AVYCON

AVC NS Series

MANUAL

HD Network Cameras

- This product is intended to be supplied by a Listed Power Unit, marked with 'Limited Power Source', 'LPS' on unit, output rated minimum 12V/1 A, no more than 2000m altitude of operation and Tma=60 Deg.C.
- 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 These changes will be unpublished in the latest version without special notification.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 face recognition 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.

Regulatory Information

FCC Information

1. FCC compliance

The products have be tested and found in compliance with the council FCC rules and regulations part 15 subpart B. These limits are designed to provide reasonable protection against harmful interference. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. The user will be required to correct the interface at his own expense in case the harmful interference occurs.

2. FCC conditions:

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 Information

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

RoHS

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

Thank you for using our network camera products. Our network camera products are integrated and developed for network video monitoring, including Storage Network Bullet, Wireless Storage Network Bullet, IR Network Dome, IR Network Weather-Proof Cameras and High-Speed Network Ball. High-performance single SOC chips are used in media processor for audio/video acquisition, compression and transmission/transfer. Standard H.264 encoding algorithm is applied to ensure clear and smooth video representation and transfer performance. Embedded Web Server offers users access to real-time surveillance and remote control of front-end camera through IE browser.

The network cameras are easy to install and operate. The network cameras are applicable to large and medium-size enterprises, governmental projects, large mall, chain supermarkets, intelligent buildings, hotels, Hospitals and schools and other group customers, as well as to applications requiring remote network video transmission and monitoring.

Instructions:

- For purpose of this manual, IP camera means network camera.
- Single click means a single click on the left mouse button.
- Double click means a double-click on the left mouse button.
- The unit comes with DHCP enabled so it will obtain its IP from the router.
- The default factory administrator user name for IP camera is admin (in lowercase), and no password (You are requested to create a password if you log in to the camera IP address via your browser.
- The default Web port number is 80 and the default media port number is 9988.

Statement:

Some information contained in this manual may differ from the actual product. For any problems you cannot solve using this manual, please contact our technical support or the authorized dealers. This manual may be subject change without prior notice

2 Overview

2.1 Range of Application

The network cameras with powerful image processing capacity may be applied at various public places such as mall, supermarket, school, factory and workshop, as well as in environments requiring HD video image such as bank and traffic control system, as shown below:

2.2 Product Description

An IP camera is a digital online surveillance camera embedded with Web server and capable of independent operation, giving user access to real-time monitoring through web browser or client software from any place across the world.

IP camera is based on the latest digital solution, an integrated media processing platform for audio/video acquisition, compression and network transmission on a single board. It is in compliance with H.264/H265 High Profile encoding standards. Any remote user can have access to real-time monitoring by entering the IP address or domain name of the IP camera in web browser. This network camera solution is applicable to residential or business environments well as a wide range of situations requiring remote network video monitoring and transmission. The IP camera products are easy to install and operate.

The IP cameras can be managed by several users with different authorization levels.

IP cameras allows mobile detection, and sends e-mail and snapshot taken in case of emergency and store the image or video snapshot in SD card for retrieval.

2.3 Operation Environment

Operating system: Windows 7/Windows 8/Windows 2008 (32/64-bit), Windows 2003/Windows XP/Windows 2000 (32-bit)
CPU: Intel Core Duo II dual-core processor or higher
Memory: 1G or more Video memory: 256M or more
Display: 1024 × 768 or higher resolution
IE: IE 6.0 or higher version

3 Device Connection

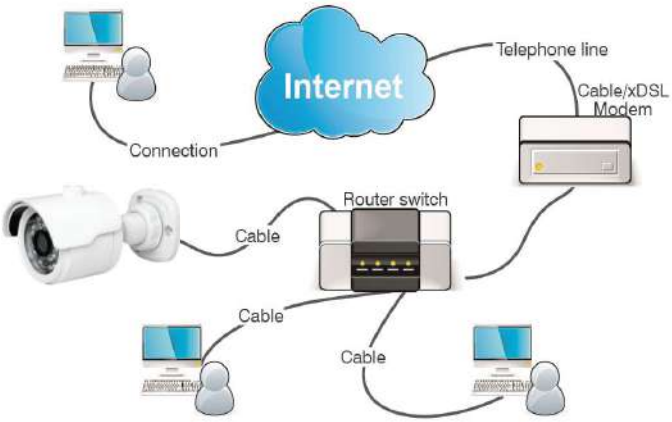
IP camera can be connected in two ways:

1. Connection to PC

Connect IP camera to PC via straight-through network cable, with power input connected to a DC 12V adapter, and set the IP addresses of the PC and IP camera in one network segment. The IP camera will communicate with PC within one minute after being powered on if the network operates normally.

2. Connection to router/switch

Connect IP camera to PC via straight-through network cable, with power input connected to a DC 12V adapter, and set the IP addresses of the PC and IP camera in one network segment. The IP camera will communicate with PC within one minute after being powered on if the network operates normally.

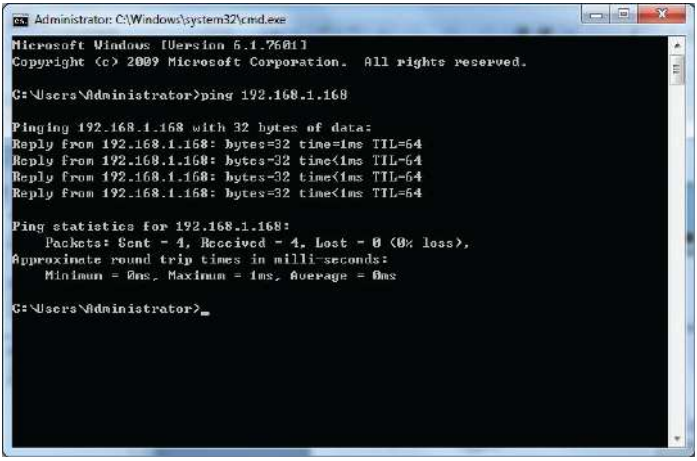


4 Device Operation Instruction

4.1 Check Connection

1. The camera is set for DHCP enabled to obtain its IP address from the DHCP server, and the subnet mask is 255.255.255.0. Allocate your computer an IP address in the same network segment as the IP camera and the same subnet mask as the IP camera.

2. Test whether the IP camera is connected properly and started normally by clicking on Start > Run and entering "cmd" and pressing ENTER, and entering "ping 192.168.1.168" in the command line window to check whether the IP camera is accessible. If the PING command is executed successfully, it indicates that the IP camera operates normally and the network is connected properly. If the PING command fails, check IP address and gateway setting of the PC and connectivity of the network

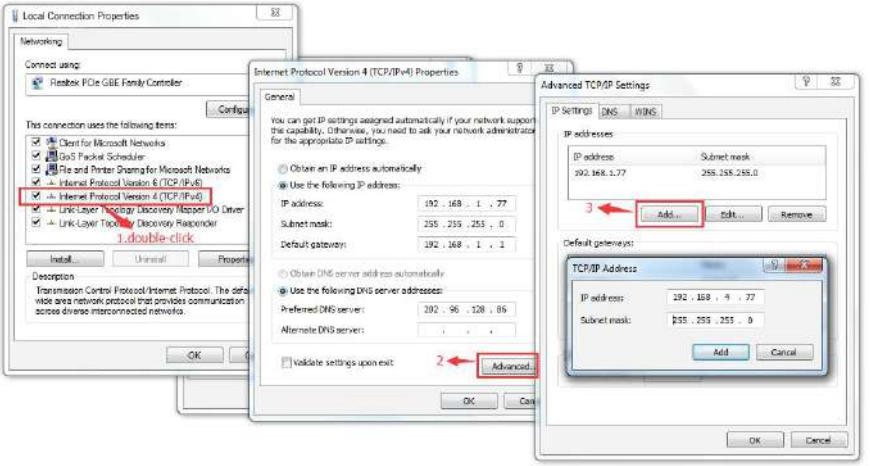


4.2 Searching Device

Tips: IPC Device Search may be used for device searching across network segments. Before running IPC

Device Search, click on the local connection icon  at the lower right corner of the desktop;

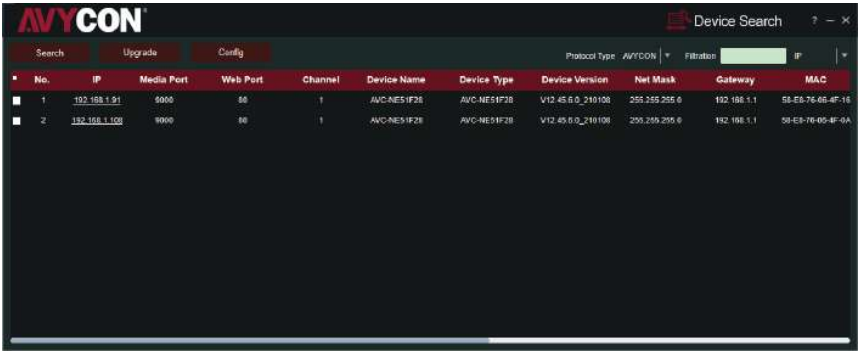
1. Add IP addresses of several network segments in TCP/IP setting for local connection (as shown below). By running the searching tool you can search any device with IP address in the same network segment.



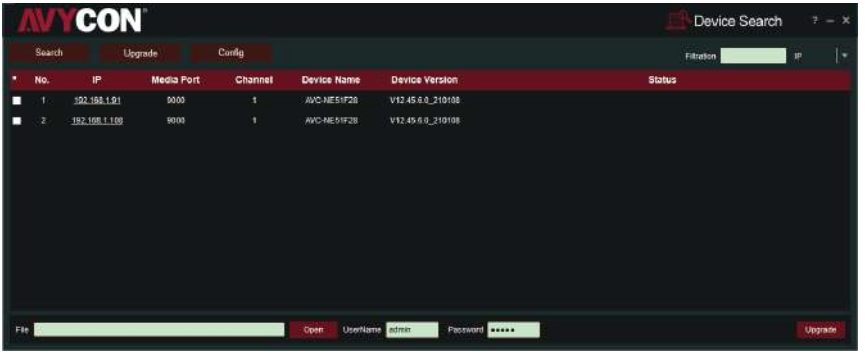
IPC Device Search uses multicast protocol for device searching across segments but any firewall forbids traffic of multicast data packets, so any firewall must be disabled in order that network the information on device can be acquired.

Online device searching procedure

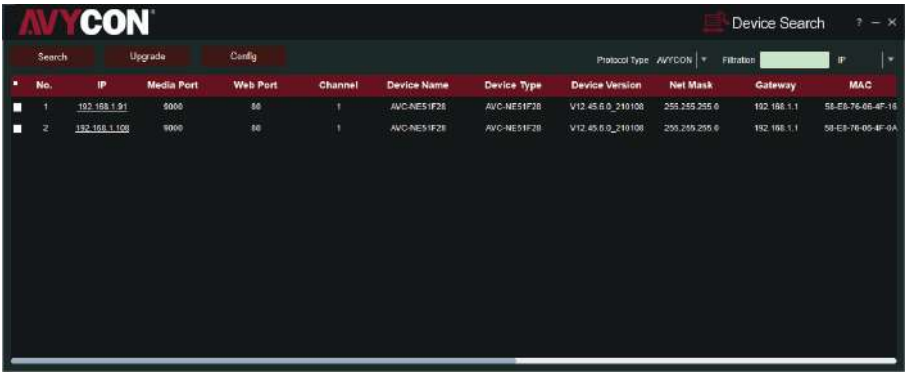
1. Run IPC Device Search by double clicking icon  It will search and display any online IPC and its IP address, port number, number of channels, device type and version, subnet mask, gateway, MAC address and connection pattern.



Upgrade：Allows you to upgrade one or more cameras.
On the Upgrade Tab, please choose the IP camera you want to upgrade in the left frame. Click the Open button, select the firmware files you want ,put in the user name and password, and press the right corner button to upgrade.



Config: Double-click the selected camera in the search page, turn to the Config page to reboot the camera, change passwords, and reset the camera.



4.3 Installation of Controls and Login to System

Before using IE (Internet Explorer) browser to access the IP camera for the first time, related plug-in components must be installed by following the procedure below:

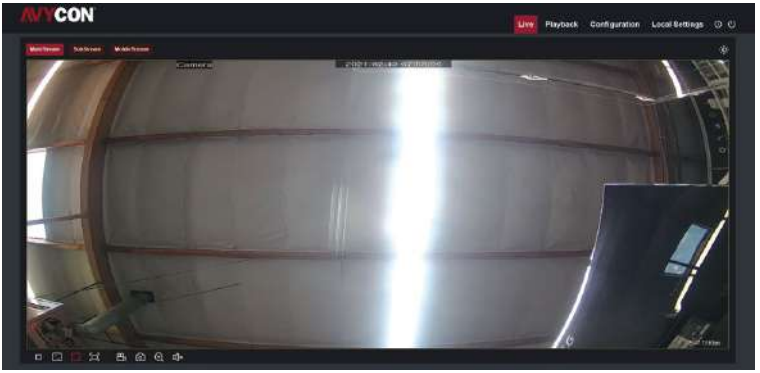
Access IP address of the IP camera to automatically load the controls from it.

In a pop-up plug-in installation dialog box, choose an installation option to perform the installation process.

4.3.1 Preview

Open Internet Explorer and enter the IP address of the camera to open a login box, as shown below:

In the login box you can choose a language for the IE client. Enter your user name (admin by default) and password (user defined) and then press OK to open a preview frame as shown below:



Some buttons in the preview frame are described below:

(note: except the red "H", other red mark means recording, and the green mark means not recording)

R ：Normal recording

M：Motion is triggered and recording

M：Motion is triggered, but no recording

I： I/O alarm triggered and recording

I： I/O alarm, but no recording

S：Intelligence alarm is triggered and recording

S：Intelligence alarm is triggered but no recording

PIR：PIR is triggered and recording

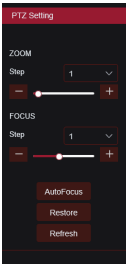
PIR：PIR is triggered, but no recording

C： Cover alarm is triggered, means the lens covered

H：No TF card or TF card is in error to work

: Color setting button, for color settings, brightness, contrast, saturation and sharpness of the frame.

: PTZ CONTROL press the icon ,then it shows the picture below:



: It has eight difference angle to control in the circle button, 0-10, it means difference PTZ speed

ZOOM: adjust lens
FOCUS: fix lens
Restore: restore factory setting

Playback : read the recording file from SD card, and then playback from browser.

Remote Setting : access to device setting menu, for customized setting of various device parameters.

Local Setting : for setting of snapshot, video file type and storage path.

: help information (including current user, Web browser and plug-in versions), logout button, for returning to the login page.

: turn off preview

: Turn on preview

: Original proportion, The preview showed on 4:3

: Stretch

(Manual recording): Click to manually record the channel immediately. If the manually recording is in process, the icon will be in red color. Click one more time to stop manual record. And save in the set storage path

(Snapshot): Click to save a snapshot of the current camera image. Manual Capture must be enabled to use this feature, and save in the set storage path

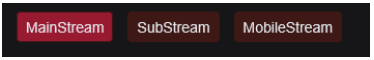
(Zoom-in): Click to zoom-in the channel. When the icon appears, press and hold the left button of your mouse to drag the area you want to zoom in.

(Volume): Click to adjust audio volume

(Voice intercom): Click to speak with the IPC

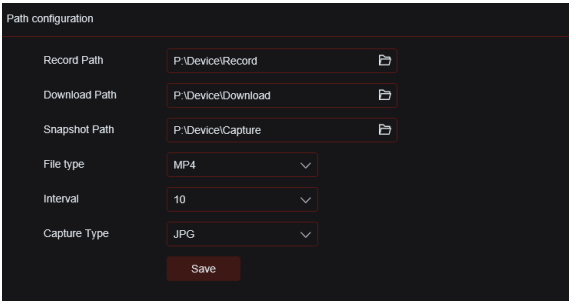
(White light): Click to turn on/off the white light, and adjust the brightness of the white light according to the level bar

(Alarm bell): click to turn on/ off the white light alarm bell, and adjust the voice of the alarm bell according to the level bar



: Dynamic switching of bit stream for the preview frame

Click Path Configuration button to pop up the following dialog box: In this dialog box you can set video storage location, paths for download of remote file and storage of image snapshot, file type (RF by default, in H265 encoding) and video recording duration.



4.3.2 Playback (optional function)

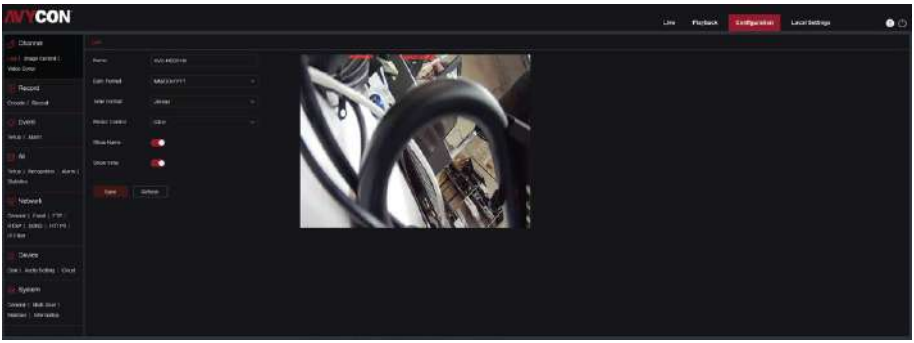
Click record file to playback, select the corresponding date, then click the Search to go to below page

User can search video by file type as needed, and operate the video through the simple tool on the toolbar, e.g. open/stop video , bit stream video, recording, snapshot, download recording , quick motion video playback, Sound On/Off.

