Fisheye Network Camera

User Manual

Please read this instruction carefully before using the product and keep it for further reference

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

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

About the Manual

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

Use of the Product

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

Electrical Safety

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

Environment

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

Operation and Daily Maintenance

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

Privacy Protection

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

Disclaimer

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

Cybersecurity Recommendations

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

is really very convenient for users, but this will increase the risk of data leakage when the system automatically forwards ports. Disabling UPnP is recommended when the function is not used in real applications.

- Check the log. If you want to know whether your device has been accessed by unauthorized users or not, you can check the log. The system log will show you which IP addresses were used to log in your system and what was accessed.

Regulatory Information

FCC Information

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

1. FCC compliance

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

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

2. FCC conditions:

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

RoHS

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



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

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

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

Table of Contents

1 Introduction 1
2 Network Configuration 3
2.1 LAN 3
2.1.1 Access through IP-Tool 3
2.1.2 Directly Access through IE 5
2.2 WAN 6
3 Live View 10
4 Network Camera Configuration 14
4.1 System Configuration 14
4.1.1 Basic Information 14
4.1.2 Date and Time 14
4.1.3 Local Config 15
4.1.4 Storage 15
4.1.5 Configuring Fisheye Parameters 17
4.2 Image Configuration 18
4.2.1 Display Configuration 18
4.2.2 Video / Audio Configuration 20
4.2.3 OSD Configuration 21
4.2.4 Video Mask 22
4.2.5 ROI Configuration 23
4.3 PTZ Configuration 24
4.4 Alarm Configuration 24
4.4.1 Motion Detection 24
4.4.2 Other Alarms 26
4.4.3 Alarm In 28
4.4.4 Alarm Out 28
4.4.5 Alarm Server 29
4.5 Network Configuration 30
4.5.1 TCP/IP 30
4.5.2 Port 31
4.5.3 Server Configuration 31
4.5.4 DDNS 32
4.5.5 SNMP 33
4.5.6 802.1x 34
4.5.7 RTSP 35
4.5.8 UPNP 36
4.5.9 Email 36
4.5.10 FTP 37
4.5.11 HTTPS 38
4.5.12 QoS 39

4.6 Security Configuration 40
4.6.1 User Configuration 40
4.6.2 Online User 41
4.6.3 Block and Allow Lists 42
4.6.4 Security Management 42
4.7 Maintenance Configuration 42
4.7.1 Backup and Restore 42
4.7.2 Reboot 43
4.7.3 Upgrade 43
4.7.4 Operation Log 44
5 Search 45
5.1 Image Search 45
5.2 Video Search 46
5.2.1 Local Video Search 46
5.2.2 SD Card Video Search 47
Appendix 49
Appendix 1 Q & A 49

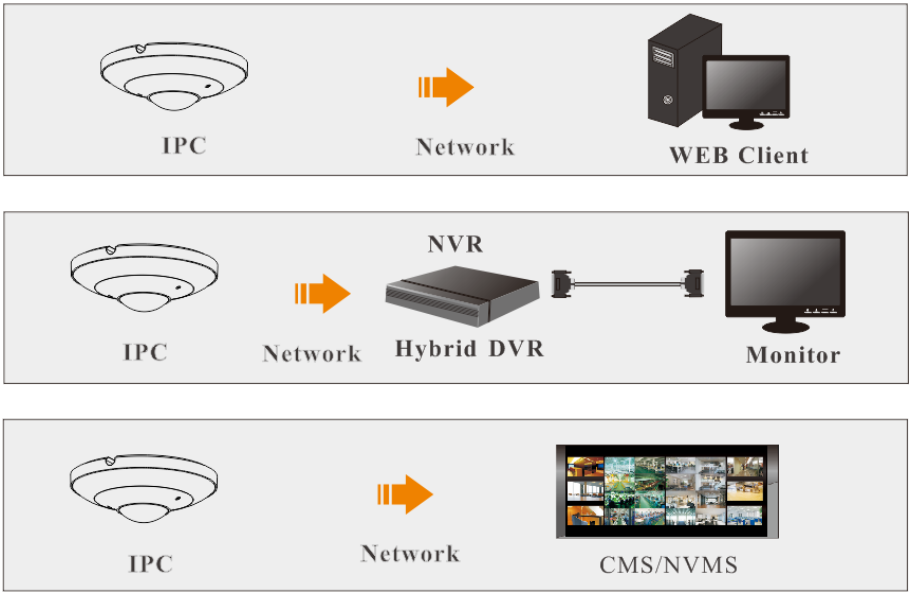
1 Introduction

The fisheye network camera which adopts high-definition fisheye lens and high performance image sensor can meet 360° high definition surveillance requirements. With the advanced H.265/H.264 video compression technology, high compression rate, accuracy and stable stream control, the camera ensures higher quality image and less occupancy of storage space. This product can be widely used in banks, telecommunication systems, electricity power departments, law systems, factories, storehouses, uptowns, etc. In addition, it is also an ideal choice for surveillance sites with middle or high risks.

Main Features

- ICR auto switch, true day/night
- 3D DNR, digital WDR
- ROI coding
- Support BLC, HLC, Anti-flicker
- Support smart phone, iPad, remote monitoring

Surveillance Application



Installation Recommended Distance:

Performance	Face details	Facial contour	Human movement
			
Object distance	3 m	6 m	12 m

2 Network Configuration

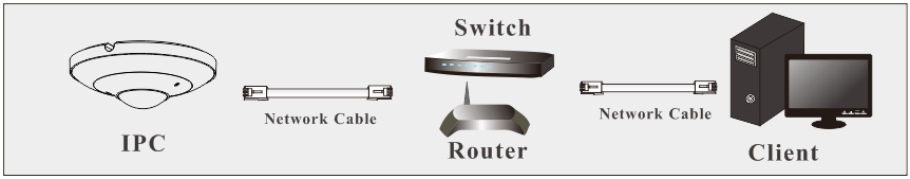
Connect IP-Cam via LAN or WAN. Here only take IE browser for example. The details are as follows:

2.1 LAN

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

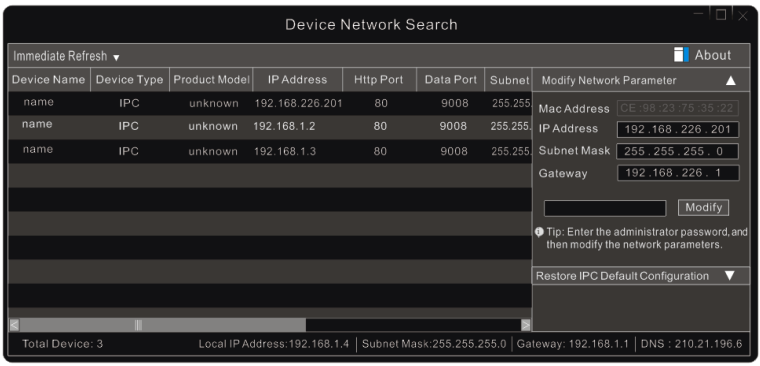
2.1.1 Access through IP-Tool

Network connection:

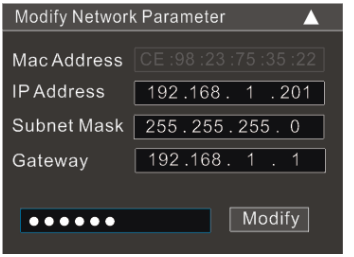


① Make sure the PC and IP-Cam are connected to the LAN and the IP-Tool is installed in the PC from the CD.

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



③ Modify the IP address. The default IP address of this camera is 192.168.226.201. Click the information of the camera listed in the above table to show the network information on the right hand. Modify the IP address and gateway of the camera and make sure its network address is in the same local network segment as that of the computer. Please modify the IP address of your device according to the practical situation.



For example, the IP address of your computer is 192.168.1.4. So the IP address of the camera shall be changed to 192.168.1.X. After modification, please enter the password of the administrator and click "Modify" button to modify the setting.

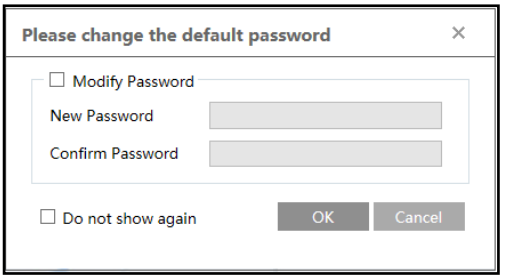
The default password of the administrator is "***123456***".

④ Double click the IP address and then the system will pop up the IE browser to connect IP-CAM. Follow directions to download and install the Active X control. The login interface is as follow.



Enter the username and password to log in.

The default username is "***admin***"; the default password is "***123456***".

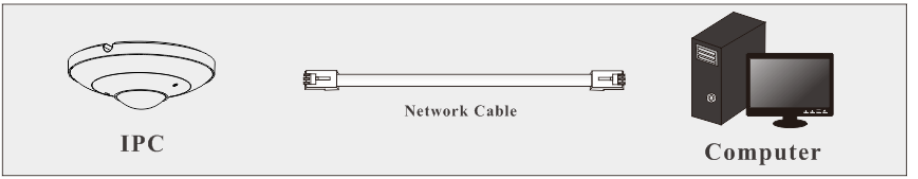


The system will pop up the above-mentioned textbox to ask you to change the default password. It is strongly recommended to change the default password for account security. If "Do not show again" is checked, the textbox will not appear next time.

