2 Megapixel

NETWORK CAMERA

User Manual

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

Notes on Safety

- Please use the specified power supply to connect.
- Do not attempt to disassemble the camera; in order to prevent electric shock, do not remove screws or covers.
- There are no user-serviceable parts inside. Please contact the nearest service center as soon as possible if there is any failure.
- Avoid from incorrect operation, shock vibration, heavy pressing which can cause damage to product.
- Do not use corrosive detergent to clean main body of the camera. If necessary, please use soft dry cloth to wipe dirt; for hard contamination, use neutral detergent. Any cleanser for high grade furniture is applicable.
- Avoid aiming the camera directly towards extremely bright objects, such as, sun, as this may damage the image sensor.
- Please follow the instructions to install the camera. Do not reverse the camera, or the reversing image will be received.
- Do not operate it in case temperature, humidity and power supply are beyond the limited stipulations.
- 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.
- This is product instructions not quality warranty. We may reserve the rights of amending the typographical errors, inconsistencies with the latest version, software upgrades and product improvements, interpretation and modification. These changes will be published in the latest version without special notification.
- When this product is in use, the relevant contents of Microsoft, Apple and Google will be involved in. The pictures and screenshots in this manual are only used to explain the usage of our product. The ownerships of trademarks, logos and other intellectual properties related to Microsoft, Apple and Google belong to the above-mentioned companies.
- This manual is available for many models. Some functions introduced in the manual may be not available for some models. All pictures and examples used in the manual are for reference only. Please take the real models as the standard.

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.

FCC Marking

The products have be tested and found in compliance with the council FCC rules and regulations part 15 subpart B. Operation of this product is subject the following two conditions: (1) this device may not cause harmful interface, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CE Marking

The products have been manufactured to comply with the following directives.
EMC Directive 2014/30/EU

RoHS Marking

The products have 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.

Table of Contents

1 Introduction 1

2 Network Connection 2

2.1 Wi-Fi Connection 2

2.2 Wired Network Connection 2

2.2.1 Access through IP-Tool 3

2.2.2 Directly Access through IE 4

2.2.3 WAN 6

3 Live View 9

4 Camera Configuration 11

4.1 System Configuration 11

4.1.1 Basic Information 11

4.1.2 Date and Time 11

4.1.3 Local Config 12

4.1.4 Storage 12

4.2 Image Configuration 14

4.2.1 Display Configuration 15

4.2.2 Video / Audio Configuration 17

4.2.3 OSD Configuration 18

4.2.4 Video Mask 19

4.2.5 ROI Configuration 20

4.3 Alarm Configuration 20

4.3.1 Motion Detection 20

4.3.2 PIR Alarm 22

4.3.3 Other Alarms 22

4.3.4 Alarm In 24

4.3.5 Alarm Out 25

4.3.6 Alarm Server 26

4.4 Event Configuration (Optional) 26

4.4.1 Exception 27

4.4.2 Line Crossing 28

4.4.3 Intrusion 29

4.5 Network Configuration 31

4.5.1 TCP/IP 31

4.5.2 Port 32

4.5.3 Server Configuration 33

4.5.4 DDNS 33

4.5.5 SNMP 34

4.5.6 802.1x 35

4.5.7 RTSP 36

4.5.8 UPNP 37

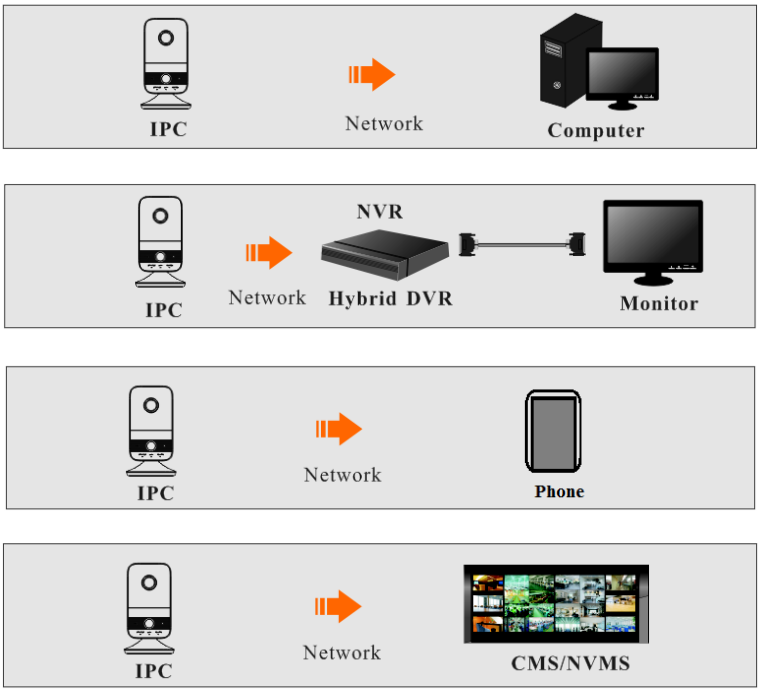
4.5.9 Email 37
4.5.10 FTP 38
4.5.11 HTTPS 39
4.5.12 P2P (Optional) 40
4.5.13 QoS 41
4.5.14 Wi-Fi Settings 41
4.6 Security Configuration 43
4.6.1 User Configuration 43
4.6.2 Online User 45
4.6.3 Block and Allow Lists 45
4.6.4 Security Management 46
4.7 Maintenance Configuration 46
4.7.1 Backup and Restore 46
4.7.2 Reboot 47
4.7.3 Upgrade 47
4.7.4 Operation Log 48
5 Search 49
5.1 Image Search 49
5.2 Video Search 51
5.2.1 Local Video Search 51
5.2.2 SD Card Video Search 52
Appendix 55
Appendix 1 Q & A 55
Appendix 2 Specifications 57

1 Introduction

Main Features

- ICR auto switch, true day/night
- Wi-Fi
- 3D DNR, true WDR, ROI coding
- Support BLC, HLC, true WDR, Anti-flicker
- Support mobile surveillance by smart phones with iOS or Android OS

Surveillance Application



2 Network Connection

You may connect IP-Cam via the wired network or wireless network. The details are as follows:

2.1 Wi-Fi Connection

There are three ways to connect Wi-Fi.

Method one: use the WPS (Wi-Fi Protected Setup) function. Press the WPS button on the router and then press the RST button on the camera within 120s to quickly connect the Wi-Fi. Pressing the RST button on the camera and then pressing the WPS button on the router will work as well. The red alarm indicator will flash if the Wi-Fi is connected.

Method two: Log in the camera through the wired network. Then go to Config→Network→WI-FI interface. Enable Wi-Fi and select the desired wireless router. Then enter the key. Refer to Wi-Fi Settings for more details.

Method three: Log in the camera through the wired network. Then go to Config→Network→WI-FI interface to enable and configure WPS function (See Wi-Fi Settings–Easy Wi-Fi Connection with WPS Function for more details).

APP Monitoring

① Enable Wi-Fi function in your mobile phone.

② Open your phone's APP store and search "Surperlive Plus".

③ Install this APP in your phone.

④ Run this APP and then add the IP address, username and password of the IPC or scan the QRcode of the IPC (Go to Config→System→Basic Information interface through Web Client. Please make sure the P2P function is enabled first).

IP address: please view the IP address of the IPC in the wireless router.

Username: the default username is "admin".

Password: the default password is "123456".

⑤ View the image through the APP. Please refer to the Mobile Surveillance User Manual for more details.

If 3G/4G/5G network is used in your mobile phone, you shall view the IP address of the IPC in the router and then forward the IP address and ports of the IPC in the router (Config→Network→Port menu to set the port number). Then use the WAN IP address and port of the IPC to log in the APP. If P2P function is enabled in the IPC, you can skip this step.

Note：Only some specified version supports P2P function.

2.2 Wired Network Connection

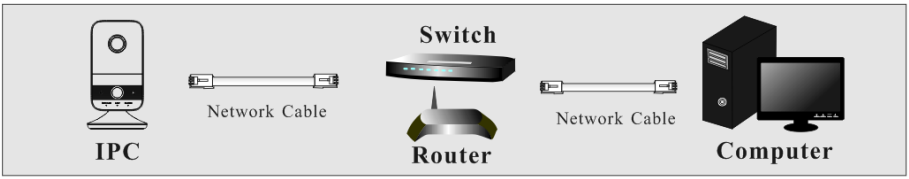
Here we take IE browser for example to introduce how to access the camera.

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

through IE browser.

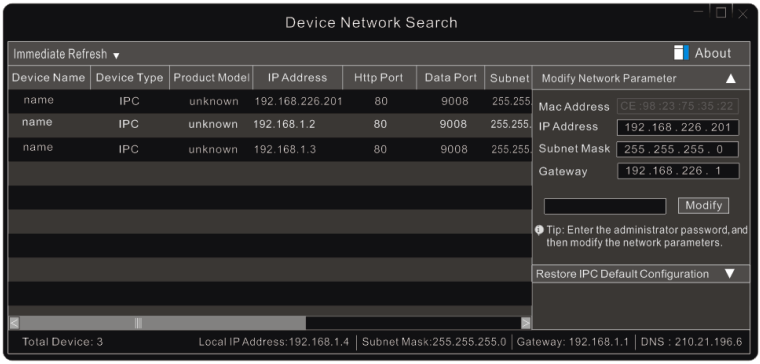
2.2.1 Access through IP-Tool

Network connection:

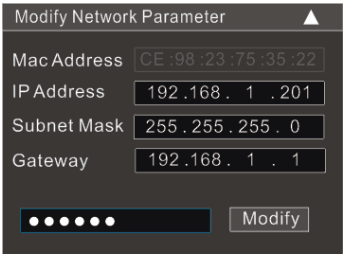


①Make sure the PC and IP-Cam are connected to the LAN and the IP-Tool is installed in the PC from the CD.

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 the computer's. Please modify the IP address of your device according to the practical situation.



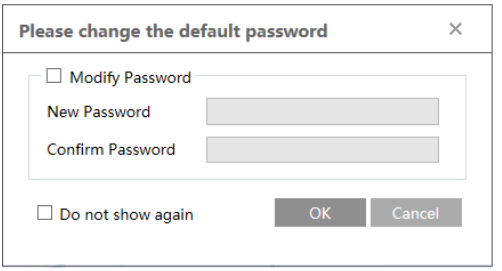
For example, the IP address of your computer is 192.168.1.4. So the IP address of the camera shall be changed to 192.168.1.X. After modification, please enter the password of the administrator and click "Modify" button to modify the setting.

☞ 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 plugin.

Enter the username and password to log in.

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



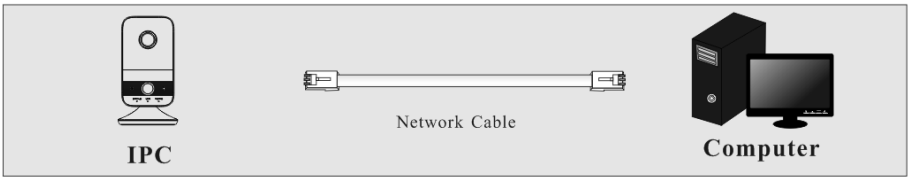
The system will pop up the above-mentioned textbox to ask you to change the default password. It is strongly recommended to change the default password for account security. If "Do not show again" is checked, the textbox will not appear next time.

