Secure the word with you

4 Megapixel
Network Camera
User Manual

Notes on 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(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.
- 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 manual is for using and managing the product. 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.
- All pictures, charts, images in this manual are only for description and explanation of our products. The ownerships of trademarks, logos and other intellectual properties related to Microsoft, Apple and Google belong to the above-mentioned companies.
- This manual is suitable for IR water-proof network cameras.

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 Configuration 2
2.1 LAN 2
2.1.1 Access through IP-Tool 2
2.1.2 Directly Access through IE 4
2.2 WAN 5
3 Live View 8
4 Network Camera Configuration 9
4.1 System Configuration 9
4.1.1 Basic Information 9
4.1.2 Date and Time 9
4.1.3 Local Config 10
4.2 Image Configuration 10
4.2.1 Display Configuration 10
4.2.2 Video Configuration 12
4.2.3 OSD Configuration 14
4.2.4 Video Mask 14
4.2.5 ROI Configuration 15
4.3 Alarm Configuration 16
4.3.1 Motion Detection 16
4.3.2 Alarm Server 18
4.4 Event Configuration 18
4.4.1 Object Removal 18
4.4.2 Exception 20
4.4.3 Line Crossing 21
4.4.4 Intrusion 22
4.5 Network Configuration 24
4.5.1 TCP/IP 24
4.5.2 Port 25
4.5.3 Server Configuration 25
4.5.4 DDNS 26
4.5.5 802.1x 27
4.5.6 RTSP 28
4.5.7 UPNP 29
4.5.8 Email 29
4.5.9 FTP 30
4.5.10 HTTPS 31
4.5.11 P2P (Optional) 32
4.5.12 QoS 33
4.6 Security Configuration 33

4.6.1 User Configuration 33
4.6.2 Online User 34
4.6.3 Block and Allow Lists 35
4.6.4 Security Management 35
4.7 Maintenance Configuration 35
4.7.1 Backup and Restore 35
4.7.2 Reboot 36
4.7.3 Upgrade 36
4.7.4 Operation Log 37
5 Search 38
5.1 Image Search 38
5.2 Video Search 39
Appendix 41
Appendix 1 Q & A 41
Appendix 2 Specifications 43

1 Introduction

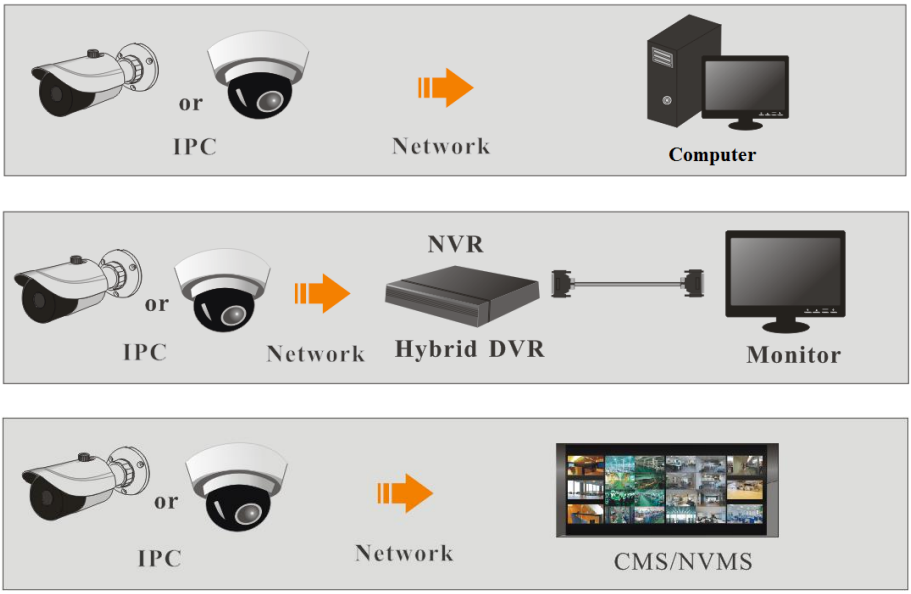
This IP-CAMERA (short for IP-CAM) is designed for high performance CCTV solutions. It adopts state of the art video processing chips, integrated with the most advanced technologies (like video encoding and decoding technology) to make the image transmission more stable and smooth. Moreover, the built-in WEB server of this series improves the performance of the traditional surveillance system so that users can be easy to operate and monitor.

This product is 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
- Intelligent analytics: object abandoned/missing, scene change detection, video blur detection, line crossing detection, region intrusion detection
- Support BLC, Defog, Anti-flicker
- Support smart phone, iPad, remote monitoring

Surveillance Application



2 Network Configuration

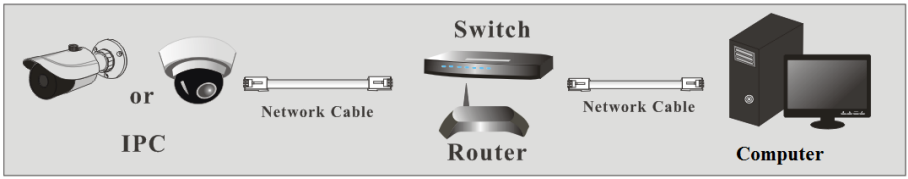
Connect IP-Cam via LAN or WAN. Here only take IE browser for example. The details are as follows:

2.1 LAN

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

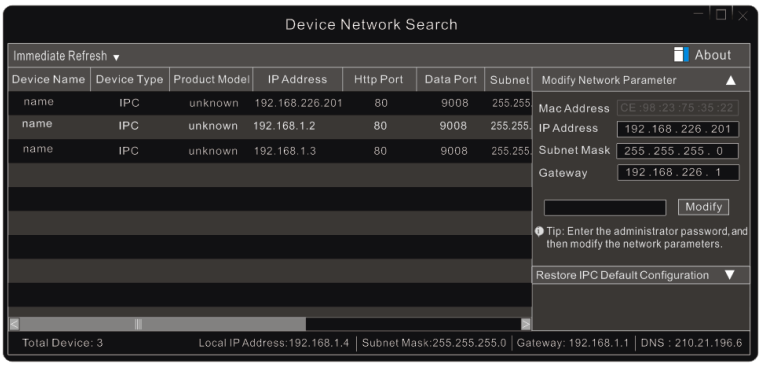
2.1.1 Access through IP-Tool

Network connection:

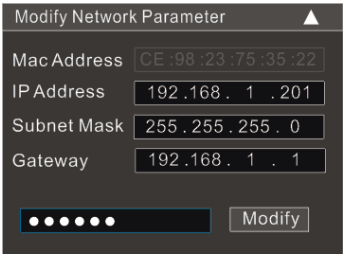


① Make sure the PC and IP-Cam are connected to the local network and the IP-Tool is installed in the PC from the CD.

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



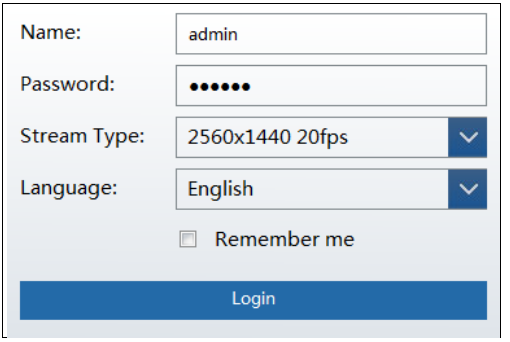
③ Modify the IP address. The default IP address of this camera is 192.168.226.201. Click the information of the camera listed in the above table to show the network information on the right hand. Modify the IP address and gateway of the camera and make sure its network address is in the same local network 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 the "Modify" button to modify the setting.

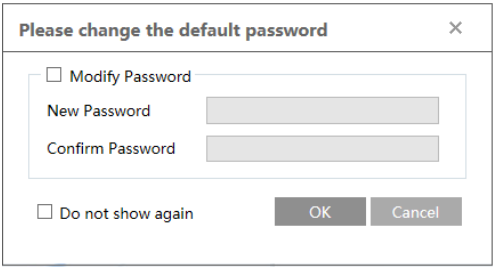
☞ The default password of the administrator is "***123456***".

④ Double click the IP address and then the system will pop up the IE browser to connect IP-CAM. Follow directions to download, install and run the Active X control.



Enter the username and password in the login window to log in.

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

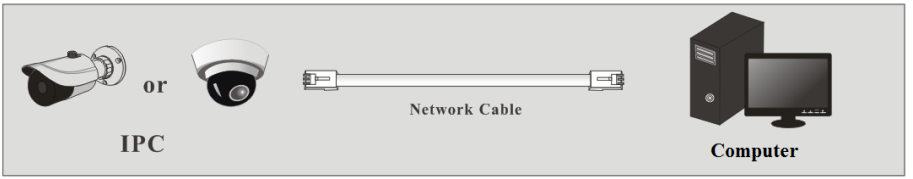


The system will pop up the above-mentioned textbox to ask you to change the default password. It is strongly recommended to change the default password for account security. If "Do not show again" is checked, the textbox will not appear next time.

