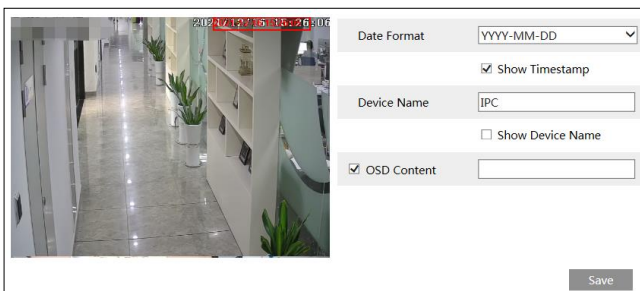
Audio Encoding: G711A and G711U are selectable.

Audio Type: MIC.

MIC IN Volume: MIC IN volume can be set as needed.

3.2.3 OSD Configuration

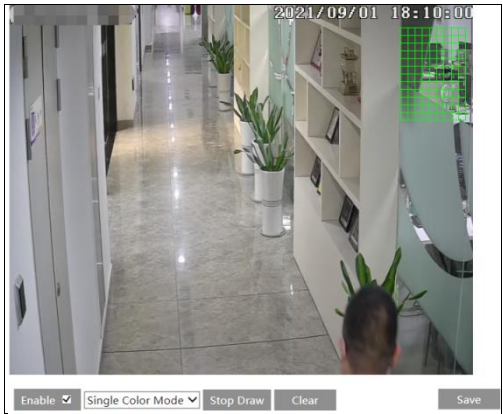
Go to Image→OSD interface as shown below.



Set time stamp, device name and 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.

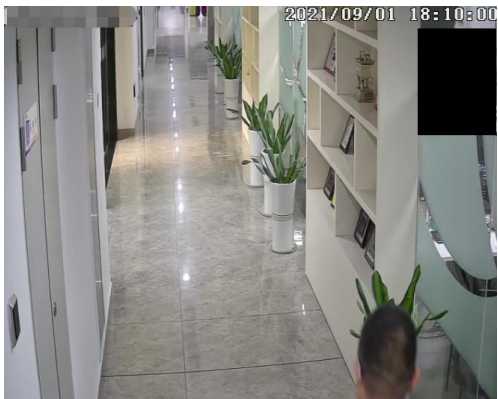
3.2.4 Video Mask

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 have been drawn as shown as blocked out in the image.

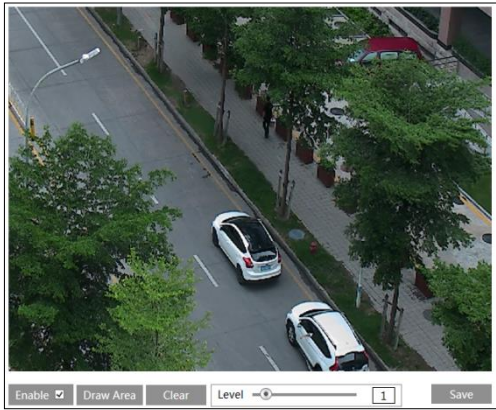


To clear the video mask:

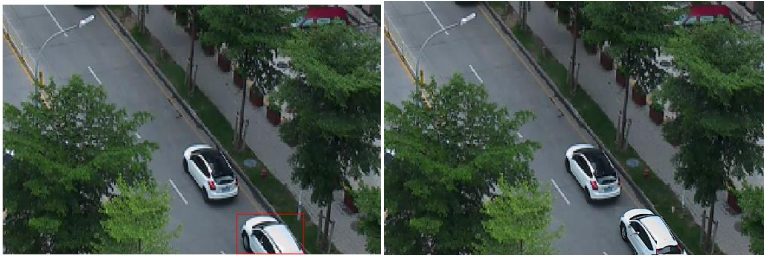
Click the “Clear” button to delete the current video mask area.

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.