2.2.2 Directly Access through IE

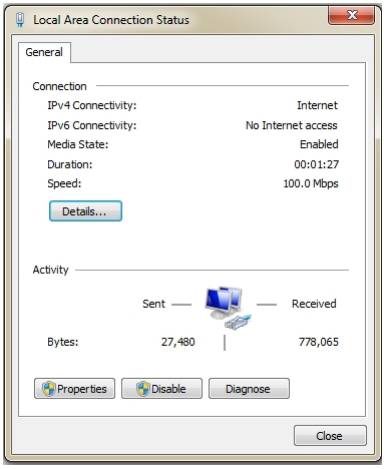
The default network settings are as shown below:
IP address: **192.168.226.201**
Subnet Mask: **255.255.255.0**

Gateway: **192.168.226.1**
HTTP: **80**
Data port: **9008**

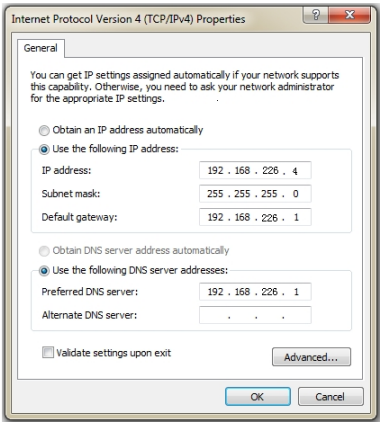
You may use the above default settings when you log in the camera for the first time. You may directly connect the camera to the computer through network cable.



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.



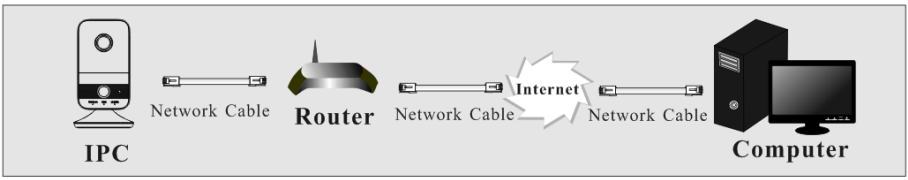
② Open the IE browser and enter the default address of IP-CAM and confirm.

③ Follow directions to download and install the Active X control.

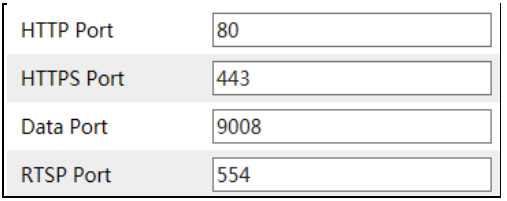
④ Enter the default username and password in the login window and then enter to view.

2.2.3 WAN

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

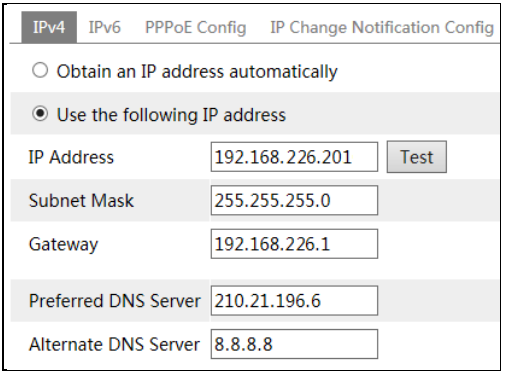


① Make sure the camera is well connected via LAN and then log in the camera via LAN and go to Config→Network→Port menu to set the port number.



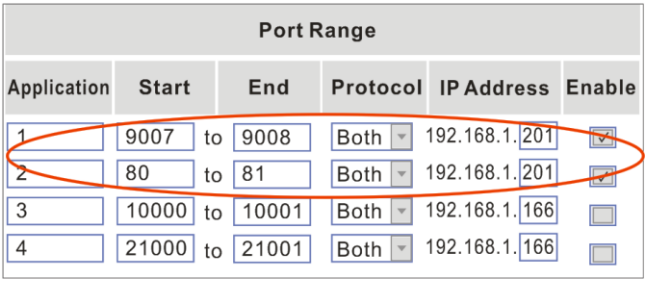
Port Setup

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".

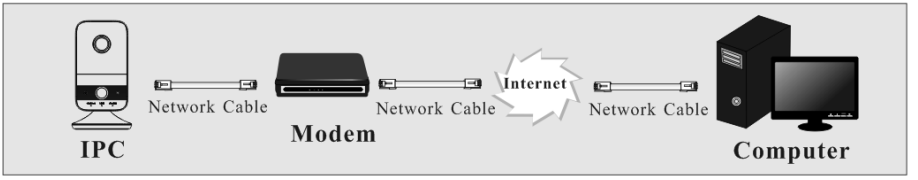


Router Setup

④ Open the IE browser and enter its WAN IP and http port to access. (for example, if 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**

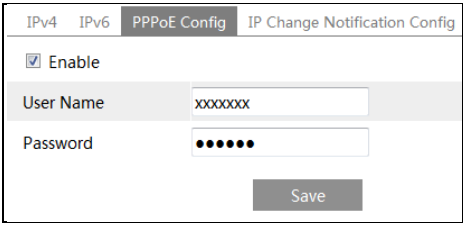
Network connection



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:

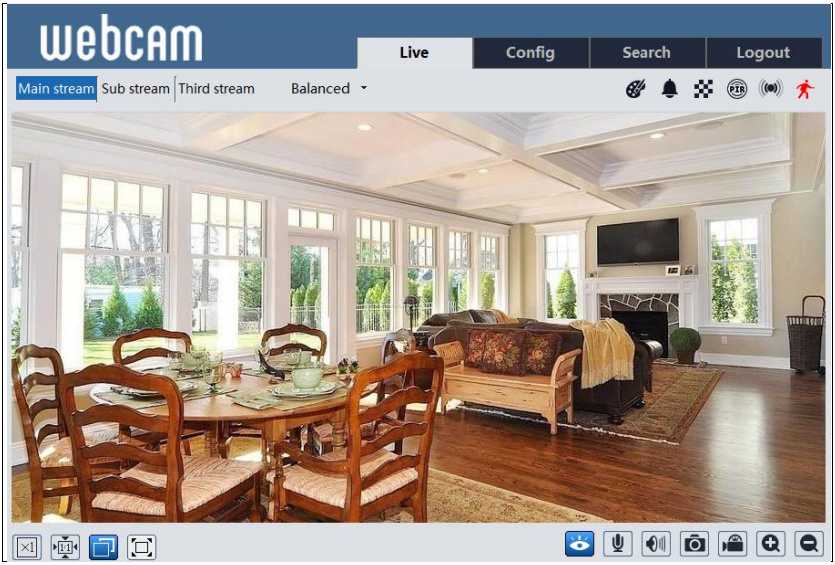
① Go to Config→Network→Port menu to set the port number.

② Go to Config →Network→TCP/IP menu to set the IP address. Check "Use the following IP address" and then enter 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 you log in through the Web Client, you will see the following window.



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

Icon	Description	Icon	Description
	Original size		Zoom in
	Fit correct scale		Zoom out
	Auto (fill the window)		Scene change indicator
	Full screen		Abnormal clarity indicator
	Start/stop live view		Color abnormal indicator
	Start/stop two-way audio		PIR (Passive Infrared) alarm indicator
	Enable/disable audio		Sensor alarm indicator
	Snapshot		Motion alarm indicator
	Start/stop local recording		

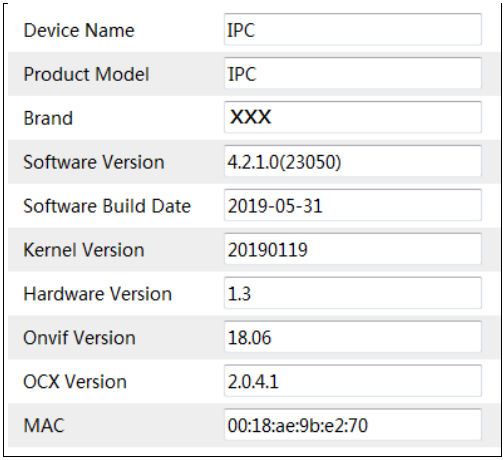
- All above-mentioned indicators will flash in live view interface only when the corresponding events are enabled.
- In full screen mode, double click on the mouse to exit or press the ESC key on the keyboard.

4.1 System Configuration

The “System” configuration includes four submenus: Basic Information, Date and Time, Local Config and Storage.

4.1.1 Basic Information

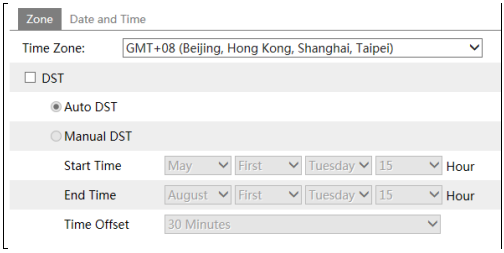
In the “Basic Information” interface, the system information of the device is listed.



Some versions may support device ID and QR code. If P2P is enabled (see Network Configuration-P2P), the network camera can be quickly added to mobile surveillance APP by scanning the QR code or entering device ID.

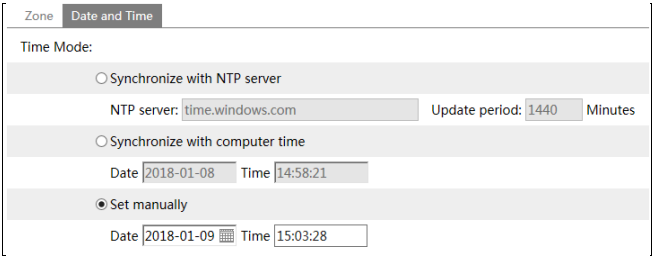
4.1.2 Date and Time

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



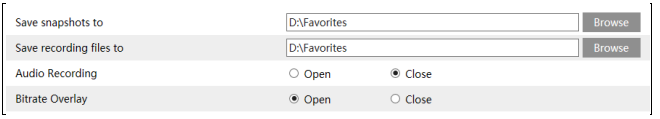
Select the time zone and DST as required.

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



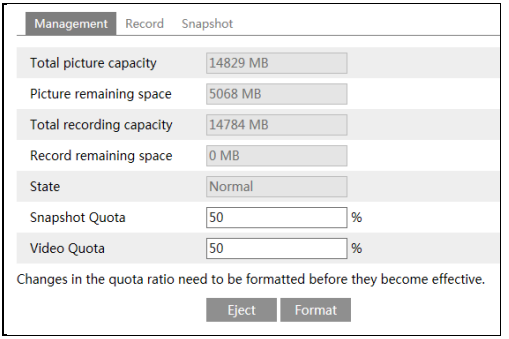
4.1.3 Local Config

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.