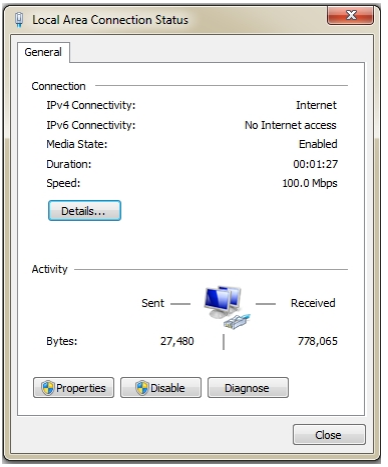
2.1.2 Directly Access through IE

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**

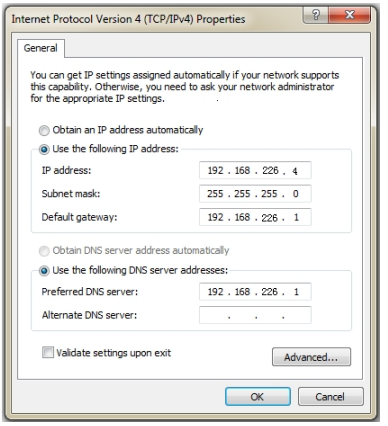
Use the above default settings when logging in the camera for the first time. Directly connect the camera to the computer through network cable.



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 the "Properties" button to set the network of the PC.



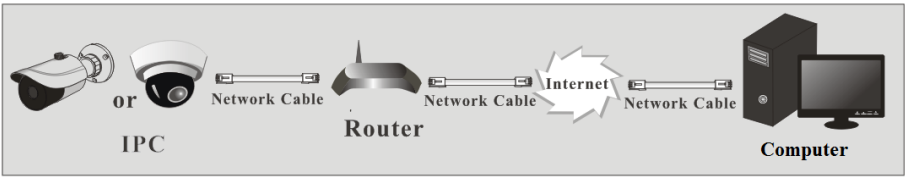
② Open the IE browser and enter the default address of IP-CAM and confirm.

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

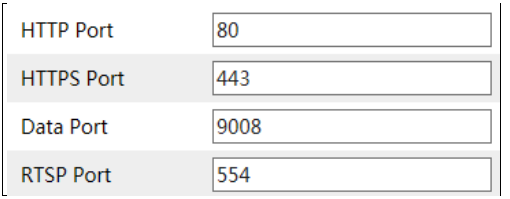
④ Enter the default username and password in the login window and then enter to view.

2.2 WAN

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

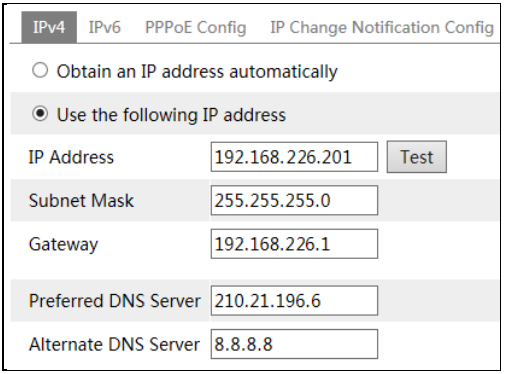


① Make sure the camera is well connected via LAN and then log in the camera via LAN and go to Config→Network→Port menu to set the port number.



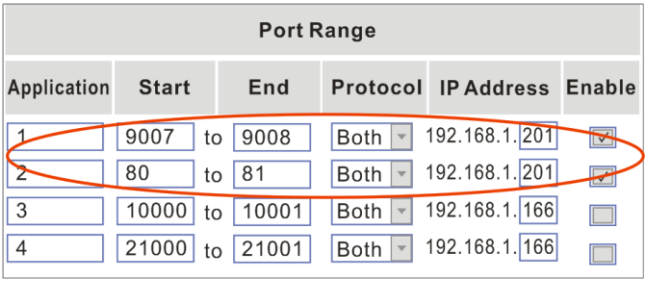
Port Setup

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".

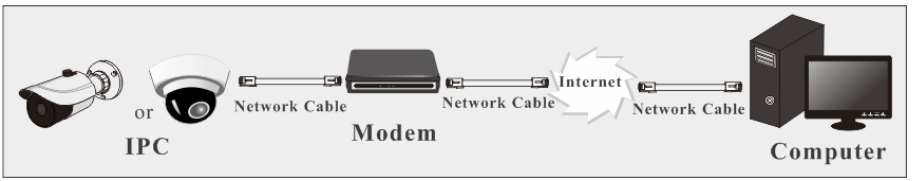


Router Setup

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**

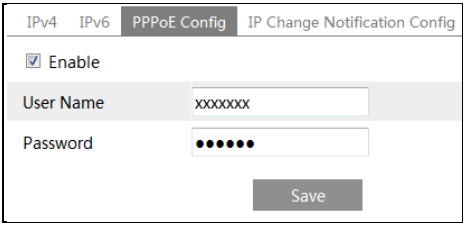
Network connection



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 from your internet service provider.

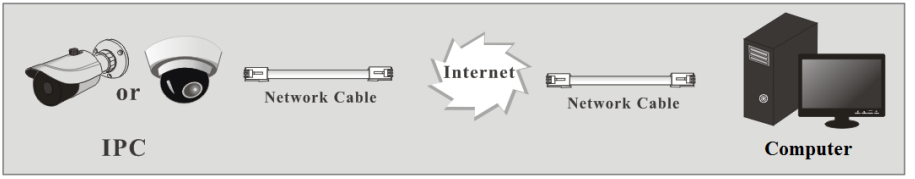


③ Go to Config →Network→DDNS menu. Before configuring the DDNS, please apply for a domain name first. Please refer to DDNS configuration for detail information.

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

➢ **Access through static IP**

Network connection



The setting steps are as follow:

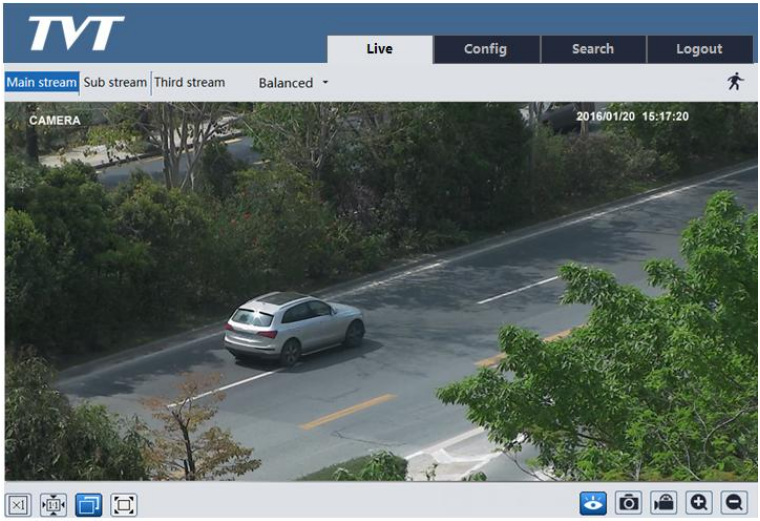
① Go to Config→Network→Port menu to set the port number.

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 logging in, the following window will be shown.



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

Icon	Description	Icon	Description
	Original size		Zoom in
	Fit correct scale		Zoom out
	Auto (fill the window)		Abnormal clarity indicator
	Full screen		Scene change indicator
	Start/stop live view		Line crossing indicator
	Enable/disable audio (only available for some models)		Object removal indicator
	Snapshot		Intrusion indicator
	Start/stop local recording		Motion alarm indicator

- Those smart alarm indicators will flash only when the camera supports those functions and the corresponding events are enabled.
- In full screen mode, double click on the mouse to exit or press the ESC key on the keyboard.

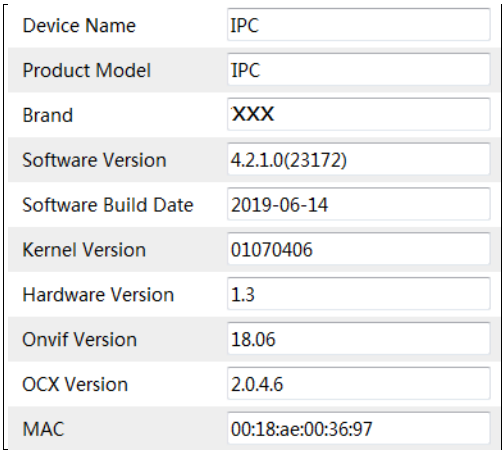
4 Network Camera Configuration

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

4.1 System Configuration

4.1.1 Basic Information

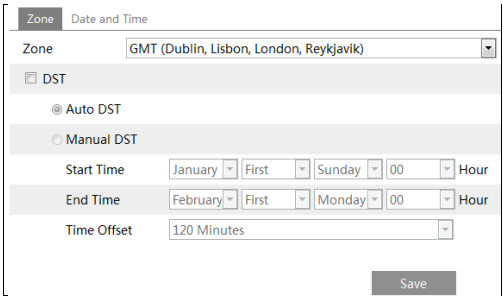
In the “Basic Information” interface, the system information of the device is listed.



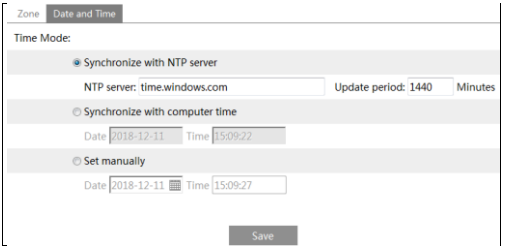
Some versions may support device ID and QR code. Having been enabled P2P (see Network Configuration-P2P), the network camera can be quickly added to mobile surveillance client, by scanning the QR code or entering device ID.