5 Parameter Settings

5.1 Display Configuration

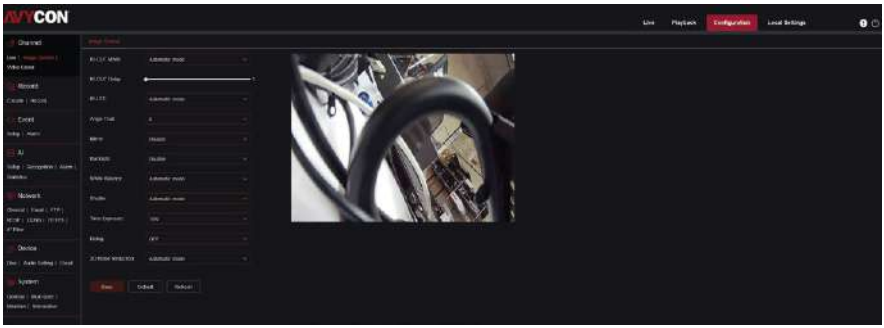
Click on Parameter Setting to open the page as below (preview setting page by default):



Name of channel: name of the IP camera
Display of channel: Choose to display or conceal it.
Time display: Choose to display or conceal it.
Blinking control: Choose 50Hz, 60Hz or disable it.
Transparency: Choose transparency of display of name of channel and time on the preview frame (smaller value indicates higher transparency)
OSD: the text in red color on the frame; you can locate display of the name of channel and time by dragging it in the preview frame.

5.2 Image Control

Click on Image Control in Display Configuration to open the following page:



IR-Cut Model: Classified into GPIO Automatic, Colored, Black-White models and Schedule (B/W)

① **GPIO Auto:** In "auto" mode, the device automatically controls the day and night modes according to the brightness of the external environment.

②**Color Mode:** Regardless of the photosensitive judgment, the image will always be in a color mode

③ **Black white mode:** Forced to switch to IR (black and white) mode, and the image is always in black and white mode

④ **Schedule (Intelligent Plan B/W):** Set a start and end time period for day and night mode switching

⑤ **IR cut delay:** IR cut switching delay. Set the delay time of IR cut switching. Only when the photo-resist is bright (or dark) for a long time, and the time reaches the delay switching setting, IR cut will switch to prevent the wrong switching caused by sudden strong light.

- **Supplement Light:** The switch mode of the lamp panel is off, on, auto and manual. The manual mode can adjust the brightness of the infrared lamp panel.

- **Supplement Light Auto:** Automatically control the brightness of IR through smart detection. When the smart IR function is turned on and the camera switches to night vision, the brightness of the IR light is controlled according to the current focus setting. Then, according to the white spot in the bright area, the pulse of IR lamp is reduced to optimize the picture effect, or the power of IR

lamp is reduced to optimize the picture effect, or the power of IR lamp is increased according to the white spot in the dark area.

- **Supplement Light Manual:** Control the brightness manually, optional for Low Beam Light or High Beam Light.

- **Low Beam Light:** Low beam brightness adjustment: the IR light of the camera is divided into two groups: high beam light and low beam light. By manually controlling the pulse output, the brightness of low beam light is controlled when night vision is triggered.

- **High Beam Light:** Low beam brightness adjustment: the IR light of the camera is divided into two groups: high beam light and low beam light. By manually controlling the pulse output, the brightness of high beam light is controlled when night vision is triggered.

Image Flip-Over: this includes Lens Flip, Angle Flip, Corridor Mode and Angle Rotation (0°, 180°)

- **Lens Flips:** Image flipped 180° from top to bottom

- **Angle Flips:** Image flipped 180° from left to right

- **Corridor Mode:** Turn the camera image to the side, so as to obtain more image information in depth and up, and its output ratio changes from the original 16:9 to 9:16.

- **Angle Rotation:** Rotate the image at (0°, 180°) 180° clockwise.

- **Image Control:** Back-light compensation, 3D noise reduction, WDR, Automatic gain, White Balance,Shutter speed, exposure time and defog model.

- **Back Light:** System will automatically expose according to the environment, so that the image of the darkest area can be seen clearly.

- **3D Noise Reduction:** when it is turned on, the image noise will be significantly reduced, and the image will be more thorough, so as to display a pure and delicate picture.

- **DWDR:** System reduces the brightness of high brightness area and increases the brightness of low brightness area according to the ambient brightness, so that the scenery in high brightness area and low brightness area can be clearly displayed.

- **HLC:** System will suppress the brightness of the highlighted area, reduce the size of the halo area, and reduce the brightness of the whole image.

- **AGC:** When the device is in a dark scene (infrared scene), and the AGC is turned on, the overall brightness of the image will be significantly improved.

- **White Balance:** There are three modes: Auto, indoor and manual. The default mode of the system is auto. The system can automatically compensate the white balance of different color temperature, so that the image color is normal. An indicator of white accuracy after the three primary colors of red, green and blue are mixed in the display, which is usually selected as the automatic mode to ensure that there is no obvious color difference between scenes.

- **Shutter and Time Exposure(max):** The shutter is a device used to control the time of light illuminating the photosensitive element in the camera equipment. It controls the brightness and frame rate of the image by adjusting the exposure time.

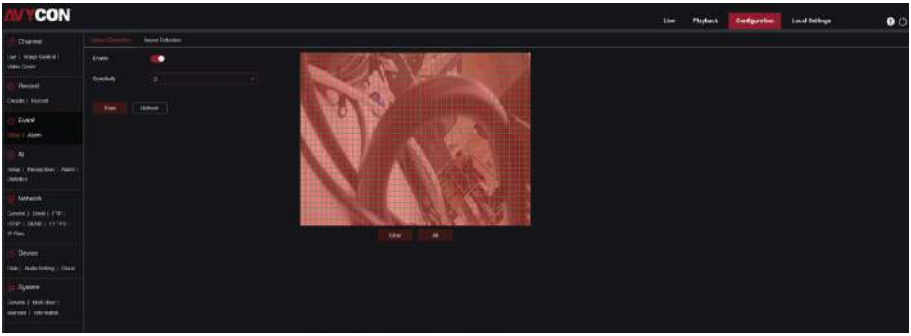
- **Defog Mode:** The image quality of the device will decline in the environment with fog and haze, the Defog Mode can be turned on to adjust the definition of the image. The system selects automatic by default, and the system automatically adjusts the definition of the image according to the actual scene. When you select Manual, you can select and adjust between 0 - 255 according to the number of displayed levels.

  - (Note: Back Light & DWDR & HLC are mutually exclusive and cannot be turned on at the same time.)

  - **Note:** Below 2MP device, it doesn't support Corridor mode and Angle rotation, fog mode.

5.3 Motion Detection

Enter【Remote Setting】, Select motion detection to enter the setting interface, as shown in following picture 5-3

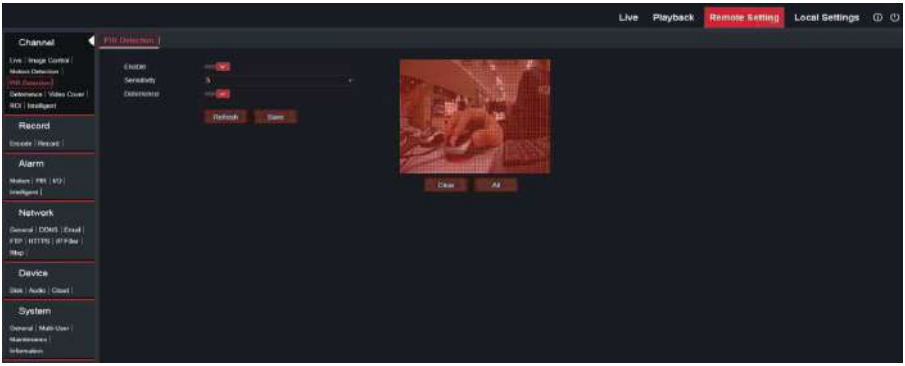


Picture 5-3 motion detection menu

- **Enable:** Enable or disable motion detection
- **Smart Motion Detection:** Enable or disable intelligent motion detection. After enable smart motion detection, the mobile detection alarm will be triggered only when the human is detected. This will reduce the false alarm rate (this function is supported by some models, please refer to the real object)
- **Sensitive:** Set the sensitivity level. Level 1 the lowest sensitivity level while level 8 is the highest sensitivity level. The system default setting is 3
- **Deterrence:** Enable or disable the white light association. If enable the white light association, the white light will be turned on when the motion detection is triggered. The details of the white light setting are as follows 2.5. Deterrence.
- **Motion Detection Area:** The trigger area map with grid window is motion detection. Click the grid cursor and then drag the mouse to highlight the scope to unmark the area into transparent blocks. Only in the selected area can motion detection be triggered.
- **Clear:** Clear all motion area.
- **All:** Select all motion area.
  (Note: there are objects moving in the motion area, and "M" will appear on the channel.)

5.4 PIR

Enter【Remote Setting】, Select PIR to enter the PIR detection setting interface, as shown in following picture 5-4.



Picture 5-4 PIR setting menu

- **Enable:** Enable or disable PIR.
- **Sensitive:** Set the sensitivity level. Level 1 the lowest sensitivity level while level 8 is the highest sensitivity level. The system default setting is 3
- **Deterrence:** Enable or disable the white light association. If enable the white light association, the white light will be turned on when the motion detection is triggered. The details of the white light setting are as follows 2.5. Deterrence.
- **PIR Detection Area:** The trigger area with grid window is PIR detection. Click the grid cursor and then drag the mouse to highlight the scope to unmark the area into transparent blocks. Only in the selected area can PIR detection be triggered.
- **Clear:** Clear all PIR area.
- **All:** Select all PIR area.
  (Note: there are human moving in the motion area, and "PIR" will appear on the channel.)

5.5 Deterrence

5.5.1 Deterrence

Enter【Remote Setting】, Select Deterrence to enter the setting interface, as shown in following picture 5-5-1.

Picture 5-5-1 Deterrence setting menu

- **Light:** Enable or disable light.
- **Light Level:** You can set the different light intensity by changing the level. You can adjust 1-100 (the higher the value, the brighter the light). The default intensity is 50.
- **Duration:** You can set the duration of the light, 5-180 seconds, and the default duration is 60 seconds.
- **Color Image:** Enable or disable the color image. Enable, white light will be started under night vision, and the screen will be forced to switch to color mode during the duration of white light.
- **Deterrence Mode:** Select Warming Light or Strobe.
- **Siren:** Enable or disable the Siren.
- **Siren Level:** The different siren intensity can be set by changing the level. 1-10 can be adjusted (the larger the value is, the louder the alarm sound is), and the default intensity is 5

- **Siren Duration:** You can set the duration of the light, 5-180 seconds, and the default duration is 10 seconds.

- **Sensitive:** Set the sensitivity level. Level 1 the lowest sensitivity level while level 8 is the highest sensitivity level. The system default setting is 4.

- **Deterrence Triggered Area:** The trigger area with grid window is Deterrence detection. Click the grid cursor and then drag the mouse to highlight the scope to unmark the area into transparent blocks. Only in the selected area can Deterrence detection be triggered.

- **Clear:** Clear all Deterrence area.

- **All:** Select all Deterrence area.

5.5.2 Schedule

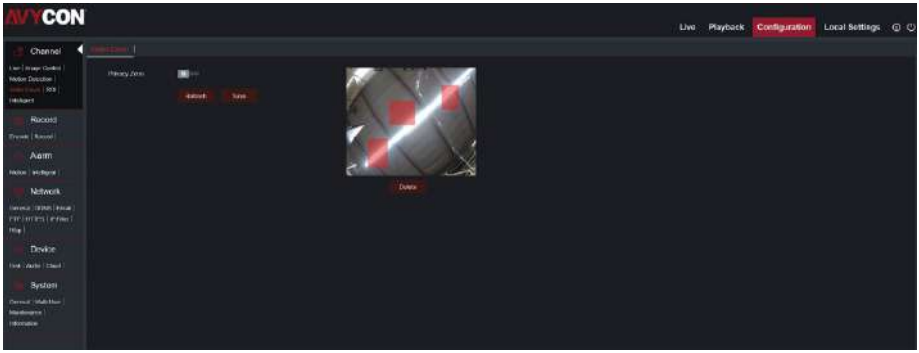
Enter【Configuration】, Select schedule to enter the setting interface, as shown in following picture 5-5-2.

Picture 5-5-12 Deterrence schedule setting menu

As shown in the picture: One grid in the table is 30 minutes, you can press and hold the left mouse button to slide and tick the table. If the table is highlighted, it will turn green. If the table is not highlighted, it will be black (blank). By default, the schedule of intelligent alarm is not specified. Users can set up according to the private requirement to choose different record types and times. The default schedule is 6:30-18:30.

5.6 Video Cover

Enter【Configuration】, Select Video Cover to enter video cover menu, as shown in following picture 5-6.



Picture 5-6 video cover menu

Procedure of setting video blocking:

1. Check Enable Video Blocking

2. Press down and hold the left mouse button and drag out an area for video blocking (up to four areas at one time)

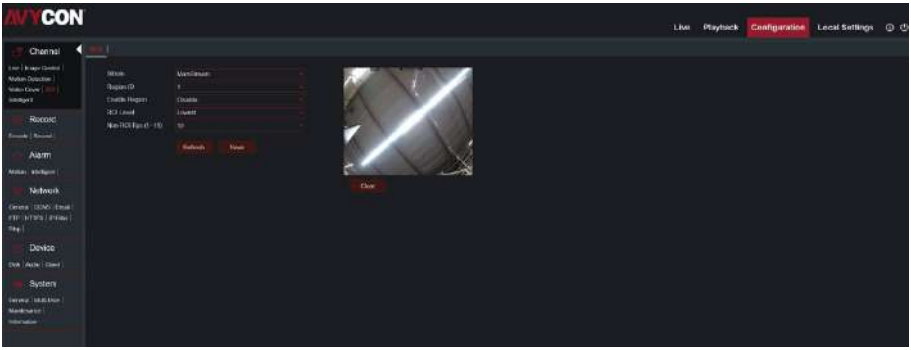
3. Click on Save to enable the video blocking area.

Remove: After clicking Refresh, choose a blocked area by clicking it and then click Remove and click Save to remove it.

5.7 ROI (if applicable)

ROI (sensitive area) is an image area selected from the video area, which is the important area of your attention. This area can be circled for further processing, and ROI can be used to circle the area of your focus, which can reduce processing time and increase accuracy.

After entering the [remote setting], select ROI to enter the sensitive area setting menu, as shown in following picture 5-7.



Picture 5-7

Procedure of setting ROI:

1. Choose an area of application

2. Press and hold the left mouse button and drag out a ROI area (only one ROI can be set for each area)

3. Click on Save to apply the ROI area.

Bit stream type: Choose bit stream effective for ROI among Main Bit Stream, Sub-Bit Stream and Cell Phone Stream.

Area Numbering: Up to 8 ROI areas can be set in one bit stream.

Enable ROI area: Enable or disable ROI area

Area image quality: Set quality of the image in the area (relative quality, absolute quality)

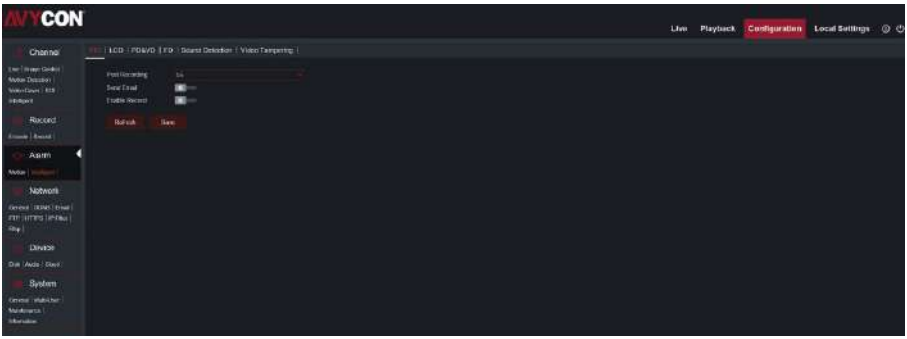
ROI level: Set ROI level in one bit stream; larger value indicates higher-quality image in ROI area (1~6 Levels)

Non-ROI frame rate: Set frame rate out of RIO area; smaller value indicates higher-quality image in ROI area. Range of frame rate is in relation to video standard and resolution. (Note: Different non-ROI frame rates may be allocated to different ROI areas, but the minimum value among them is used as the frame rate to be applied for the non-ROI area on the preview frame.)

5.8 Intelligent

5.8.1 PID—Perimeter Intrusion Detection

After entering [Remote Setting], select Intelligent to enter PID MENU setting. Default enter PID—Perimeter Intrusion Detection menu, as shown in following picture 5-8.



Picture 5-8 PID setting menu

Switch: Switch: PID function master switch

Sensitive: Sensitive level, range is 1-4, default to 2. If the detected object sensitivity is higher, the moving Object can be detected easily. Meanwhile, the false detection rate is higher. Suggest to use default level.

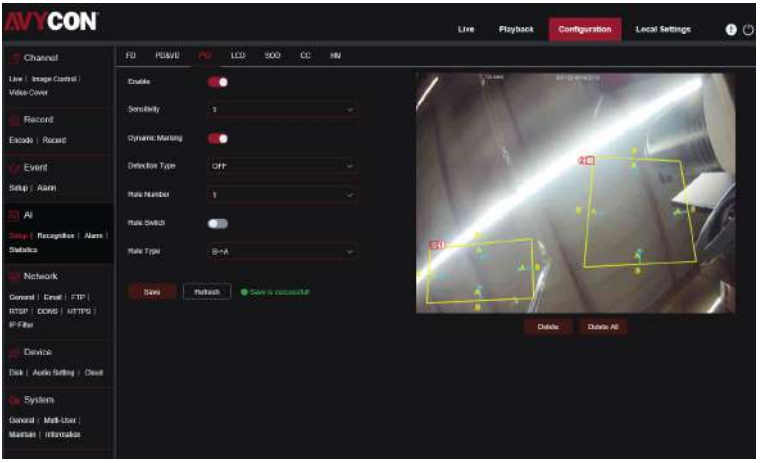
Scene: Scene setup, user can choose Indoor or outdoor according to real situation Enable I/O Out：Trigger alarm then if will be I/O output

- **Detection Type:** The detection types include pedestrian and vehicle. When the settings are enabled, the only detect the alarms triggered by human or vehicles, but need to consume more CPU of IPC. If it is not turned on, all objects passing through the line will be detected.