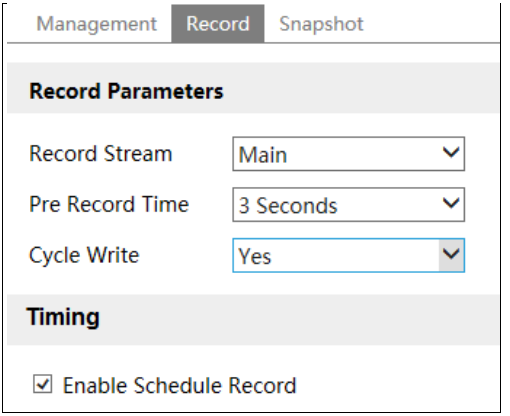
Click the “Eject” button to stop writing data to SD card. Then the SD card can be ejected safely.

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**

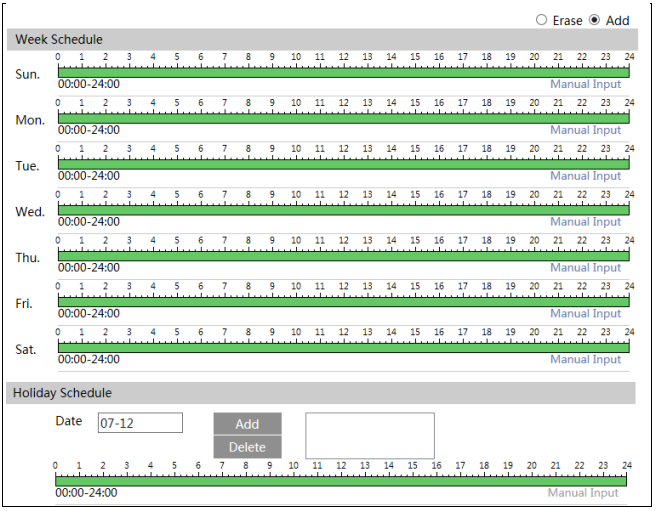
1. Go to Config→System→Storage→Record to go to the interface as shown below.



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

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

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



Weekly schedule

Set the alarm time from Monday to Sunday for a single week. Each day is divided 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.

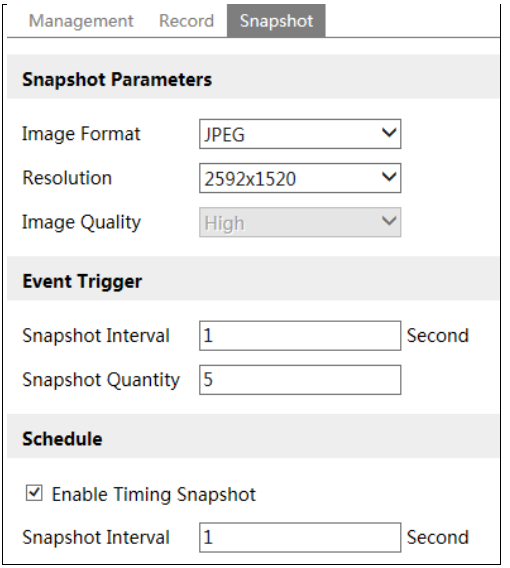
"Erase": Delete the schedule. Drag the mouse to erase the time on the timeline.

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.

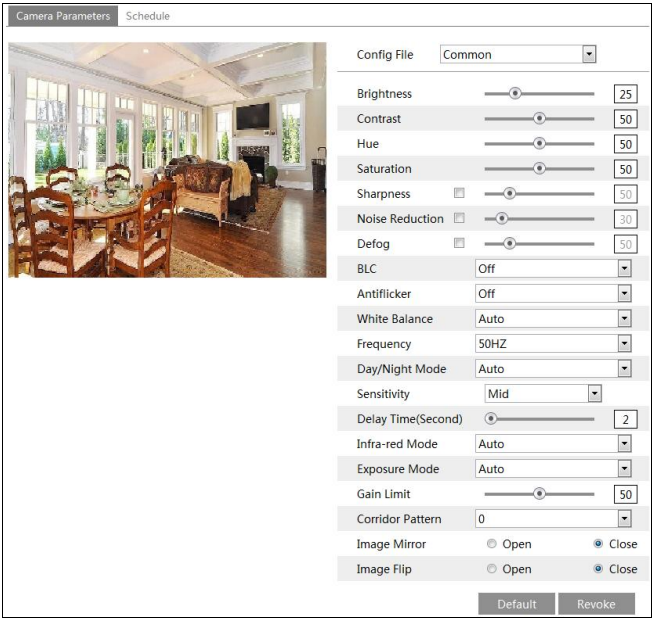
Timing Snapshot: Enable timing snapshot first and then set the snapshot interval and schedule. The setup steps of schedule are the same as the schedule recording (See Schedule Recording).

4.2 Image Configuration

Image Configuration includes Display, Video/Audio, OSD, Video Mask and ROI Config.

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.
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: disables the backlight compensation function. It is the default mode.
- HWDR

◆ WDR can adjust the camera to provide a better image when there are both very bright and very dark areas simultaneously in the field of 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.

- 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:

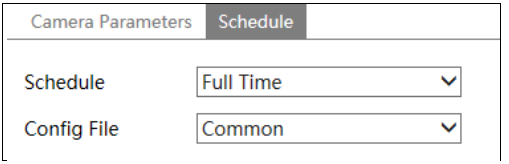
- Off: Close the anti-flicker function.
- 50Hz: Make sure the horizontal stripes will not appear in the image while the device is adjusting the exposure automatically according to the brightness of the scene when the electric supply is 50Hz.
- 60Hz: Make sure the horizontal stripes will not appear in the image while the device is adjusting the exposure automatically according to the brightness of the scene when the electric supply is 60Hz.

Antiflicker:

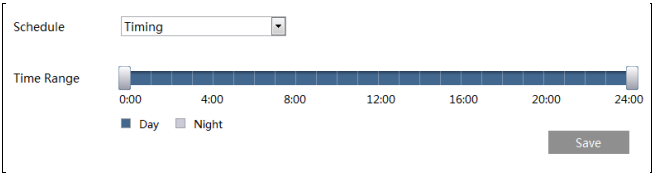
- Off: disables the anti-flicker function. This is used mostly in outdoor installations.
- 50Hz: reduces flicker in 50Hz lighting conditions.
- 60Hz: reduces flicker in 60Hz lighting conditions.

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 for switching back and forth from day to night modes.
Infrared Mode: Choose "ON", "OFF" or "Auto".
Exposure Mode: Choose "Auto" or "Manual". If manual is chosen, the digital shutter speed can be adjusted.
Corridor Pattern: Corridor viewing modes can be used for situations such as long hallways. 0, 90, 180 and 270 are available. The default value is 0. The video resolution should be 1080P or below if this function is used.
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.



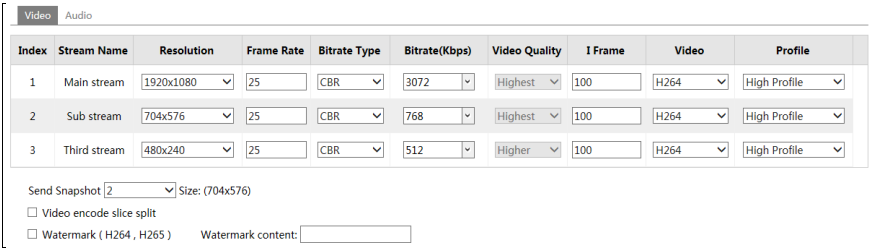
Set full time schedule for common, day, night mode and specified time schedule for day and night. Choose "Schedule" in the drop-down box of schedule as shown below.



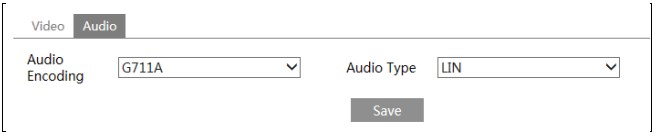
Drag " " icons to set the time of day and night. Blue means day time and blank means night time. If the current mode of camera parameters is set to schedule, the image configuration mode will automatically switch between day and night according to the schedule.

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.



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



Three 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.

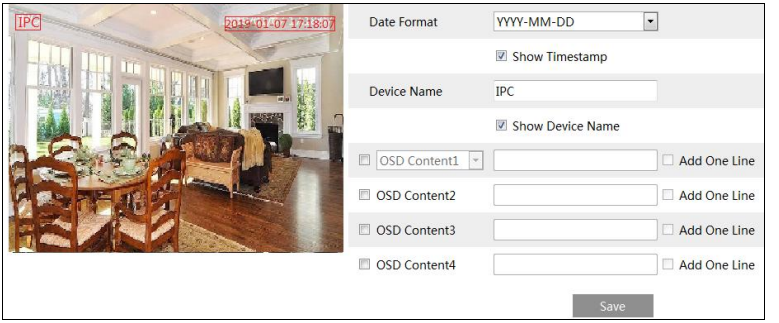
Bitrate: it can be adjusted when the mode is set to CBR. The higher the bitrate, the better the image quality will be.

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

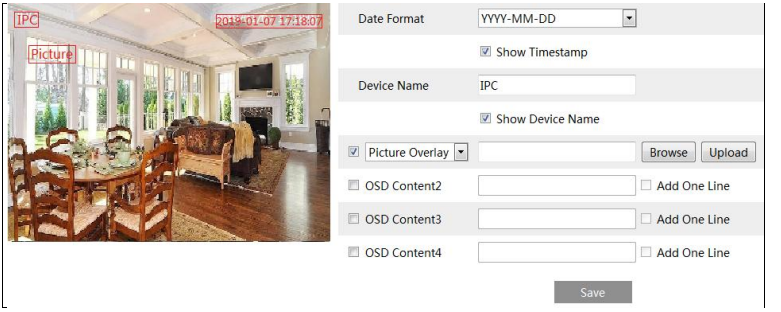
I Frame interval: that is group of pictures. It determines how many frames are allowed between a "group of pictures". When a new scene begins in a video, until that scene ends, the entire group of frames (or pictures) can be considered as a group of pictures. If there is not much movement in the scene, 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 can be 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: How many snapshots to generate for an event.
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.
Audio Encoding: G711A and G711U are selectable.
Audio Type: LIN.

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.

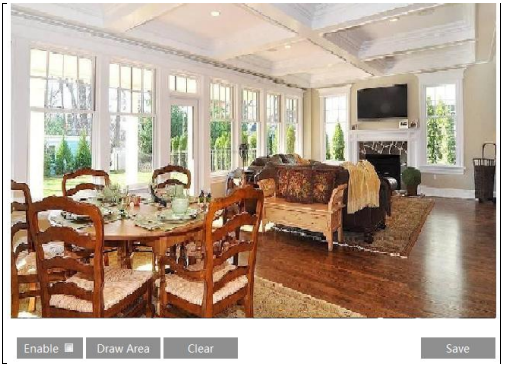


Picture Overlap Settings:

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.