4.1.2 Date and Time

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

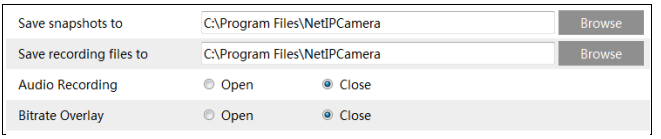


Select the time zone and DST as desired.
Click the “Date and Time” tab to set the time mode.



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.



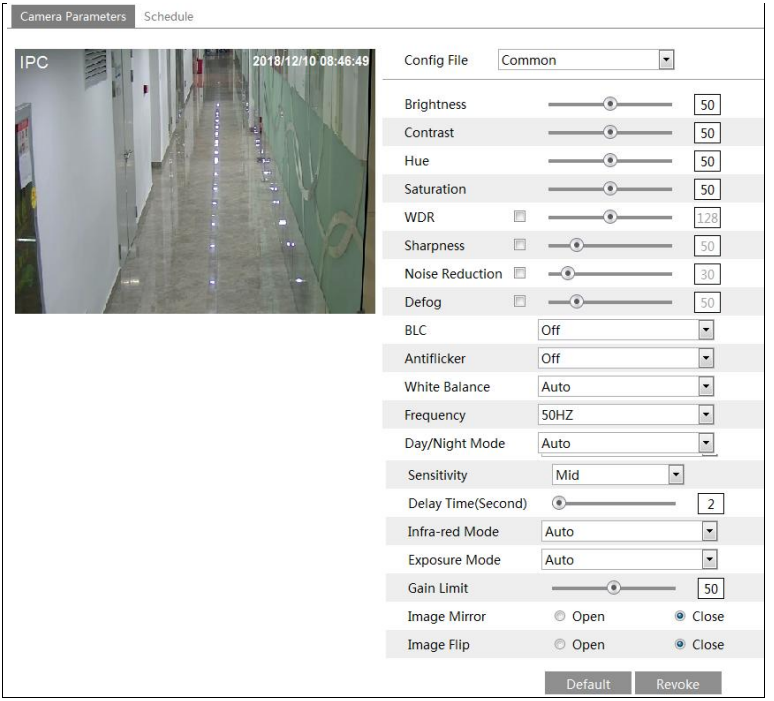
For the model with built-in MIC, there is also an option to enable or disable audio recording.

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.
WDR: WDR can adjust the camera to provide a better image when there are both very bright and very dark areas simultaneously in the field of the view by lowering the brightness of the bright area and increasing the brightness of the dark area. Recording will be stopped for a few seconds while the mode is changing from non-WDR to WDR mode.
Sharpness: Set the resolution level of the image plane and the sharpness level of the image edge.
Noise Reduction: Decrease the noise and make the image more thorough. Increasing the value will make the noise reduction effect better but it will reduce the image resolution.
Defog: Activating this function and setting an appropriate value as needed in foggy, dusty, smoggy or rainy environment to get clear images.
Backlight Compensation:

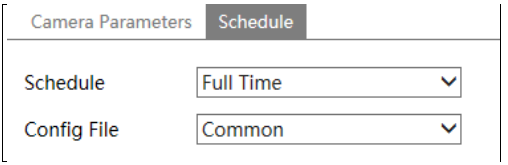
- Off: disables the backlight compensation function. It is the default mode.
- HLC: lowers the brightness of the entire image by suppressing the brightness of the image's bright area and reducing the size of the halo area.
- BLC: If enabled, the auto exposure will activate according to the scene so that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

Antiflicker:

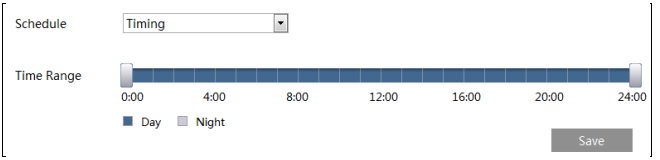
- Off: disables the anti-flicker function. This is used mostly in outdoor installations.
- 50Hz: reduces flicker in 50Hz lighting conditions.
- 60Hz: reduces flicker in 60Hz lighting conditions.

White Balance: Adjust the color temperature according to the environment automatically.
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" and "Auto".
Exposure Mode: Choose "Auto" or "Manual". If manual is chosen, the digital shutter speed can be adjusted.
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.



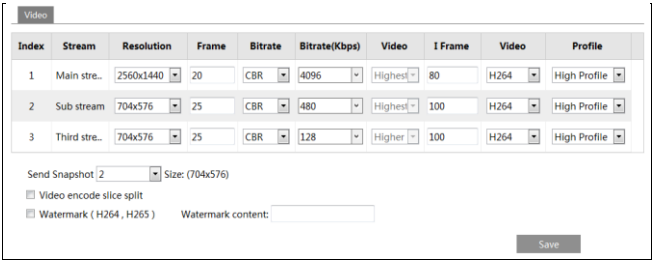
Set full time schedule for common, day, night mode and specified time schedule for day and night. Choose "Timing" in the drop-down box of schedule as shown below.



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

4.2.2 Video Configuration

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



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: 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 and H265 are optional. If H.265 is chosen, make sure the client system is able to decode H.265.

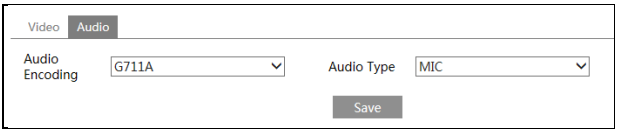
Profile: For H.264. Baseline, main and high profiles are selectable.

Send Snapshot: How many snapshots to generate for an event.

Video encode slice split: If this function is enabled, more fluent 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.

For the model with built-in MIC, audio encoding and type can be set. Click the "Audio" tab to go to the interface as shown below.



Audio Encoding: G711A and G711U are selectable.
Audio Type: MIC.

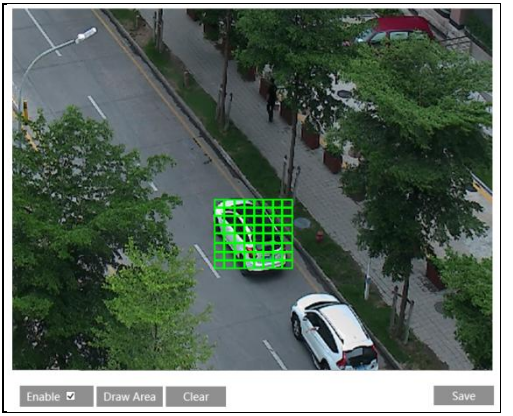
4.2.3 OSD Configuration

Go to Image→OSD interface as shown below.

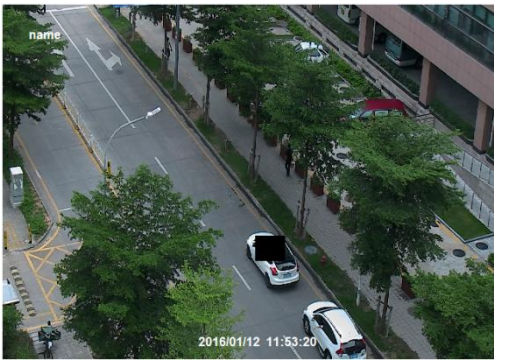
Set time stamp, device name and OSD content here. After enabling the corresponding display and entering the content, drag them to change their position. Then click the "Save" button to save the settings.

4.2.4 Video Mask

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



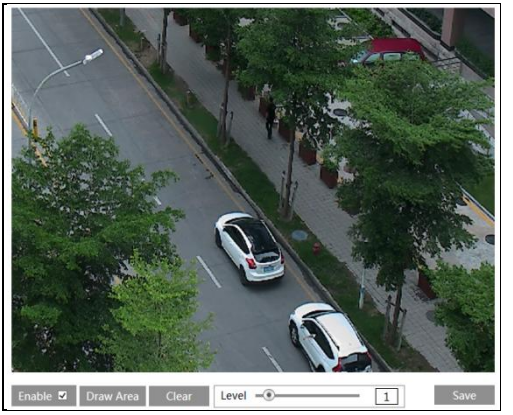
To set up video mask:
1. Enable video mask.
2. Click the "Draw Area" button and then drag the mouse to draw the video mask area.
3. Click the "Save" button to save the settings.
4. Return to the live to verify that the area have been drawn as shown as blocked out in the image.



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 then have a higher bitrate than the rest of the image, resulting in better image quality for the identified area.

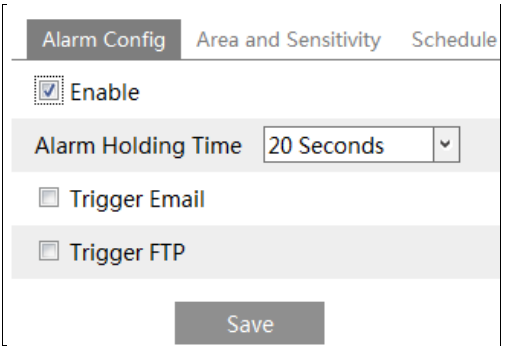


1. Check “Enable” and then click the “Draw Area” button.
2. Drag the mouse to set the ROI area.
3. Set the level.
4. Click the “Save” button to save the settings.