Rule Number: Max set 4 rule number. Draw a rule area on the area map, and click to the next few rules, then you can draw rules on the area map. The rule switch and rule type of each rule are independent, and they need to be opened, closed or set separately.
Rule Switch: The switch to every rule
Rule Type: Setup to each rule, A->B means can detect A to B direction moving, B->A means can detect B to A direction moving, A ←→B means can detect two directions moving.

- **PID (perimeter intrusion detection):** Click on the area, draw a square area of four points, and then set it as a perimeter intrusion detection rule. You can draw four rule areas; each rule has a corresponding digital ID. Click the small red box next to the rule's digital ID, and you can drag or stretch the perimeter intrusion detection rule area.

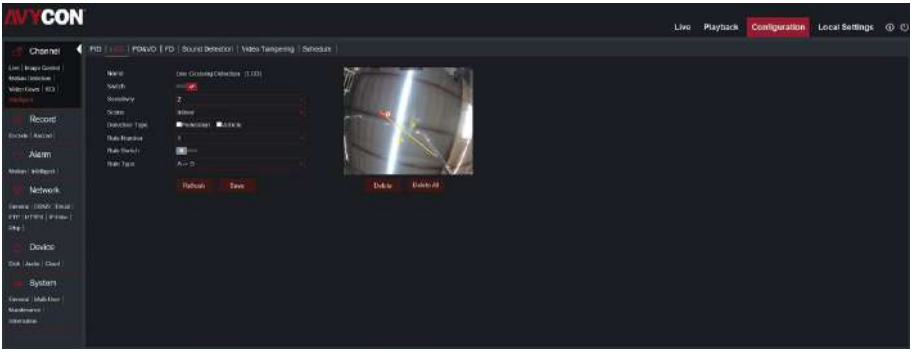
  (Note: when PID (perimeter intrusion detection) is triggered, "S" will appear on the channel, and a pop-up window will appear in the lower-left corner of the page, as shown in picture 4-9. Also, PID / LCD and PD & VD / FD are mutually exclusive and cannot be enabled at the same time)



Picture 5-9

5.8.2 LCD—Line Crossing Detection

Function description: In the preview page, detect and follow up the moving object to pass through the guard line. After entering the [remote setting], select intelligent to enter the intelligent alarm setting interface, and click LCD line crossing detection to enter the crossing detection setting interface, as shown in picture 5-9.



Picture 5-9 LCD—Line Crossing Detection

Switch: LCD master switch

Sensitive: Sensitive level, range is 1-4, default to 2. If the detected object sensitivity is higher, the moving Object can be detected easily. Meanwhile, the false detection rate is higher. Suggest to use default level.

Scene: Scene setup, user can choose Indoor or outdoor according to real situation Enable I/O Out：Trigger alarm then if will be I/O output

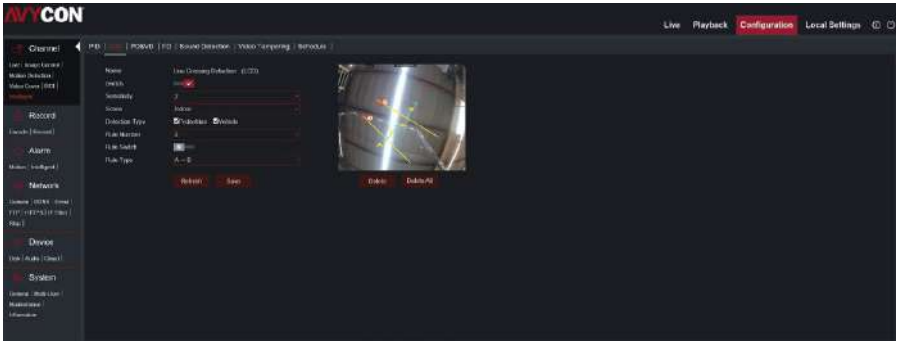
- **Detection Type:** The detection types include pedestrian and vehicle. When the settings are enabled, they only detect the alarms triggered by humans or vehicles but need to consume more CPU of IPC. If it is not turned on, all objects passing through the line will be detected.

- **Rule Number:** Max set 4 rule number. Draw a rule area on the area map, and click to the next few rules, then you can draw rules on the area map. The rule switch and rule type of each rule are independent, and they need to be opened, closed or set separately.

Rule Switch: The switch to every rule
Rule Type: Setup to each rule, A->B means can detect A to B direction moving, B->A means can detect B to A direction moving, A ←→B means can detect two directions moving.

- **LCD (Line Crossing Detection):** Click on the area, draw a square area of four points, and then set it as a perimeter intrusion detection rule. You can draw four rule areas; each rule has a corresponding digital ID. Click the small red box next to the rule's digital ID, and you can drag or stretch the perimeter intrusion detection rule area.

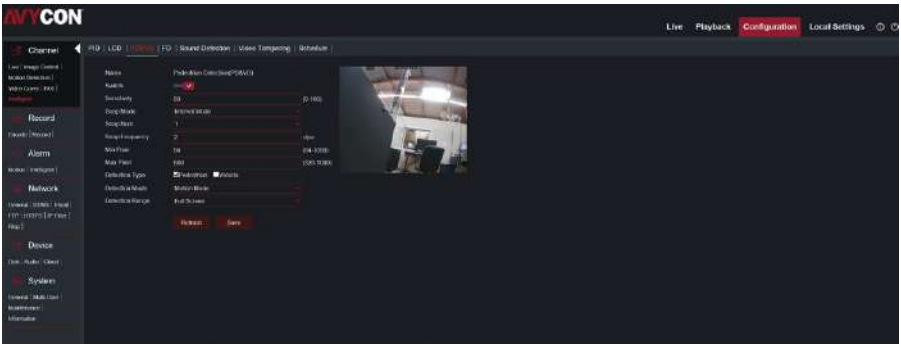
  (Note: when LCD (Line Crossing Detection) is triggered, "S" will appear on the channel, and a pop-up window will appear in the lower-left corner of the page, as shown in picture 5-10. Also, PID / LCD and PD & VD / FD are mutually exclusive and cannot be enabled at the same time)



Picture 5-10

5.8.3 PD&VD—Pedestrian & Vehicle Detection

Function description: in the preview page, detect and follow up the moving object to pass through the guard line. After entering the [remote setting], Select Intelligent to enter PD&VD setting menu. Click PD&VD — Pedestrian&Vehicle Detection to enter PD&VD detection menu. As the shown in picture 5-11.



Picture 5-11 PD&VD detection menu

- **Switch:** Enable or disable PD&VD detection
- **Sensitive:** PD &VD detection can be set to 1-100. The larger the value is, the more accurate the triggering, and the more like the shape of Pedestrian & Vehicle, the more accurate the triggering. The default sensitive detection is 60.
- **Snap Mode:** There are three recognition modes, default mode, real-time mode and interval mode
- **Default:** The default optimal mode. When human or a vehicle enters the monitoring area, the camera will always capture. After a human or a vehicle leaves the monitoring area, the best and clearest of the captured images in this period will be saved in NVR. Default (IPC can't save picture).

- **Realtime Mode:** One picture will be send to the device when a human or vehicle enters the monitoring area in IPC, and the second picture will be send to NVR when a person or vehicle leaves the monitoring area.

- **Interval Mode:** Push pictures to the docking device. You can set the maximum number of times to send and the interval for each picture to be sent.

- **Snap Number:** Number of push pictures for each locked target can be set as 1, 2, 3 and infinite times, that is, push pictures to the board end device once every N seconds, and push once, 2, 3 and infinite times. (Note: this function is available in interval mode)

- **Snap Frequency:** n s/pic（n can set to 1—255）, Select the best snapshot every N seconds and push it to the docking recorder.

- **Min Pixel:** The lowest pixel setting of human and vehicle. When the recognized object is smaller than the pixel, no alarm is generated accordingly. It can be set to 64-1080. Note: the figure recognition function recognizes the whole picture as a 1080p picture.

- **Detection Type:** There are two type of Pedestrian & Vehicle, select the type to detect. Two detection types, pedestrian and vehicle, can be opened at the same time.

- **Detection Mode:** There are two detection mode. Motion Mode & Static Mode.

- **Motion Mode:** Can snap the human or vehicle in motion.

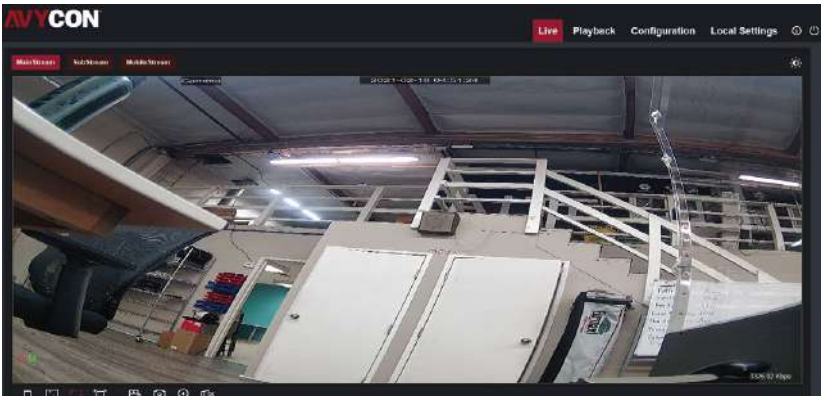
- **Static Mode:** Can snap the human or vehicle in motion or static.

- **Detection Range:** Setting detection area. There are two mode, Full Screen & Customize.

- **Full Screen:** The detection area is the camera all cover area.

- **Customize:** Select this mode and a region box will appear on the small window. Click the red small box next to the digital ID of the region box to drag or stretch the region.

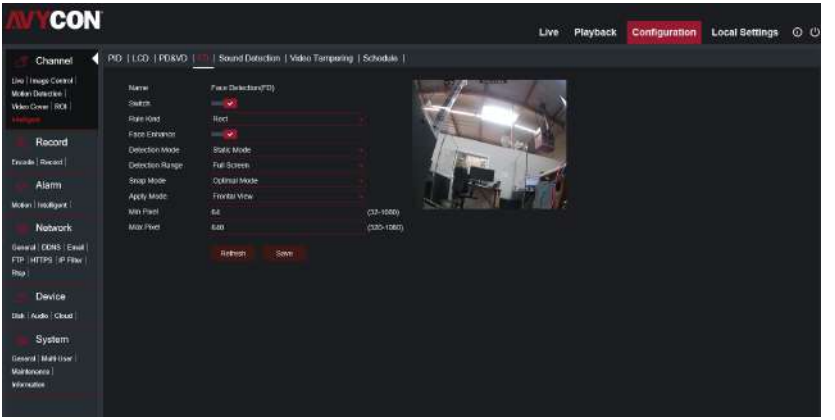
  (Noted: Trigger PD&VD, "S" will appear on the channel, identify the pedestrian line in green box, and identify the vehicle line in blue box. A pop-up window will appear in the lower left corner of the page, as shown in picture 4-12. In addition, PID / LCD and PD & VD / FD are mutually exclusive and cannot be enable at the same time)



Picture 5-12

5.8.3 PD&VD—Pedestrian & Vehicle Detection

After entering【Remote Setting】, Select Intelligent to enter FD—Face Detection . As shown in the picture 5-13



Picture 5-13 FD—Face Detection menu

- **Switch:** Enable or disable FD—Face Detection.

- **Sensitive:** Turn on the face enhance function to enhance the effect of the face image captured by the moving target, so as to make it clearer. However, enable this function will take up more resources of IPC, making the overall effect of the screen worse.

- **Rule Kind:** There are two rule. Rect & Line. It has its own detection scope and rule type.

  ① **Rect:**

  Detection Range: There are two rule. Rect & Line. It has its own detection scope and rule type.
  ●**Full Screen:** The detection area is the camera all cover area.
  ●**Customize:** Select this mode and a region box will appear on the small window. Click the red small box next to the digital ID of the region box to drag or stretch the region.

  ② **Line:**

  Rule Type: There are two types, A→ B and B → A. Draw a regular line from A to B (or B to A) on the area. When the face moves from A to B (or from B to A), the rule will be triggered to capture the human face.

- **Detection Mode:** There are two type. Motion Mode & Static Mode.

  ① **Motion Mode:** Can snap the human and human face in motion.
  ② **Static Mode:** Can snap the human and human face in static.

- **Snap Mode:** There are three recognition modes, default mode, real-time mode and interval mode.

- **Optimal:** When person enters the monitoring area, the camera will always capture. After a person leaves the monitoring area, the best and clearest of the captured images in this period will be send to the recorder.

- **Realtime Mode:** One picture will be send to the device when a human or vehicle enters the monitoring area in IPC, and the second picture will be send to NVR when a person or vehicle leaves the monitoring area.

- **Interval Mode:** Push pictures to the docking device. You can set the maximum number of times to send and the interval for each picture to be sent.

- **Snap Number:** Number of push pictures for each locked target can be set as 1, 2, 3 and infinite times, that is, push pictures to the board end device once every N seconds, and push once, 2, 3 and infinite times. (Note: this function is available in interval mode)

- **Snap Frequency:** n s/pic（n can set to 1—255）, Select the best snapshot every N seconds and push it to the docking recorder.

① **Apply Mode:** Frontal View, Multi Angle & Customize.

② **Frontal View:** Only snap frontal view.

③ **Multi Angle:** Can capture video from multiple perspectives.

④ **Customize:** Custom snap angle:

Roll Range: The roll range of face capture can be set to 0-180.

Pitch Range: The pitch range of face capture can be set to 0-180.

Yaw Range: The YAW range of face capture can be set to 0-180.

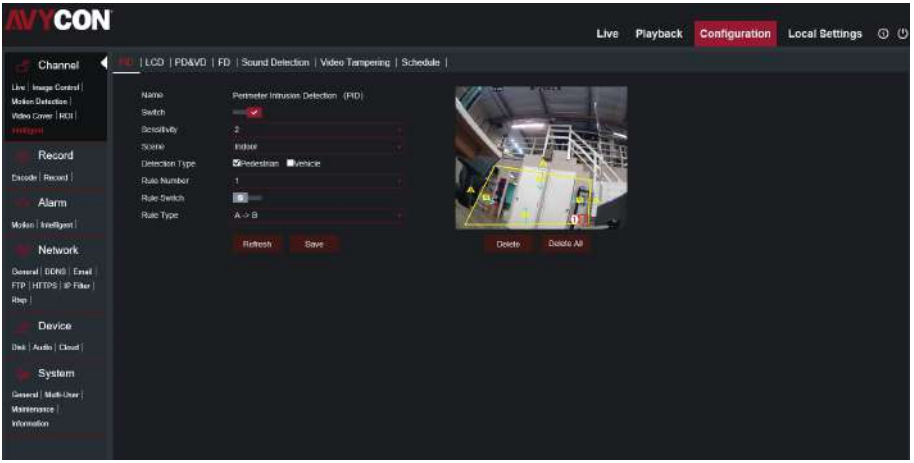
Picture Quality: The picture quality of face capture can be set to 0-180.

Min Pixel: The lowest pixel setting of human and vehicle. When the recognized object is smaller than the pixel, no alarm is generated accordingly. It can be set to 64-1080. Note: the figure recognition function recognizes the whole picture as a 1080p picture

Frontal Default: Can set the frontal view to load default.

Multi Default: Can set the multi view to load default.

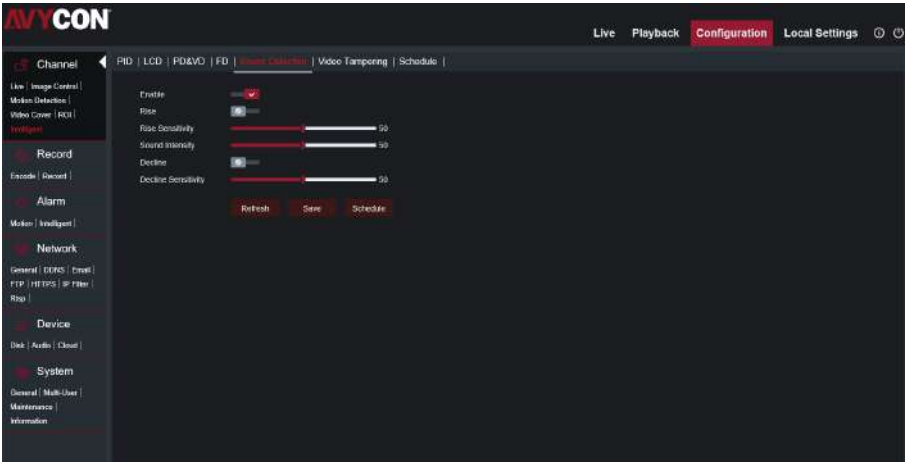
(Note: Trigger FD, "S" will appear on the channel, A pop-up window will appear in the lower left corner of the page, as shown in picture 5-14. In addition, PID / LCD and PD & VD / FD are mutually exclusive and cannot be enable at the same time)



Picture 5-14

5.8.5 Sound Detection

After entering【Remote Setting】, Select Intelligent to enter Sound Detection . As the shown in picture 5-15



Picture 5-15 sound detection menu

- **Enable:** Enable or disable sound detection.