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 “Draw Area” button and then drag the mouse to draw the video mask area.
3. Click “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

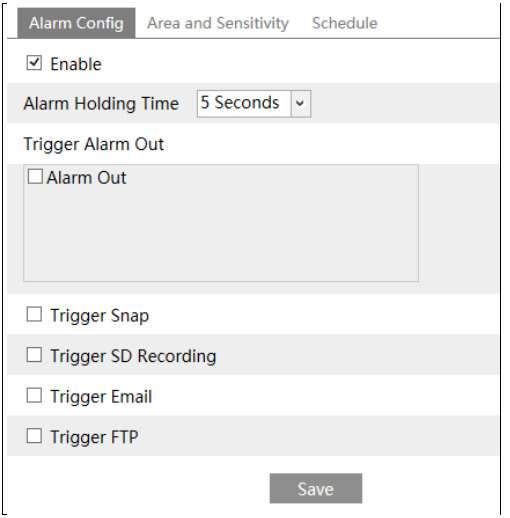
Go to Image→ROI Config interface as shown below. An area in the image can be set as a region of interest. This area will have a higher bitrate than the rest of the image, resulting in better image quality for the identified area.

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 Alarm Configuration

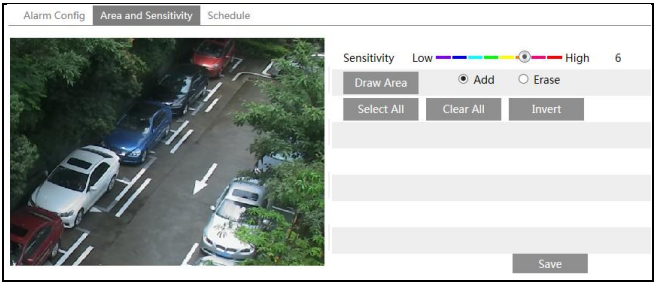
4.3.1 Motion Detection

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 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 (this function is only available for the models with SD slot).
Trigger SD Recording: If selected, video will be recorded on an SD card on motion detection (this function is only available for the models with SD card slot).
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 the “Area and Sensitivity” tab to go to the interface as shown below.

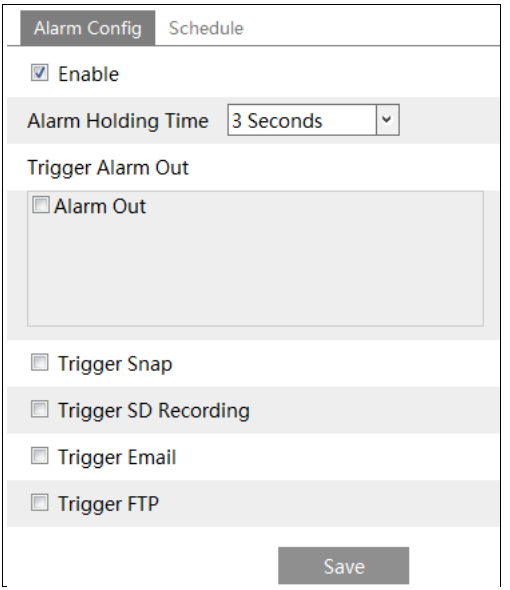


Move the “Sensitivity” scroll bar to set the sensitivity. Higher sensitivity value means that motion will be triggered more easily.
Select “Add” and click “Draw”. Drag the mouse to draw the motion detection area; Select “Erase” and drag the mouse to clear motion detection area.
After that, click the “Save” to save the settings.

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

4.3.2 PIR Alarm

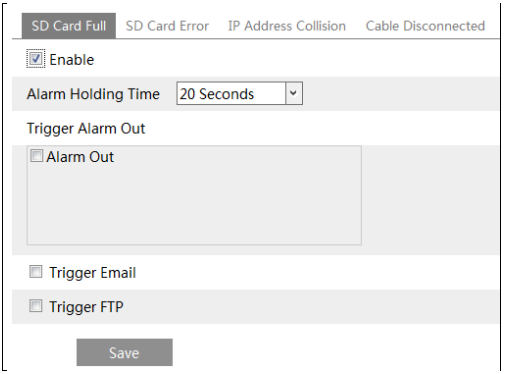
PIR alarm: Alarms will be triggered when the camera detects human bodies or animals.
1. Enable PIR alarm and then set the alarm holding time.
2. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection chapter for details.
3. Set the schedule for PIR alarm. The schedule setup steps of the PIR alarm are the same as the schedule recording setup (See Schedule Recording).



4.3.3 Other Alarms

- **SD Card Full**

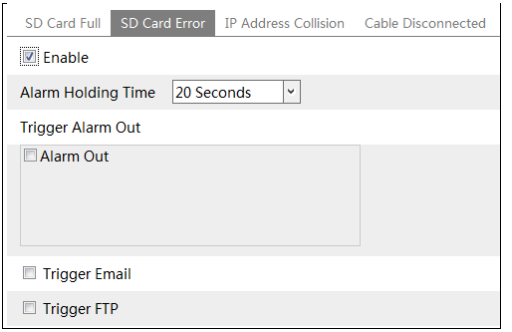
1. Go to Config→Alarm→Anomaly→SD Card Full.



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**

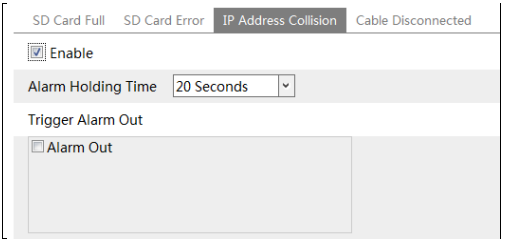
When there are some errors in writing SD card, the corresponding alarms will be triggered.
1. Go to Config→Alarm→Anomaly→SD Card Error as shown below.



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.
Note: **SD card full and SD card error are only available for the models with SD slot.**

- **IP Address Conflict**

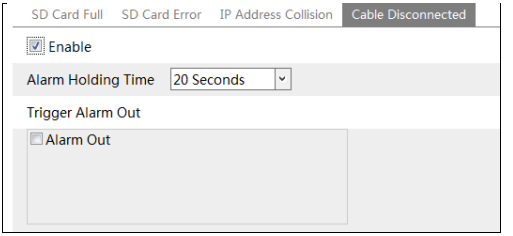
1. Go to Config→Alarm→Anomaly→IP Address Collision as shown below.



2. Click "Enable alarm" 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.
Note: **This function is only available for the models with alarm output interface.**

- **Cable Disconnection**

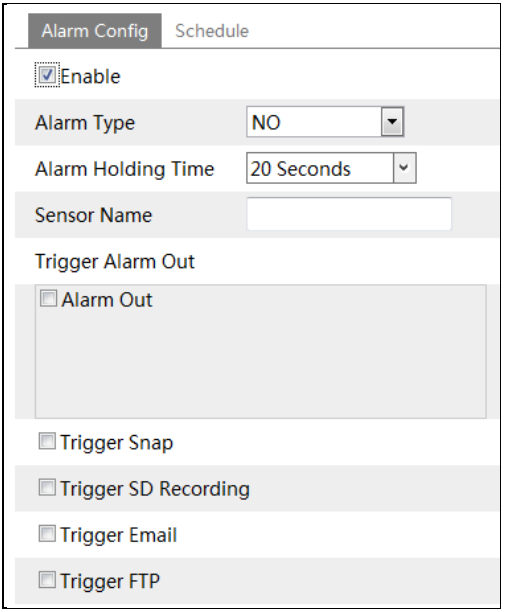
1. Go to Config→Alarm→Anomaly→Cable Disconnected as shown below.



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.
Note: **This function is only available for the models with alarm output interface.**

4.3.4 Alarm In

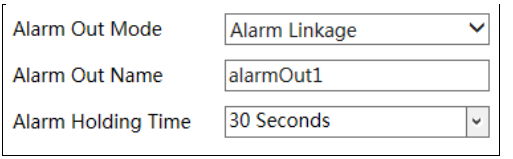
This function is only available for some models. To set sensor alarm (alarm in):
Go to Config→Alarm→Alarm In interface as shown below.



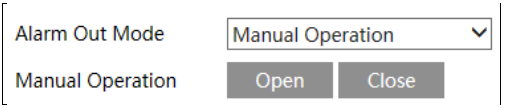
1. Enable alarm and set the alarm type, alarm holding time and sensor name.
2. Set alarm trigger options. The setting steps are the same as motion detection. Please refer to motion detection chapter for details.
3. Click the "Save" button to save the settings.
4. Set the schedule of the sensor alarm.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

4.3.5 Alarm Out

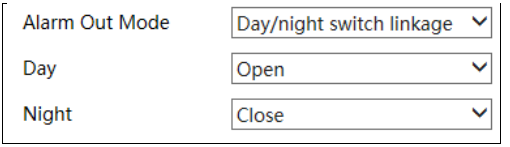
Go to Config→Alarm→Alarm Out interface as shown below:



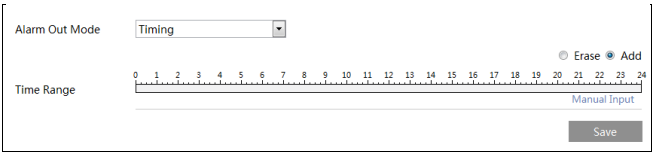
Alarm Out Mode: Alarm linkage, manual operation, day/night switch linkage and timing are optional.
Alarm Linkage: Having selected this mode, select alarm out name and alarm holding time at the "Alarm Holding Time" pull down list box.
Manual Operation: Having selected this mode, click "Open" to trigger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



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



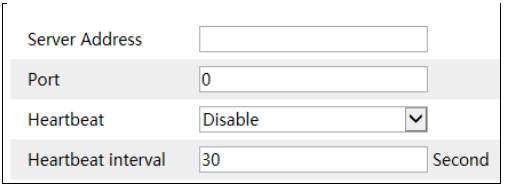
Timing: Click "Add" and drag the mouse on the timeline to set the schedule of alarm out; click "Erase" and drag the mouse on the timeline to erase the set time schedule. After this schedule is saved, the alarm out will be triggered in the specified time.



4.3.6 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.



4.4 Event Configuration (Optional)

(Only some customized version may support the following functions).

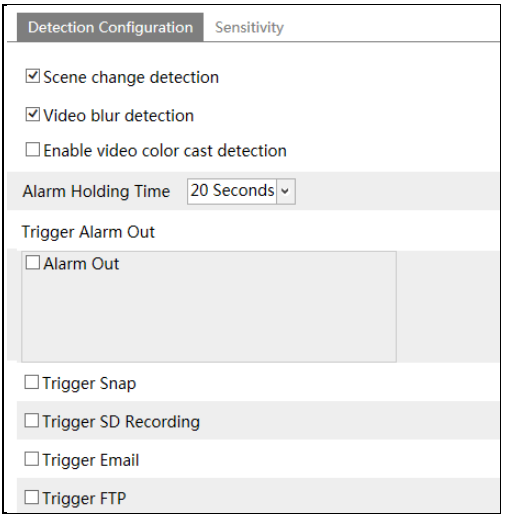
For more accuracy, here are some recommendations for installation.

- 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.