4.3 Alarm Configuration

4.3.1 Motion Detection

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

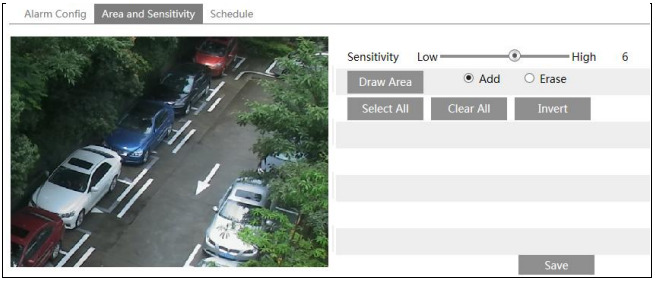


1. Check “Enable” check box to activate motion based alarms. If unchecked, the camera will not send out any signals to trigger motion-based recording to the NVR or CMS, even if there is motion in the video.

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

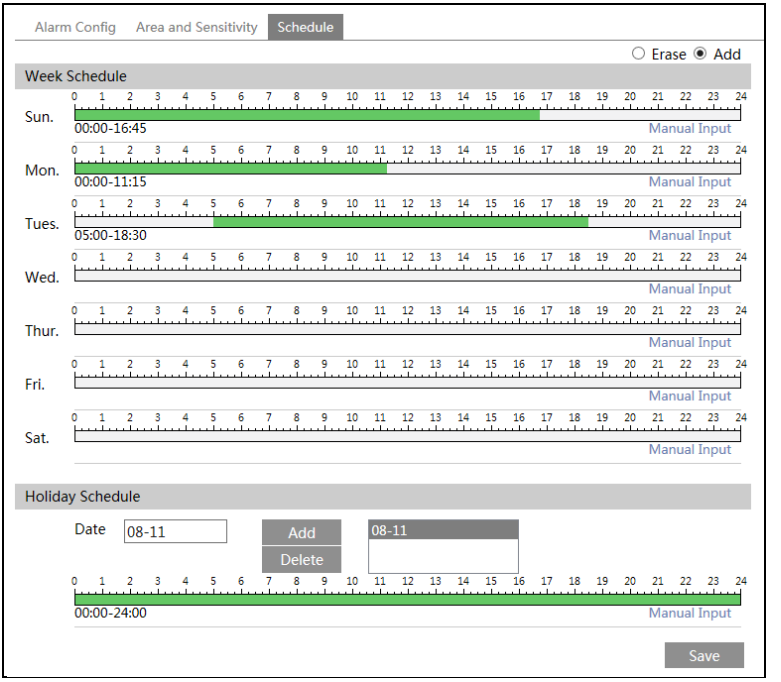
Trigger FTP: If “Trigger FTP” and “Attach Picture” checkbox are checked, the captured pictures will be sent into FTP server address. Please refer to FTP configuration chapter for more details.

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 "Save" to save the settings.

3. Set the schedule of the motion detection. Click the "Schedule" tab to go to the interface as shown below.



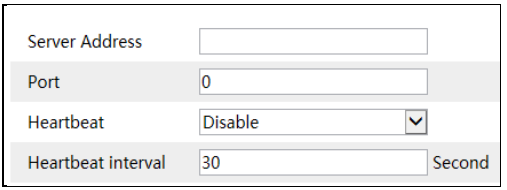
Weekly schedule
Set the alarm time from Monday to Sunday for a single week. Each day is divided in one hour increments. Green means scheduled. Blank means unscheduled. Note that if a specific time

period is not scheduled for motion, the camera will not generate a motion alarm even if motion is enabled.
"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.

4.3.2 Alarm Server

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



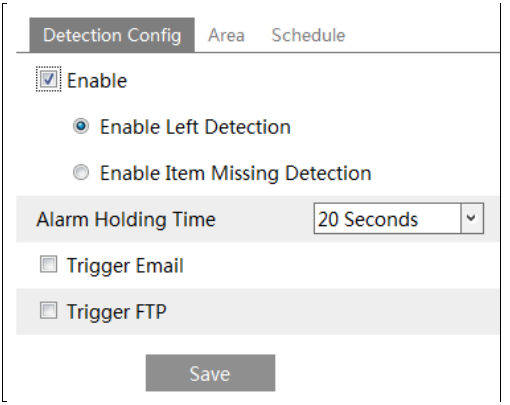
4.4 Event Configuration

For more accuracy, here are some recommendations for installation.

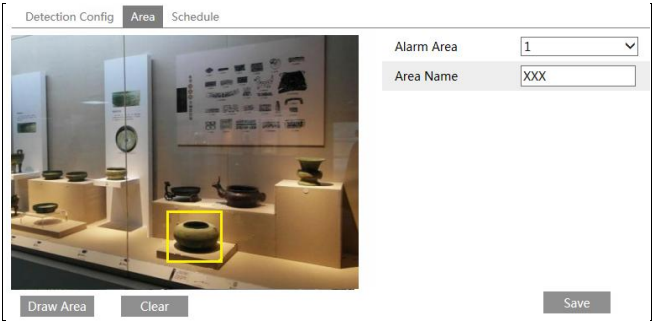
- Cameras should be installed on stable surfaces, as vibrations can affect the accuracy of detection.
- Avoid pointing the camera at the reflective surfaces (like shiny floors, mirrors, glass, lake surfaces and so on).
- Avoid places that are narrow or have too much shadowing.
- Avoid scenario where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

4.4.1 Object Removal

Alarms will be triggered when the objects are removed from or left at the pre-defined area.
To set object removal:
Go to Config→Event→Object Removal interface as shown below.



1. Enable object removal detection and then select the detection type.
Enable Left Detection: Alarms will be triggered if there are items left in the pre-defined area.
Enable Item Missing Detection: Alarms will be triggered if there are items missing in the pre-defined area.
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 "Save" button to save the settings.
4. Set the alarm area of the object removal detection. Click the "Area" tab to go to the interface as shown below.



Set the alarm area number and then enter the desired alarm area name. Only one alarm area can be added. Click the "Draw Area" button and then click around the area where you want to set as the alarm area in the image (the alarm area should be a closed area). Click the "Stop Draw" button to stop drawing. Click the "Clear" button to delete the alarm area. Click the "Save" button to save the settings.
5. Set the schedule of the object removal detection. The setup steps of the schedule are the same as motion detection schedule setup.

※ The configuration requirements of camera and surrounding areas

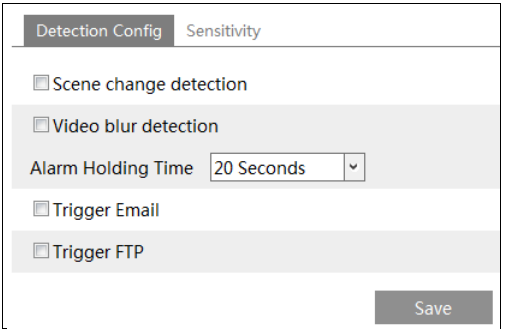
1. The range of the detection object should occupy from 1/50 to 1/3 of the entire image.
2. The detection time of objects in the camera shall be from 3 to 5 seconds.
3. The defined area cannot be covered frequently and continuously (like people and traffic flow).
4. It is necessary for object removal detection that the drawn frame must be very close to the margin of the object in enhancing the sensitivity and accuracy of the detection.
5. Object removal detection cannot determine the objects' ownership. For instance, there is an unattended package in the station. Object removal detection can detect the package itself but it cannot determine to whom it belongs to.
6. Try not to enable object removal detection when light changes greatly in the scene.
7. Try not to enable object removal detection if there are complex and dynamic environments in the scene.
8. Adequate light and clear scenery are very important to object removal detection.

4.4.2 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.

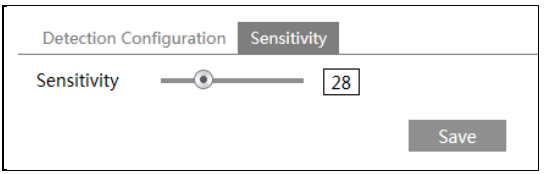


1. Enable the applicable detection that's desired.

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.

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 "Save" button to save the settings.
4. Set the sensitivity of the exception detection. Click "Sensitivity" tab to go to the interface as shown below.



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

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

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

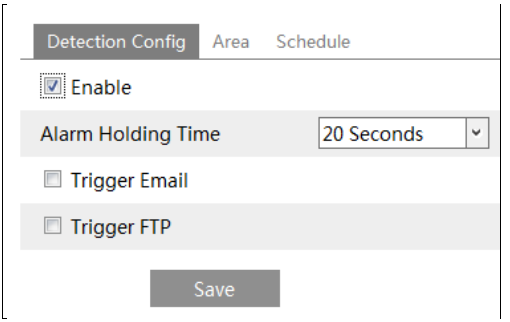
※ The requirements of camera and surrounding area

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.