- **Rise:** Turn on the sound sharp rise detection, when the sound suddenly increases in a short period of time, trigger the sharp rise alarm.

- **Rise Sensitive:** Fine-tuning sound rise sensitive detection, and the sensitivity can be set to 1-100. The larger the value the lower the sound detection threshold.

- **Sound Intensity:** Coarse-tuning sound rise sensitive detection, and the sensitivity can be set to 1-100. The larger the value, the higher sound detection threshold. Hard to trigger alarm.

- **Decline:** Turn on the sound drop detection, when the sound suddenly increases and decreases in a short period of time, trigger the sharp drop alarm.

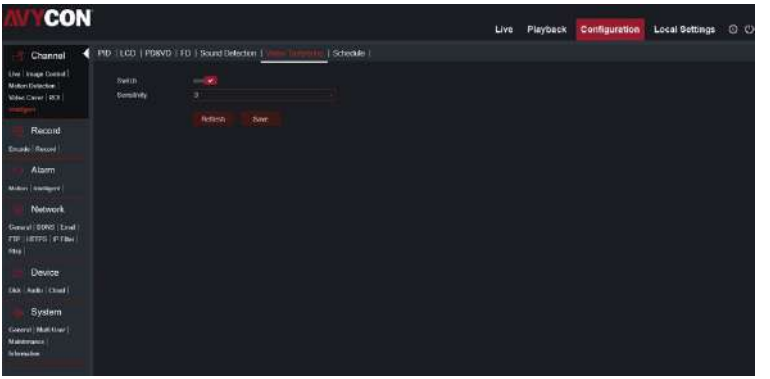
- **Decline Sensitive:** The decline sensitive can be set to 1-100, and the higher the value is, the higher the sensitivity. More easy to trigger alarm.

- **Schedule:** Set the time schedule of sound detection. It is fully enable by default. The user can customize the time period of touch sound alarm.

(Note: when sound detection is triggered, "S" will appear on the preview interface, and a pop-up prompt will appear in the lower left corner of the page to trigger the sound alarm)

5.8.6 Video Tampering

After entering【Remote Setting】, Select Intelligent to enter video tampering. As shown in picture 5-16.

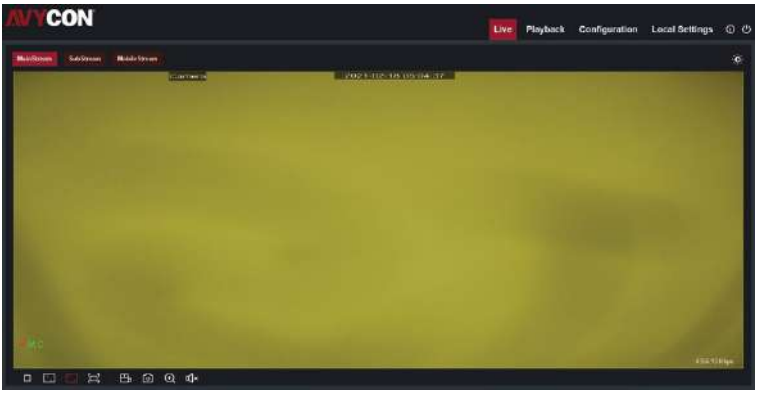


Picture 5-16 video tampering menu

- **Switch:** Enable or disable video tampering.

- **Sensitive:** The sensitivity of triggering video tempering detection can be set as 1-6. The larger the value is, the more sensitive the occlusion alarm is. The default sensitivity of perimeter intrusion detection is set as 3

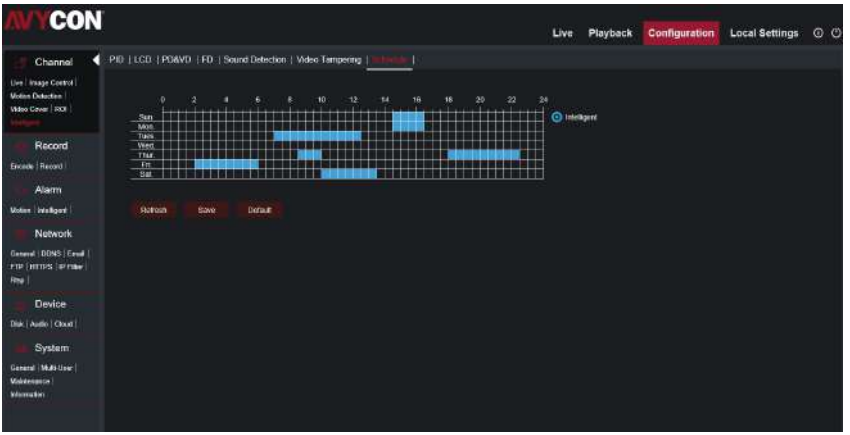
  (Note: triggering video tampering detection means that occlusion alarm is triggered, lens is blocked by objects, and "C" will appear on preview interface, as shown in Figure 5-17 below)



Picture 5-17

5.8.7 Schedule

After entering【Remote Setting】, Select Intelligent to enter schedule the intelligent alarm recording schedule setting interface As the shown in picture 5-18



Picture 5-18 intelligent schedule

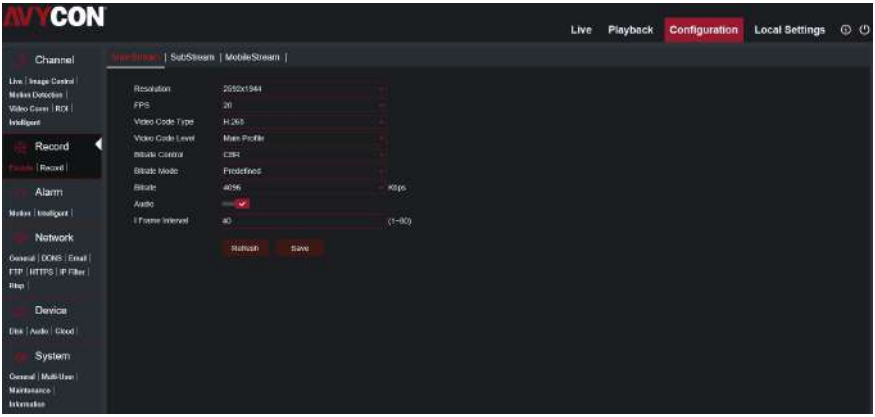
One grid in the table is 30 minute, you can press and hold the left mouse button to slide the tick time table. If you check the time table, it will turn blue. If you do not check the time table, it will be blank. If you record the schedule of intelligent alarm by default, it will be blank. User can setup according to private requirement to choose different record type and time.

6 Record

This function includes encode, record and capture (the function needs to be supported by the camera), and sets the specific way to write the video or capture when the camera triggers the alarm. In SD card format, the file system divides the SD card into storage partition (about 1g partition read by connecting the SD card to the computer, different model settings may be different) and hidden partition (invisible area, used to store video recording or snapshot). According to the size, the hidden partition can be divided into several 256M files (the available size of each file is 254M, which can be checked in serial port printing during format Query file-nr, to find out how many files there are in total. For example, file-nr: 53 means that there are 53 files to written. One file is used each time. When the overwrite function is enable and the SD card is full, the new video will overwrite the files that have not been modified for the longest time.

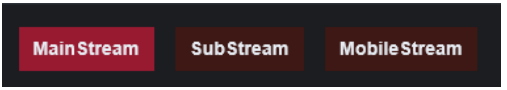
6.1 Encode

This setting is the basis for converting the camera image data into storable data when encoding. The camera can generate three kinds of streams: mainstream, sub stream and mobile stream (the function needs to be supported by the camera). The interface is shown in picture 6-1.



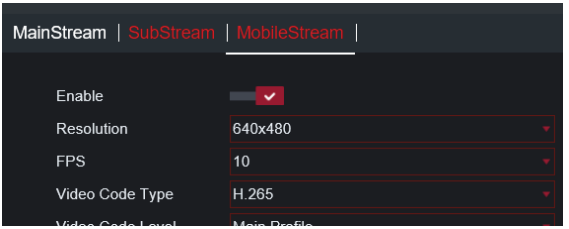
Picture 6-1 Encode settings page

- **Stream selection:** select the stream for which the current parameter setting is targeted, including three settings: mainstream, sub stream and mobile stream (the function needs to be supported by the camera), as shown in picture 6-2.



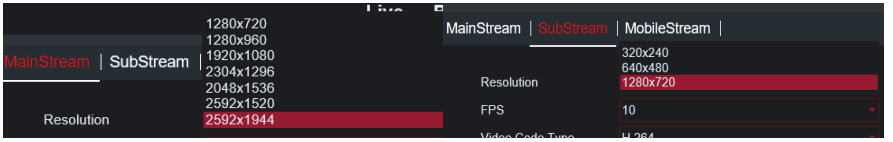
Picture 6-2

Enable: Switch for mobile stream. Only mobile stream supports this function. As shown in picture 6-3, Disable this function can reduce the consumption of camera resource



Picture 6-3

- **Resolution:** Set the resolution of the image when encoding the corresponding code stream. Different cameras has different streams. As shown in picture 6-4, it is the resolution options of the main stream and sub stream for the 5MP camera



Picture 6-4

- **FPS:** Encoding recording consists of several pictures per second, with a difference of ± 1 frame allowed. You can check whether the data saved in SD card meets the requirements through the forward by one frame function of playback.

  Each chipset has a different performance, so this setting item's value is affected by the selected resolution. The maximum frames that can be chosen for different resolutions are different. For example, for a v12.45.6.0 camera, the highest frames can be set to 20fps under 5MP resolution and 30fps under 2MP resolution. At the same time, it is also affected by data from the value of remote setting → live → Flickr control. If it is set to NTSC-format 60Hz, the 2MP resolution can be set to 30 frames, and if it is set to PAL-format 50Hz, the 2MP resolution can be set to 25 frames.

- **Video Code Type:** There are two types of coding: H.264 and H.265.

  H.265 and H.264 are video coding standards developed by ITU-T VCEG. H. 265 standard around the existing video coding standard H.264, retain some of the original technology, while improving some of the relevant technologies. The new technology uses the advanced technology to improve the relationship between the bit stream, coding quality, delay and algorithm complexity, so as to achieve the optimal settings. Specific research contents include: improving compression efficiency, improving robustness and error recovery ability, reducing real-time delay, reducing channel acquisition time and random access delay, reducing complexity, etc. H.264 can transmit standard definition digital image at a speed lower than 1Mbps due to algorithm optimization; H.265 can transmit 720p (resolution 1280 * 720) ordinary high-definition audio and video at a transmission speed of 1-2Mbps. So the video and preview effect of H.265 is better than that of H.264, but H.265 requires a higher patent fee.

- **Video Code Level:** H.265 only has the main profile option. H264 has three options of baseline, main profile and high profile, corresponding to three levels of low quality, normal and high quality. When the set stream is large, the higher video coding, the better image quality.

- **Bitrate Control:** Bitrate control can be set as CBR (static bitrate) and VBR (dynamic bitrate).

  ① **CBR (static bitrate):** According to the bitrate, the whole video recording as a fixed stream to encode the video.

② **VBR (dynamic bitrate):** Encode according to the selected video quality, and complete the storage and propagation of the video quality with a lower bitrate.

You can place the camera in a static scene, use the same camera to select these two modes, and compare the consumed network bandwidth and memory.

- **Video Quality:** The options that appear only in VBR mode control the highest picture quality during image coding. There are 6 option: lowest, lower, low, medium, higher and highest.

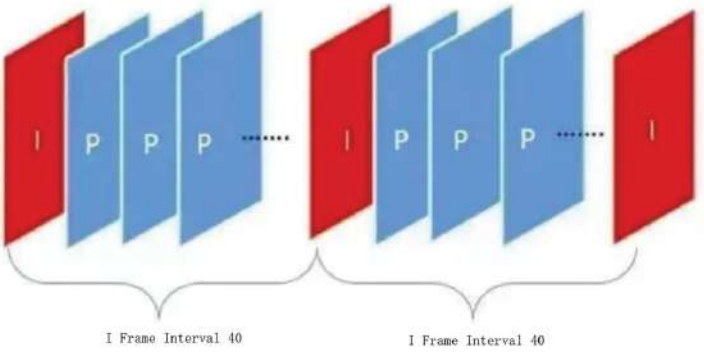
- **Bitrate Mode:** There are predefined and user-defined mode. When predefined is selected, the user can only select the default value through drop-down when setting bitrate. When user defined is selected, user-defined input can be customized when the user sets bitrate, but it cannot be less than the preset minimum value or more than the preset maximum value.

- **Bitrate:** The amount of data encoded per second. In the case of large resolution, low stream is used, for example, 512Kbps stream is used for 20 frames at 5M resolution, because the current setting is not enough to generate clear image, which will cause abnormal blur of the picture. But using 4096kbps stream can generate clear image.

  When the main stream is 4096kbps for recording, and the video is static, the CBR mode consumes 4M memory of SD card per second. The average memory of SD card used by VBR mode is less than 4M, but the video recording effect of VBR mode is not as good as that of CBR when the picture changes greatly.

- **Audio:** Disable the Audio. No sound coding when during image coding, and there is no sound in live and recording at WEB. Enable the Audio, the camera encodes the image, but it needs to consume an additional 8.5kbps per second.

- **I frame interval:** I frame interval setting, default 2 times of FPS. Default resolution of 5MP is 20FPS, and the I-frame interval is 40. At this time, when an I-frame is generated, 39 P-frames will be generated, and then another I-frame will be generated. The effect is shown in picture 6-5.



Picture 6-5

I frame: I frame represents key frame, which can be understood as the complete reservation of this frame; only the data of this frame is needed for decoding (because the complete frame is included)

I frame can be regarded as a complete picture, and can be decoded independently.

P frame: Forward prediction coding frame. P frame refers to the difference between this frame and the previous key frame (or P frame). When decoding, it needs to use the previously cached picture to overlay the difference defined in this frame to generate the final picture. (That means there is no complete picture data in frame P, only the picture data different from the previous frame)

P frame is only a part of a picture. Only by combining with I frame can the decoding be completed to form a picture.

As shown in picture 6-6, only the upper left corner area of the picture composed of I frame and I and P frame is different. The effect is that P frame directly replaces the data in the upper left corner of I frame to form a new picture.

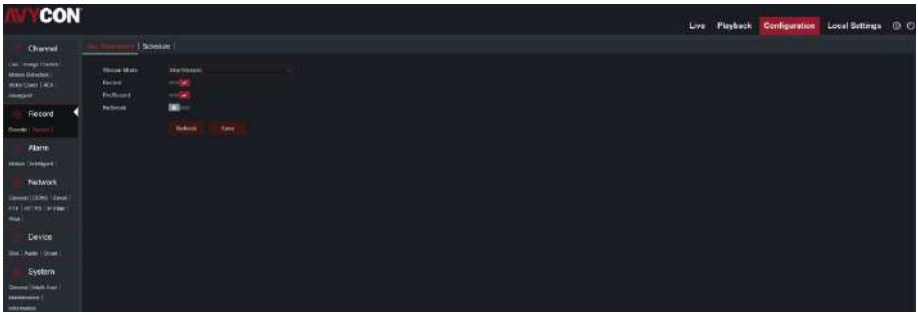
Picture 6-6

6.2 Record

Recording related settings written to SD card include rec parameters and schedule.

6.2.1 Rec Parameters

Video recording setting: set whether to write the SD card code stream when triggering the video recording function, whether to write the SD card, whether to mark the previous short video recording time as an event of alarm type when triggering the alarm, and whether to add the mark of offline video recording to the video recording when the network is disconnected. The interface is shown in the picture 6-7.



Picture 6-7 Rec Parameters setting menu

- **Stream mode:** The type of the stream written to SD card during recording, including mainstream and substream.

- **Record:** The switch for the recording to SD card when the recording is triggered.

- **Prerecord:** Enable this function,the data saved in the cache will be written to the SD card together. For example, when only motion recording is turned on (it is recommended to turn on only one recording to eliminate other interferences), the motion alarm will be triggered at 10:10:08, and the recording will be written. At this time, the video recording of the alarm starts at 10:10:06

- **Network break:** the function of off network video recording: Enable/disable network video recording. When the camera is off network, add the off network flag to the recorded video, which can be viewed through playback query.

6.2.2 Schedule

The recording schedule function allows you to customize the recording time range according to the actual application, and the interface is shown in picture 6-8. The schedule is set by week. Each row has 48 cells, that is, each cell represents half an hour of recording time. At the same time, according to the camera function, it can be defined that the video can only be recorded when the general video recording or the alarm triggering such as motion, IO, PIR, SD (according to the opening settings of the camera specific functions, some intelligent functions follow the intelligent schedule for recording) are triggered.

Picture 6-8 Schedule setting menu

As shown in the image: one grid in the table is 30 minutes, green is normal record, yellow is motion detection alarm, red is I/0, light purple is PIR detection, and dark purple is sound detection.

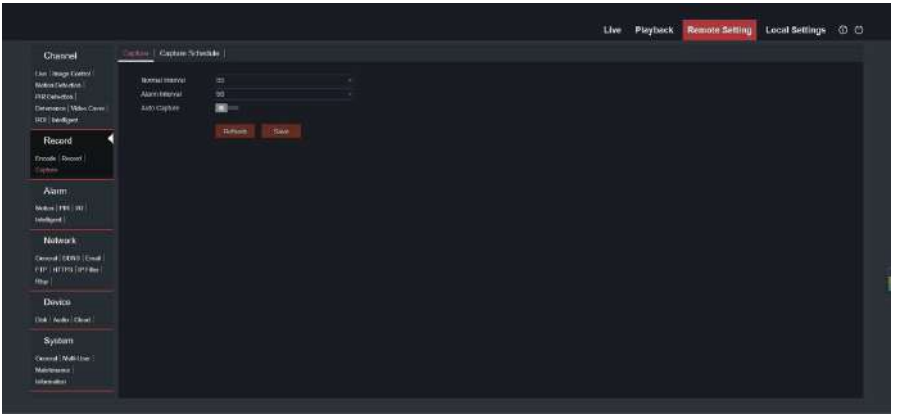
User can setup according to private requirement to choose different record type and time.