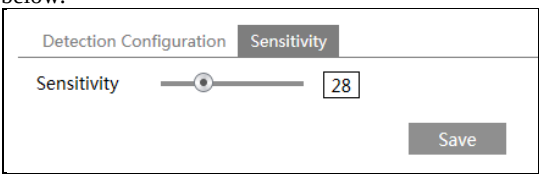
- Avoid scenario where the object's color is similar to the background color.
- At any time of day or night, please make sure the image of the camera is clear and with adequate and even light, avoiding overexposure or too much darkness on both sides.

4.4.1 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.



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.
Enable Video Color Cast Detection: Alarms will be triggered if the video becomes obscured.
2. Set the alarm holding time and alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection chapter for details.
3. Click the "Save" button to save the settings.
4. Set the sensitivity of the exception detection. Click the "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 the "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 Video Cast Detection: The higher the value is, the more sensitive the system responds to the color cast of the device image.

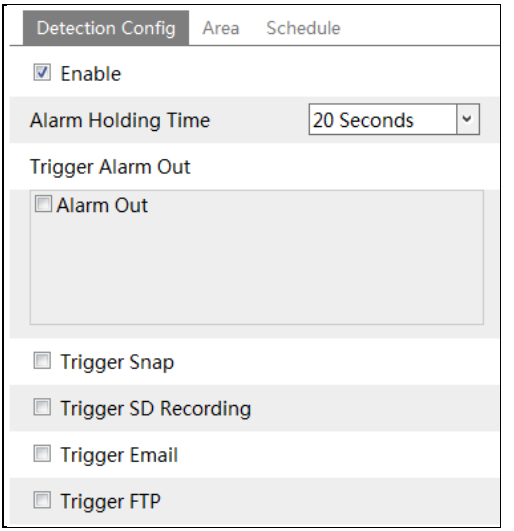
※ The requirements of camera and surrounding area

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

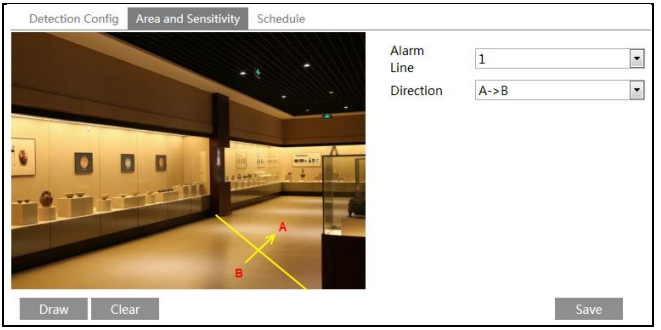
4.4.2 Line Crossing

Line Crossing: Alarms will be triggered if someone or something crosses the pre-defined alarm lines. It can replace the electronic fence, warning line of flood prevention, etc.

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



1. Enable line crossing alarm and set the alarm holding time.
2. Set the alarm holding time and alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection chapter for details.
3. Click the "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. Up to 4 lines can be added. Multiple lines cannot be added simultaneously.

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

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

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

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

Click the "Draw" button and then drag the mouse to draw an alarm line in the image on the left side. Click the "Stop" button to stop drawing. Click the "Clear" button to delete the cordons. Click the "Save" button to save the settings.

5. Set the schedule of the line crossing alarm. The setup steps of the schedule are the same as the schedule recording setup (See Schedule Recording).

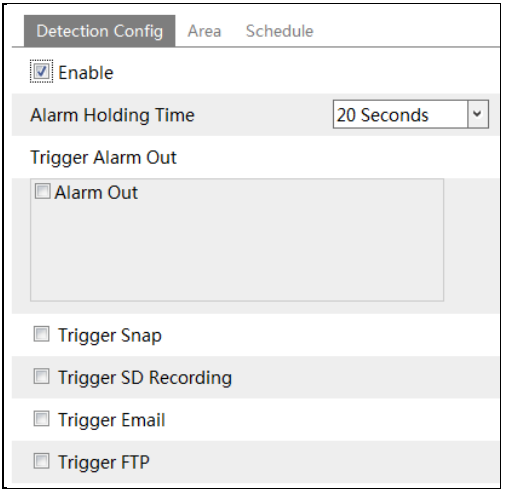
※ Configuration of camera and surrounding area

1. Auto-focusing function should not be enabled for line crossing detection.
2. Avoid the scenes with many trees or the scenes with various light changes (like many flashing headlights). The ambient brightness of the scenes shouldn't be too low.
3. Cameras should be mounted at a height of 2.8 meters or above.
4. Keep the mounting angle of the camera at about 45 °.
5. 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.
6. Make sure cameras can view objects for at least 2 seconds in the detected area for accurate detection.
7. Adequate light and clear scenery are crucial for line crossing detection.
8. Please contact us for more detailed application scenarios.

4.4.3 Intrusion

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→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 chapter 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. Up to 4 alarm areas can be set up.
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 intrusion detection. The setup steps of the schedule are the same as

the schedule recording setup (See Schedule Recording).

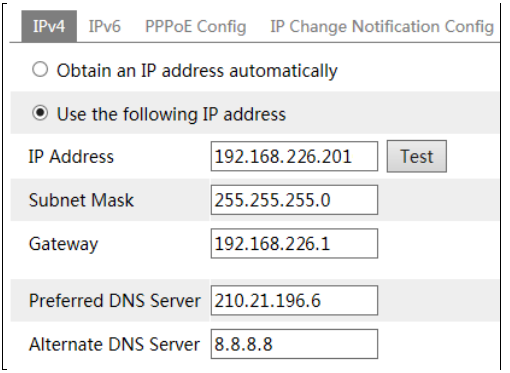
※ Configuration requirements of camera and surrounding area

1. Auto-focusing function should not be enabled for intrusion detection.
2. Avoid the scenes with many trees or the scenes with various light changes (like many flashing headlights). The ambient brightness of the scenes shouldn't be too low.
3. Cameras should be mounted at a height of 2.8 meters or above.
4. Keep the mounting angle of the camera at about 45 °.
5. 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.
6. Make sure cameras can view objects for at least 2 seconds in the detected area for accurate detection.
7. Adequate light and clear scenery are crucial to line crossing detection.
8. Please contact us for more detailed application scenarios.

4.5 Network Configuration

4.5.1 TCP/IP

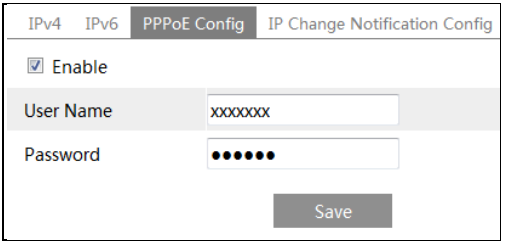
Go to Config→Network→TCP/IP interface as shown below. There are two ways for network connection.



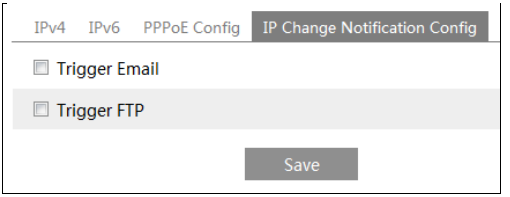
Use IP address (take IPv4 for example)-There are two options for IP setup: obtain an IP address automatically by DHCP and use the following IP address. Please choose one of the options as needed.

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.



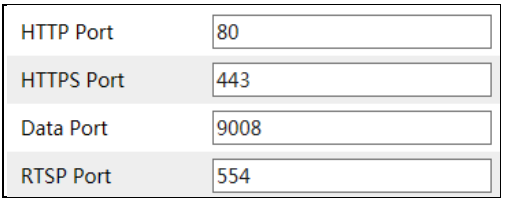
Either method of network connection can be used. If PPPoE is used to connect internet, the camera will get a dynamic WAN IP address. This IP address will change frequently. To be notified, the IP change notification function can be used.
Click "IP Change Notification Config" to go to the interface as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

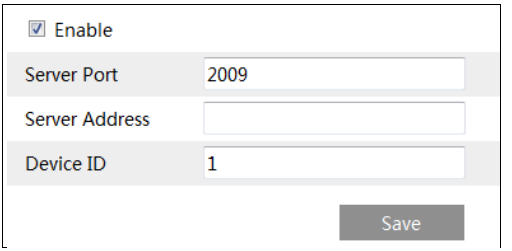
Go to Config→Network→Port interface as shown below. HTTP port, Data port and RTSP port can be set.



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. It can be changed to any port which is not occupied.
RTSP Port: The default port is 554. It can be changed to any port which is not occupied.

4.5.3 Server Configuration

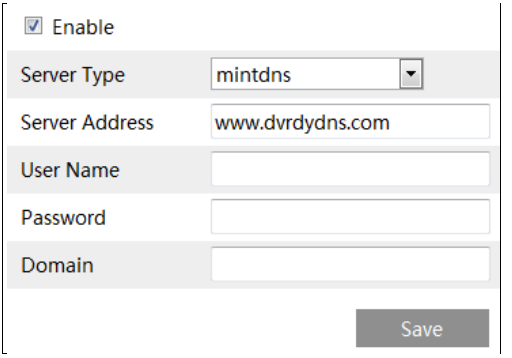
This function is mainly used for connecting network video management system.



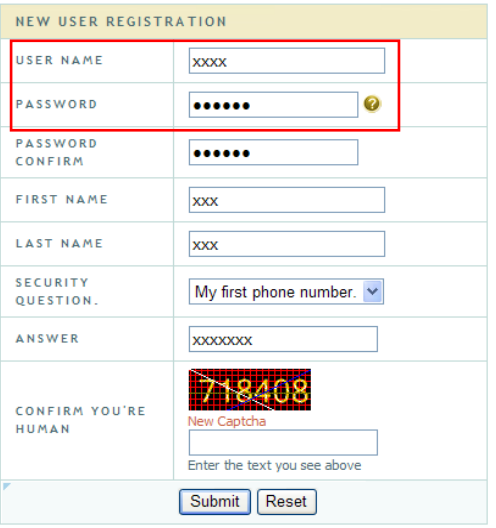
1. Check “Enable”.
2. Check the IP address and port of the transfer media server in the ECMS/NVMS. Then enable the auto report in the ECMS/NVMS when adding a new device. Next, enter the remaining information of the device in the ECMS/NVMS. After that, the system will auto allot a device ID. Please check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

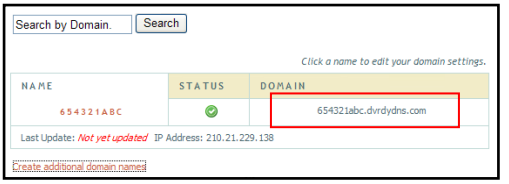


2. Apply for a domain name. Take www.dvrdyndns.com for example.
Enter www.dvrdydns.com in the IE address bar to visit its website. Then click “Registration” button.



Create domain name.