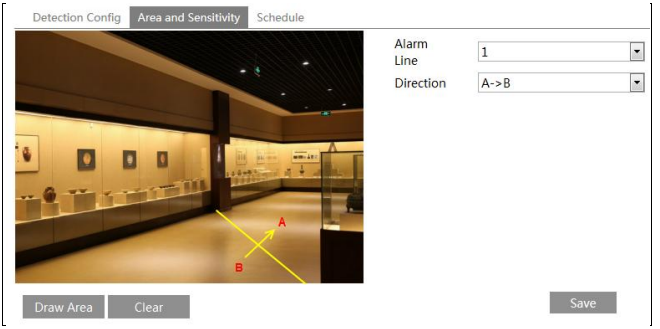
4.4.3 Line Crossing

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

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



1. Enable line crossing alarm and set the alarm holding time.
2. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection chapter for details.
3. Click "Save" button to save the settings.
4. Set area and sensitivity of the line crossing alarm. Click the "Area and Sensitivity" tab to go to the interface as shown below.



Set the alarm line number and direction. Only one line can be added. Multiple lines cannot be added simultaneously.

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

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

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

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

Click the "Draw Area" button and then drag the mouse to draw a line in the image. Click the "Stop Draw" button to stop drawing. Click the "Clear" button to delete the lines. Click the "Save" button to save the settings.

5. Set the schedule of the line crossing alarm. The setup steps of the schedule are the same as motion detection schedule setup.

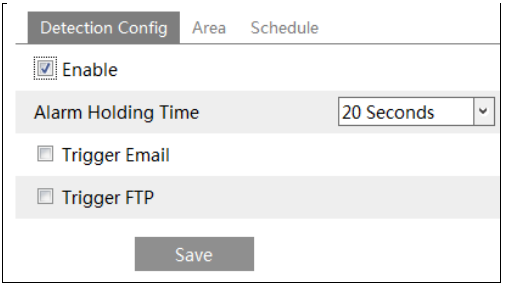
※ Configuration of camera and surrounding area

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.

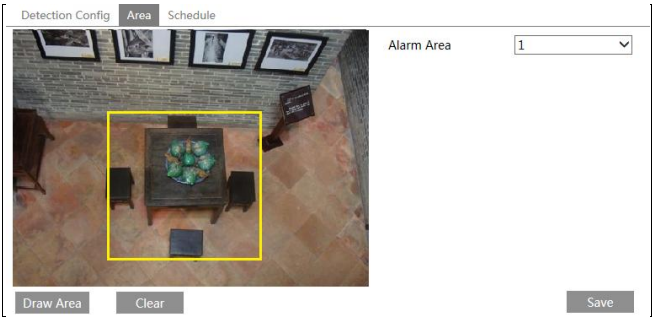
4.4.4 Intrusion

Intrusion: Alarms will be triggered if someone or something intrudes into the pre-defined areas

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. Only one alarm area can be added.
Click the "Draw Area" button and then click around the area where you want to set as the alarm area in the image on the left side (the alarm area should be a closed area). Click the "Stop Draw" button to stop drawing. Click the "Clear" button to delete the alarm area. Click the "Save" button to save the settings.
5. Set the schedule of the intrusion detection. The setup steps of the schedule are the same as motion detection schedule setup.

※ Configuration requirements of camera and surrounding area

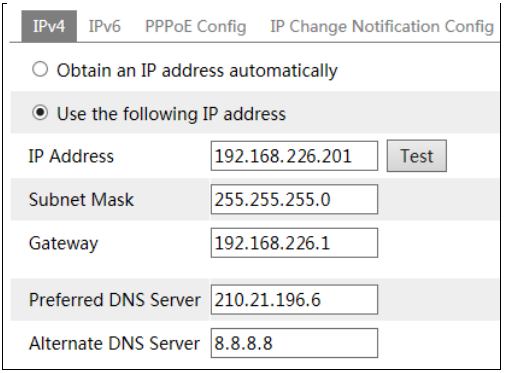
1. Auto-focusing function should not be enabled for intrusion detection.
2. Avoid the scenes with many trees or the scenes with various light changes (like many flashing headlights). The ambient brightness of the scenes shouldn't be too low.
3. Cameras should be mounted at a height of 2.8 meters or above.
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.

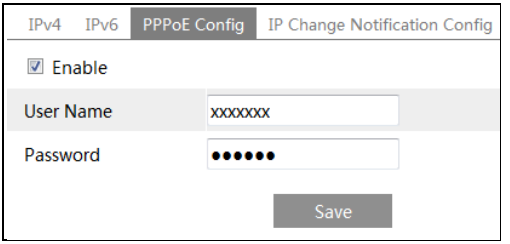
4.5 Network Configuration

4.5.1 TCP/IP

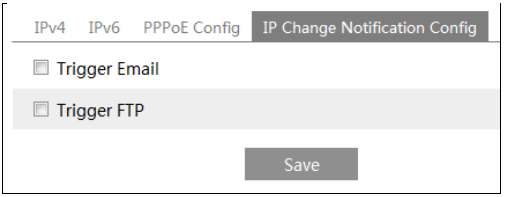
Go to Config→Network→TCP/IP interface as shown below. There are two ways for network connection.



Use IP address (take IPv4 for example)-There are two options for IP setup: obtain an IP address automatically by DHCP protocol 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.



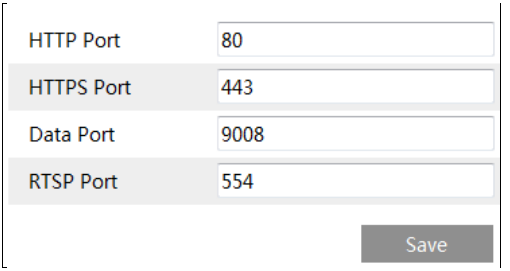
Either method of network connection can be used. If PPPoE is used to connect internet, the camera will get a dynamic WAN IP address. This IP address will change frequently. To be notified, the IP change notification function can be used.
Click "IP Change Notification Config" to go to the interface as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

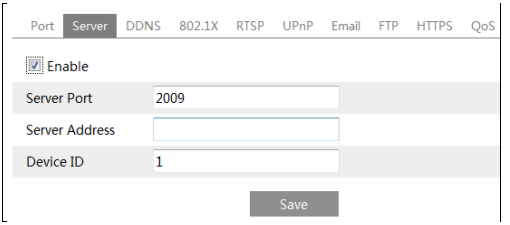
Go to Config→Network→Port interface as shown below. HTTP port, Data port and RTSP port can be set.



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

4.5.3 Server Configuration

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

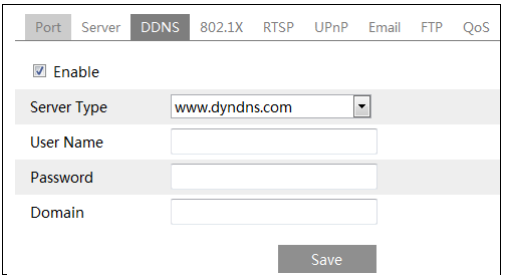


1. Check “Enable”.

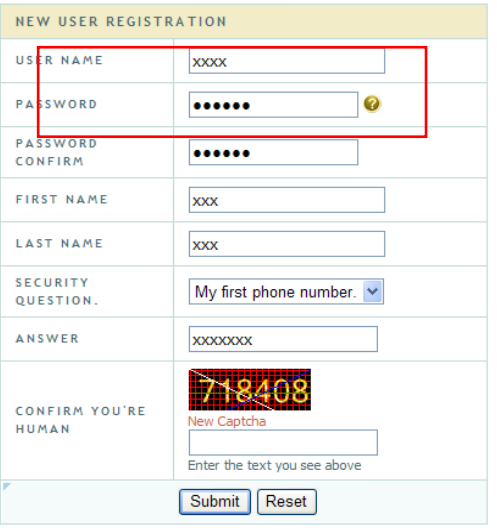
2. Check the IP address and port of the transfer media server in the ECMS/NVMS. Then enable the auto report in the ECMS/NVMS when adding a new device. Next, enter the remaining information of the device in the ECMS/NVMS. After that, the system will automatically allot a device ID. Please check it in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

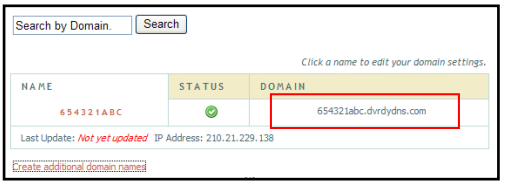


2. Apply for a domain name. Take www.dvrdyndns.com for example.
Enter www.dvrdydns.com in the IE address bar to visit its website. Then click the "Registration" button.



Create domain name.

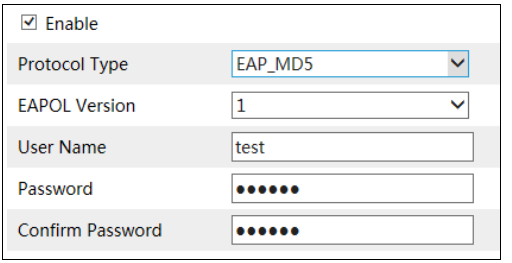
After the domain name is successfully applied for, the domain name will be listed as below.