6.3 Capture

Camera capture function: according to the settings, the captured pictures are stored in SD card. The writing mode is the same with video recording. Both of them occupy one 256M file of hidden partition for reading and writing.

6.3.1 Capture

Automatic snapshot setting, you can set whether to use the snapshot function and the time interval of snapshot. The screenshot is shown in picture 6-9.

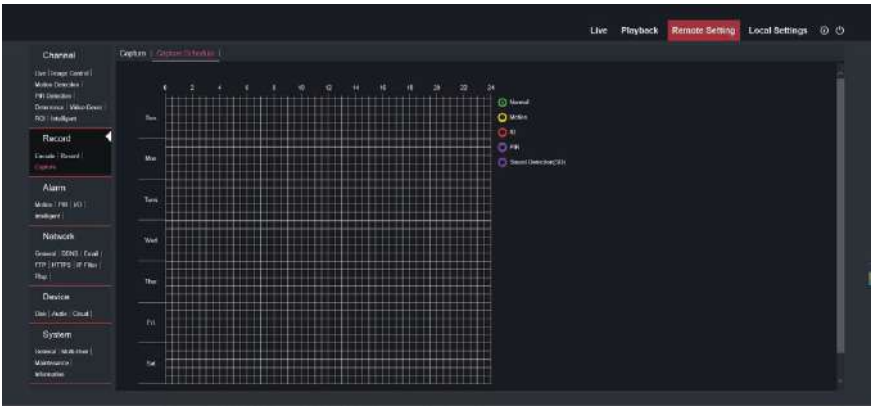


Picture 6-9 Capture setting menu

- **Normal Interval:** Normal video capture interval setting.
- **Alarm Interval:** Alarm event capture interval setting. For specific supported alarm events, refer to the alarm events that capture schedule supports.
- **Auto Capture:** Auto capture switch, turn on the function device to support auto capture.

6.3.2 Capture Schedule

According to the actual use scenario, the capture schedule function can customize the snapshot time range, and its interface is shown in picture 6-10. The schedule is set by week. Each row has 48 cells, that is, each cell represents half an hour of recording time.



Picture 6-10 Capture Schedule

7 Alarm

The alarm function is the action setting of the IPC when the alarm is triggered. IPC has different alarm types according to different models. Take the 3516dv300 AI camera (v12.45.6.0, equipped with product models supporting white light PIR function) as an example. The alarm types include motion, PIR, I / O, intelligent - > PID, intelligent - > LCD, intelligent - > PD & VD, intelligent - > FD, intelligent - > sound detection, intelligent - > occlusion detection, etc. When the camera detects the corresponding alarm event and generates the corresponding alarm signal, the camera itself will make operations such as recording, capture uploading, alarm output, etc. according to the alarm settings.

7.1 Motion

When camera has motion alarm, the corresponding alarm operation of the camera is shown in picture 7-1.

Picture 7-1 motion setting menu

- **Latch Time:** The camera that supports the IO alarm function has this page. When the camera triggers the motion alarm, the IO alarm output time.

- **Post Recording:** When the camera triggers the motion alarm, the duration of the alarm recording.

- **Alarm Out:** The camera that supports the IO alarm function has this page. When the camera triggers the motion, whether to output the IO alarm.

- **Send Email:** When the camera triggers the motion alarm. An email will be sent to the emailed box in the system.

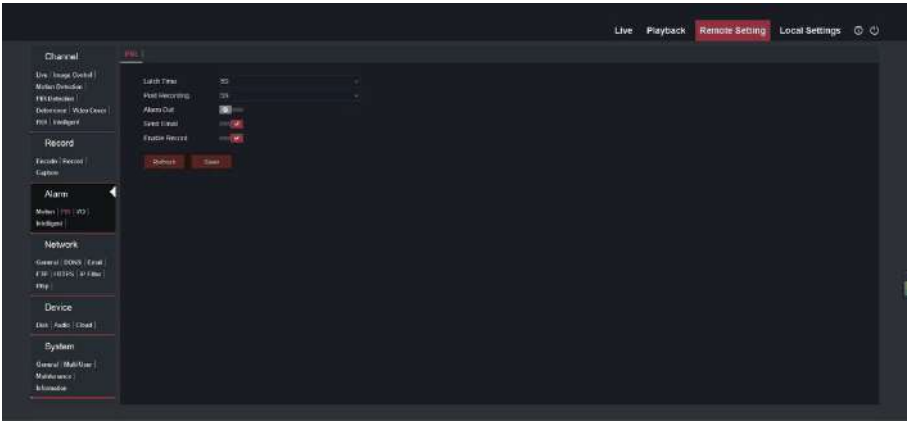
- **FTP Upload:** Whether to upload the alarm information to the FTP server when the camera triggers the motion alarm.

- **Send to Cloud:** When the camera triggers the motion alarm, whether to upload the screenshot to the FTP server.

- **Enable Record:** Whether to record when the camera triggers motion alarm.

7.2 PIR

When the camera has PIR alarm, the alarm operation of the camera is shown in picture 7-2.



Picture 7-2 PIR setting menu

- **Latch Time:** The camera that supports the IO alarm function has this page. When the camera triggers the PIR alarm, the IO alarm output time.

- **Post Recording:** When the camera triggers the PIR alarm, the duration of the alarm recording.

- **Alarm Out:** The camera that supports the IO alarm function has this page. When the camera triggers the PIR, whether to output the IO alarm.

- **Send Email:** When the camera triggers the PIR motion alarm. An email will be sent to the emailed box in the system.

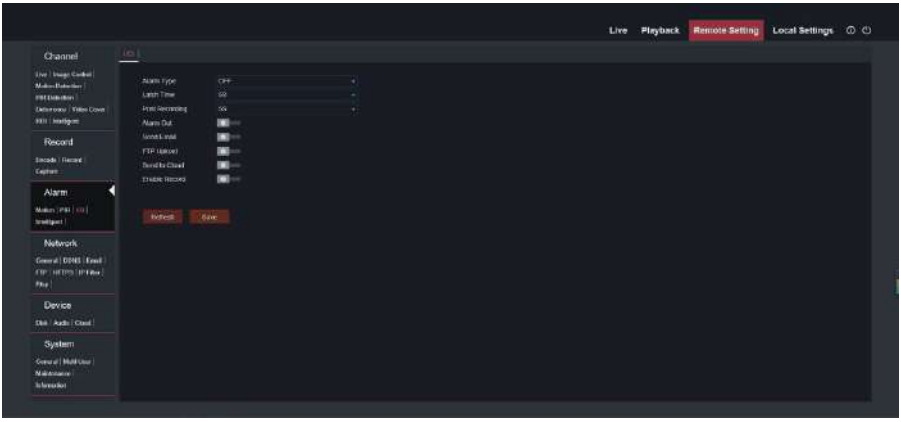
- **FTP upload:** Whether to upload the alarm information to the FTP server when the camera triggers the PIR alarm.

- **Send to Cloud:** When the camera triggers the PIR alarm, whether to upload the screenshot to the FTP server.

- **Enable Record:** Whether to record when the camera triggers PIR alarm.

7.3 I/O

When the camera has I/O alarm, the alarm operation of the camera is shown in picture 7-3.



Picture 7-3 I/O setting menu

- **Alarm Type:** IO alarm switch, there are 3 types.

- **Normal Open:** When camera is in the normally open mode and the external alarm equipment can form a closed circuit, the equipment will give an alarm. When the external alarm device is not connected by default, the device is in a non-alarm state.

- **Normal Close:** When the IPC is in the normally closed mode and the external alarm equipment cannot form a closed circuit, the equipment will give an alarm. That is, when the external alarm device is not connected by default, the device is in the IO alarm state.

- **OFF:** Turn off IO alarm function.

- **Latch Time:** The camera that supports the IO alarm function has this page. When the camera triggers the motion alarm, the IO alarm output time. Set I/O alarm output time (5s, 10s, 20s, 30s).

- **Post Recording:** When the camera triggers the PIR alarm, the duration of the alarm recording. After checking Enable Triggered Recording, you can set recording delay time (5S/10S/20S/30S).

- **Alarm Out:** The camera that supports the IO alarm function has this page. When the camera triggers the motion, whether to output the IO alarm.

- **Send Email:** When the camera triggers the IO alarm. An email will be sent to the emailed box in the system.

- **FTP Upload:** Whether to upload the alarm information to the FTP server when the camera triggers the IO alarm.

- **Send to Cloud:** When the camera triggers the IO alarm, whether to upload the screenshot to the FTP server.

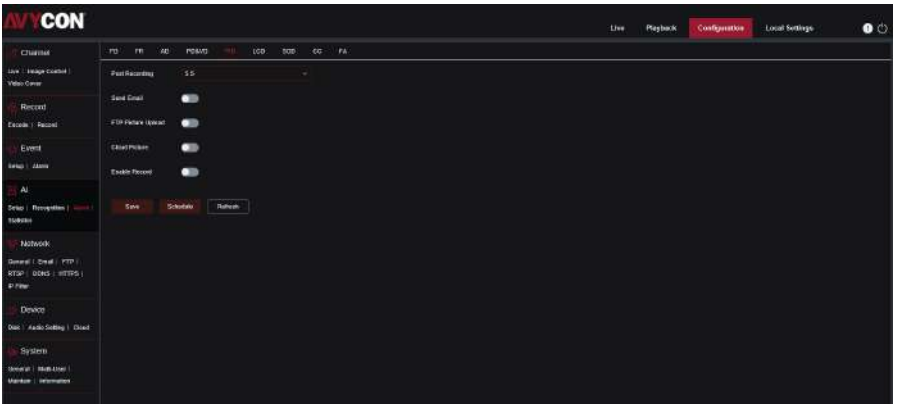
- **Enable Record:** Whether to record when the camera triggers IO alarm.

7.4 Intelligent

Intelligent analysis alarm response settings: when the camera detects the intelligent alarm, it will respond according to the corresponding settings, intelligent including PID, LCD, PD&VD, FD, sound detection, occlusion detection, and so on intelligent analysis.

7.4.1 PID

Function description: in the preview page, to detect and follow up the invaded object. When the camera detects that the moving track of the object in the picture meets the surrounding intrusion alarm detection setting (Channel - > intelligent - > PID), an intelligent alarm signal will be generated, and the camera will alarm accordingly according to the alarm setting, as shown in picture 7-4.

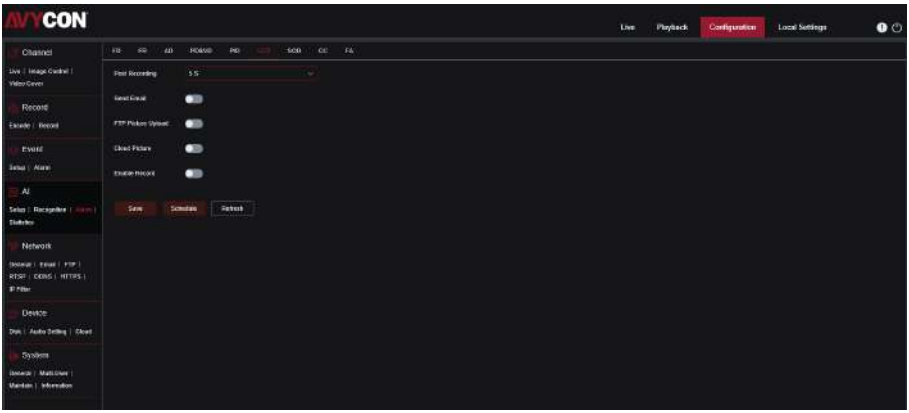


Picture 7-4 PID setting menu

- **Post Recording:** After triggered alarm, the post record time, selected time period is 5S, 10S, 20S, 30S.
- **Send Email:** If trigger alarm, send the Email to notify, the Email setup need to set in Remote Setting –> Network-Email
- **FTP Picture Upload:** Whether to transfer files to another device.
- **Cloud Picture:** Whether to transfer files to the cloud server.
- **Enable Record:** Whether to record when triggering alarm.

7.4.2 LCD

When the camera detects that the object motion track in the screen meets the out of range alarm detection setting (Channel - > intelligent - > LCD), an intelligent alarm signal will be generated. The camera will alarm accordingly according to the alarm setting, and the interface is shown in picture 7-5.

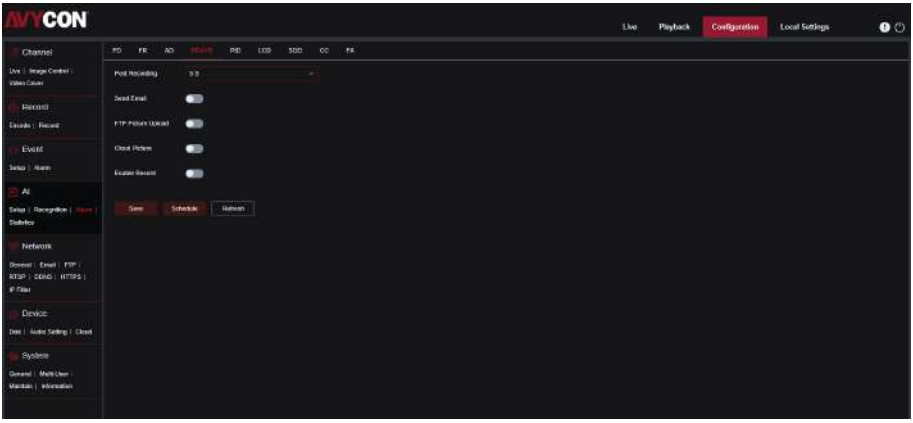


Picture 7-5 LCD setting menu

- **Post Recording:** After triggered alarm, the post record time, selected time period is 5S, 10S, 20S, 30S.
- **Send Email:** If trigger alarm, send the Email to notify, the Email setup need to set in Remote Setting –> Network-Email
- **FTP Picture Upload:** Whether to transfer files to another device.
- **Cloud Picture:** Whether to transfer files to the cloud server.
- **Enable Record:** Whether to record when triggering alarm.

7.4.3 PD&VD

When the camera detects that the object in the picture is a human or vehicle and meets the alarm detection setting of the humanoid (Channel - > intelligent - > PD & VD), an intelligent alarm signal will be generated. The camera will alarm accordingly according to the alarm setting, and the interface is shown in picture 7-6.

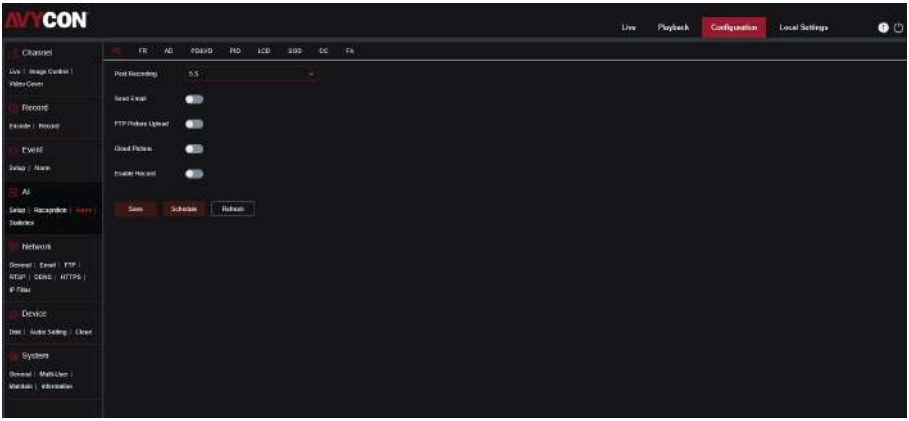


Picture 7-6 PD&VD setting menu

- **Post Recording:** After triggered alarm, the post record time, selected time period is 5S, 10S, 20S, 30S.
- **Send Email:** If trigger alarm, send the Email to notify, the Email setup need to set in Remote Setting –> Network-Email
- **FTP Picture Upload:** Whether to transfer files to another device.
- **Cloud Picture:** Whether to transfer files to the cloud server.
- **Enable Record:** Whether to record when triggering alarm.

7.4.4 FD

Face detection alarm response setting. When the camera detects that the object in the recording is a human being, and obtains its facial features, and this meets the alarm detection setting (channel-> intelligent-> PD & VD), an intelligent alarm signal will be generated. The camera responds to the alarm according to the alarm settings, as shown in Picture 7-7.

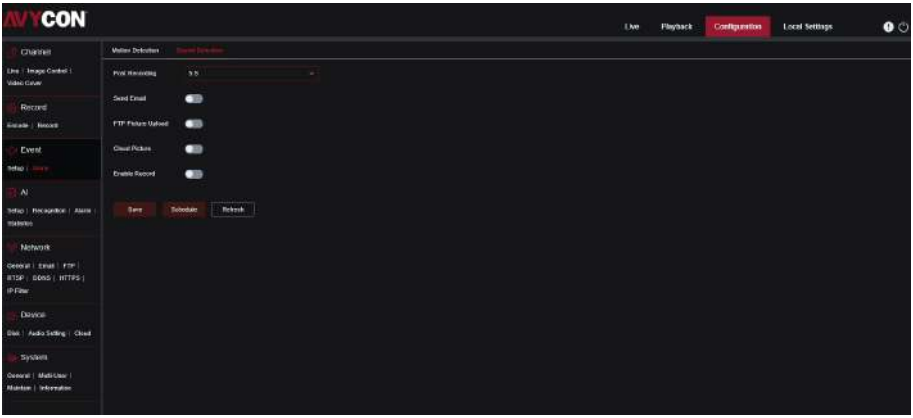


Picture 7-7 FD setting interface

- **Post Recording:** After triggered alarm, the post record time, selected time period is 5S, 10S, 20S, 30S.
- **Send Email:** If trigger alarm, send the Email to notify, the Email setup need to set in Remote Setting –> Network-Email
- **FTP Picture Upload:** Whether to transfer files to another device.
- **Cloud Picture:** Whether to transfer files to the cloud server.
- **Enable Record:** Whether to record when triggering alarm.