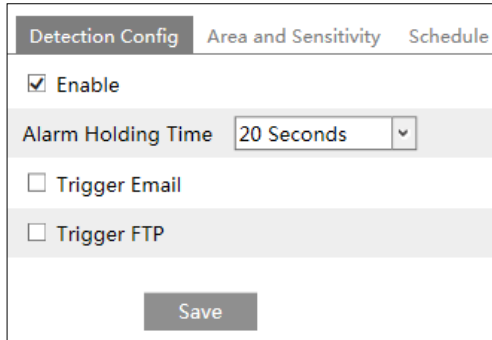
1. Check “Enable” and then click the “Draw Area” button.
2. Drag the mouse to set the ROI area.
3. Set the level.
4. Click the “Save” button to save the settings.



3.3 Alarm Configuration

3.3.1 Motion Detection

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



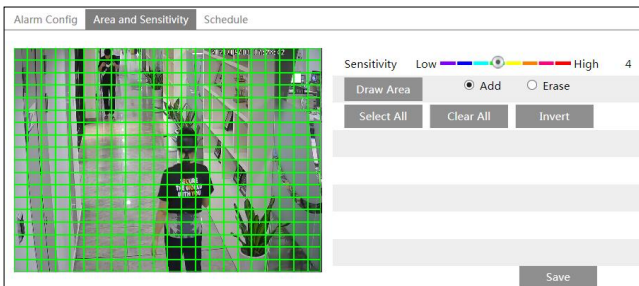
1. Check “Enable” check box to activate motion based alarms. If unchecked, the camera will not send out any signals to trigger motion-based recording to the NVR or CMS, even if there is motion in the video.

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.

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

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

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

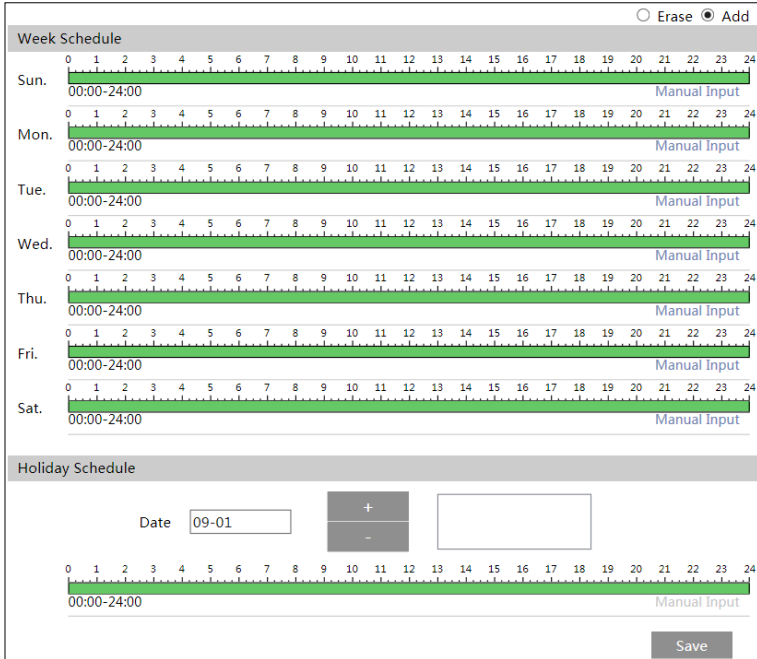


Move the “Sensitivity” scroll bar to set the sensitivity. Higher “sensitivity” value means that motion will be triggered more easily.

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

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

3. Set the schedule for motion detection.



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 Alarm Server

Go to Alarm→Alarm Server interface as shown below.

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

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

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.

3.4.1 Video Exception

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

To set exception detection:

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

Detection Config		Sensitivity
<input checked="" type="checkbox"/>	Scene Change Detection	
<input checked="" type="checkbox"/>	Video Blur Detection	
<input checked="" type="checkbox"/>	Abnormal Color Detection	
Alarm Holding Time	<input type="text" value="20 Seconds"/>	▼
<input type="checkbox"/>	Trigger Email	
<input type="checkbox"/>	Trigger FTP	
<input type="button" value="Save"/>		

1. Enable the applicable detection that's desired.

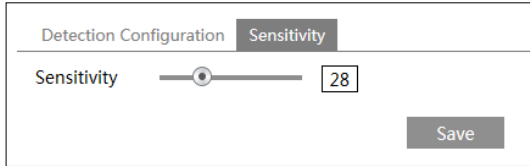
Scene Change Detection: Alarms will be triggered if the scene of the monitor video has changed.