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

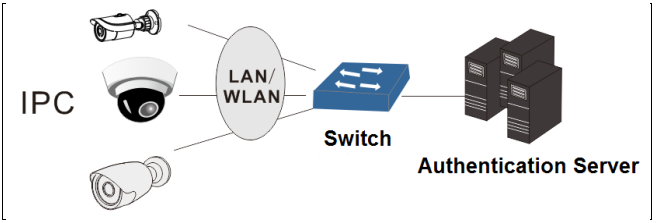
4.5.5 802.1x

IEEE802.X is an access control protocol. The setting 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.

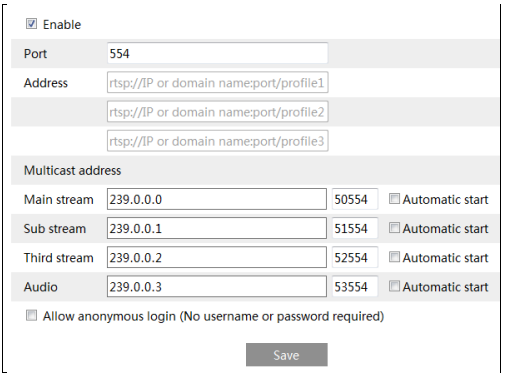
The structure of 802.1x



① The network camera initiates the authentication of 802.1x protocol via web client and then the authentication is received by the switch supporting 802.1x protocol.
② The switch provides the camera with a physical or logic local network interface and verifies the camera.
③ Authentication server provides the entity of authentication service for the switch, stored the relative information of web client, realizing the authentication of web client.
Please refer to the user manual of the connected switch for more details.

4.5.6 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: **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".

If “auto start” is enabled, the multicast received data should be added into a VLC player to play the video.
If “Allow anonymous login…” is checked, there is no need to enter the username and password to view 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.

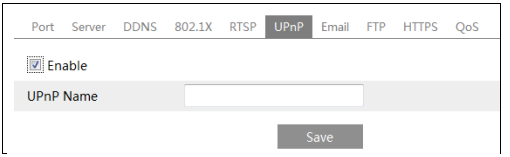
3. Avoid the use of the same multicast address in the same local network.

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.

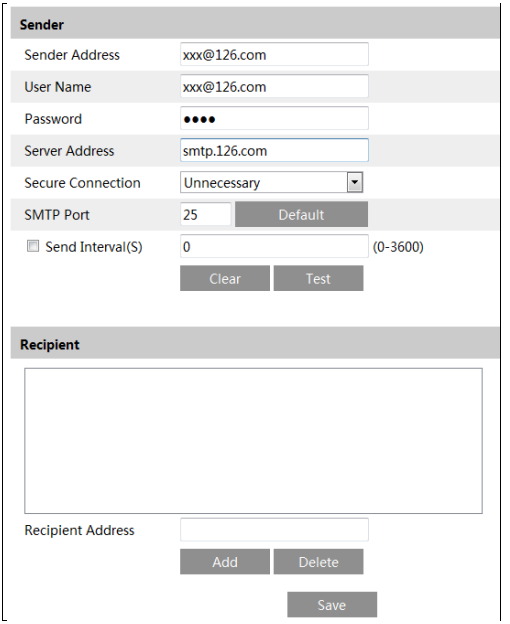
4.5.7 UPNP

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.



4.5.8 Email

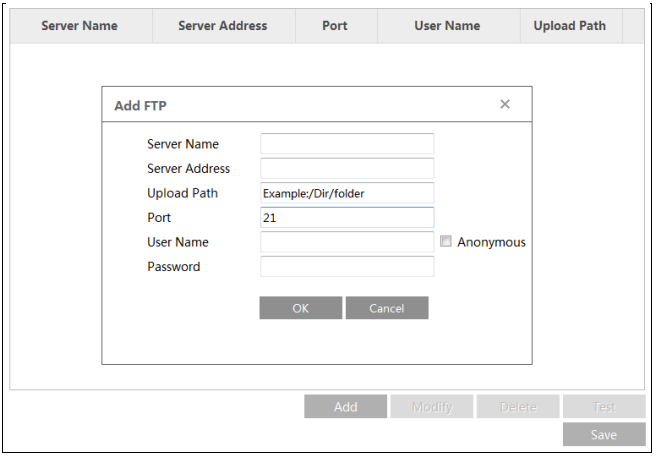
If you need to trigger Email when an alarm happens or IP address is changed, please set the Email here first.
Go to Config→Network →Email.



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.

4.5.9 FTP

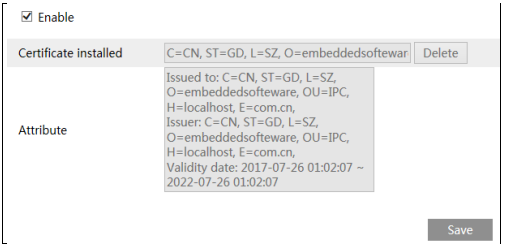
After an FTP server is set up, captured pictures from events will be uploaded to the FTP server.
Go to Config→Network →FTP.



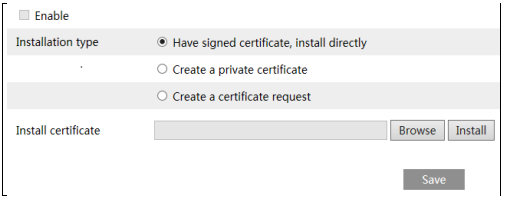
Server Name: The name of the FTP server.
Server Address: The IP address or domain name of the FTP.
Upload Path: The directory where files will be uploaded to.
Port: The port of the FTP server.
Use Name and Password: The username and password that are used to login to the FTP server.

4.5.10 HTTPS

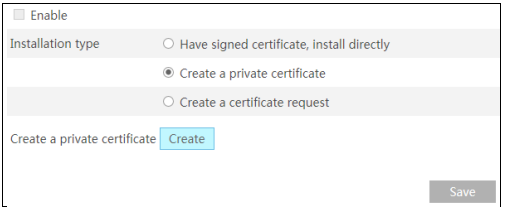
HTTPs provides authentication of the web site and protects user privacy.
Go to Config Config→Network→HTTPS as shown below.



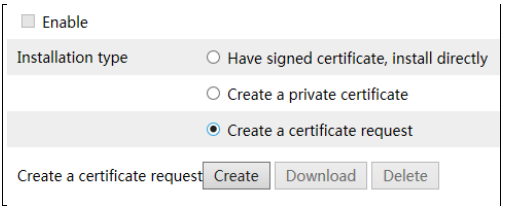
There is a certificate installed by default as shown above. Enable this function and save it. Then the camera can be accessed by entering https://IP: https port via the web browser (eg. https://192.168.226.201:443).
A private certificate can be created if users don't want to use the default one. Click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

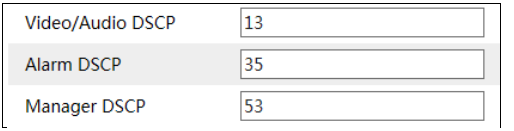
4.5.11 P2P (Optional)

Only some specified version support this function. 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.

4.5.12 QoS

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

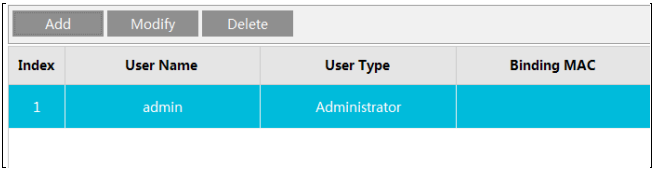


Video/Audio DSCP: The range is from 0 to 63.
Alarm DSCP: The range is from 0 to 63.
Manager DSCP: The range is from 0 to 63.
Generally speaking, the larger the number is, the higher the priority is.

4.6 Security Configuration

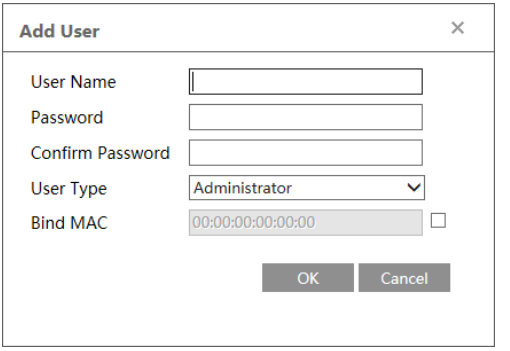
4.6.1 User Configuration

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



Add user:

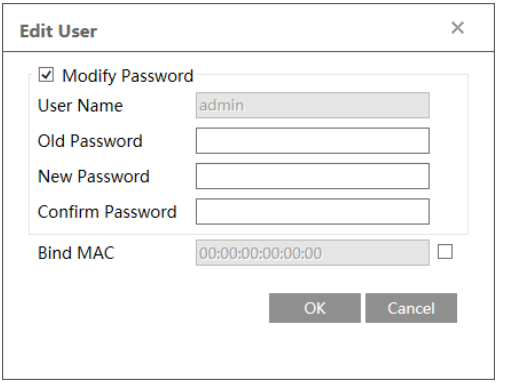
1. Click the "Add" button to pop up the following textbox.



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.

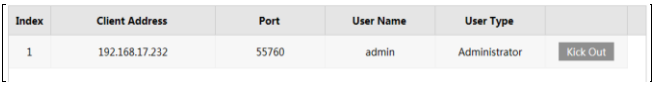
Modify user:
1. Select a user to modify password and MAC address if necessary in the user configuration list box.
2. The “Edit user” dialog box pops up by clicking the “Modify” button.