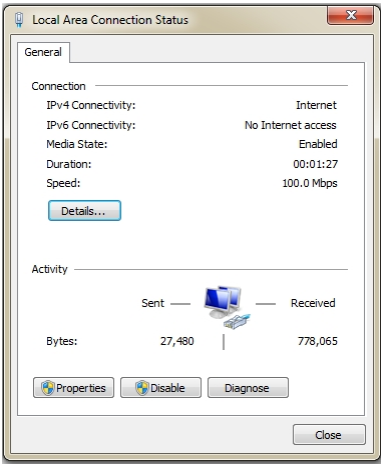
2.1.2 Directly Access through IE

The default network settings are as shown below:
IP address: **192.168.226.201**
Subnet Mask: **255.255.255.0**
Gateway: **192.168.226.1**
HTTP: **80**
Data port: **9008**

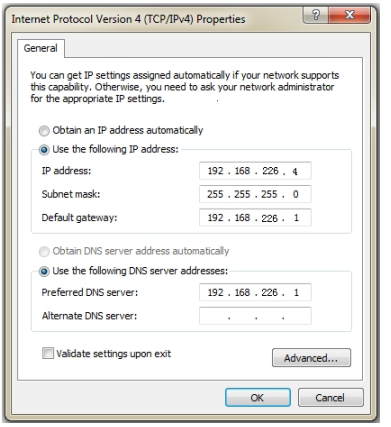
Use the above default settings when logging in the camera for the first time. Directly connect the camera to the computer through network cable.



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



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



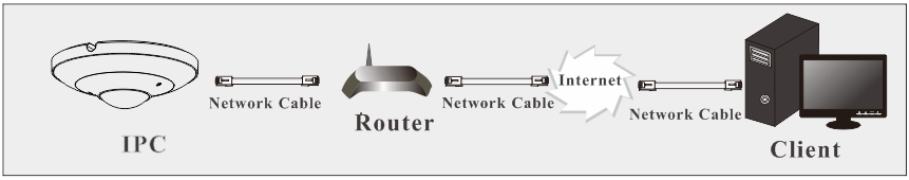
② Open the IE browser and enter the default address of IP-CAM and confirm.

③ Follow directions to download and install the applicable plug-in.

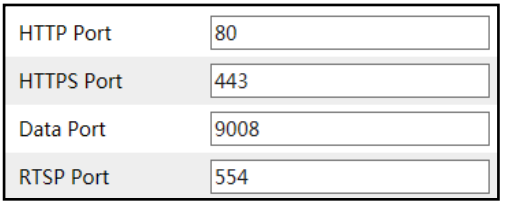
④ Enter the default username and password and then click “Login” to view.

2.2 WAN

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

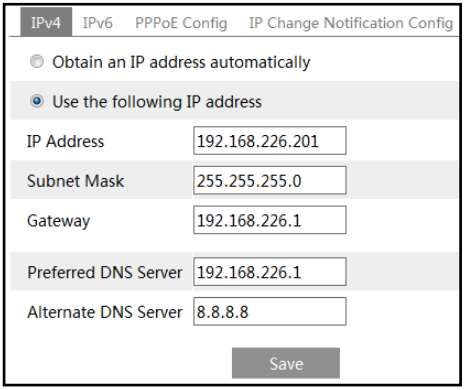


① Make sure the camera is connected via LAN and then log in the camera via LAN and go to Config→Network→Port menu to set the port number.



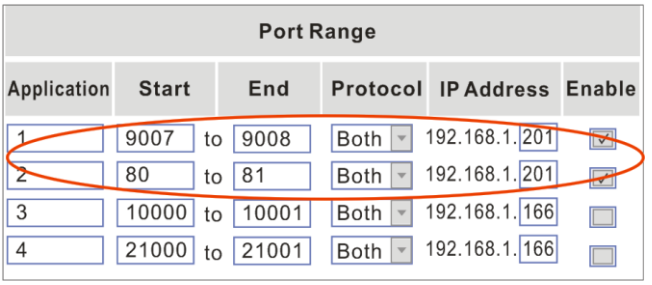
Port Setup

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



IP Setup

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

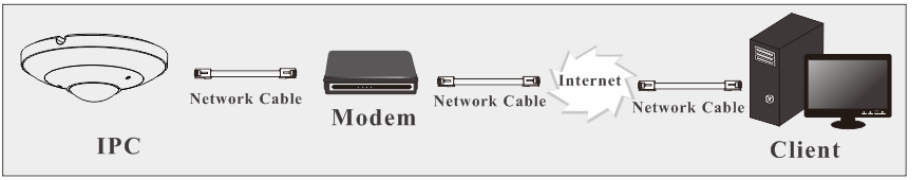


Router Setup

④ Open the IE browser and enter its WAN IP and http port to access. (for example, if you change your http port as 81, you may enter "192.198.1.201:81" in the address bar of web browser to access).

➢ **Access through PPPoE dial-up**

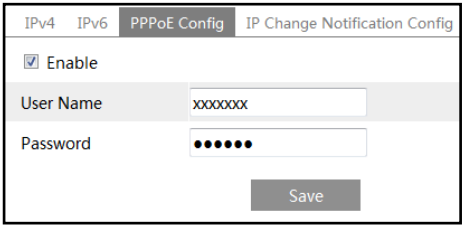
Network connection



You may access the camera through PPPoE auto dial-up. The setting 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 which you can get from your internet service provider.

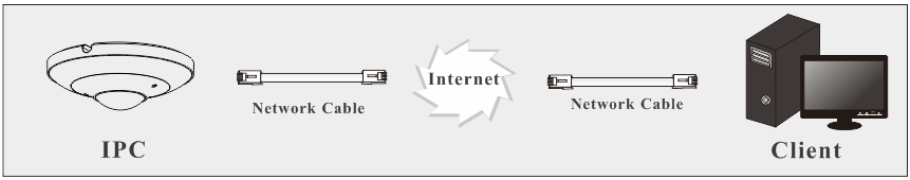


③ Go to Config →Network→DDNS menu. Before you configure the DDNS, please apply for a domain name first. Please refer to DDNS configuration for detail information.

④ Open the IE browser and enter the domain name and http port to access.

➢ **Access through static IP**

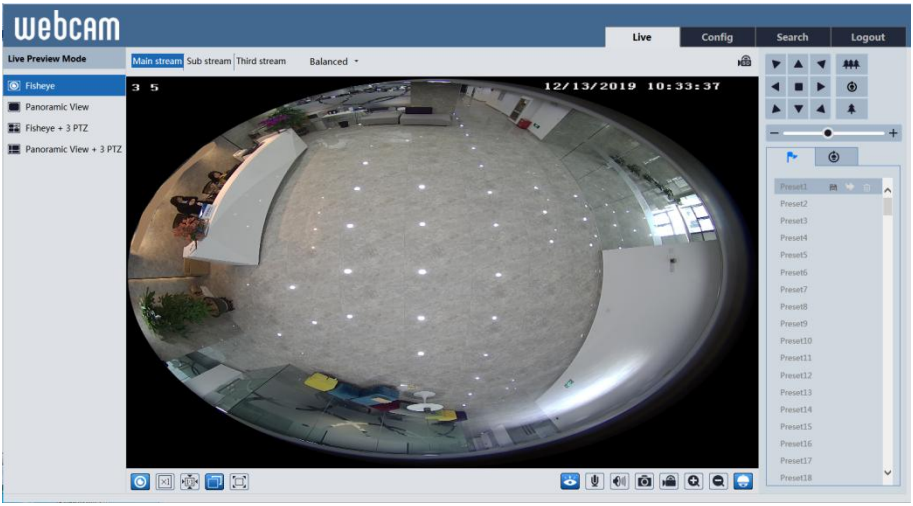
Network connection



The setting 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 input the static IP address and other parameters.
③ Open the IE browser and enter its WAN IP and http port to access.

3 Live View

After logging in, the following window will be shown. Before you view the live image, please set the stream mode and installation method as needed (see Configuring Fisheye Parameters for details).



In the live mode, the different streams and live view modes can be switched as needed. The following table is the instructions of the icons on the live view interface.

Icon	Description	Icon	Description
	Select live preview mode		Snap
	Original size		Start/stop recording
	Appropriate size		PTZ control
	Auto		Sensor alarm indicator icon
	Full screen		Motion alarm indicator icon
	Start/stop live view		Zoom in
	Start/stop two-way audio		Zoom out
	Enable/disable audio		

- In full screen mode, double click to exit.

Click  to select the live view mode.

Fisheye view mode: See the picture as shown above.

Panoramic view mode



Fisheye+ 3PTZ view mode



Panoramic + 3PTZ view mode



4PTZ view mode (you need to switch the stream mode in the fisheye parameter interface)



In panoramic + 3PTZ view mode or fisheye + 3PTZ view mode or 4PTZ view mode, select a PTZ window and view the image from every direction by controlling PTZ panel.

Click  to display the control panel. The descriptions of the control panel are as follows:

Icon	Description	Icon	Description
	Move upper left direction		Move upper right direction
	Move up		Stop movement
	Move left		Move right
	Move lower left direction		Move lower right direction
	Move down		Speed adjustment
	Zoom out		Zoom in
	Automatic cruise		Preset
	Create and call cruise		

Select preset and click  to call the preset. Select and set the preset and then click  to save the position of the preset. Select the set preset and click  to delete it.

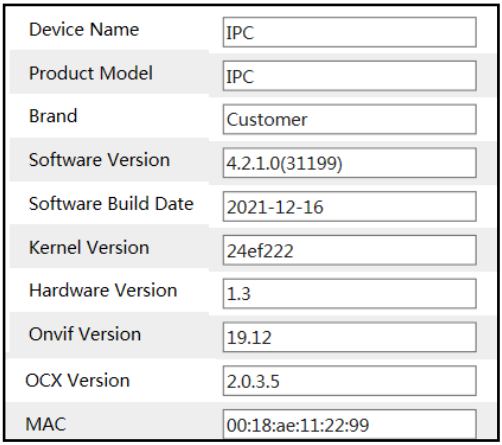
Select cruise and click  to set the cruise and add presets to this cruise. Click  to start cruise; click  to stop cruise.