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

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

color deviation.

2. Set the alarm holding time and alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection section for details.
3. Click “Save” button to save the settings.
4. Set the sensitivity of the exception detection. Click “Sensitivity” tab to go to the interface as shown below.



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

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

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

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

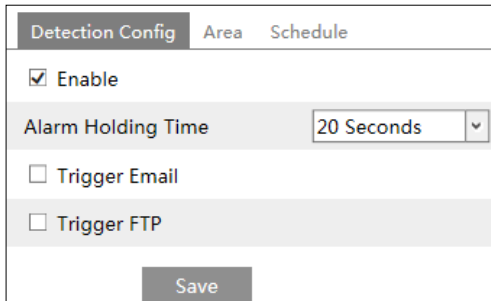
※ The requirements of camera and surrounding area

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

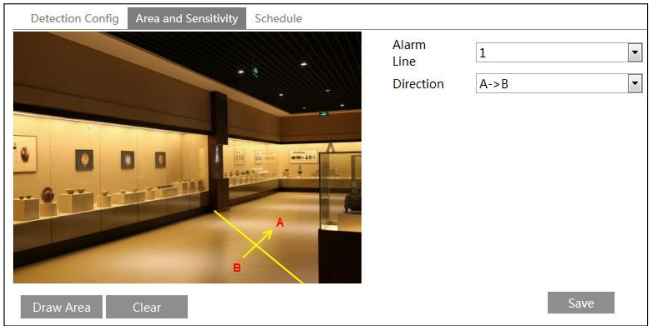
3.4.2 Line Crossing

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

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



1. Enable line crossing alarm and set the alarm holding time.
2. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to [Motion Detection](#) section for details.
3. Click “Save” button to save the settings.
4. Set area and sensitivity of the line crossing alarm. Click the “Area and Sensitivity” tab to go to the interface as shown below.



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

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.

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

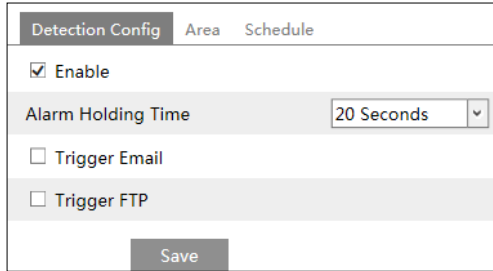
✖ Configuration of camera and surrounding area

1. 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.
2. Cameras should be mounted at a height of 2.8 meters or above.
3. Keep the mounting angle of the camera at about 45°.
4. The detected objects should not be less than 1% of the entire image and the largest sizes of the detected objects should not be more than 1/8 of the entire image.
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.

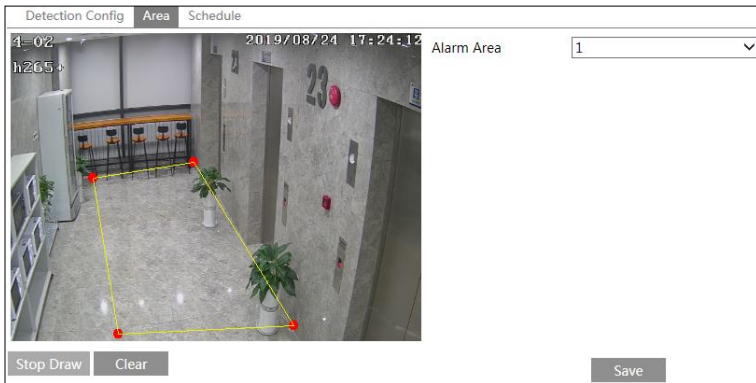
3.4.3 Region Intrusion

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

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



1. Enable region intrusion detection alarm and set the alarm holding time.
2. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to [Motion Detection](#) section for details.
3. Click the “Save” button to save the settings.
4. Set the alarm area of the intrusion detection. Click the “Area” tab to go to the interface as shown below.