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

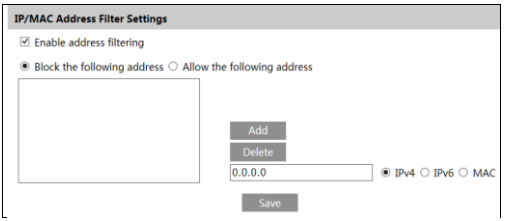
Go to Config→Security→Online User. View the user who is viewing the live video.



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

4.6.3 Block and Allow Lists

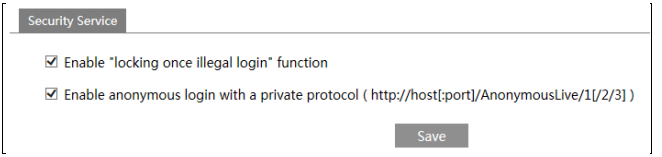
Go to Config→Security→Block and Allow Lists as shown below.



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.

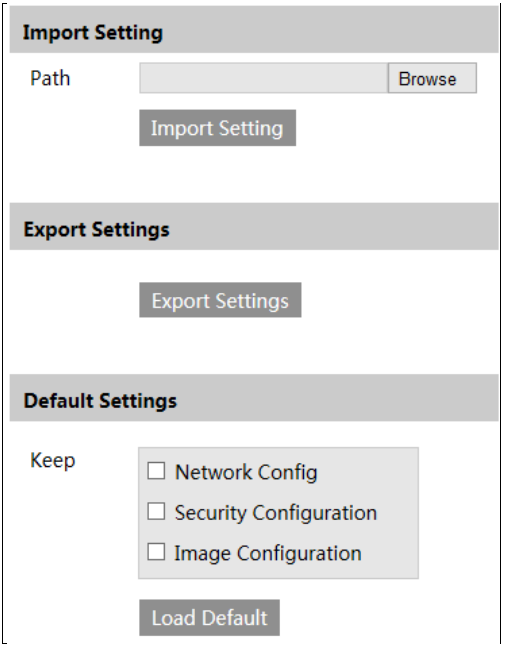


In order to prevent against malicious password unlocking, "locking once illegal login" function can be enabled here. If this function is enabled, login failure after trying six times will make the login interface locked. The camera can be logged in again after a half hour or after the camera reboots.
For some specified versions, anonymous login with a private protocol can be enabled here (if your camera doesn't support this function, please skip the following instructions). 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.

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**

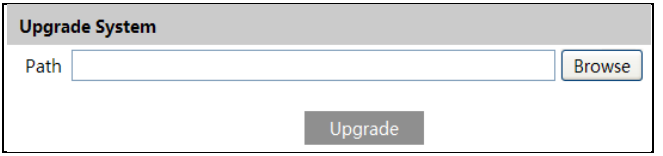
Click the "Load Default" button to restore all system settings to the default factory settings except those you want to keep.

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.



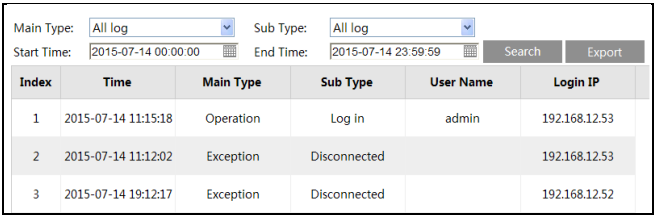
1. Click the “Browse” button to select the save path of the upgrade file
2. Click the “Upgrade” button to start upgrading the firmware.
3. The device will restart automatically

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.

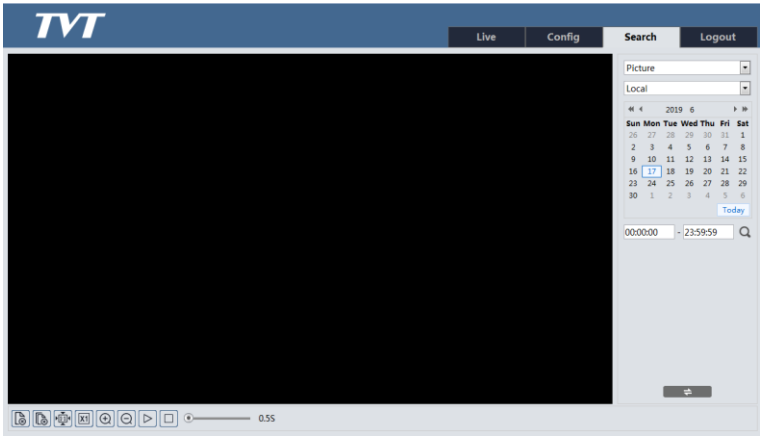


Index	Time	Main Type	Sub Type	User Name	Login IP
1	2015-07-14 11:15:18	Operation	Log in	admin	192.168.12.53
2	2015-07-14 11:12:02	Exception	Disconnected		192.168.12.53
3	2015-07-14 19:12:17	Exception	Disconnected		192.168.12.52

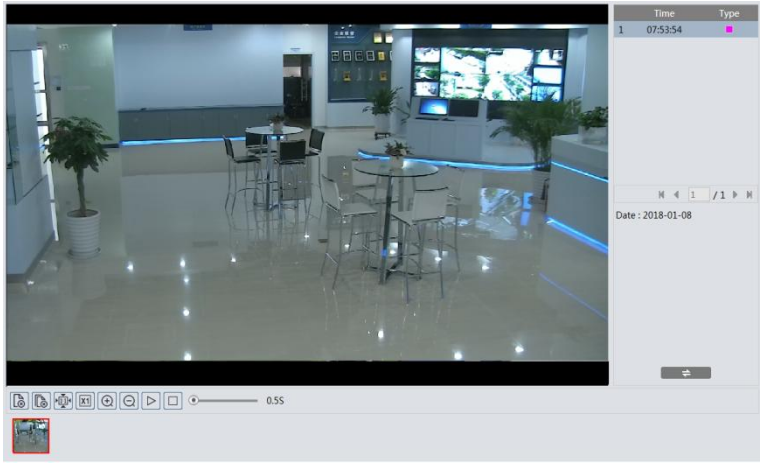
2. Select the main type, sub type, start and end time.
3. Click “Search” to view the operation log.
4. Click “Export” to export the operation log.

5.1 Image Search

Click Search to go to the interface as shown below.



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



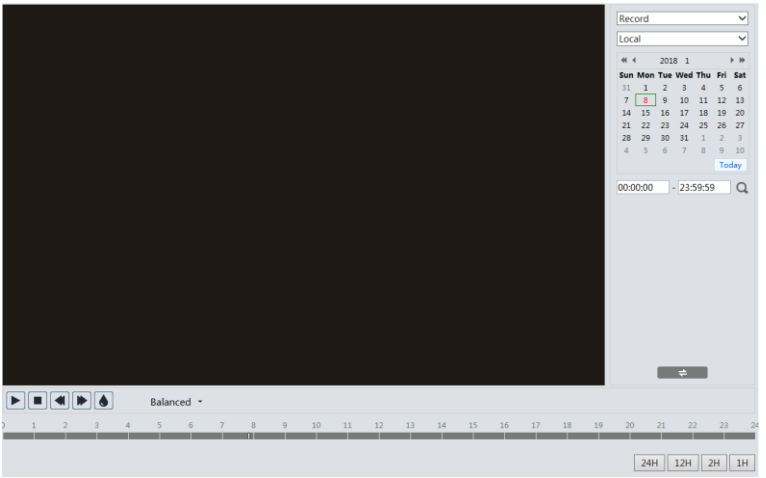
Click to return to the previous interface.

The descriptions of the buttons are shown as follows.

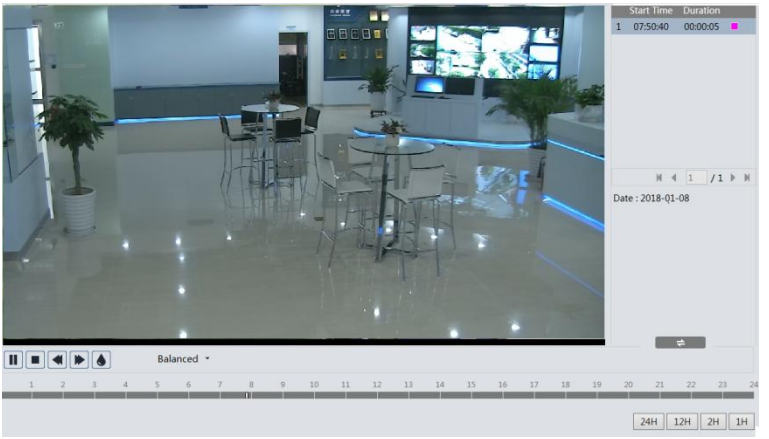
Icon	Description	Icon	Description
	Close: Select an image and click this button to close the image.		Close all: Click this button to close all images.
	Fit size: Click to fit the image on the screen.		Actual size: Click this button to display the actual size of the image.
	Zoom in: Click this button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

5.2 Video Search

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



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. (Only available for the model with built-in MIC)		