In the Webcam client, choose “Config” to go to the configuration interface.
Note: Wherever applicable, click the “Save” button to save the settings.

4.1 System Configuration

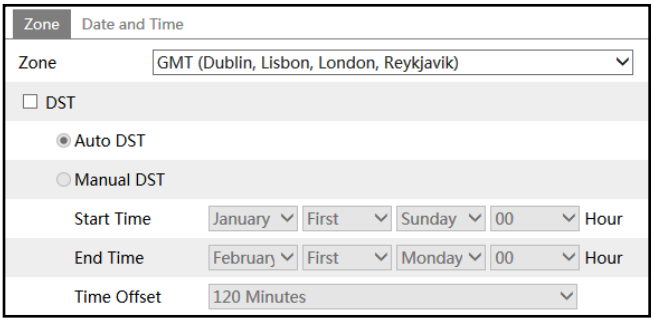
4.1.1 Basic Information

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

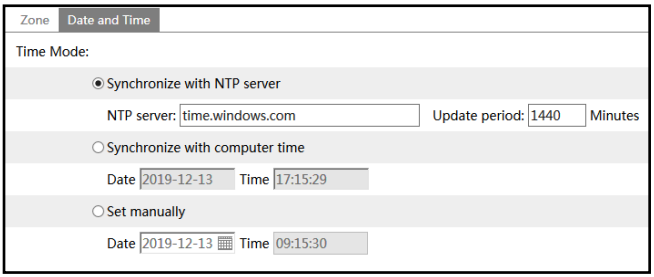


4.1.2 Date and Time

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

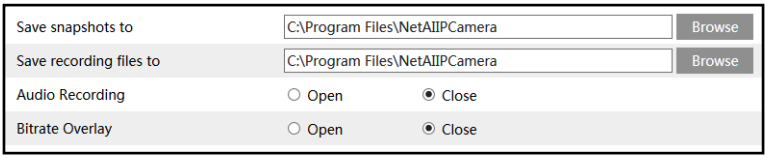


Please select the time zone and DST as needed.
Click “Date and Time” tab to set the time mode.



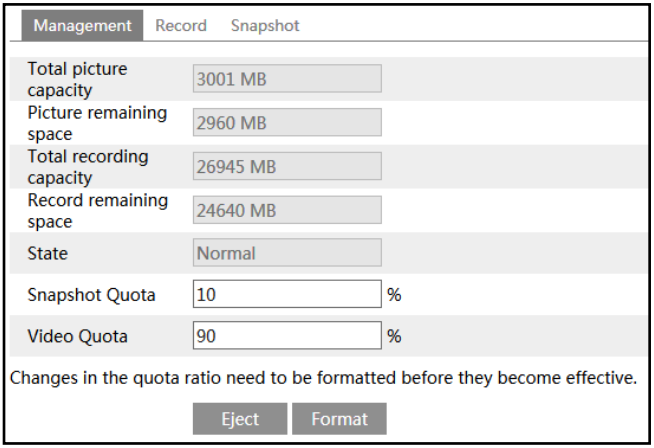
4.1.3 Local Config

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



4.1.4 Storage

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



- **SD Card Management**

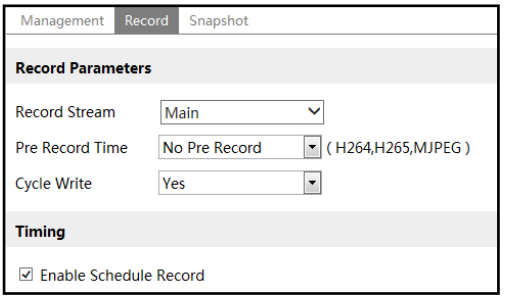
Click the "Format" button to format the SD card. All data will be cleared by clicking this button.

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

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

- **Schedule Recording Settings**

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



2. Set record stream, pre-record time, cycle writing.
Pre Record Time: Set the time to record before the actual recording begins.

3. Set schedule recording. **C**heck "Enable Schedule Record" and set the schedule.



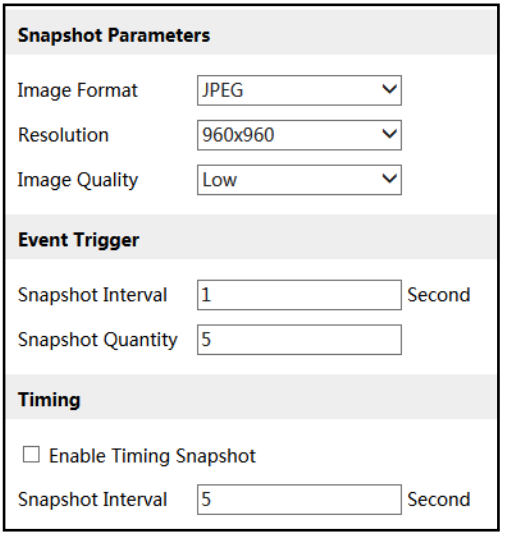
Weekly schedule
Set the alarm time from Monday to Sunday for a single week. Each day is divided in one hour increments. Green means scheduled. Blank means unscheduled.
"Add": Add the schedule for a special day. Drag the mouse to set the time on the timeline.
"Erase": Delete the schedule. Drag the mouse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

granularities (minutes).

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

- **Snapshot Settings**

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

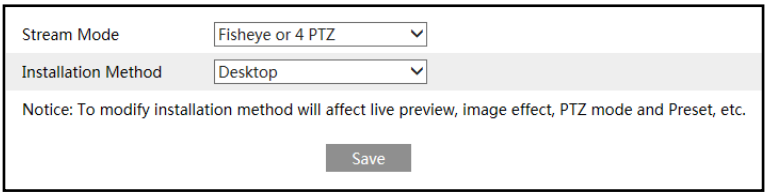


Set the format, resolution and quality of the image saved on the SD card and the snapshot interval and quantity and the timing snapshot here.
Snapshot Quantity: The number you set here is the maximum quantity of snapshots. The actual quantity of snapshots may be less than this number. Supposing the occurrence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

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

4.1.5 Configuring Fisheye Parameters

Before viewing the live image, please go to Config→System→Fisheye Parameters menu to set the stream mode and installation method.

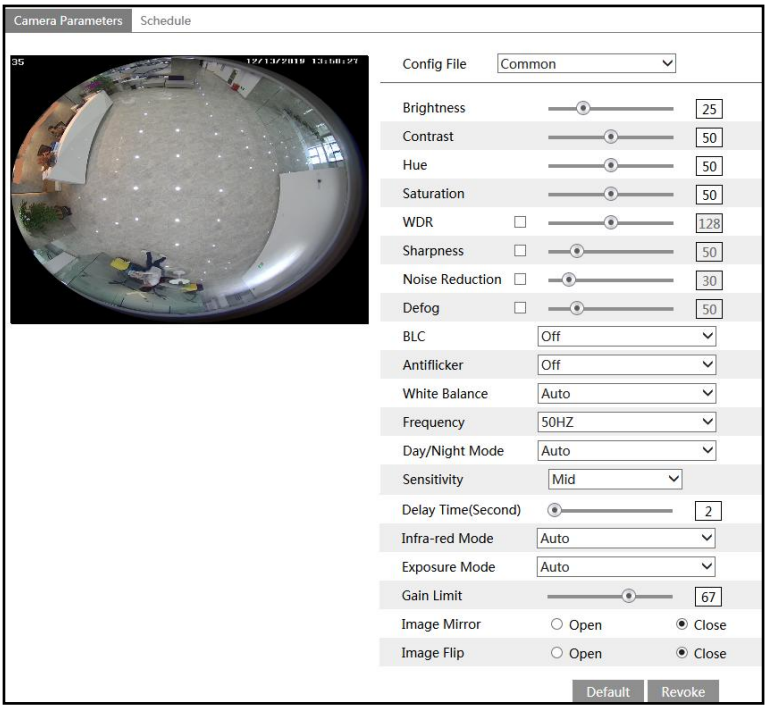


Stream mode: Fisheye + Panoramic view + 3PTZ and Fisheye or 4PTZ mode are optional.
Installation method: ceiling and desktop are optional. Please select the installation mode according to the actual way of installation.

4.2 Image Configuration

4.2.1 Display Configuration

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



Brightness: Set the brightness level of the camera's image.
Contrast: Set the color difference between the brightest and darkest parts.
Hue: Set the total color degree of the image.

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

◆ There will be some record lost in a few seconds during mode 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:

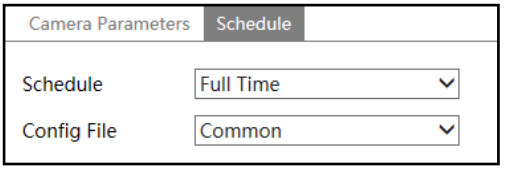
- Off: close the backlight compensation function. It is the default mode.
- HWDR
- HLC: lower the brightness of the whole image by suppressing the brightness of the image's highlight area and reducing the size of the halo area.
- BLC: if enabled, the auto exposure will activate according to the scene 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.