- Set the alarm area number on the right side. 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 on the left side (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.
5. Set the schedule of the region intrusion detection. The setup steps of schedule are the same as the motion detection schedule settings (See [Motion Detection](#) section for details).

※ Configuration requirements of camera and surrounding area

1. 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.
2. Cameras should be mounted at a height of 2.8 meters or above.
3. Keep the mounting angle of the camera at about 45°.
4. The detected objects should not be less than 1% of the entire image and the largest sizes of the detected objects should not be more than 1/8 of the entire image.
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 to line crossing detection.

3.5 Network Configuration

3.5.1 TCP/IP

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

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

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

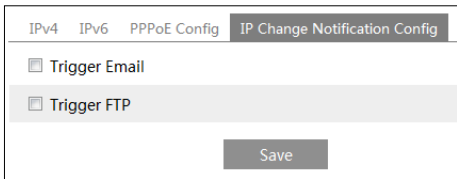
Test: Test the effectiveness of the IP address by clicking this button.

Use PPPoE-Click the “PPPoE Config” tab to go to the interface as shown below. Enable PPPoE and then enter the user name and password from your ISP.

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

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

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



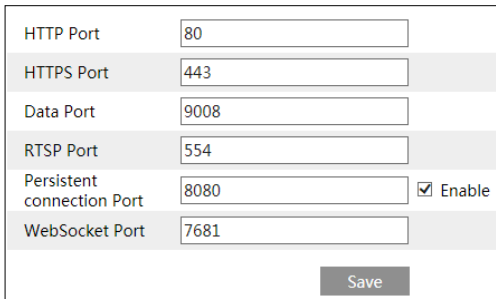
The screenshot shows a configuration page with a top navigation bar containing tabs for IPv4, IPv6, PPPoE Config, and IP Change Notification Config. The IP Change Notification Config tab is selected. Below the tabs, there are two checkboxes: "Trigger Email" and "Trigger FTP", both of which are currently unchecked. At the bottom center of the page is a "Save" button.

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 interface as shown below. HTTP port, Data port and RTSP port can be set.



The screenshot shows a configuration page for ports. It contains several input fields for different ports: HTTP Port (80), HTTPS Port (443), Data Port (9008), RTSP Port (554), Persistent connection Port (8080), and WebSocket Port (7681). There is also a checkbox labeled "Enable" which is checked. At the bottom center of the page is a "Save" button.

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

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

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

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

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

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

3.5.3 Server Configuration

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

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

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

3.5.4 Onvif

The camera can be searched and connected to the third-party platform via ONVIF/RTSP protocol.

If “Activate Onvif User” is enabled in the device activation interface, the ONVIF user can be activated simultaneously. When you connect the camera through the ONVIF protocol in the third-party platform, you can use this onvif user to connect.

You can also add new users in the Onvif interface.

The screenshot shows the Onvif user management interface. At the top, there are tabs for Port, Server, Onvif, and DDNS. Below the tabs are buttons for Add, Modify, and Delete. A table lists existing users with columns for Index, User Name, and User Type. The 'Add' button is circled in red, and a red arrow points to the 'Add User' dialog box. The dialog box contains the following fields and options:

Index	User Name	User Type
1	admin	Administrator

Add User dialog box fields:

- User Name:
- Password:
- Level:
- Confirm Password:
- User Type:

The password field has a note: "The password can be composed of numbers, special characters, upper or lower case letters."

Buttons:

Note: when adding the device to the third-party platform with ONVIF/RTSP protocol, please

use the onvif user in the above interface.

3.5.5 DDNS


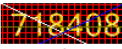
If the camera is set up with a DHCP connection, DDNS should be set for the internet.