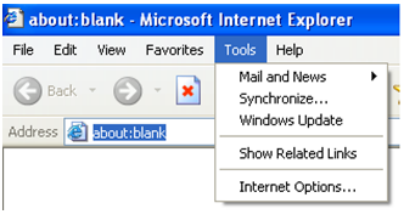
Appendix 1 Q & A

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

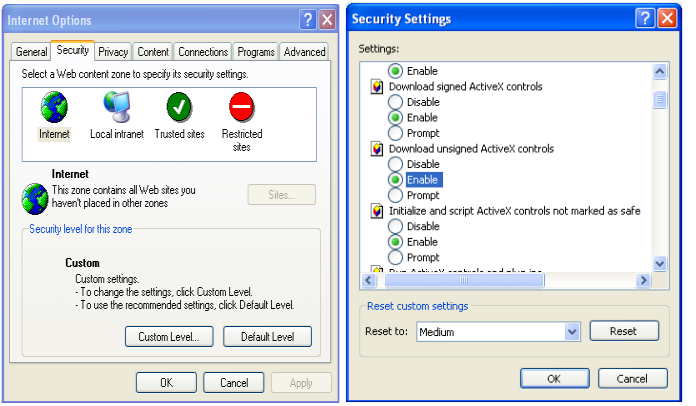
Fail to connect devices through IE browser.
A: Network is not well connected. Check the connection and make sure it is connected well.
B: IP address is not available. Reset the IP address.
C: Web port number has been changed: contact administrator to get the correct port number.
D: Exclude the above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



Q：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		**IR Water-proof Bullet Network Camera**
Camera	Image Sensor	1/2.7 " CMOS
	Image Size	2560×1440
	Electronic Shutter	1/25s~1/100000s
	Iris Type	Fixed Iris
	Min. llumination	0.011 lux@F1.2, AGC ON: 0 lux with IR 0.04 lux@F2.2, AGC ON: 0 lux with IR
	Lens	2.8mm@F2.0, horizontal field of view: 110° 3.6mm@F2.2, horizontal field of view: 89°
	Lens Mount	M12
	Day&Night	ICR
	Digital NR	3D DNR
	WDR	Digital WDR
	Angle Adjustment	Pan: 0 °~360 °; Tilt: 0 °~80 °; Rotation:0 °~360 °
Image	Video Compression	H.265/H.264
	H.265 Type	Main Profile @Leve4.1 High Tier
	Video Bit Rate	64Kbps~5Mbps
	Resolution	4MP(2560×1440), 3MP (2304 ×1296),1080P(1920×1080), 720P(1280×720), D1, CIF, 480×240
	Main Stream	60Hz: 4MP (1~20fps) /3MP(1~30fps)/1080P(1~30fps) 50Hz:4MP (1~20fps)/ 3MP (1~25fps)/ 1080P (1~25fps)
	Sub Stream	60Hz: 720P(1~15fps)/D1(1~30fps)/CIF(1~30fps) 50Hz: 720P(1~12fps)/D1(1~25fps)/CIF(1~25fps)
	Third Stream	60Hz:D1/CIF/480×240(1~30fps); 50Hz: D1/CIF/480×240(1~25fps)
	Image Settings	Saturation, Brightness, Chroma, Contrast, Wide Dynamic, Sharpen, NR, Anti-flicker, etc. adjustable through client or web browser
	ROI	Support
Interface	Network	RJ45
Fucntion	Remote Monitoring	Web browsing, 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, 802.1x,HTTP, HTTPs, QoS
	Interface Protocol	ONVIF
	Storage	Network remote storage
	Smart Alarm	Motion alarm, object abandoned/missing, scene change detection, video blur detection, line crossing detection, region intrusion detection
Others	IR Distance	10~20 m
	Ingress Protection	IP67
	Power	DC12V/PoE
	Power Consumption	< 4W
	Opterating Environment	Temperature: -20℃~55℃; Relative humidity : less than 95% (non-condensing)
	Dimension (mm)	162.1×74.8×73.8
	Weight（net）	Approx. 0.24KG
	Installation	Wall mounting; ceiling mounting

Specification /Model		**IR Water-proof Bullet Network Camera**
Camera	Image Sensor	1/2.7 " CMOS
	Image Size	2560×1440
	Electronic Shutter	1/25s~1/100000s
	Iris Type	Fixed Iris
	Min. llumination	0.011 lux@F1.2, AGC ON: 0 lux with IR 0.04 lux@F2.2, AGC ON: 0 lux with IR
	Lens	3.6mm@F2.2, horizontal field of view: 89° 6mm@F2.0, horizontal field of view: 54.9° 8mm@F2.0, horizontal field of view: 41.5°
	Lens Mount	M12
	Day&Night	ICR
	Digital NR	3D DNR
	WDR	Digital WDR
Image	Video Compression	H.265/H.264
	H.265 Type	Main Profile @Leve4.1 High Tier
	Video Bit Rate	64Kbps~5Mbps
	Resolution	4MP(2560×1440), 3MP (2304 ×1296),1080P(1920×1080), 720P(1280×720), D1, CIF, 480×240
	Main Stream	60Hz: 4MP (1~20fps) /3MP(1~30fps)/1080P(1~30fps) 50Hz:4MP (1~20fps)/ 3MP (1~25fps)/ 1080P (1~25fps)
	Sub Stream	60Hz: 720P(1~15fps)/D1(1~30fps)/CIF(1~30fps) 50Hz: 720P(1~12fps)/D1(1~25fps)/CIF(1~25fps)
	Third Stream	60Hz:D1/CIF/480×240(1~30fps); 50Hz: D1/CIF/480×240(1~25fps)
	Image Settings	Saturation, Brightness, Chroma, Contrast, Wide Dynamic, Sharpen, NR, Anti-flicker, etc. adjustable through client or web browser
	ROI	Support
Interface	Network	RJ45
Fucntion	Remote Monitoring	Web browsing, 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, 802.1x,HTTP, HTTPs, QoS
	Interface Protocol	ONVIF
	Storage	Network remote storage
	Smart Alarm	Motion alarm, object abandoned/missing, scene change detection, video blur detection, line crossing detection, region intrusion detection
Others	IR Distance	20~30 m
	Ingress Protection	IP67
	Power	DC12V(PoE power supply optional)
	Power Consumption	<5.5W
	Opterating Environment	Temperature: -20℃~55℃; Relative humidity : less than 95% (non-condensing)
	Dimension (mm)	144.6×85.8×76.6
	Weight（net）	Approx. 0.26KG
	Installation	Wall mounting

Specification /Model		**IR Water-proof Eyeball Network Camera**
Camera	Image Sensor	1/2.7 " CMOS
	Image Size	2560×1440
	Electronic Shutter	1/25s~1/100000s
	Iris Type	Fixed Iris
	Min. llumination	0.011 lux@F1.2, AGC ON: 0 lux with IR 0.04 lux@F2.2, AGC ON: 0 lux with IR
	Lens	2.8mm@F2.0, horizontal field of view: 110 ° 3.6mm@F2.2, horizontal field of view: 89 ° 6mm@F2.0, horizontal field of view: 54.9 °
	Lens Mount	M12
	Day&Night	ICR
	Digital NR	3D DNR
	WDR	Digital WDR
	Angle Adjustment	Pan: 0 °~360 °; Tilt: 0 °~75 °; Rotation:0 °~360 °
Image	Video Compression	H.265/H.264
	H.265 Type	Main Profile @Leve4.1 High Tier
	Video Bit Rate	64Kbps~5Mbps
	Resolution	4MP(2560×1440), 3MP (2304 ×1296),1080P(1920×1080), 720P(1280×720), D1, CIF, 480×240
	Main Stream	60Hz: 4MP (1~20fps) /3MP(1~30fps)/1080P(1~30fps) 50Hz:4MP (1~20fps)/ 3MP (1~25fps)/ 1080P (1~25fps)
	Sub Stream	60Hz: 720P(1~15fps)/D1(1~30fps)/CIF(1~30fps) 50Hz: 720P(1~12fps)/D1(1~25fps)/CIF(1~25fps)
	Third Stream	60Hz:D1/CIF/480×240(1~30fps); 50Hz: D1/CIF/480×240(1~25fps)
	Image Settings	Saturation, Brightness, Chroma, Contrast, Wide Dynamic, Sharpen, NR, Anti-flicker, etc. adjustable through client or web browser
	ROI	Support
Interface	Network	RJ45
Fucntion	Remote Monitoring	Web browsing, 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, 802.1x,HTTP, HTTPs, QoS
	Interface Protocol	ONVIF
	Storage	Network remote storage
	Smart Alarm	Motion alarm, object abandoned/missing, scene change detection, video blur detection, line crossing detection, region intrusion detection
Others	IR Distance	10~20 m
	Ingress Protection	IP67
	Power	DC12V/PoE
	Power Consumption	< 4W
	Opterating Environment	Temperature: -20 ℃~55 ℃; Relative humidity : less than 95% (non-condensing)
	Dimension (mm)	Ø94.8×82.8
	Weight（net）	Approx. 0.284KG
	Installation	Wall mounting; ceiling mounting

SuperCam Plus

Shenzhen TVT Digital Technology Co., Ltd
Address: 23th Floor, Block B4, Building No.9, Shenzhen Bay Eco-Technology Park, Nanshan District, Shenzhen, Guangdong Province, PR China
Email: overseas@tvt.net.cn
Website: http//en.tvt.net.cn