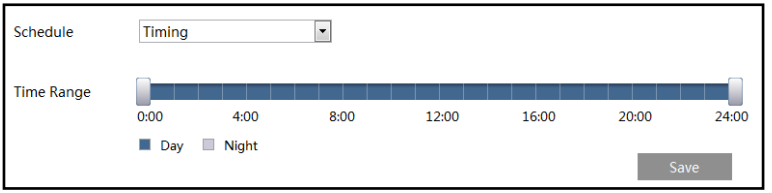
White Balance: Adjust the color temperature according to the environment automatically.
Frequency: 50Hz and 60Hz can be optional.
Day/night Mode: Please choose the mode as needed.
Sensitivity: High, middle and low can be selected.
Infrared Mode: Choose "ON", "OFF" or "Auto".
Exposure Mode: Choose "Auto" or "Manual". If manual is chosen, the digital shutter speed can be adjusted.
Gain Limit: The higher the value is, the brighter the image is.
Image Mirror: Turn the current video image horizontally.
Image Flip: Turn the current video image vertically.

Schedule Settings of Image Parameters:
Click the "Schedule" tab as shown below.



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

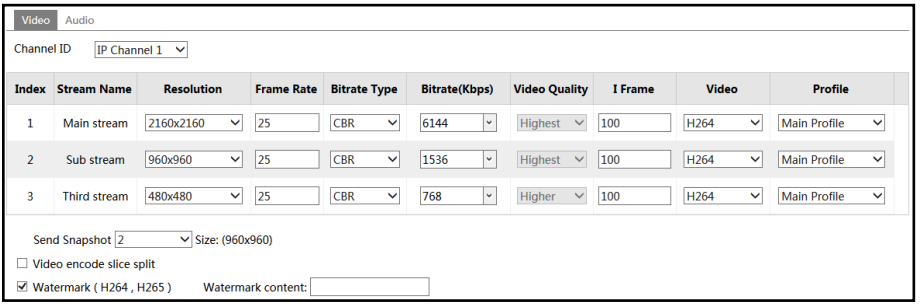
night. Choose “Timing” in the drop-down box of schedule as shown below.



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 “Timing”, the image configuration mode will automatically switch between day and night according to the schedule.

4.2.2 Video / Audio Configuration

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



You can select streams for different channels.
IP Channel 1: Fisheye view channel, 3 streams can be set. Please set them according to the actual network condition.
IP Channel 2: Panoramic view channel, 2 streams can be set. Please set them according to the actual network condition.
IP Channel 3/4/5: PTZ view channel, 2 streams can be set for each channel. Please set them according to the actual network condition.
Resolution: The size of image.
Frame rate: The higher the frame rate is, 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, H265 or MJPEG is optional. If H.265 is chosen, make sure the client system is able to decode H.265.

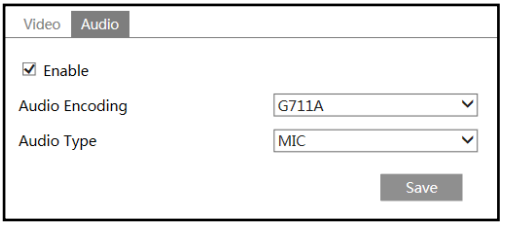
Profile: For H.264. Baseline, main and high profiles are selectable.

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 "Audio" tab to go to the interface as shown below.

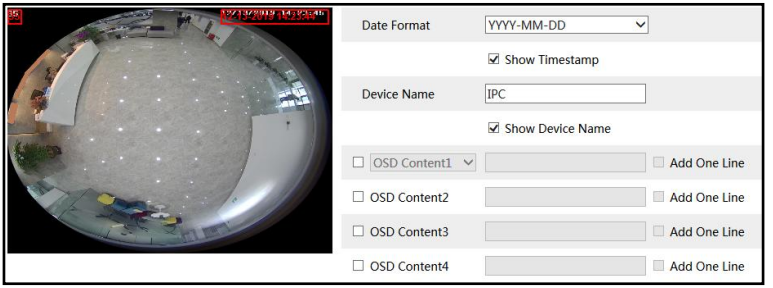


Audio Encoding: G711A and G711U are selectable.

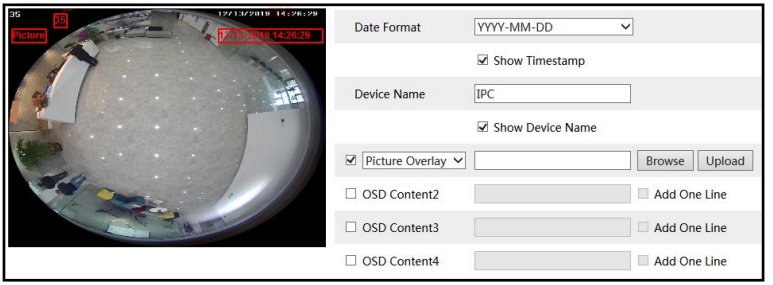
Audio Type: MIC and LIN are selectable.

4.2.3 OSD Configuration

Go to Image→OSD interface as shown below.



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



Picture Overlap Settings:
Check “OSD Content1”, choose “Picture Overlay” and click “Browse” to select the overlap picture. Then click “Upload” to upload the overlap picture. The pixel of the image shall not exceed 200*200, or it cannot be uploaded.
Note: The OSD information only can be overlaid on fisheye channel.

4.2.4 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.

4.2.5 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.

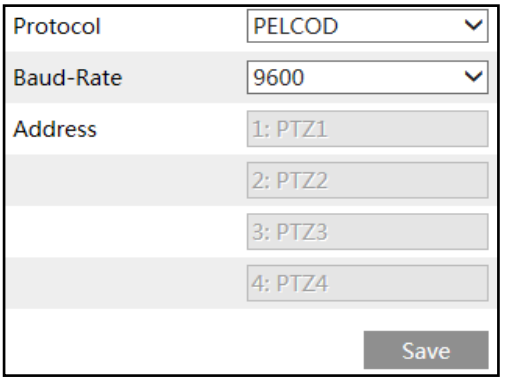


1. Check “Enable” and then click “Draw Area” button.

2. Drag the mouse to set the ROI area.
3. Set the level.
4. Click “Save” button to save the settings.

4.3 PTZ Configuration

The PTZ of this camera can be controlled by the keyboard. Connect the keyboard and the camera through RS485 interface and then set the corresponding protocol and baud-rate in the camera and keyboard.
Go to PTZ→Protocol interface as shown below.

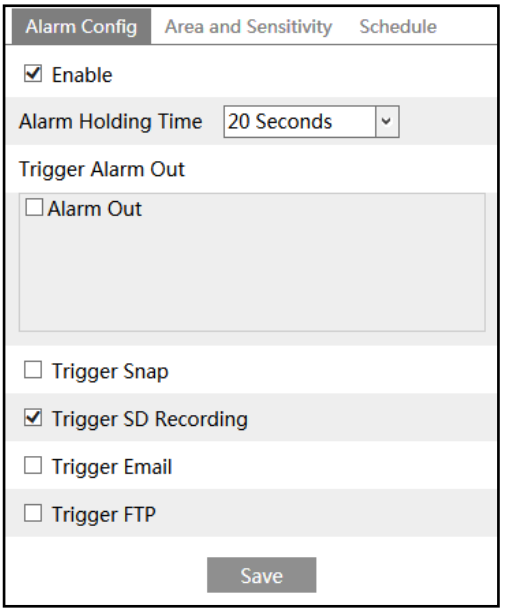


Here the protocol and baud-rate must be the same with these of the keyboard.
Address: 1; you can control PTZ channel 1 by using this address in the keyboard.
Address: 2; you can control PTZ channel 2 by using this address in the keyboard.
……

4.4 Alarm Configuration

4.4.1 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.

Alarm Out: If selected, this would trigger an external relay output that is connected to the camera on detecting a motion based alarm.

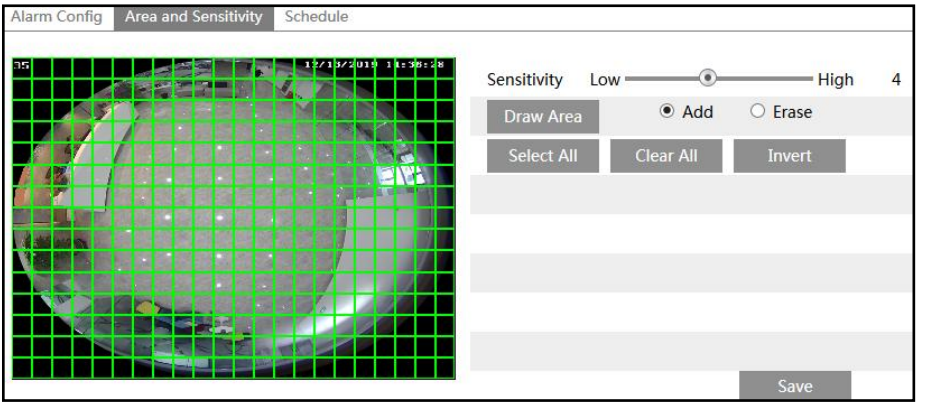
Trigger Snap: If selected, the system will capture images on motion detection and save the images on an SD card.

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

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

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

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



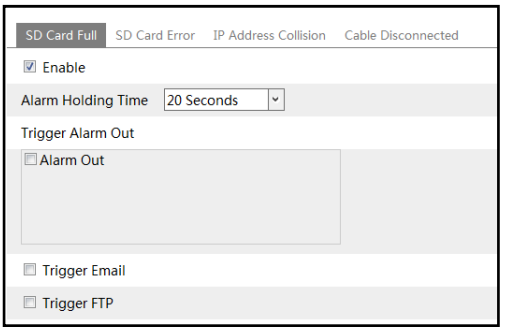
Move the “Sensitivity” scroll bar to set the sensitivity.
Select “Add” and click “Draw” button and drag mouse to select the motion detection area;
Select “Erase” and drag the mouse to clear motion detection area.
After that, click “Save” to save the settings.