1. Go to Config→Network→ DDNS.

<input checked="" type="checkbox"/> Enable	
Server Type	www.dyndns.com ▼
User Name	<input type="text"/>
Password	<input type="password"/>
Domain	<input type="text"/>
<input type="button" value="Save"/>	

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

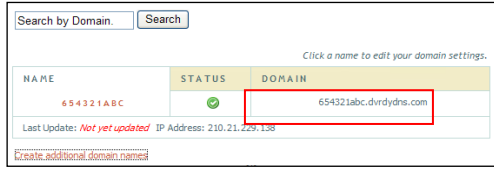
Enter www.dvrddns.com in the IE address bar to visit its website. Then Click the “Registration” button.

NEW USER REGISTRATION	
USER NAME	<input type="text" value="xxxx"/>
PASSWORD	<input type="password" value="•••••"/> 
PASSWORD CONFIRM	<input type="password" value="•••••"/>
FIRST NAME	<input type="text" value="xxx"/>
LAST NAME	<input type="text" value="xxx"/>
SECURITY QUESTION.	My first phone number. ▼
ANSWER	<input type="text" value="xxxxxxxx"/>
CONFIRM YOU'RE HUMAN	 New Captcha <input type="text"/> Enter the text you see above
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Create domain name.

<i>You must create a domain name to continue.</i>	
<small>Domain name must start with (a-z, 0-9). Cannot end or start, but may contain a hyphen and is not case-sensitive.</small>	
<input type="text"/>	dvrddns.com ▼ <input type="button" value="Request Domain"/>

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



Search by Domain

Click a name to edit your domain settings.

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

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

[Create additional domain names!](#)

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

3.5.6 SNMP

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

1. Go to Config→Network→SNMP.

SNMP v1/v2	
<input checked="" type="checkbox"/> Enable SNMPv1	
<input checked="" type="checkbox"/> Enable SNMPv2	
Read SNMP Community	public
Write SNMP Community	private
Trap Address	192.168.226.201
Trap Port	162
Trap community	public
SNMP v3	
<input type="checkbox"/> Enable SNMPv3	
Read User Name	public
Security Level	auth, priv
Authentication Algorithm	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Authentication Password	●●●●●●●●
Private-key Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES
Private-key Algorithm	●●●●●●●●
Write User Name	private
Security Level	auth, priv
Authentication Algorithm	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Authentication Password	●●●●●●●●
Private-key Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES
Private-key Algorithm	●●●●●●●●
Other Settings	
SNMP Port	161

2. Check the corresponding version checkbox (Enable SNMPv1, Enable SNMPv2, Enable SNMPv3) according to the version of the SNMP software that will be used.

3. Set the values for “Read SNMP Community”, “Write SNMP Community”, “Trap Address”, “Trap Port” and so on. Please make sure the settings are the same as that of the SNMP software.

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

3.5.7 802.1x

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

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

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

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

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

3.5.8 RTSP

Go to Config→Network→RTSP.

<input checked="" type="checkbox"/> Enable			
Port	554		
Address	rtsp://IP or domain name:port/profile1		
	rtsp://IP or domain name:port/profile2		
Multicast address			
Main stream	239.0.0.0	50554	<input type="checkbox"/> Automatic start
Sub stream	239.0.0.2	52554	<input type="checkbox"/> Automatic start
Audio	239.0.0.3	53554	<input type="checkbox"/> Automatic start
<input type="checkbox"/> Allow anonymous login (No username or password required)			
Save			

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=mcst”.

Sub stream: The address format is

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

Audio: Having entered the main/sub stream in a VLC player, the video and audio will play automatically. (Only the model with the built-in MIC supports this function)

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

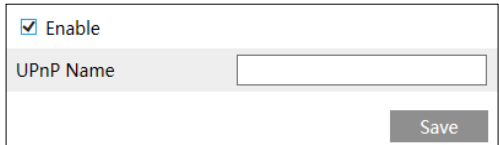
If “auto start” is enabled, the multicast received data should be added into a VLC player to play the video.