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



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

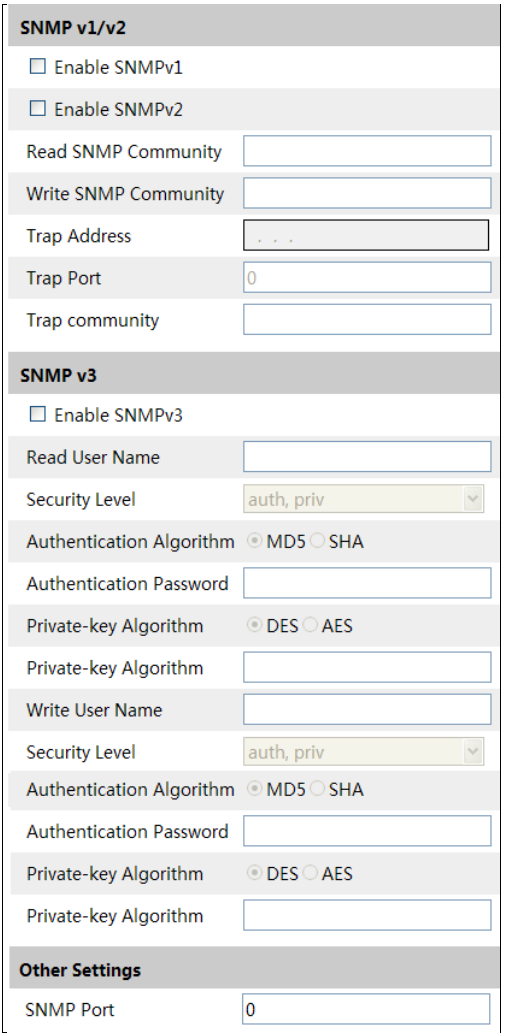
4.5.5 SNMP

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

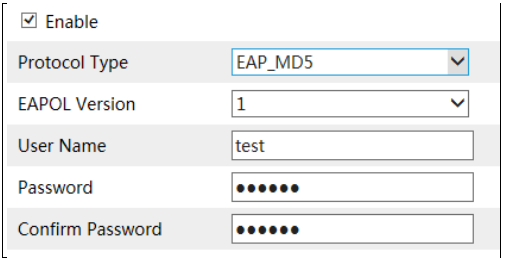
Port" and so on. Please make sure the settings are the same as that of your SNMP software.

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

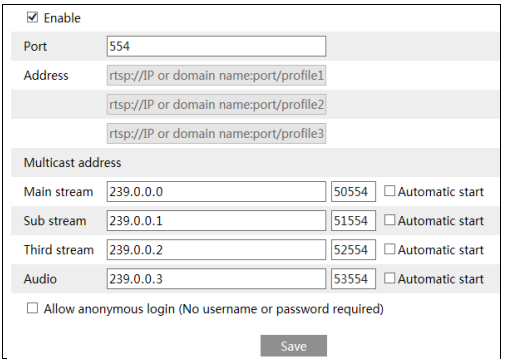
IEEE802.X which is an access control protocol manages the device in connection with the local network by authentication. The setup steps are as follows:



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 support local play 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 play 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

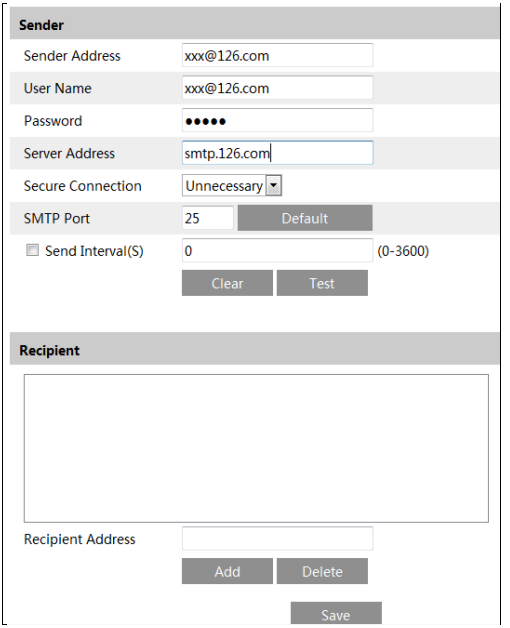
If this function is enabled, the camera can be quickly accessed through the LAN.

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.

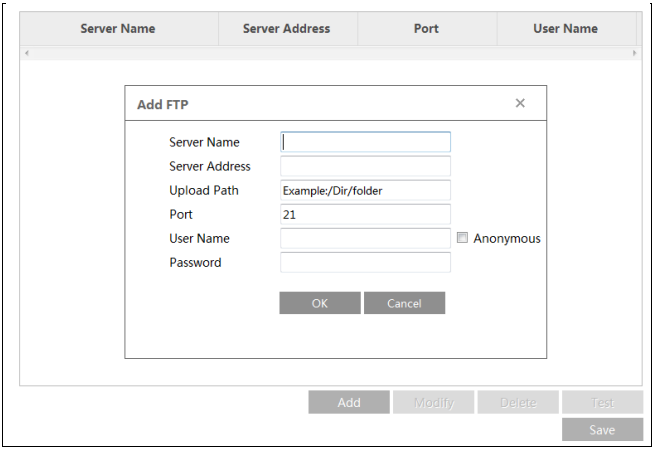
Go to Config→Network →Email.



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

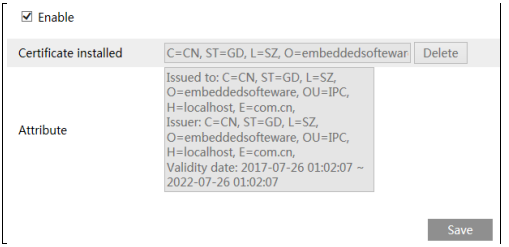
After you set the FTP server, captured pictures from events will be uploaded to the FTP server.
Go to Config→Network →FTP.



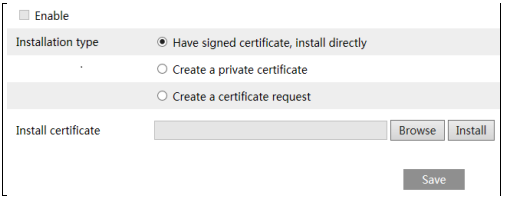
Server Name: The name of the FTP server.
Server Address: The IP address or domain name of the FTP.
Upload Path: The directory where files will be uploaded to.
Port: The port of the FTP server.
Use Name and Password: The username and password that are used to login to the FTP server.

4.5.11 HTTPS

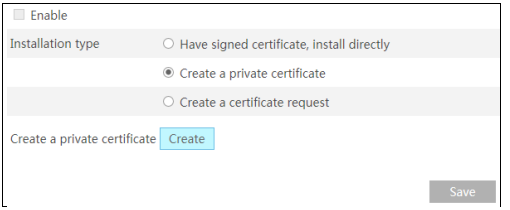
HTTPs provides authentication of the web site and protects user privacy.
Go to Config Config→Network→HTTPS as shown below.



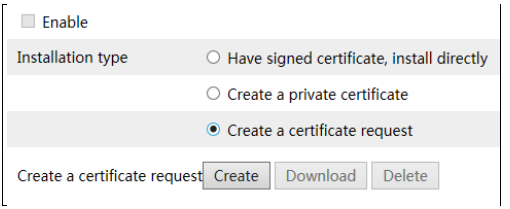
There is a certificate installed by default as shown above. Enable this function and save it. Then the camera can be accessed by entering https://IP: https port via the web browser (eg. https://192.168.226.201:443).
A private certificate can be created if you don't want to use the default one. Click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

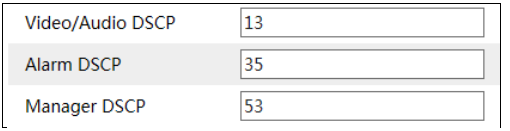
4.5.12 P2P (Optional)

If this function is enabled, the network camera can be quickly accessed by adding the device ID in mobile surveillance client or CMS/NVMS client via WAN. Enable this function by going to Config→Network→P2P interface.

4.5.13 QoS

QoS (Quality of Service) function is used to provide different quality of services for different network applications. Under the shortage of 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.



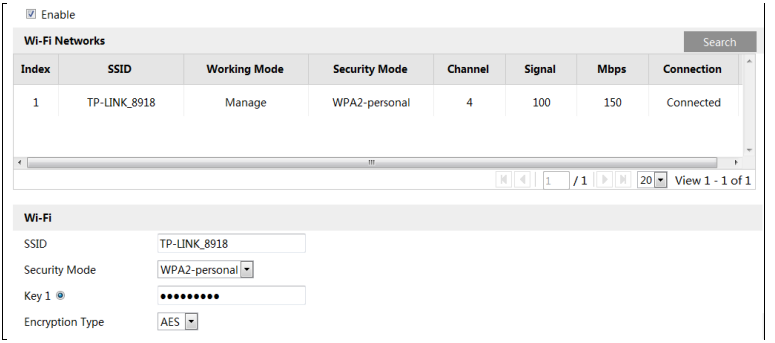
Video/Audio DSCP: The range is from 0 to 63.
Alarm DSCP: The range is from 0 to 63.
Manager DSCP: The range is from 0 to 63.
Generally speaking, the larger the number is, the higher the priority is.

4.5.14 Wi-Fi Settings

Go to Config→Network→WIFI interface as shown below.

There are two ways to connect Wi-Fi.

① **Wi-Fi Connection**



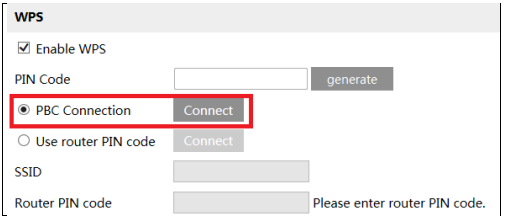
1. Enable Wi-Fi function and then click “Search” to search the online wireless routers.
2. Choose a wireless router on the list. The SSID and security mode of the wireless router will be shown automatically. Please don’t change it manually.
3. Enter the key to connect the wireless router. This key should be set on the router in advance for wireless network connection.

② **Easy Wi-Fi Connection with WPS Function**

If you enable the WPS (Wi-Fi Protected Setup) function, there is no need for you to configure the parameters, such as the key of the wireless connection, encryption type and so on. The WPS connection has two modes--- the PBC mode and the PIN mode.

PBC mode:

PBC refers to the Push-Button-Configuration. You can simply push a button, either an actual or virtual one, on both the wireless router and the camera to quickly connect the wireless network.



1. Enable WPS by checking “Enable WPS”.
2. Select “PBC Connection”.
3. Press the WPS button on the wireless router. If there is no such button, please go to its setting interface to enable the WPS function (please see the user manual of the router for details).
4. Press the WPS (RST) button on the camera or click “Connect” button in the above interface.

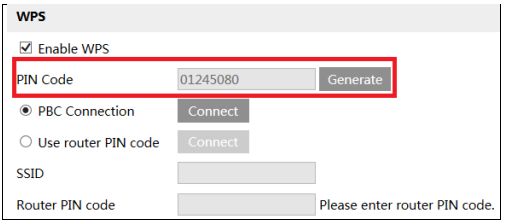
When the PBC mode is both enabled in the router and the camera, the camera and the wireless network will be connected automatically.

PIN Mode

PIN refers to personal identification number. If you choose this mode, you shall enter a PIN to connect the network.