7.4.5 Sound Detection

Sound detection alarm response setting. When the camera detects that the connected audio sound changes to meet the requirement of alarm detection setting (channel-> intelligent-> Sound Detection), an intelligent alarm signal will be generated. The camera will alarm according to the alarm setting. The interface is as follows: Picture 7-8

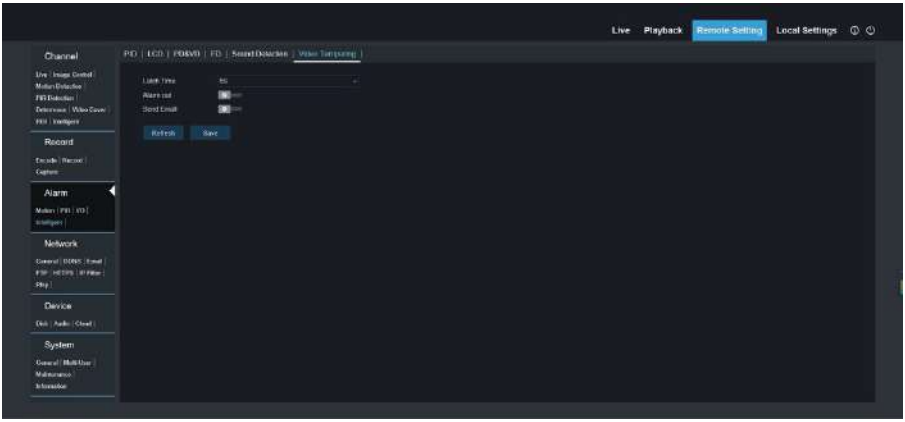


Picture 7-8 Sound Detection setting interface.

- **Post Recording:** After triggered alarm, the post record time, selected time period is 5S, 10S, 20S, 30S.
- **Send Email:** If trigger alarm, send the Email to notify, the Email setup need to set in Remote Setting –> Network-Email
- **FTP Picture Upload:** Whether to transfer files to another device.
- **Cloud Picture:** Whether to transfer files to the cloud server.
- **Enable Record:** Whether to record when triggering alarm.

7.4.6 Video Tampering

Video Tampering detection alarm response setting. When the camera detects that the object is blocking the lens and the blocking area exceeds the alarm trigger limit (channel-> intelligent-> Occlusion Detection), an intelligent alarm signal will be generated at this moment. The interface is shown in Picture 7-9.



Picture 7-9 Occlusion Detection setting interface

- **Latch Time:** This setting is provided for cameras that support IO alarm function. When the camera triggers Occlusion Detection alarm, the time of IO alarm output.

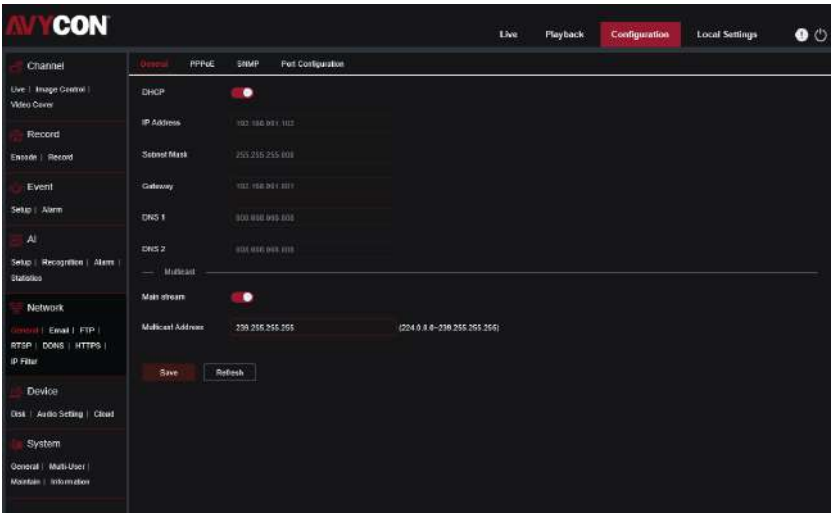
- **Alarm Out:** This setting is provided for cameras that support the IO alarm function. Whether to output IO alarms when the camera triggers Occlusion Detection.

- **Send Email:** When the camera triggers Occlusion Detection alarm, whether to add the alarm record to email.

8.1 General

8.1.1 General

Click the [General]->[General] column under the [Network] menu. The [General] screen shown in Picture 8-1 appears.



Picture 8-1 General interface

- **DHCP:** DHCP is turned on by default (automatic acquisition).

  ① **Static (Disable DHCP):** manually set the IP address, subnet mask, and gateway. After clicking the "Save" button, the IP and other information are successfully modified. At this time, the modified IP address needs to be logged in to access the device normally.

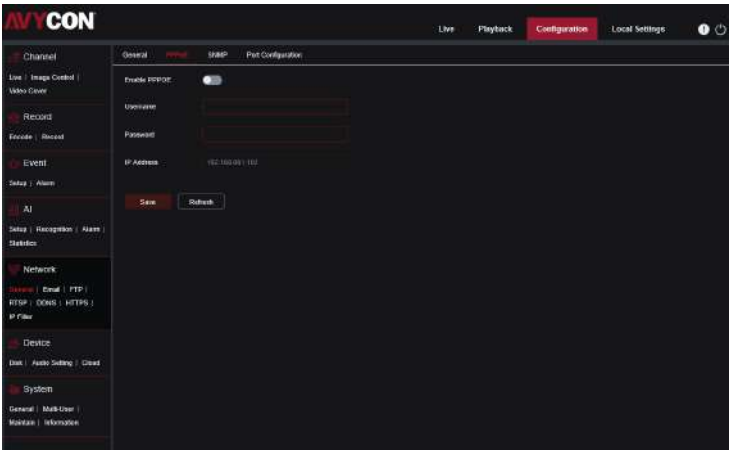
  ② **DHCP (Enable DHCP):** Obtain an IP address automatically. When DHCP is enabled, the IP address, subnet mask, default gateway, and DNS cannot be set.

- **IP Address:** IP address of IPC
- **Subnet Mask:** Subnet mast of IPC
- **Gateway:** Default gateway of the device , The gateway must be on the same network segment as the IP address.
- **DNS1 (Preferred DNS server):** DNS server IP address.
- **DNS2(Backup DNS server):** NS server backup IP address.
- **Multicast (Multicast - communication between one sender and multiple recipients)**: Set the multicast button on or off (the device supports multicasting to be discovered by devices in the network, but when the device is unable to do so due to multicast storms In normal use, you can try to turn off the multicast search function to solve the problem).
- **Multicast Address:** Multicast Address setting , address arrange is (224.0.0.0 —239.255.255.255).

After modifying the parameters, click the "Save" button to save the settings.

8.1.2 PPPOE (Point-to-Point Protocol Over Ethernet)

Click【Network】—>【General】—>【PPPOE】, shows the Pic 8-2【PPPOE】interface:



Picture 8-2 PPPOE interface

- **Enable PPPOE:** Enable or disable PPPOE dialing.
- **Username:** Username of PPPOE.
- **Password:** Password of PPPOE.
- **IP Address:** After PPPOE dialing is successful, the dialed IP address will be displayed (IP address cannot be modified).
- **Subnet Mask:** Subnet mask of IP CAMERA (subnet mask can't be modified).
- **Gateway:** Default gateway of device. (gateway can't be modified).
- **DNS1 (Preferred DNS server):** DNS server IP address (Preferred DNS server can't be modified)
- **DNS2 (Backup DNS server):** DNS server backup IP address.

The point-to-point protocol on Ethernet is a network tunneling protocol that encapsulates the point-to-point protocol (PPP) in the Ethernet framework. Because the protocol integrates the PPP protocol, it realizes authentication, encryption, and compression functions that traditional Ethernet cannot

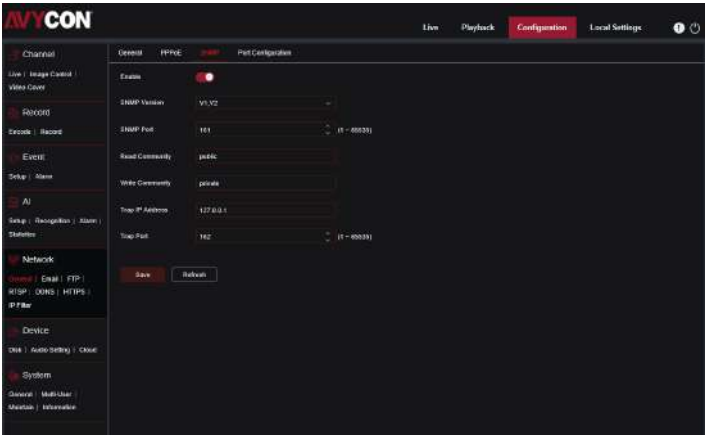
provide. It can also be used for cable modems and digital subscriber lines (DSL) to provide users with Ethernet protocols. Protocol system for access services.

After the PPPOE configuration is complete, click Save and restart the IP camera. The device will obtain a public IP address, which can be used to access the IP camera.

After modifying the parameters, click the "Save" button to save the settings.

8.1.3 SNMP

Click【Network】->【General】->【SNMP】column, shows Pic 7-3, 7-4【SNMP】interface:



Picture 8-3 SNMP (V1, V2, V1, V2) interface

- **Enable:** enable or disable SNMP function.
- **SNMP Version:** Device program processing selects the corresponding version information (there are V1, V2, V1, V2, V3), choose SNMP protocol version V1, V2 or V1, V2, Pic 8-3 shows.
- **SNMP Port:** Device agent listening port (it's 161).
- **Read Community:** Read community string that the agent supports.
- **Write Community:** Represents a write community string supported by the agent.

- **Trap IP Address:** Represents the destination address of the trap messages sent by the agent on the device.

- **Trap Port:** Indicates the destination port (162) of the trap message sent by the agent on the device.

  After modifying the parameters, click the "Save" button to save the settings.

- **SNMP Version:** When the SNMP protocol version is V3, as shown in Figure 7-4, you can set the account, password, and authentication mode. When the server accesses the device, you must set the corresponding account, password, and authentication mode for security verification, and V1 V2 version is not optional.

- **Read-Only User Name:** default as authOnlyUser.

- **Authentication Type:** it can be chose MD5 or SHA. Default as MD5.

- **Authentication Password:** The length of password is lower than 8 characters.

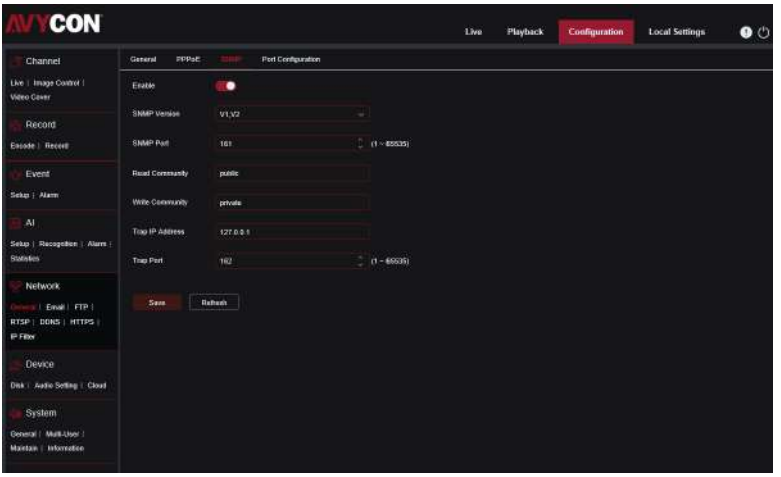
- **Encrypted Type:** Default as CBC-DES.

- **Encrypted Password:** The length of password is lower than 8 characters.

- **Read/Write User Name:** default as authPrivUser

Simple Network Management Protocol (SNMP) is a standard protocol specifically designed to manage network nodes (servers, workstations, routers, switches, HUBS, etc.) in an IP network. It is an application layer protocol. SNMP enables network administrators to manage network performance, identify and resolve network problems, and plan for network growth. Receive random messages (and event reports) via SNMP. Network management system learns about network problems.

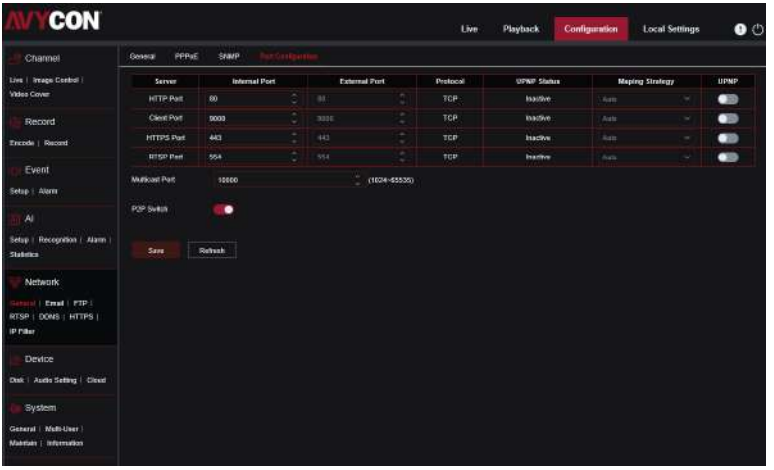
After modifying the parameters, click the "Save" button to save the settings.



Picture 8-4 SNMP (V3) interface

8.1.4 Port Configuration

Click【Network】--【General】—>【Port Configuration】column, shows Pic 7-5【Port Configuration】interface:



Picture 8-5 Port Configuration

- **HTTP Port:** HTTP communication port. The default is 80. The recommended setting range is 1024 ~ 65535.
- **Client Port:** Media communication port. The default is 9000. The recommended setting range is 1024~65535.
- **RTSP Port:** RTSP default is 554. The recommended setting range is 1024~65535.
- **HTTPS Port:** HTTPS communication port. The default is 443. The recommended setting range is 1024~65535.
- **Multicast Port:** The default is 10000. The recommended setting range is 1024~65535.
- **UPNP (Universal Plug and Play):** Enable or disable port forwarding. Routers map ports to allow IPCs to connect to the Internet for data sharing.
- **Mapping Strategy:** Auto, manual are optional.
- **Client External Port:** Automatic or manual port settings, which ranges from 1024~65535.
- **HTTP External Port:** Automatic or manual port settings, which ranges from 1024~65535.
- **RTSP External Port:** Automatic or manual port settings, which ranges from 1024~65535.
- **HTTPS External Port:** Automatic or manual port settings, which ranges from 1024~65535.

Port mapping methods are divided into automatic and manual. Enable UPNP and select the automatic mode, users do not need to do port mapping on the router, just enable the UPNP function on the router to achieve port opening; if you choose the manual mode, users need to fill in the mapped port number and enable UPNP on the router Function, the port can be opened. At this time, there is no need to modify the port of the device itself.

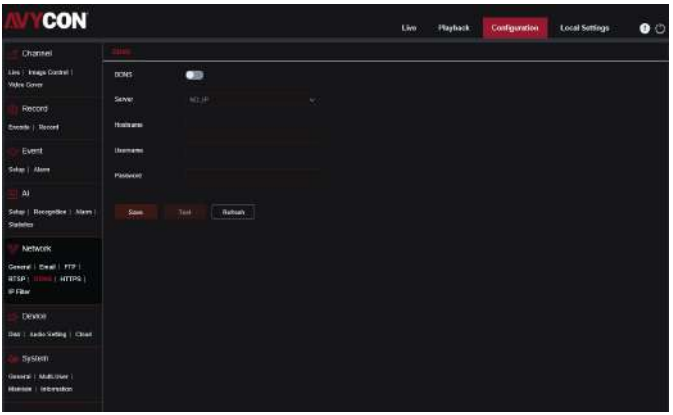
- **Latch Time:** Turn on/off the two-dimensional code sequence and column number switches. The two-dimensional code and serial number of the device can be displayed on the Information interface, which is used to access devices such as Netview and mobile APP.

After modifying the parameters, click the "Save" button to save the settings.

8.2 DDNS (Dynamic Domain Name Server)

Click【Network】--【DDNS】, shows Pic 8-6【DDNS】interface:

DDNS configuration: Dynamic DNS configuration - used with server for access from an extranet.



Picture 8-6 DDNS interface

DDNS: Enable or disable DDNS

Server: 3322, DYNDNS, NO-IP are optional

Hostname: Enter domain address

Username: name of the user

Password: password of the user.