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

- 2. The IP address mentioned above cannot be the address of IPv6.
- 3. Avoid the use of the same multicast address in the same local network.
- 4. When playing the video through the multicast streams in a VLC player, please pay attention to the mode of the VLC player. If it is set to TCP mode, the video cannot be played.

3.5.9 UPNP

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



Enable

UPnP Name

Save

3.5.10 Email

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

Go to Config→Network →Email.

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

Sender Address: sender’s e-mail address.

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

Server Address: The SMTP IP address or host name.

Select the secure connection type at the “Secure Connection” pull-down list according to what’s required.

SMTP Port: The SMTP port.

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

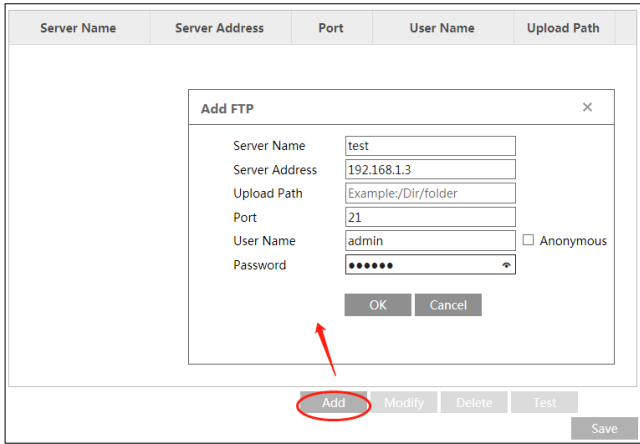
Click the “Test” button to test the connection of the account.

Recipient Address: receiver’s e-mail address.

3.5.11 FTP

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

1. Go to Config→Network →FTP.



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

Server Name: The name of the FTP server.

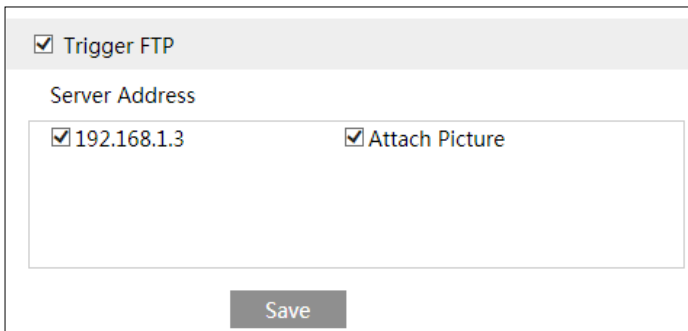
Server Address: The IP address or domain name of the FTP.

Upload Path: The directory where files will be uploaded to.

Port: The port of the FTP server.

User Name and Password: The username and password that are used to login to the FTP server.

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



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
AVD	Video exception
TRIPWIRE	Line crossing detection
PERIMETER	Region intrusion detection

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

3.5.12 HTTPS

HTTPS provides authentication of the web site and protects user privacy.

Go to Config →Network→HTTPS as shown below.

The screenshot shows a configuration window with an "Enable" checkbox at the top left. Below it, a "Certificate installed" field displays "C=CN, ST=GD, L=SZ, O=IPC, OU=embeddec" with a "Delete" button to its right. An "Attribute" field shows detailed certificate information: "Issued to: C=CN, ST=GD, L=SZ, O=IPC, OU=embeddedsoftware, H=localhost, Issuer: C=CN, ST=GD, L=SZ, O=IPC, OU=embeddedsoftware, H=localhost, Validity date: 2020-03-14 08:12:45 ~ 2033-11-21 08:12:45". A "Save" button is located at the bottom right of the window.

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

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

The screenshot shows a configuration window with an "Enable" checkbox at the top left. Below it, the "Installation type" section has three radio button options: "Have signed certificate, install directly" (which is selected), "Create a private certificate", and "Create a certificate request". Below this, the "Install certificate" field is empty, with "Browse" and "Install" buttons to its right. A "Save" button is located at the bottom right of the window.