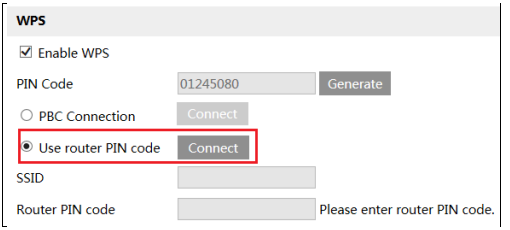
You can generate the code on the camera side and then enter this code to the router.

1. Enable WPS by checking “Enable WPS”.
2. Click “Generate”.



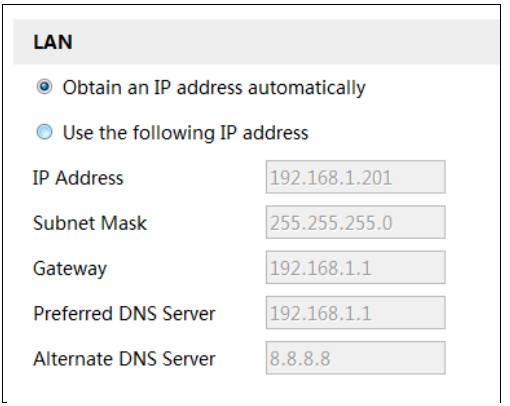
3. Enter the generated code to the router.

You can also use the PIN code of the router and then enter this code to the camera.



1. Select a wireless router on the list and the SSID is loaded automatically.
2. Enable WPS.
3. Enable “Use Router PIN Code”.
4. Enter the PIN code of the router.
5. Click “Connect”.

After the above-mentioned wireless network is configured, you can choose “Obtain an IP address automatically” or “Use the following IP address”.

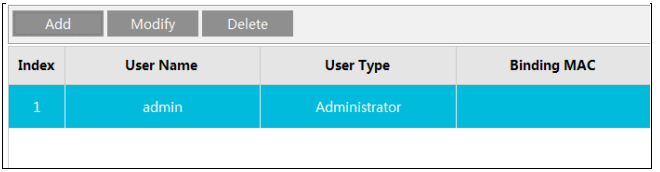


If you choose “Obtain an IP address automatically”, you shall get the IP address from the router.
Or you can choose “Use the following IP address” to set the network parameters manually. Then you can use this IP address to log in mobile surveillance APP/ web client/CMS/NVR/…

4.6 Security Configuration

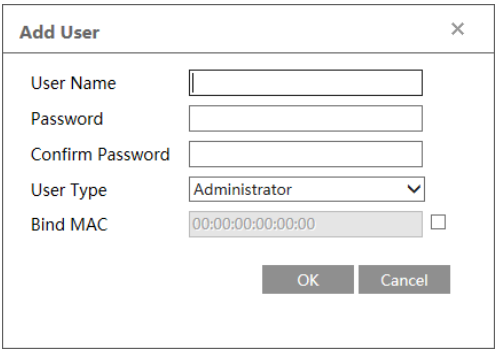
4.6.1 User Configuration

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



Add user:

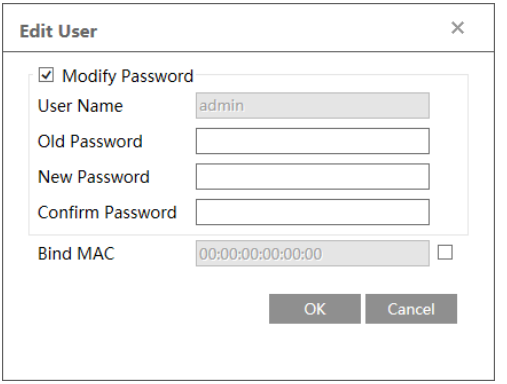
1. Click “Add” button to pop up the following textbox.



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.

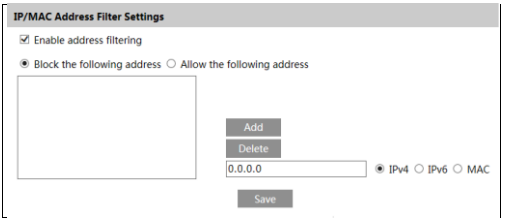
4.6.2 Online User

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 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

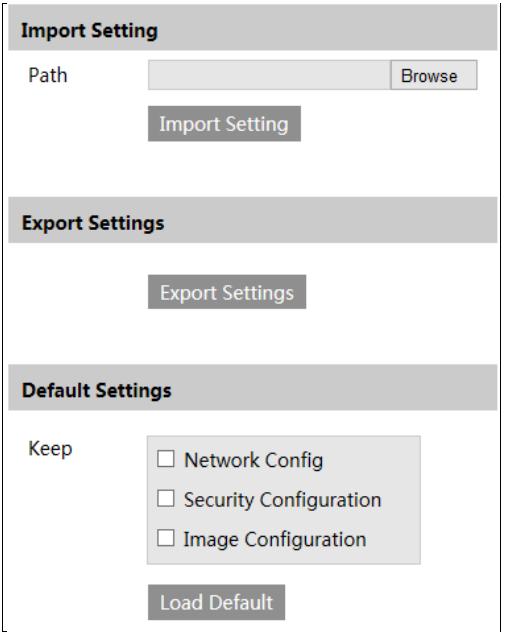
Go to Config→Security→Security Management as shown below.

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.
For some specified versions, anonymous login with a private protocol can be enabled here. If this function is enabled, enter http://host:port/Anonymous/1[2/3] (eg. http://192.168.226.201:80/Anonymous/1) via web browser to access the camera. 1 indicates main stream; 2 indicates sub stream; 3 indicates third stream. Only video can be viewed by this means and no other operations can be done. If no such function, please skip the instruction.

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 form a camera into another camera.

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

- **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.

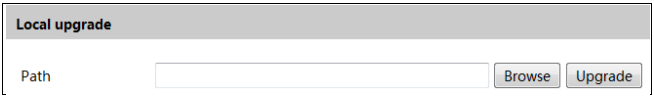
Click the “Reboot” button to reboot the device.

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 the “Save” button to save the settings.

4.7.3 Upgrade

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



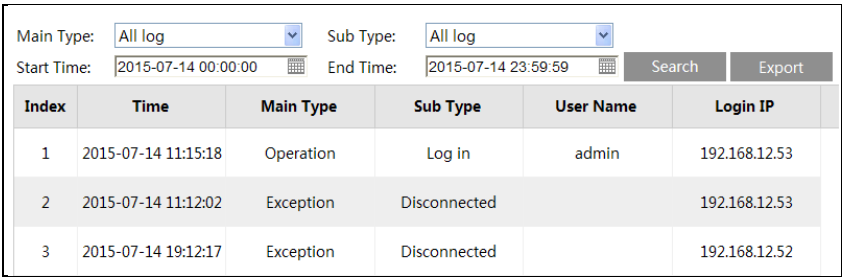
1. Click the “Browse” button to select the save path of the upgrade file
2. Click the “Upgrade” button to start upgrading the firmware.
3. The device will restart automatically

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.

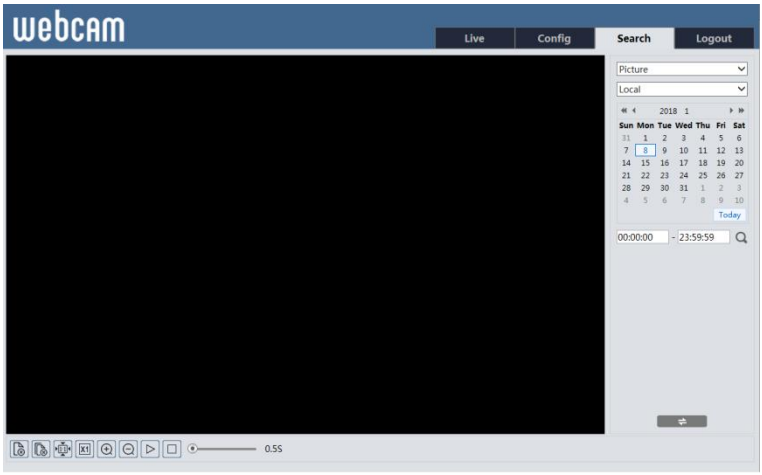


2. Select the main type, sub type, start and end time.
3. Click “Search” to view the operation log.
4. Click “Export” to export the operation log.

5.1 Image Search

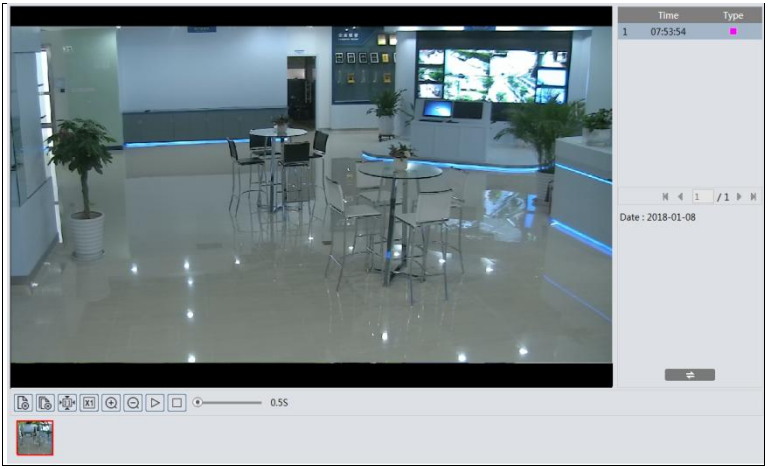
Click Search to go to the interface as shown below. Images that are saved on the SD card can be found here.

Note: If there is no SD card installed in the camera or the SD card is not compatible with the camera, a pop-up message will show stating that there is no card.



- **Local Image Search**

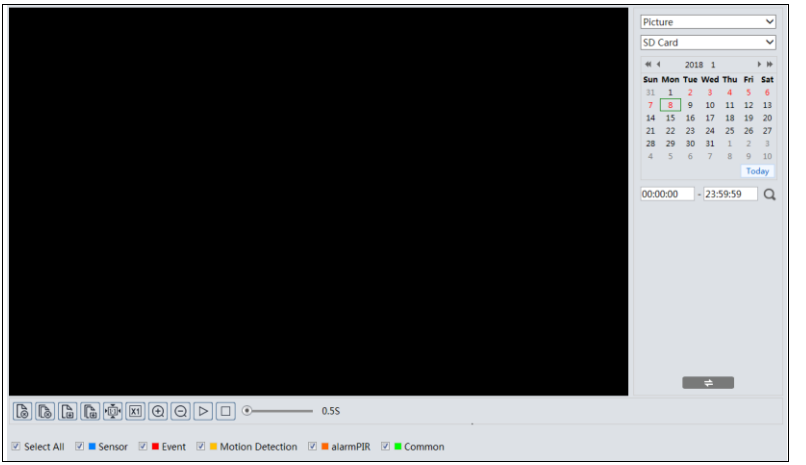
1. Choose “Picture”—“Local”.
2. Set time: Select date and choose the start and end time.
3. Click to search the images.
4. Double click a file name in the list to view the captured photos as shown above.



Click ⇌ to return to the previous interface.

- **SD Card Image Search**

1. Choose “Picture”—“SD Card”.



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

Click ⇌ to return to the previous interface.