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

4.4.2 Other Alarms

- **SD Card Full**

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

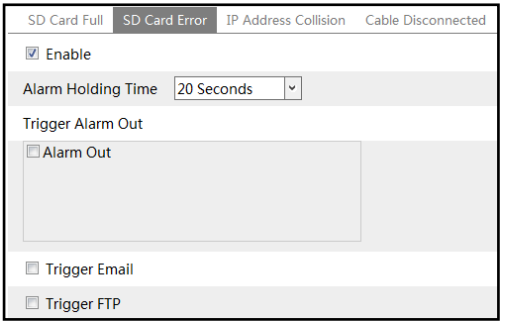


2. Click “Enable” and set the alarm holding time.
3. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection chapter for details.

- **SD Card Error**

When some errors occur for writing data to the SD card, the corresponding alarms will be triggered.

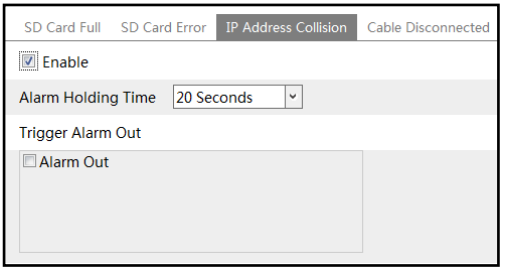
1. Go to Config→Alarm→Anomaly→SD Card Error as shown below.



2. Click "Enable" and set the alarm holding time.
3. Set alarm trigger options. Trigger alarm out, Email and FTP. The setup steps are the same as motion detection. Please refer to motion detection chapter for details.

- **IP Address Conflict**

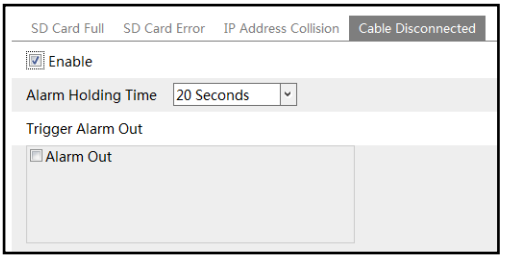
1. Go to Config→Alarm→Anomaly→IP Address Collision as shown below.



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

- **Cable Disconnection**

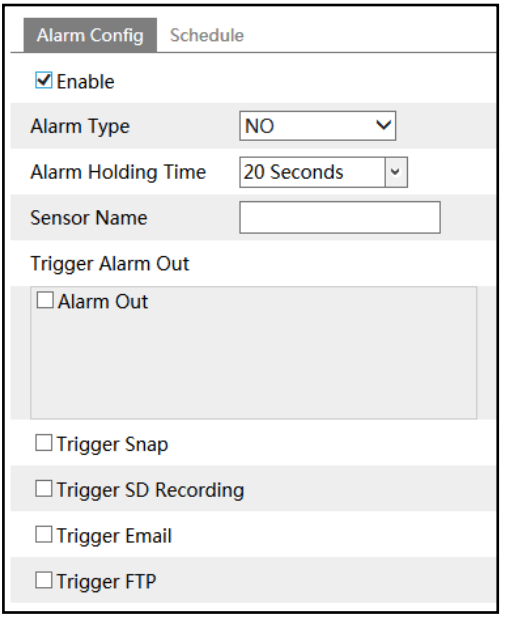
1. Go to Config→Alarm→Anomaly→Cable Disconnected as shown below.



2. Click “Enable” and set the alarm holding time.
3. Trigger alarm out. When the camera is disconnected, the system will trigger the alarm out.

4.4.3 Alarm In

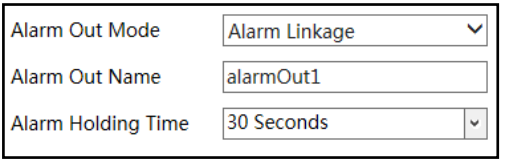
To set sensor alarm (alarm in):
Go to Config→Alarm→Alarm In interface as shown below.



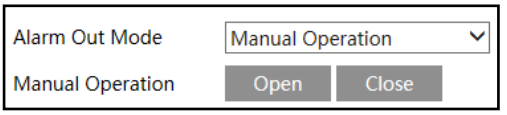
1. Enable alarm and set the alarm type, alarm holding time and sensor name.
2. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection chapter for details.
3. Click “Save” button to save the settings.
4. Set the schedule of the sensor alarm. The setup steps of the schedule are the same as the schedule recording setup. (See Schedule Recording).

4.4.4 Alarm Out

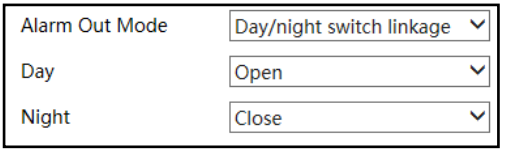
Go to Config→Alarm→Alarm Out interface as shown below:



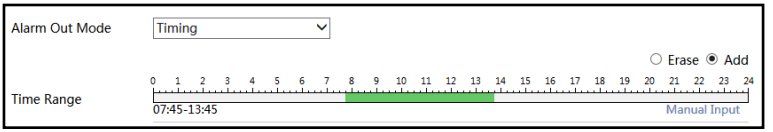
Alarm Out Mode: Alarm linkage, manual operation, day/night switch linkage and timing are optional.
Alarm Linkage: Having selected this mode, select alarm out name and alarm holding time at the "Alarm Holding Time" pull down list box.
Manual Operation: Having selected this mode, click "Open" to trigger the alarm out immediately; click "Close" to stop alarm.



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

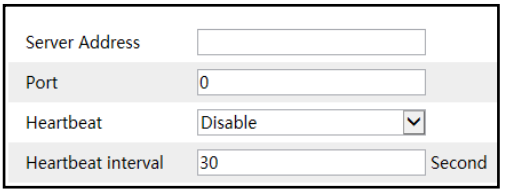


Timing: Click "Add" and drag the mouse on the timeline to set the schedule of alarm out; click "Erase" and drag the mouse on the timeline to erase the set time schedule. After this schedule is saved, the alarm out will be triggered in the specified time.



4.4.5 Alarm Server

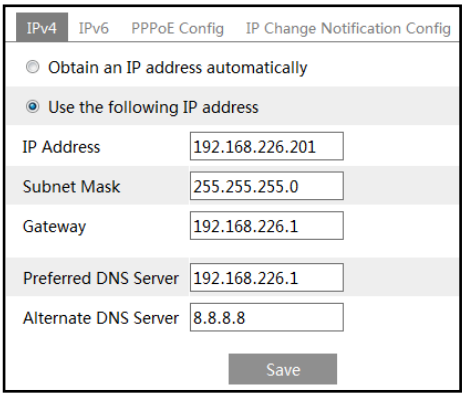
Go to Alarm→Alarm Server interface as shown below.
Set the server address, port, heartbeat and heartbeat interval. When an alarm occurs, the camera will transfer the alarm event to the alarm server. If an alarm server is not needed, there is no need to configure this section.



4.5 Network Configuration

4.5.1 TCP/IP

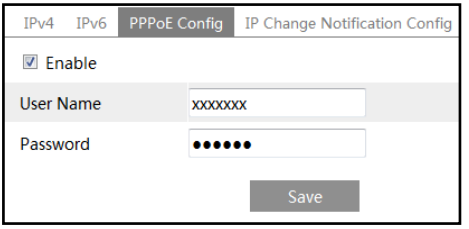
Go to Config→Network→TCP/IP interface as shown below. There are two ways for network connection.



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.

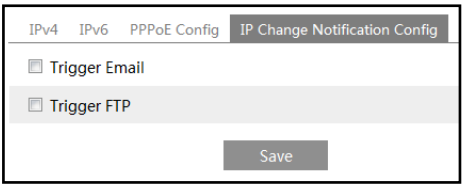
Test: Test the effectiveness of the IP address by clicking this button.

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.



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

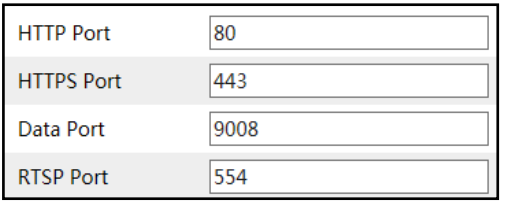
Click "IP Change Notification Config" to go to the interface as shown below.



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

4.5.2 Port

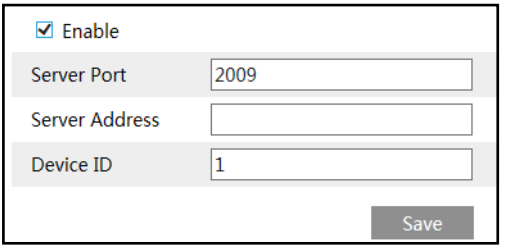
Go to Config→Network→Port interface as shown below. HTTP port, HTTPS port, Data port and RTSP port can be set.



HTTP Port: The default HTTP port is 80. It can be changed to any port which is not occupied.
HTTPS Port: The default HTTPs port is 443. It can be changed to any port which is not occupied.
Data Port: The default data port is 9008. Please change it as necessary.
RTSP Port: The default port is 554. Please change it as necessary.