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

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

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

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

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

Enable
 Installation type
 Have signed certificate, install directly
 Create a private certificate
 Create a certificate request
 Create a certificate request
 Install Created Certificate

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

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

Alarm DSCP: The range is from 0 to 63.

Manager DSCP: The range is from 0 to 63.

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

3.6 Security Configuration

3.6.1 User Configuration

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

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

Add user:

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

Add User [X]

User Name

Password

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

Confirm Password

User Type [v]

Select All

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

OK Cancel

2. Enter user name in 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 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 so as to reset the password after you forget the password.

3.6.2 Online User

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

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

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 screenshot shows the 'IP Address Filter Settings' window. It has a title bar with the text 'IP Address Filter Settings'. Below the title bar, there is a checked checkbox labeled 'Enable address filtering'. Underneath, there are two radio buttons: 'Block the following address' (which is selected) and 'Allow the following address'. A large empty rectangular box is provided for listing addresses. To the right of this box are two buttons: 'Add' and 'Delete'. Below these buttons is a text input field containing '0.0.0.0'. To the right of the input field are two radio buttons: 'IPv4' (selected) and 'IPv6'. At the bottom right corner of the window is a 'Save' button.

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.

The screenshot shows the 'Security Management' configuration page. At the top, there are three tabs: 'Security Service' (selected), 'Password Security', and 'Authentication'. Below the tabs, there is a checked checkbox labeled 'Enable "Illegal Login Lockout" function'. Below that is an unchecked checkbox labeled 'Trigger Email'. Underneath, there is a label 'Logout Time' followed by a text input field containing '300' and the word 'Second'. At the bottom right corner is a 'Save' button.

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

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

- **Password Security**

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

Please set the password level and expiration time as needed.

Password Level: Weak, Medium or Strong.

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

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

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

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

HTTP Authentication: Basic or Token is selectable.

Security Service	Password Security	Authentication
HTTP Authentication	Basic ▼	
		Save

3.7 Maintenance Configuration

3.7.1 Backup and Restore

Go to Config→Maintenance→Backup & Restore.

The screenshot displays a web interface for camera settings, organized into three main sections:

- Import Setting:** Contains a text input field labeled "Path" with a "Browse" button to its right. Below the input field is a button labeled "Import Setting".
- Export Settings:** Contains a single button labeled "Export Settings".
- Default Settings:** Contains a section labeled "Keep" with a list of three checkboxes: "Network Config", "Security Configuration", and "Image Configuration". Below this list is a button labeled "Load Default".

● Import & Export Settings

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

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

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

● Default Settings

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

3.7.2 Reboot

Go to Config→Maintenance→Reboot.

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

Timed Reboot Setting:

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

3.7.3 Upgrade

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

Local upgrade

Path

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

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

3.7.4 Operation Log

To query and export log:

1. Go to Config→Maintenance→Operation Log.

Main Type		<input type="text" value="Operation"/>	Sub Type		<input type="text" value="Log in"/>		
Start Time		<input type="text" value="2021-09-06 00:00:00"/>	End Time		<input type="text" value="2021-09-06 23:59:59"/>	<input type="button" value="Search"/>	<input type="button" value="Export"/>
Index	Time	Main Type	Sub Type	User Name	Login IP	Hostname	
1	2021-09-06 03:1...	Operation	Log in	admin	10.20.52.7		
2	2021-09-06 03:1...	Operation	Log in	admin	10.20.52.7		