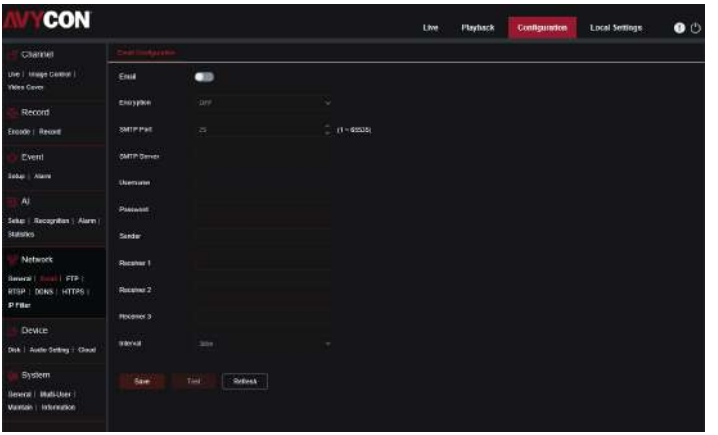
- **DDNS test:** Click the Test DDNS button to test whether the DDNS configuration is correct and whether the DNS server is connected.
  - In the public network environment, most users use dynamic IP addresses and use DDNS (Dynamic Domain Name Resolution) to access network cameras, which can effectively solve the problem of network camera public network access.
  - The DDNS function must be set to the correct IP address, mask, gateway,

and DNS server, and the Internet can be accessed in this configuration.

After modifying the parameters, click the "Save" button to save the settings.

8.3 E-Mail Configuration

Click【Network】--【Email】column, shows Pic 8-7【Email】interface:



Picture 8-7 Email

Email: Enable or disable Email service.

Encryption: Disable /SST/TLS/AUTO four option.

SMTP Port: Default as 25

SMTP Server: Enter the email server address.

Username: Sending email address.

Password: Password of the sending email.

Sender: Email address.

Receiver: Receiver email address. Maximum 3 email addresses.

Interval: Select the time interval to send the message (1 min, 3 min, 5 min, 10 min).

Email Test: After the email configuration is correct, click the Test Email button, it will

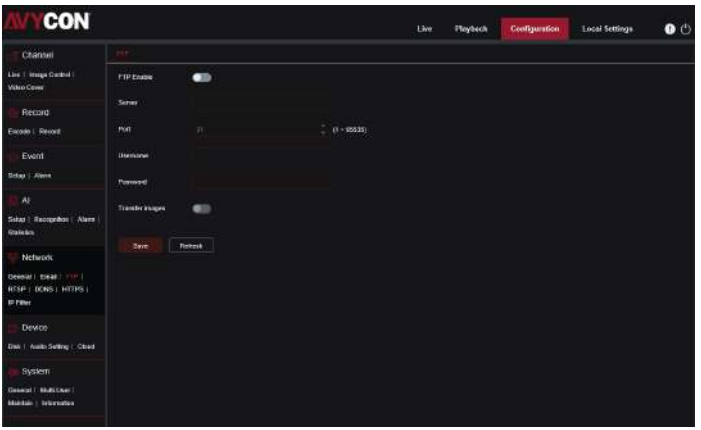
prompt the mail test successfully, and you can receive a test email.

After setting the email information and enabling the alarm linkage email function, the system will automatically send an email to notify the user when a corresponding alarm event occurs on the device (at the same time upload the captured snapshot image to the email server).

After modifying the parameters, click the "Save" button to save the settings.

8.4 FTP

Click【Network】--【FTP】column, shows Pic 8-8【FTP】interface:



Picture 8-8 FTP interface

FTP Enable: Enable or Disable FTP upload server.

Server: Enter the FTP server address.

Port: FTP server port, default as 21.

Username: User name for accessing the FTP server.

Password: Password for accessing the FTP server.

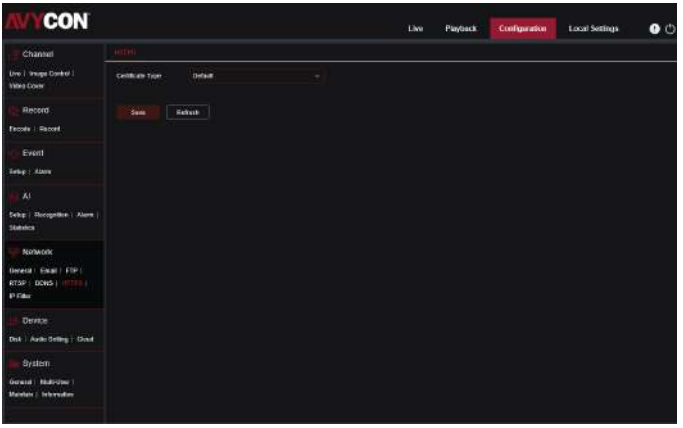
Transfer images: Enable or disable transfer images.

FTP is a standard protocol for transferring files over a network. The goal is to increase file sharing, provide indirect access to remote computers, and make the storage media transparent to users, reliable and efficient in transmitting data. By configuring FTP parameters can control the two-way transfer of files on the Internet, so that the network camera capture file can be set on the FTP server.

After modifying the parameters, click the "Save" button to save the settings.

8.5 HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer)

Click【Network】--【HTTPS】column, shows Pic 8-9【HTTPS】interface:



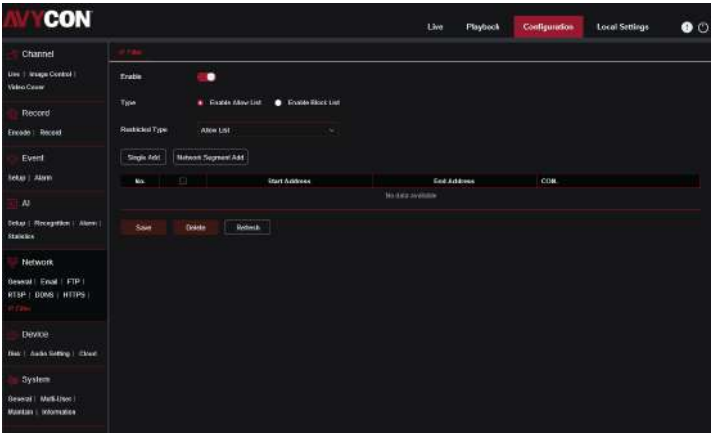
Picture 8-9 HTTPS interface

- **HTTPS:** Secure Socket Hypertext Transfer Protocol, HTTPS protocol is a network protocol built with SSL + HTTP protocol that can perform encrypted transmission and identity authentication, improving the security of WEB access. When using it, you must apply for a certificate from a CA (Certificate Authority). The application for an encryption certificate is generally a fee; there are 2 default and custom options for the certificate type. Users can select and install or uninstall the corresponding certificate according to their needs.

After modifying the parameters, click the "Save" button to save the settings.

8.6 IP Filter

Click【Network】--【IP Fitter】column, shows Pic 8-10【IP Fitter】interface:



Picture 8-10 IP Filter interface

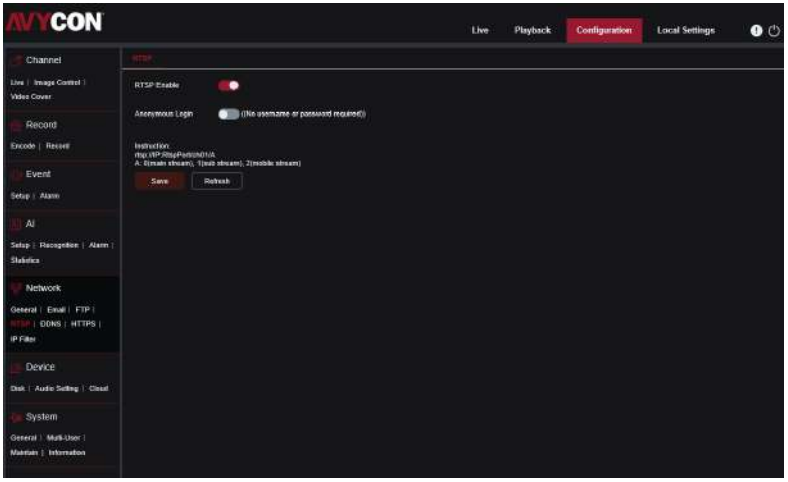
- **Enable:** Enable or disable whitelist and blacklist. Note: Only one list can be opened at the same time. Turning off this function allows all IP connections.
- **Enable Allow List:** Only IP connections on the list are allowed to access the device.
- **Enable Block List:** Deny access to the device from the IP list on the list.
- **Restricted Type:** Added whitelist or blacklist (if whitelist is enabled, select the whitelist as the restriction type; if blacklist is enabled, select the blacklist as the display type; the IP restriction will only take effect if this setting is set.
- **Start Address:** Black / white list starting IP address.
- **End Address:** Black / white list end IP address.
- **Single Add:** You can add a single IP address; click this button, the starting IP address of the black / white list added here is the same IP address.
- **Network Segment Add:** You can add a segment of IP address, click this button, the correct starting address must be filled in here, the starting address is inconsistent, and the ending address must be larger than the starting address to take effect.

The actual scenario of IP Fitter is to allow or disallow others to access the device, which has reached the effect of limiting the number of accesses and security.

After modifying the parameters, click the "Save" button to save the settings.

8.7 RTSP

Click【Network】--【RTSP】column, shows Pic 8-11【RTSP】interface:



Picture 8-11 RTSP interface

RTSP Enable: Enable or disable RTSP.

Anonymous Login: Enable or disable anonymous.

Instruction for Use: rtsp: //IP:RTSP port/ch01/A.
A:0 (MainStream), 1 (SubStream), 2 (MobileStream).

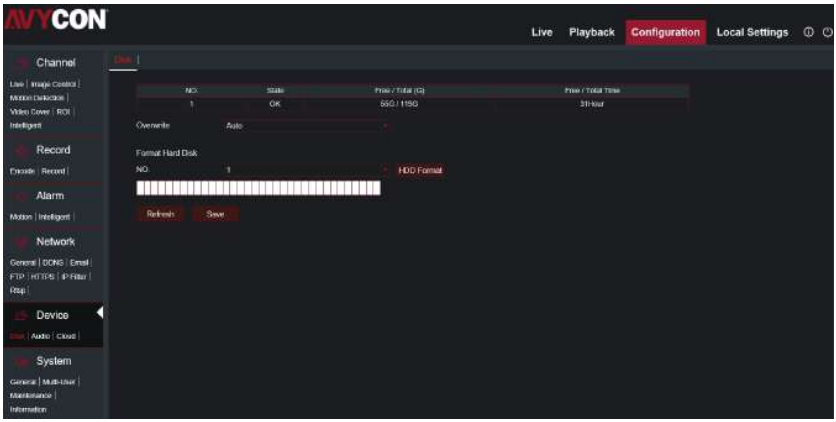
RTSP is an application-level protocol that controls the sending of real-time data. With VLC Media Player, the device can be accessed in real time via the above address.

After modifying the parameters, click the "Save" button to save the settings.

It includes Disk, Audio and Cloud. Their interfaces and functions are described below.

9.1 Disk

Click【Device】--【Disk】column, shows Pic 9-1【Disk】interface:



Picture 9-1 Disk interface

Since the device here is an IP Camera, the hard disk displayed on this interface is an SD card.

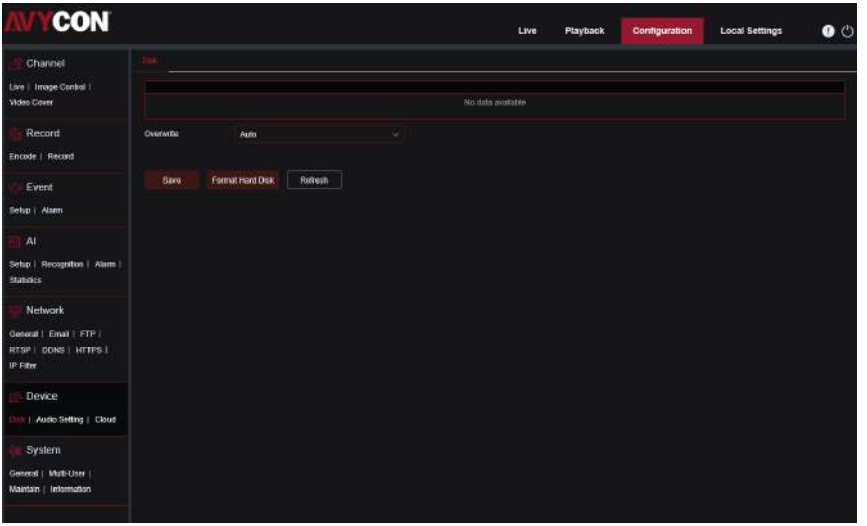
This interface can display hard disk card information: State, remaining capacity, total capacity (Free / Total), and remaining available time / total available time (Free / Total).

- **Overwrite:** Instead of defaulting to Auto, auto-rewrite; if the device is in the recording period and the remaining capacity of the hard disk is 0, the previous recording will be gradually cleared, and the device continues to record backwards.

  Select Close to close the reproduction; if the device is in the recording period and the remaining hard disk capacity is 0, the recording will not continue.

- **Format Hard Disk:** Click the HDD Format button to pop up the username and password input box, fill in the username and password of the device, and then format the hard disk.

- **Add NetHDD (NAS--Network Attached Storage):** It is generally used to store data with hard disks and SD. The difference is that it uses the network transmission to achieve the storage function (some models support, please refer to the actual product). This is shown in Pic 9-2:

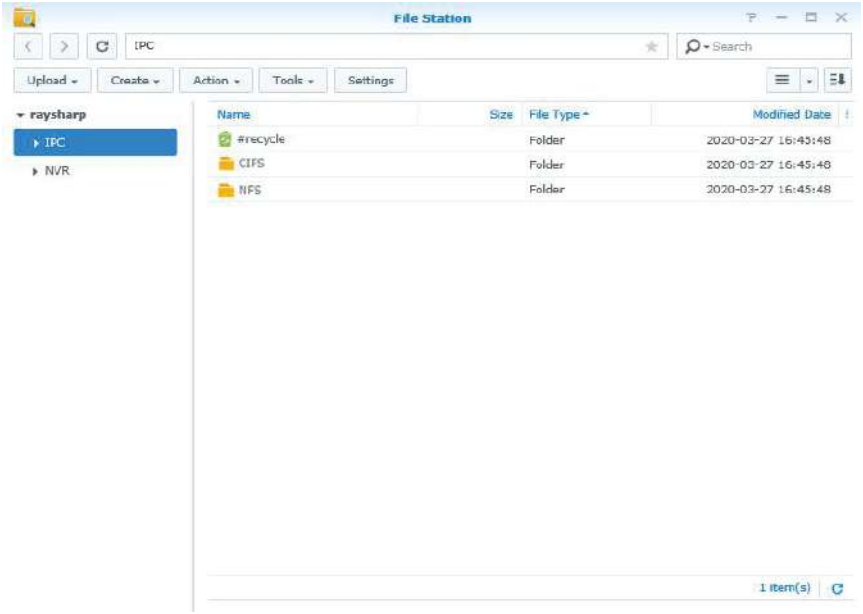


Picture 9-2 Add NetHDD

NAS testing method:

① Create a directory in NAS's IE (there are 2 types: NFS and CIFS) as shown in Pic 9-3:

② IPC supporting NAS needs to burn function code: 16777216.

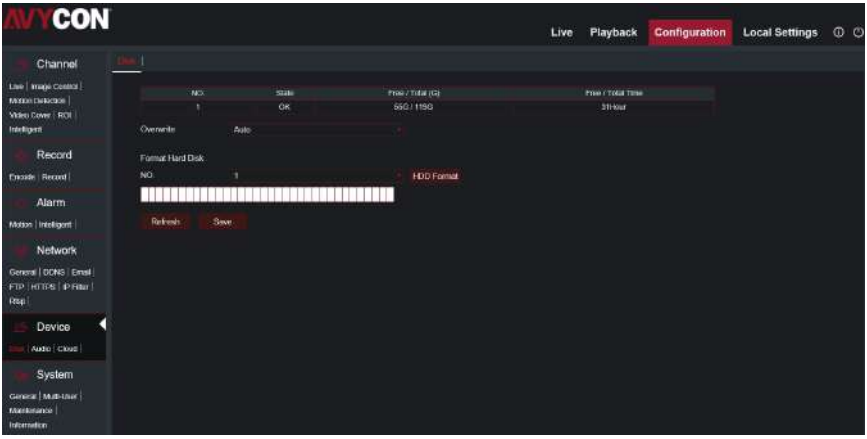


Picture 9-3 NAS interface

③ **Choose NFS:** Enter the IP address of the NAS, the path where you want to save the video (such as: / volume1 / ipc / test), and the size of the hard disk.

④ **Choose NFS:** Enter the user name of NAS(admin), password, IP address, the path for storing videos of NAS (such as:/ipc/test (no prefix required:/volume1)) and the size of the hard disk.

⑤ After filling it out, click Test to show that the test was successful, then click Add, and then format to start recording as shown in Pic 9-4:



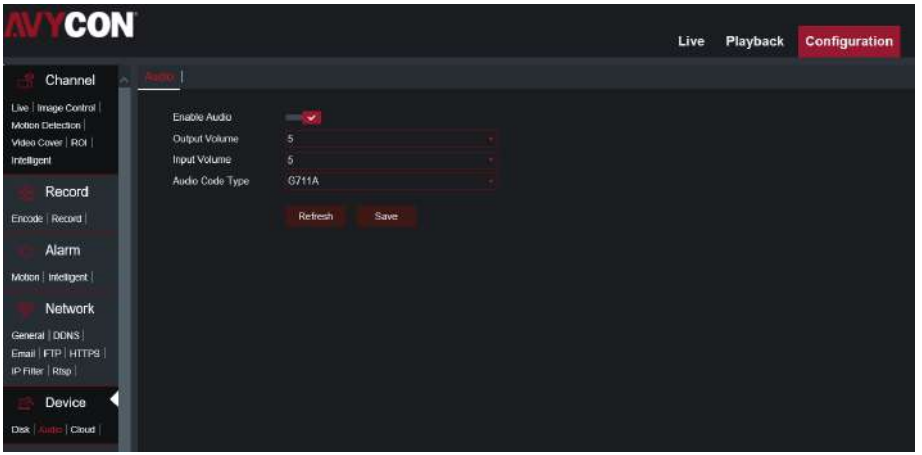
Picture 9-4 HDD Format

The setting of the Disk interface is to more easily understand the size of the storage space /remaining space. It is convenient to observe how large the stream value used to store the video will affect the storage time, so adjust the stream value to adjust the storage time; or use The overwrite function has achieved the effect of continuous recording.