4.5.3 Server Configuration

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

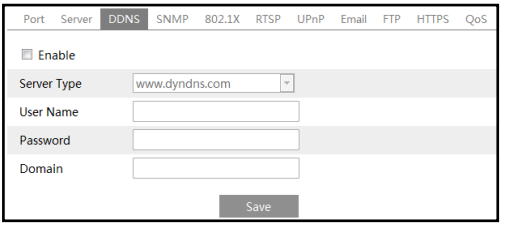


1. Check “Enable”.

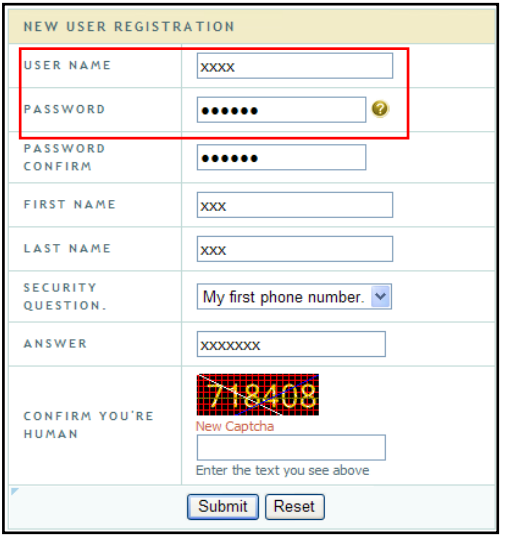
2. Check the IP address and port of the transfer media server in the ECMS/NVMS. Then enable the auto report in the ECMS/NVMS when adding a new device. Next, input the remaining information of the device in the ECMS/NVMS. After that, the system will automatically allot a device ID. Please check it in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

4.5.4 DDNS

If the camera is set up with a DHCP connection, DDNS should be set for the internet.
1. Go to Config→Network→ DDNS.



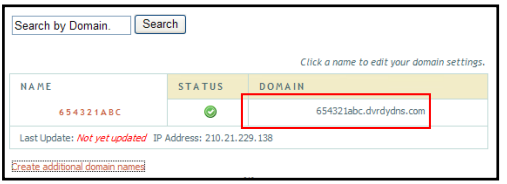
2. Apply for a domain name. Take www.dvrdyndns.com for example.
Input www.dvrdydns.com in the IE address bar to visit its website. Then click “Registration” button.



Create domain name.



After you successfully request your domain name, you will see your domain in the list.

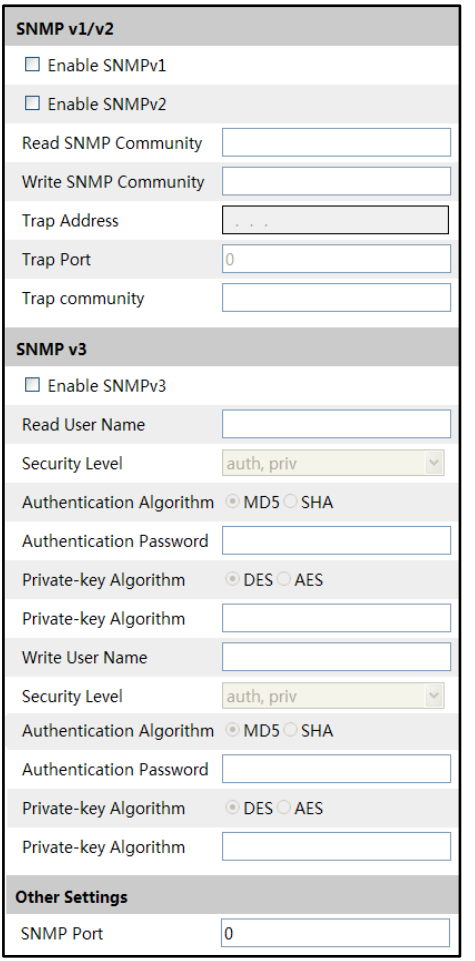


3. Input the username, password, domain you apply for in the DDNS configuration interface.
4. Click “Save” button to save the settings.

4.5.5 SNMP

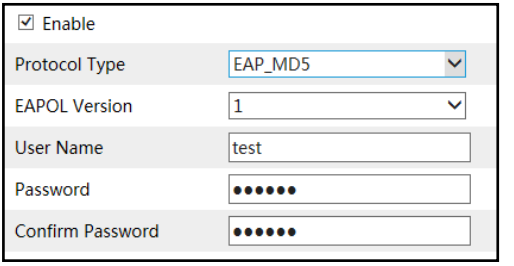
To get camera status, parameters and alarm information and remotely manage the camera, you can set the SNMP function. Before using the SNMP, please download the SNMP software and set the parameters of the SNMP, such as SNMP port, trap address.
1. Go to Config→Network→SNMP.
2. Check the corresponding version checkbox (Enable SNMPv1, Enable SNMPv2, Enable SNMPv3) according to the version of the SNMP software you download.
3. Set the “Read SNMP Community”, “Write SNMP Community”, “Trap Address”, “Trap Port” and so on. Please make sure the settings are the same as that of your 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.



4.5.6 802.1x

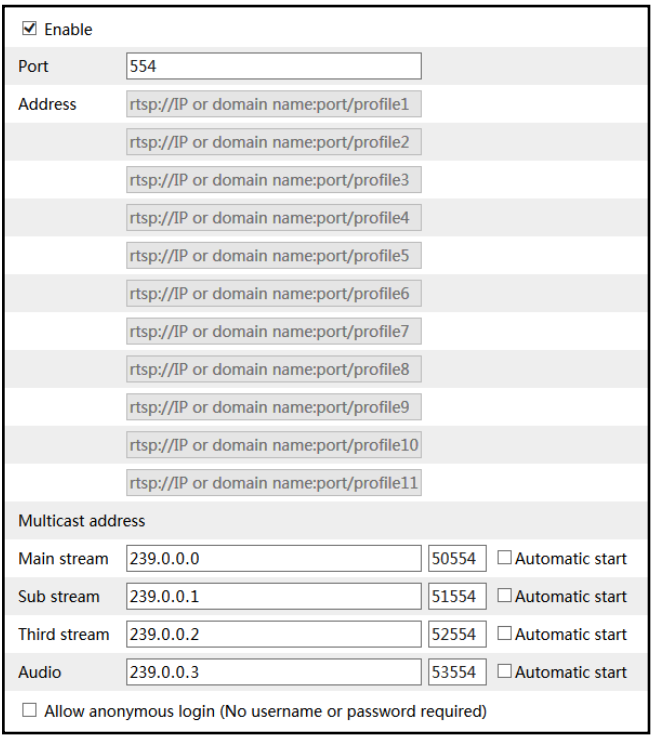
If it is enabled, the camera's data can be protected. When the camera is connected to the network protected by the IEE802.1x, user authentication is needed.



To use this function, the camera shall be connected to a switch supporting 802.1x protocol. The switch can be 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.

4.5.7 RTSP

Go to Config→Network→RTSP.



Select “Enable” to enable the RTSP function.
Port: Access port of the streaming media. The default number is 554.
RTSP Address: The RTSP address (unicast) format that can be used to play the stream in a media player.

Multicast Address
Main stream: The address format is

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

Sub stream: The address format is

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

Third stream: The address format is

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

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

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

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

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

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

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

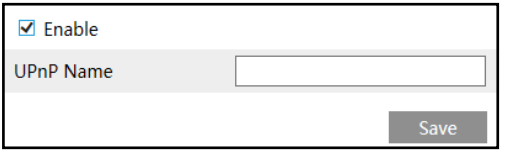
4. When playing the video through the multicast streams in a VLC player, please pay attention to the mode of the VLC player. If it is set to TCP mode, the video cannot be played.

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

4.5.8 UPNP

If this function is enabled, the camera can be quickly accessed through the LAN.

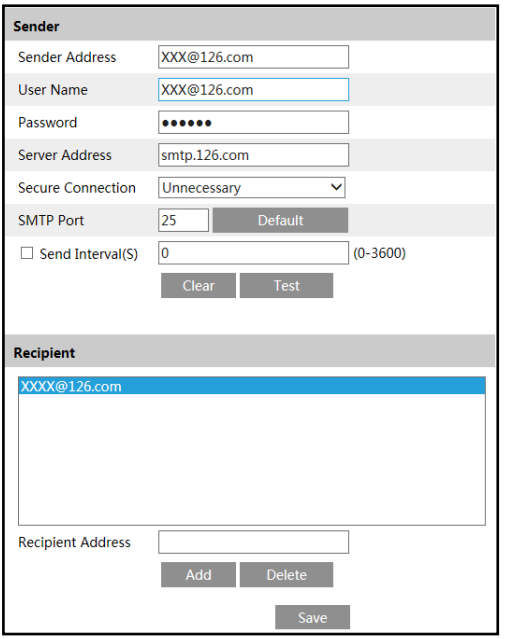
Go to Config→Network→UPnP. Enable UPNP and then enter UPnP name.



4.5.9 Email

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

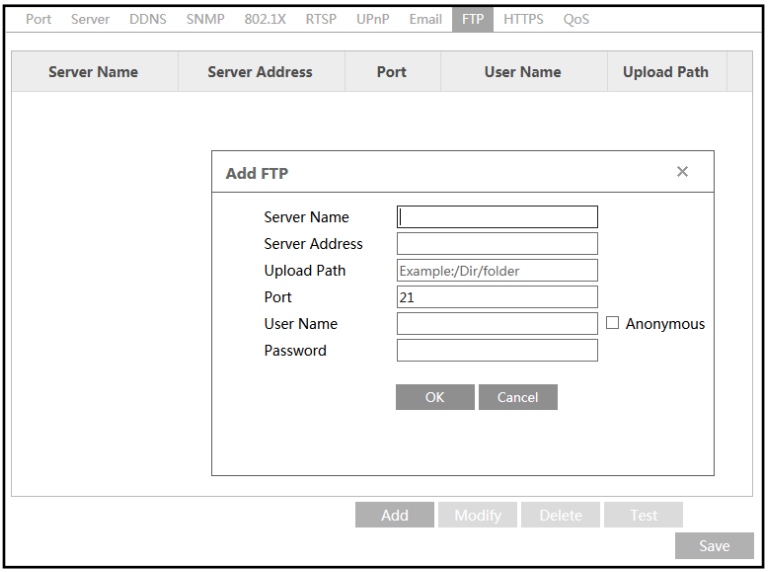
Go to Config→Network →Email.