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

4 Search


4.1 Image Search

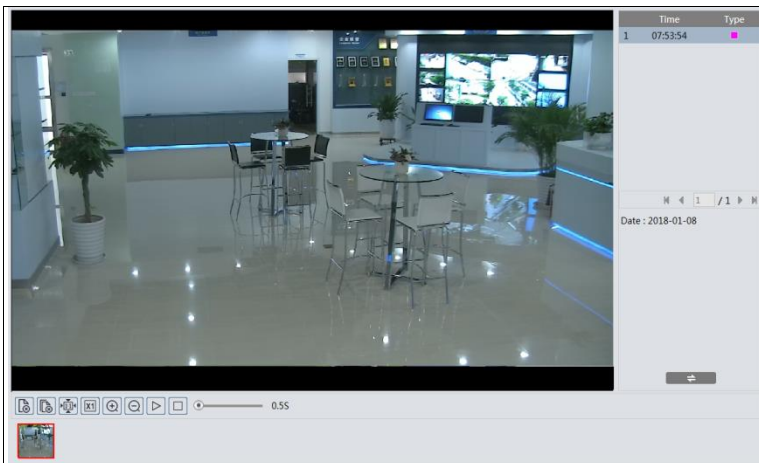
Click **Search** to go to the interface as shown below. Images that are saved on the local PC card can be found here.


Note: When using the plug-in free browser, the local images cannot be searched.












● Local Image Search

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



Click  to return to the previous interface.

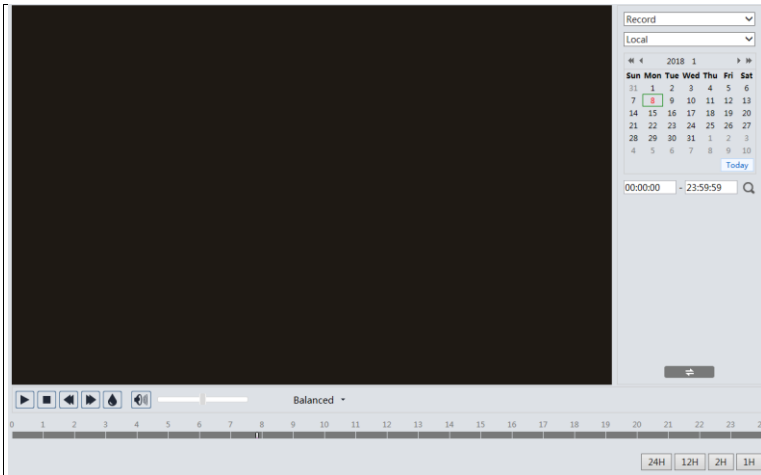
The descriptions of the buttons are shown as follows.


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

4.2 Video Search








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

Note: When using the plug-in free browser, the local videos cannot be searched.



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



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

Appendix

Appendix 1 Troubleshooting

How to find the password?

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

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

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

Fail to connect devices through IE browser.

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

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

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

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

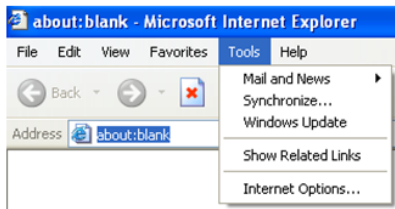
Panasonic IP Manager Tool cannot search devices.

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

IE cannot download ActiveX control.

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

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

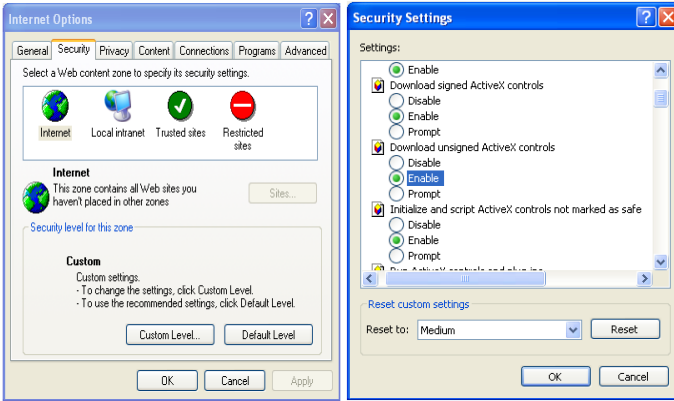


② Select Security-----Custom Level....

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

④ Click OK to finish setup.

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



No sound can be heard.

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

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