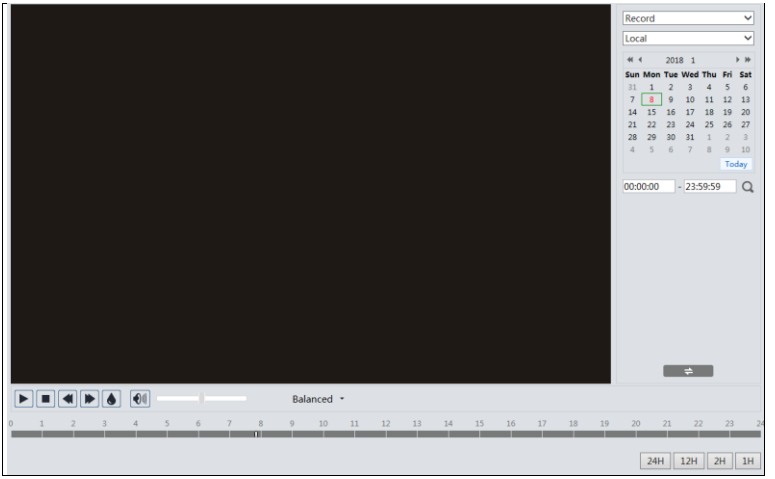
The descriptions of the buttons are shown as follows.

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

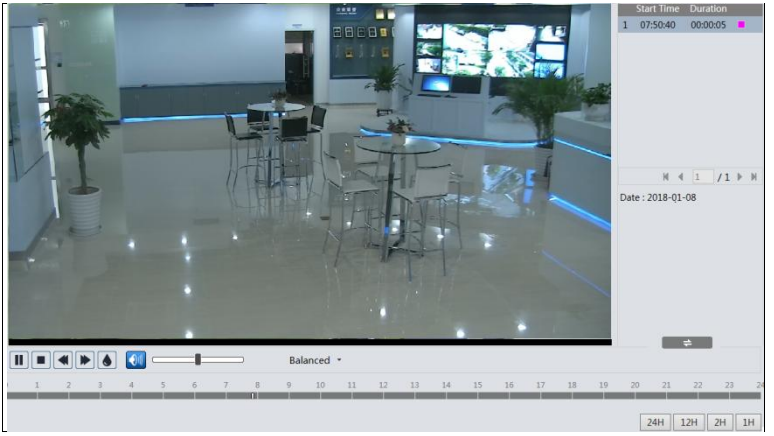
5.2 Video Search

5.2.1 Local 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.



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.



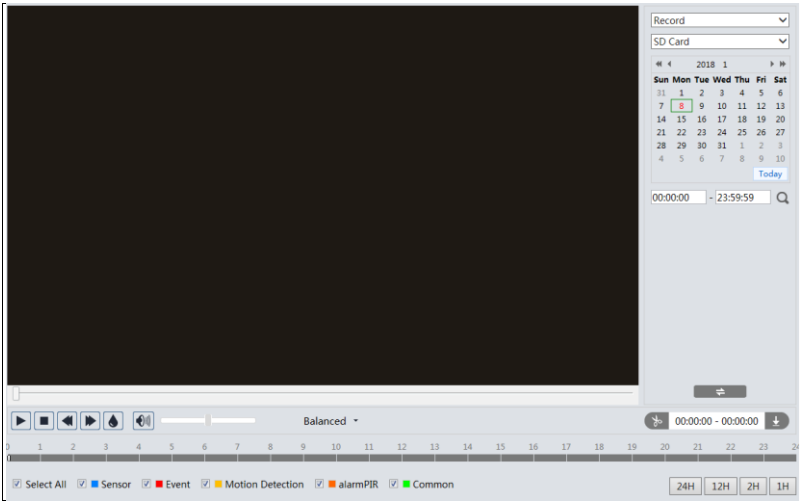
Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button
	Stop button		Speed down
	Speed up		Watermark display
	Enable / disable audio; drag the slider to adjust the volume after enabling audio.		

5.2.2 SD Card Video Search

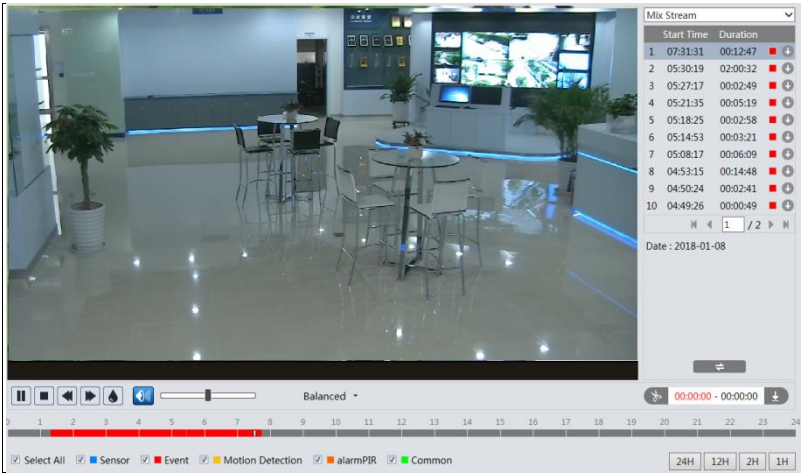
Click Search to go to the interface as shown below. Videos that were recorded on the SD card can be played in this interface.

Note: If the camera doesn't support SD card, please skip the instructions of SD card video search.

1. Choose "Record"—"SD Card".
2. Set search time: Select the date and choose the start and end time.
3. Click to search the images.



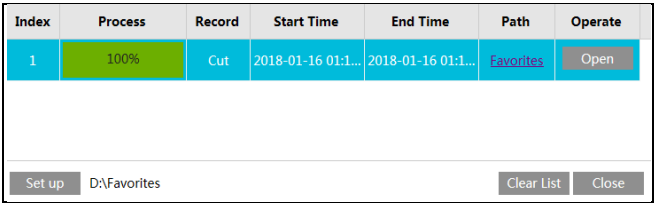
4. Select the alarm events at the bottom of the interface.
5. Select mix stream (video and audio stream) or video stream as needed.
6. Double click on a file name in the list to start playback.



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

Video clip and downloading

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



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

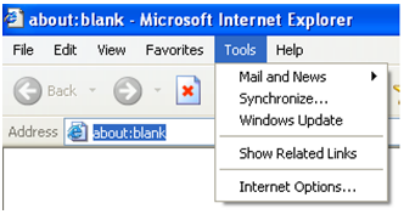
Appendix 1 Q & A

How to find the password?
A： Reset the device to the default factory settings.
Default IP: 192.168.226.201; User name: admin; Password: 123456

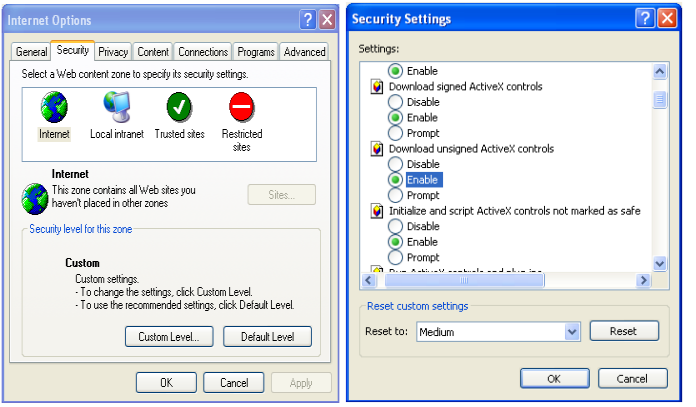
Fail to connect devices through IE browser.
A: Network is not well connected. Check the connection and make sure it is connected well.
B: IP address is not available. Reset the IP address.
C: Web port number has been changed: contact administrator to get the correct port number.
D: Exclude the above reasons. Restore to default setting by IP-Tool.

IP 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.

Appendix 2 Specifications

Specification /Model		**Cube Wi-Fi Network Camera**
Camera	Image Sensor	1/2.7 " CMOS
	Image Size	1920×1080
	Electronic Shutter	1/25s~1/100000s
	Iris Type	Fixed Iris
	Min. llumination	0.03lux@F2.5, AGC ON: 0 lux with IR; 0.007 lux@F1.2, AGC ON: 0 lux with IR
	Lens	2.8mm@F1.85, horizontal field of view: 116.6 °
	Lens Mount	M12
	Day&Night	ICR
	WDR	Digital WDR
	Digital NR	3D DNR
	Angle Adjustment	Pan: 0 °~230 °; Tilt: 0 °~71 °; Rotation: 0 °~360 °
Image	Video Compression	H.265/ H.264 / MJPEG
	H.264 Type	Baseline profile/main profile/high profile
	Video Bit Rate	128Kbps~6Mbps
	Resolution	1080P, 720P, D1, CIF, 480×240
	Main Stream	60Hz: 1920×1080/1280×720(1~30fps); 50Hz: 1920×1080/ 1280×720(1~25fps)
	Sub Stream	60Hz: D1/CIF(1~30fps); 50Hz: D1/CIF (1~25fps)
	Third Stream	60Hz: D1/CIF/ 480×240 (1~30fps); 50Hz: D1/CIF/ 480×240 (1~25fps)
	Image Settings	BLC, HLC, Defog, Saturation, Brightness, Chroma, Contrast, Wide Dynamic, Sharpen, NR, etc. adjustable through client or web browser
	ROI	Support
	Audio Compression	G.711A/U
Interfaces	Network	RJ45
	Auido	Built-in MIC ×1; Built-in Speaker ×1
	Alarm	1CH alarm input; 1CH alarm output
	Storage	Built-in micro SD card slot; up to 128GB
	Hardware Reset	Yes
Wi-Fi	Wireless Standards	IEEE802.11b/g/n
	Frequency Range	2.4GHz~2.4835GHz
	Channel Bandwidth	20MHz
	Security	WEP, WPA-PSK/WPA2-PSK
	Transfer Rates	11b:11Mbps 11g:54Mbps 11n: up to 150Mbps
	Wireless Range	50m
Fucntion	Remote Monitoring	Web browser, CMS remote control
	Online Connection	Support simultaneous monitoring for up to 4 users and multi-stream transmission
	Network Protocol	IPv4, IPv6, UDP, DHCP, NTP, RTSP, PPPoE, DDNS, SMTP, FTP, SNMP, HTTPS, 802.1x, QoS
	Interface Protocol	ONVIF, GB-T/28181-2011
	Storage	Network remote storage; micro SD card storage
	Smart Alarm	Motion detection, sensor alarm, PIR alarm, SD card full, SD card error, IP conflict, Cable disconnection
	General function	Watermark, IP address filtering, video mask, heartbeat, password protection
	PIR	Horizontal angle: 100 ° Range: 7m

Others	IR Distance	Up to 10m
	Power	DC12V/PoE
	Power Consumption	< 4.5W
	Opterating Environment	Temperature: -10℃~45℃; Relative Humidity: less than 95% (non-condensing)
	Dimension (mm)	130×71.7×71.7
	Weight（net）	Approx.0.14KG
	Installation	Wall mounting; ceiling mounting; desktop