Sender Address: sender's e-mail address.
User name and password: sender's user name and password.
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.

4.5.10 FTP

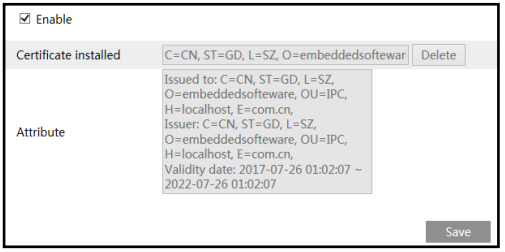
After you set the FTP server, the captured pictures on an alarm will be uploaded to the FTP server.
Go to Config→Network →FTP.



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

4.5.11 HTTPS

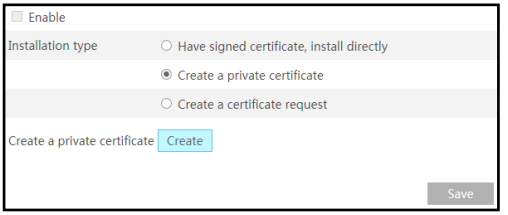
HTTPs provides authentication of the web site and protects user privacy.
Go to Config →Network→HTTPS as shown below.



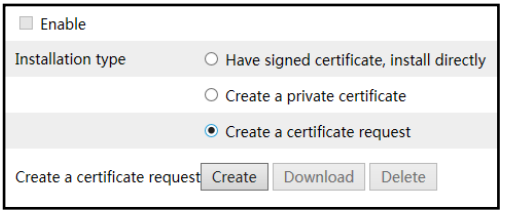
There is a certificate installed by default as shown above. Enable this function and save it. Then the camera can be accessed by entering https://IP: https port via the web browser (eg. https://192.168.226.201:443).
A private certificate can be created if users don't want to use the default one. Click "Delete" to cancel the default certificate. Then the following interface will be displayed.



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



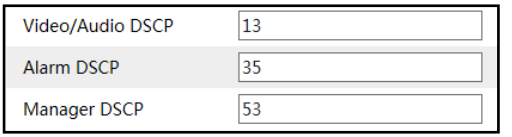
Click the “Create” button to create a private certificate. Enter the country (only two letters available), domain (camera’s IP address/domain), validity date, password, province/state, region and so on. Then click “OK” to save the settings.
* Click “Create a certificate request” to enter the following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



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

4.5.12 QoS

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

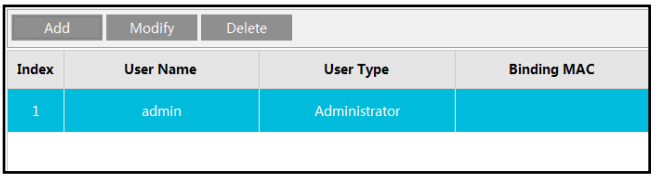


Video/Audio DSCP: The range is from 0 to 63.
Alarm DSCP: The range is from 0 to 63.
Manager DSCP: The range is from 0 to 63.
Generally speaking, the larger the number is, the higher the priority is.

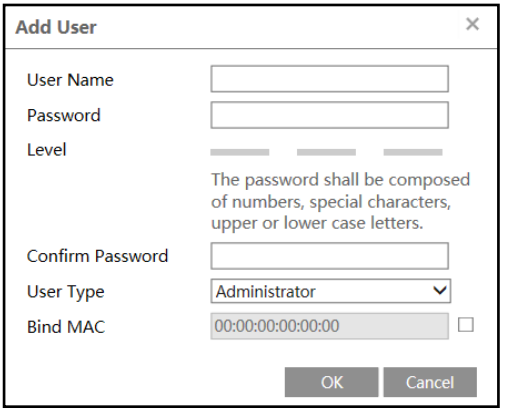
4.6 Security Configuration

4.6.1 User Configuration

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



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



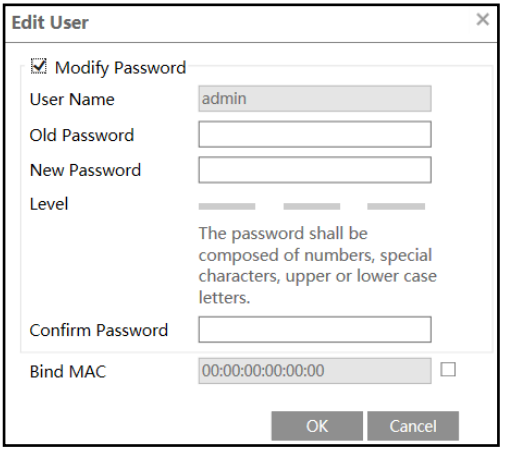
2. Enter user name in “User Name” textbox.
3. Enter letters or numbers in “Password” and “Confirm Password” textbox.
4. Choose the user type. Administrator has all permissions. Normal user can only view the live video. Advanced user has the same permissions as an Administrator except for; user, backup settings, factory reset, and upgrading the firmware.
5. Enter the MAC address of the PC in “Bind MAC” textbox.

If this option is enabled, only the PC with the specified MAC address can access the camera for that user.

6. 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 and MAC address 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. Enter computer's MAC address as necessary.
6. Click the "OK" button to save the settings.

Note: To change the access level of a user, the user must be deleted and added again with the new access level.

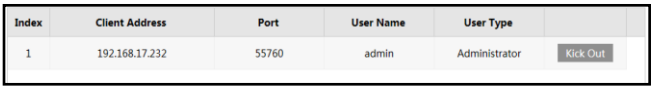
Delete user:

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.

4.6.2 Online User

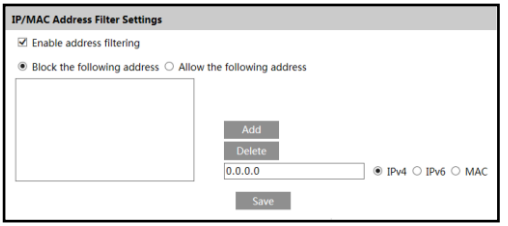
Go to Config→Security→Online User to view the user who is viewing the live video.



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

4.6.3 Block and Allow Lists

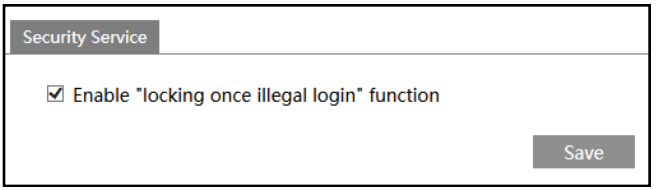
Go to Config→Security→Block and Allow Lists interface as shown below.



The setup steps are as follows:
Check the “Enable address filtering” check box.
Select “Block/Allow the following address”, IPv4/IPv6/MAC and then enter IP address or MAC address in the address box and click the “Add” button.

4.6.4 Security Management

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

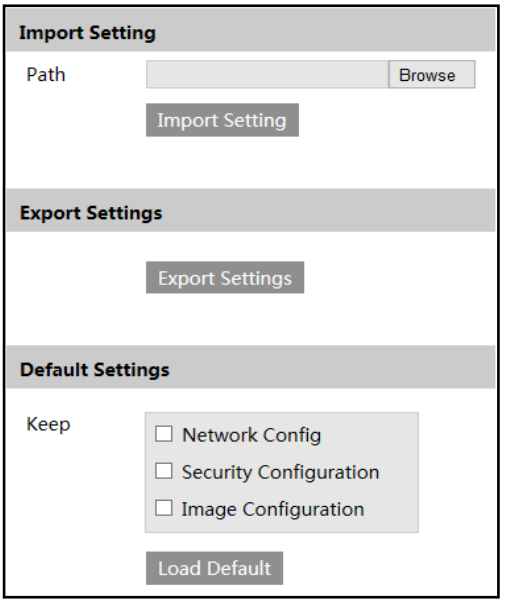


In order to prevent against malicious password unlocking, “locking once illegal login” function can be enabled here. If this function is enabled, login failure after trying six times will make the login interface locked. The camera can be logged in again after a half hour or after the camera reboots.

4.7 Maintenance Configuration

4.7.1 Backup and Restore

Go to Config→Maintenance→Backup & Restore.



- **Import & Export Settings**

Configuration settings of the camera can be exported from a camera into another camera.
1. Click “Browse” to select save path for import or export information on the PC.
2. Click “Import Setting” or “Export Setting” button.

- **Default Settings**

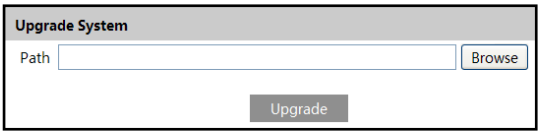
Click the “Load Default” button to restore all system settings to the default factory settings except those you want to keep.

4.7.2 Reboot

Go to Config→Maintenance→Reboot.
Click “Reboot” button 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 and then click “Save” button to save the settings.

4.7.3 Upgrade

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



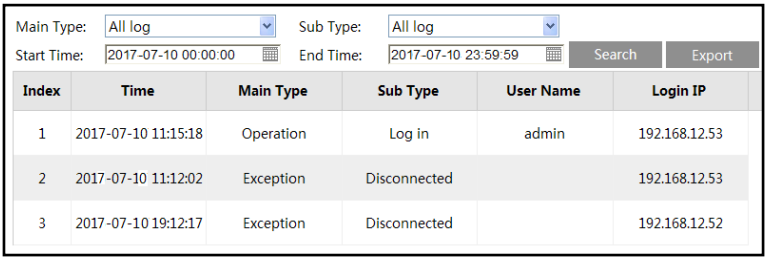
1. Click the “Browse” button to select the save path of the upgrade file
2. Click the “Upgrade” button to start upgrading the firmware.
3. The device will restart automatically

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

4.7.4 Operation Log

To query and export log:

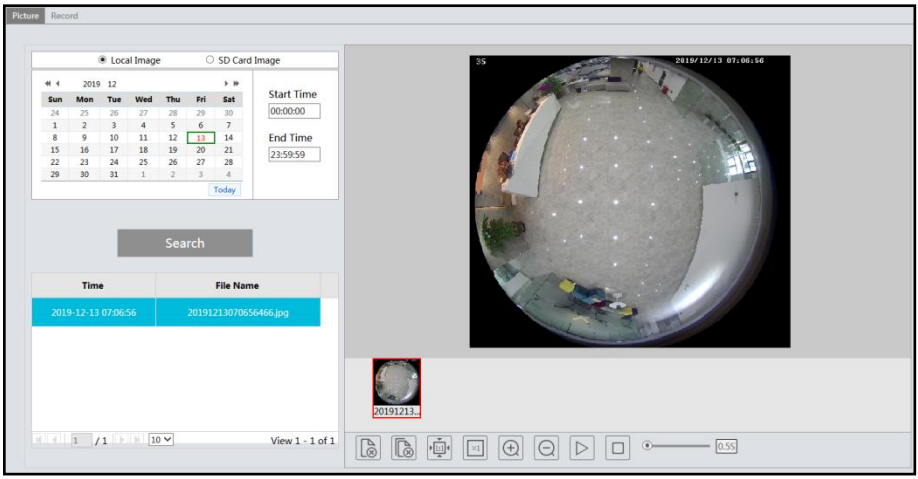
1. Go to Config→Maintenance→Operation Log.



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

5.1 Image Search

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

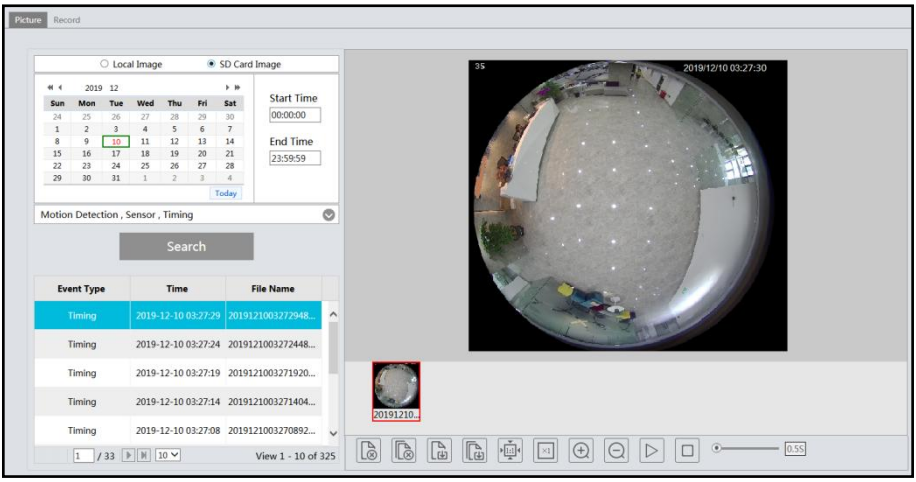


Local Image Search

1. Set time: Select date and choose the start and end time in the top left corner.
2. Click “Search” button to search the pictures.
3. Click a file name in the list to view captured pictures as shown above.

SD Card Image Search

1. Set time: Select date and choose the start and end time in the top left corner.
2. Check events.
3. Click “Search” button to search the pictures.
4. Click a file name in the list to view captured pictures as shown below.



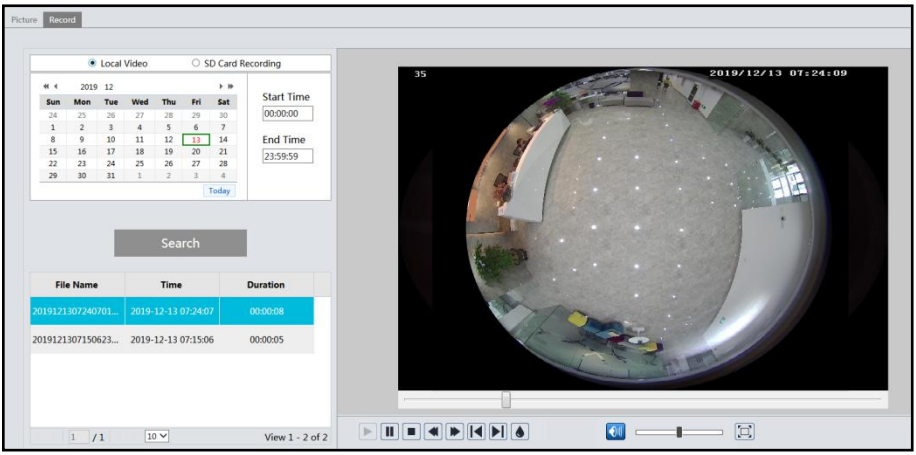
The descriptions of the buttons are shown as follows.

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

5.2 Video Search

5.2.1 Local Video Search

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

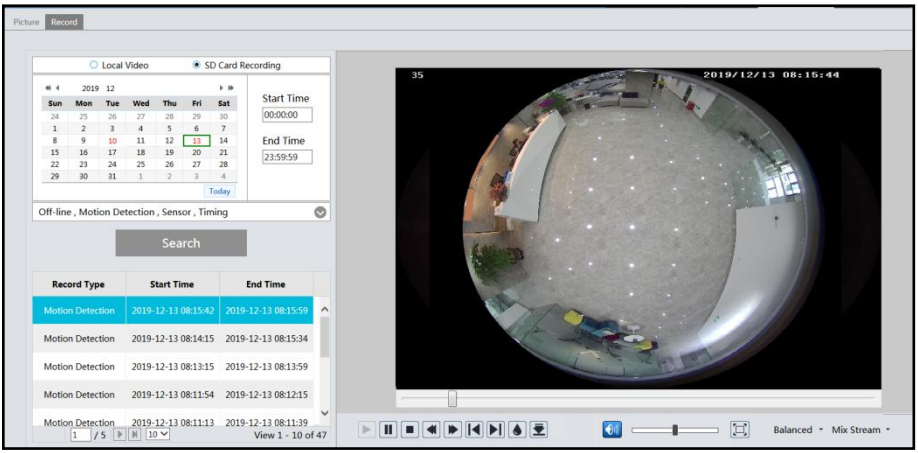


Choose the date and the start time and end time and then click “Search” button to search the record files. Double click the record file to play the record. The descriptions of the buttons on the playback interface are as follows.

Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button.
	Stop button.		Speed down.
	Speed up.		Click it to play the previous record.
	Click it to play the next record.		Watermark display.
	Click it to enable / disable audio; drag the slider to adjust the volume after enabling audio.		Full screen. Click it to display full screen. Double click to exit full screen.

5.2.2 SD Card Video Search

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



1. Set the date and the start and end time, select the record type and then click “Search” button to search the record.
2. Double click the searched file name to play the record.

Please refer to Local Video Search for the descriptions of the buttons on the playback interface.

Click  button to download the record saved in the SD card.

Appendix 1 Q & A

Q: How to find my password if I forget it?

A：Reset the device to the default factory settings.

Default IP: 192.168.226.201; User name: admin; Password: 123456

Q：Fail to connect devices through IE browser, why?

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

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

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

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

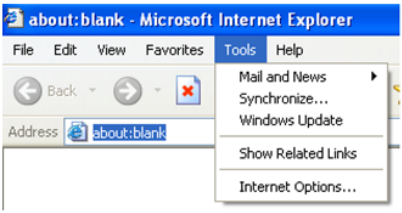
Q：IP tool cannot search devices, why?

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

Q：IE cannot download ActiveX control. How can I do?

a. IE browser blocks ActiveX. Please do setup as below.

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

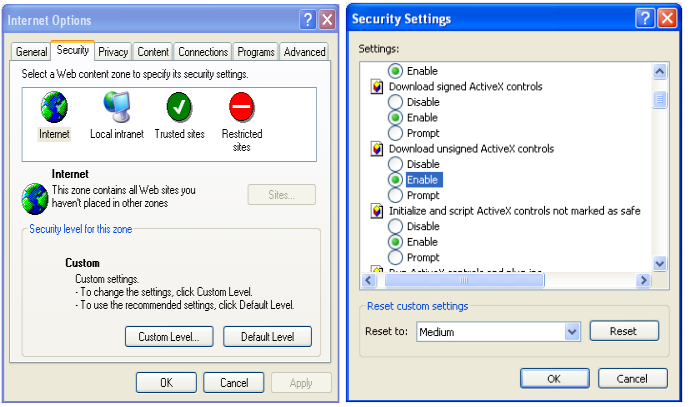


② Select Security------Custom Level….

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

④ Then click OK to finish setup.

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



Q：No sound can be heard, why?

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.


safire
SMART