After modifying the parameters, click the "Save" button to save the settings.

9.2 Audio

Click【Device】--【Audio】column, shows Pic 9-5【Audio】interface:



Picture 9-5 Audio interface

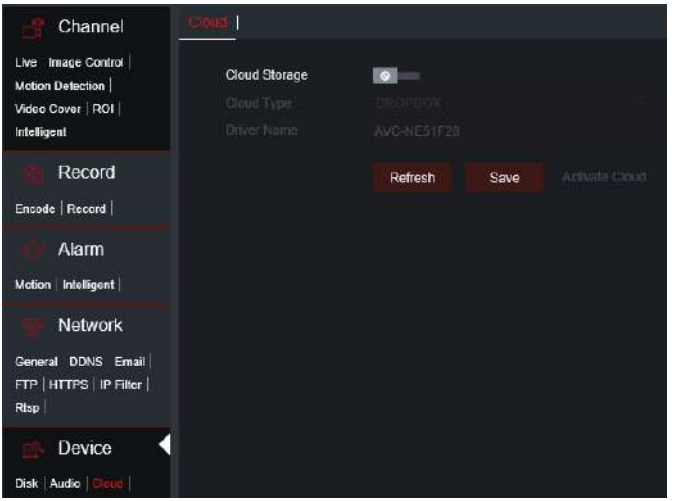
- **Enable Audio:** Enable or disable Audio.
- **Output Volume:** Default as 5; 0~10 are optional.
- **Input Volume:** Default as 5; 0~10 are optional.
- **Audio Code Type:** Default as G711A; G711A, G711U, ADPCM, G726 16K, G726 24K, G726 32K, G726 40K are optional.

The setting of the Audio interface is to select a suitable audio encoding type, and to adjust the input and output volume value, to achieve better input sound at the input end, and to hear the sound more clearly at the output end without generating a clamor.

After modifying the parameters, click the "Save" button to save the settings.

9.3 Cloud

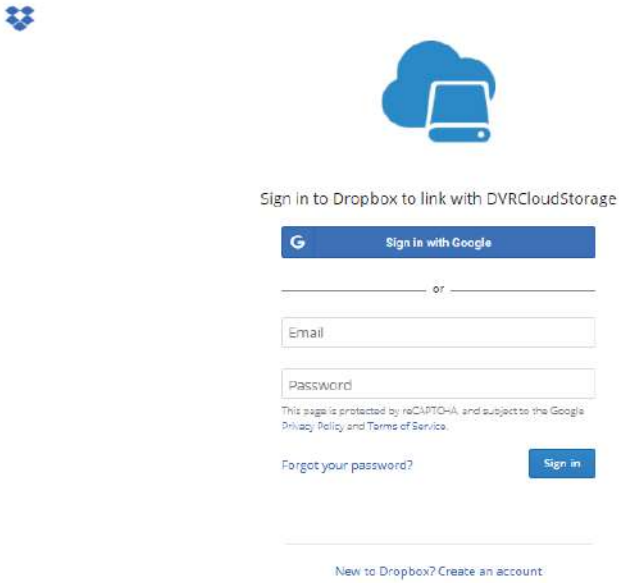
Click【Device】--【Cloud】column, shows Pic 9-6【Cloud】interface:



Picture 9-6 Cloud interface

- **Cloud Storage:** Default is off; turn cloud storage on or off.
- **Cloud Type:** Default and only Dropbox.
- **Driver Name:** Default as IP Camera; free to customize the name.

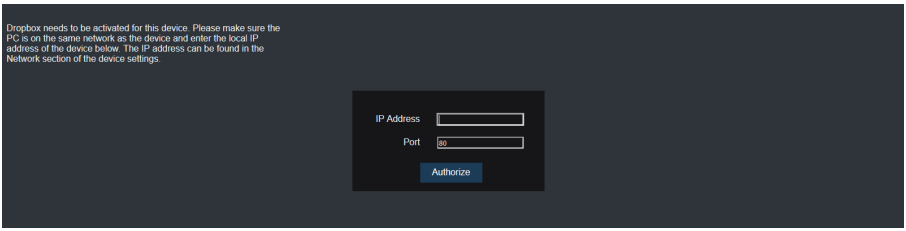
After the parameters are saved successfully, click the Activate Cloud button to jump to the Dropbox login interface as shown in pic 9-7:



Picture 9-7 Dropbox login interface

If you do not have a Dropbox account, please create a Dropbox account before logging in, or use a Google account to log in to Dropbox directly; if you have a Dropbox account, you can enter the corresponding account password to log in to Dropbox.

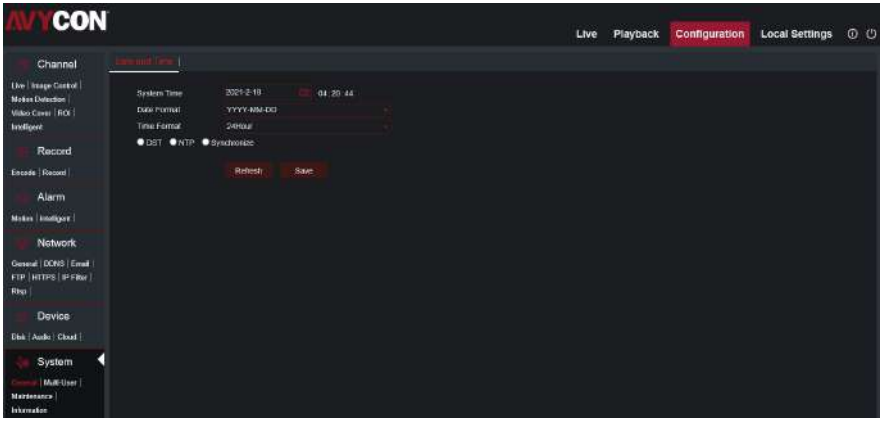
When you log in to Dropbox, an input box for the device IP address and port number will pop up, as shown in Figure 9-8. Enter the device's IP address and port here to enter Dropbox successfully. At this time, the alarm is triggered, and the folder of the corresponding device is found (the folder name is Driver Name). There are images captured in the folder when the alarm is triggered.



Picture 9-8 IP address and port interface

10.1 General

Click【System】-- 【General】column, shows Pic 10-1【Date and Time】interface:



Picture 10-1 General interface

The device time, system time, date format and time format contained in the basic information can be manually set and saved.

Three automatic time correction functions are provided in this device:

- **System Time:** Click to select the calendar or the time to the right of the calendar to manually modify the current time of the device.

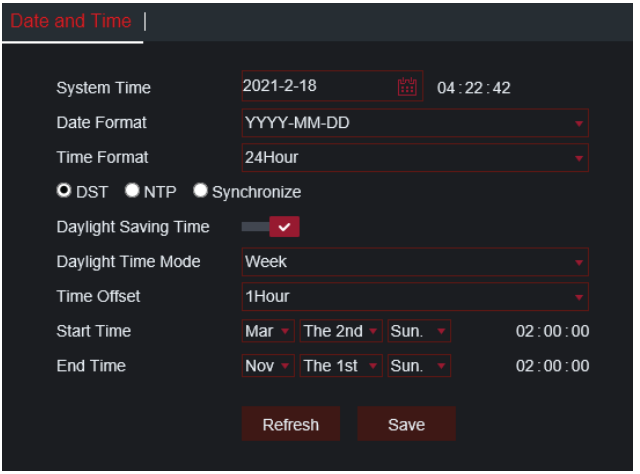
- **Date Format:** Click the drop-down box to select the date format. There are MM/DD/YYYY, YYYY-MM-DD、DD/MM/YYYY.

- **Time Format:** Click the drop-down box to select the time format. There 12Hour and 24Hour.

In addition, three automatic time adjustment functions are provided:

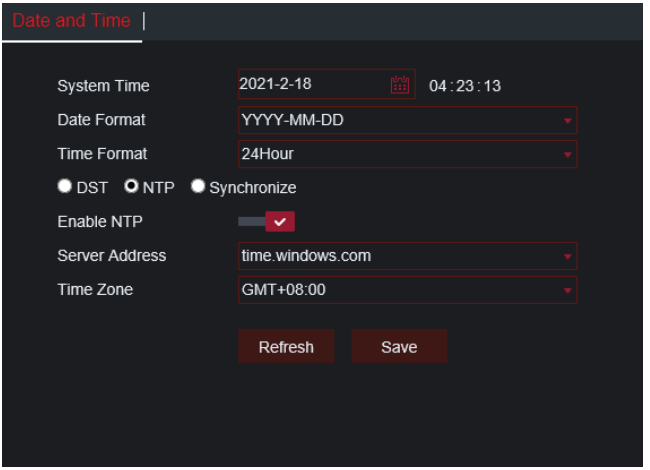
1. DST: Check Daylight Savings Time (DST) option to enable DST correction. The device will correct the time based on the time deviation as set. In Picture 10-2, This setting is to artificially adjust the time by one hour in the early summer, so that

people can get up early and go to bed early, reduce the amount of lighting, and make full use of lighting resources, thereby saving lighting electricity.



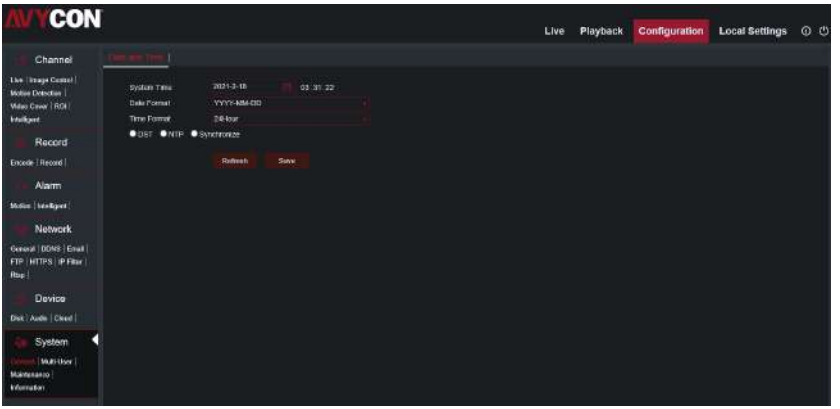
Picture 10-2 DST interface

2. NTP: Check Enable NTP option, input the address of time server and choose a time zone and then save the setting. The system will correct time in accordance with the time server. The NTP interface setting interface is shown in Picture 10-3. NTP is a protocol used to synchronize computer time and can provide high-accuracy time correction.



Picture 10-3 NTP interface

3. Synchronize: Shows Picture 10-4, The device will use PC as a time server to correct time.

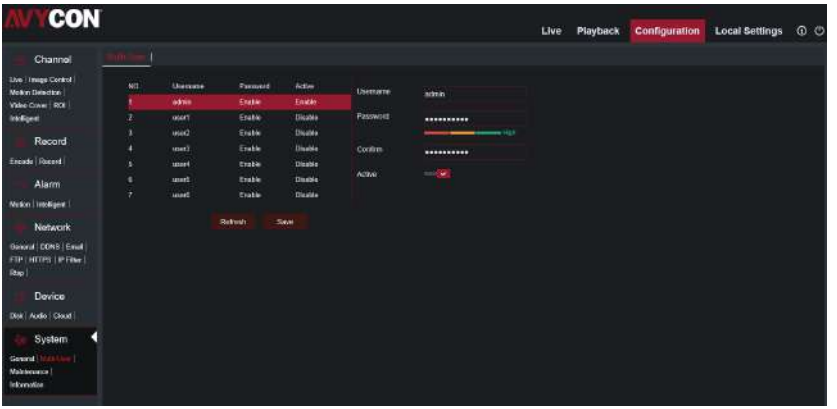


Picture 10-4 Synchronize interface

After modifying the parameters, click the "Save" button to save the settings.

10.2 Multi-User

Click on Multi-User in System Parameters menu to open the following page:



Picture 10-5 Multi User interface

Here you can set user access authority and login password. The current user is the main user "admin". The user can modify the main user information and set sub-users as required. A maximum of 6 sub-users can be set.

- **Main User Information:** The user name and password of the master user can be modified; the Active control is a function permission activation control. In the main user interface, the control is forced to open and cannot be modified to ensure

- **Sub User Information:** The user name and password of the main user can be modified, as well as the permission to activate some functions of the sub-user; Active controls are turned off by default; the sub-users can open the functions of Parameter (Parameter Setting), Live (Preview), Playback (Playback), PTZ Control (PTZ Control) And RTSP (Real-time Streaming Protocol).

- **User Name Setting Rules:** The user name cannot be empty, the length is 1 to 8 characters, and can be alphanumeric and some special characters (such as. @ #, Etc.).

- **Password Setting Rules:** The default password is 5 digits, but the password must be 8 to 15 digits. If the password length is set to 8 to 9 digits, 3 types (numbers, letters, special characters) are required; if the password length is set to 10 to 15 digits, at least two types are required.

- **Password strength rule:**

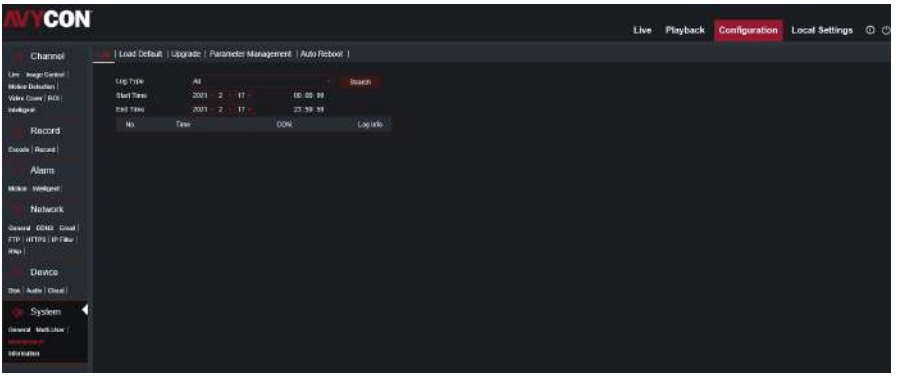
  Password is less than 8 characters long (the password is 5 alphanumeric characters by default), which is a weak password; Password length is 8 ~ 15 digits: if the password contains 2 types, it is a medium password; Password length is 8 ~ 15 digits. If the password contains 3 types, it is a strong password.

  After modifying the parameters, click the "Save" button to save the settings.

10.3 Maintain

10.3.1 Log

Click【System】--【Maintenance】column, shows Pic 10-6【Log】interface:



Picture 10-6 Log interface

- **Log Type:** Eight types of logs are available - system logs, network logs, parameter logs, alarm logs, user logs, recording logs, storage logs and all logs). Choose the starting and ending date/time for retrieval.
- **Minor Type:** If the log type is selected other than All, a minor log type selection will appear; select the type of query you want.
- **Search:** Click on "Search" to retrieve and display related logs in the table below.
- **Scan:** Click the Scan button and select the path to export the logs; or enter the path manually in the Path field.
- **Refresh:** Click on "Refresh" to refresh the logs selected.
- **Name:** Manually enter the file name of the log to be exported.
- **Export:** An Excel file of .xlsx will be exported to view the queried log.
- **Start Time:** Select the start time of the query log (default: 00:00: 00).
- **End Time:** Select the end time of the query log (23:59:59 by default on the current day).

The log query time defaults to the current day, and the log display is up to 1000.

Note: For detailed log regulations, see the log overview at the end of the manual.

10.3.2 Load Default

Click【System】--【Maintain】—>【Load Default】column, shown in the Picture 10-7【Load Default】:

Picture 10-7 Load Default interface

Check relevant options and click on Save to recover the default factory settings for the options as checked.

Clicking the All button will select all the options, and clicking Save will restore all the parameters to their default values.

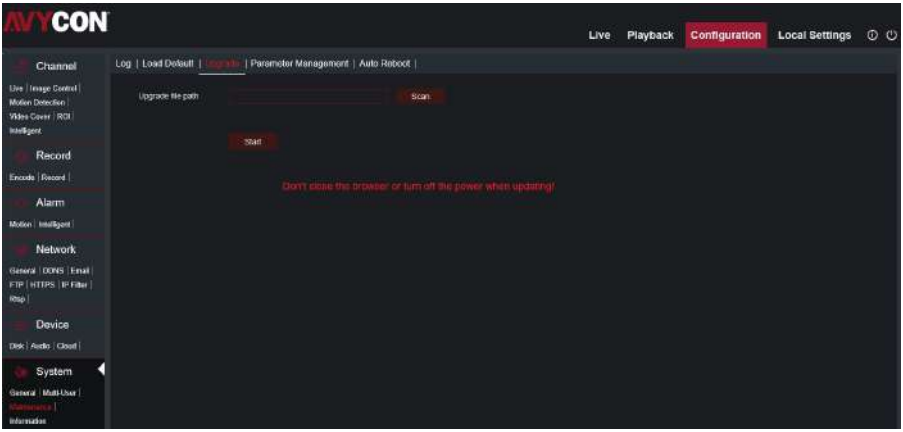
Select Network, there will be Except Network Setting Parameters (except network parameter settings that is, IP address, port number, etc.) and all. If you select Except Network Setting Parameters, parameters other than network parameter settings will be set. Restore default. If you select all, all parameters of the network will be restored to default.

Select the All option under Network and System to restore it to default and the device will restart.

After modifying the parameters, click the "Save" button to save the settings

10.3.3 Upgrade

Click【System】--【Maintain】—>【Upgrade】column, to show picture 10-8【Upgrade】interface:



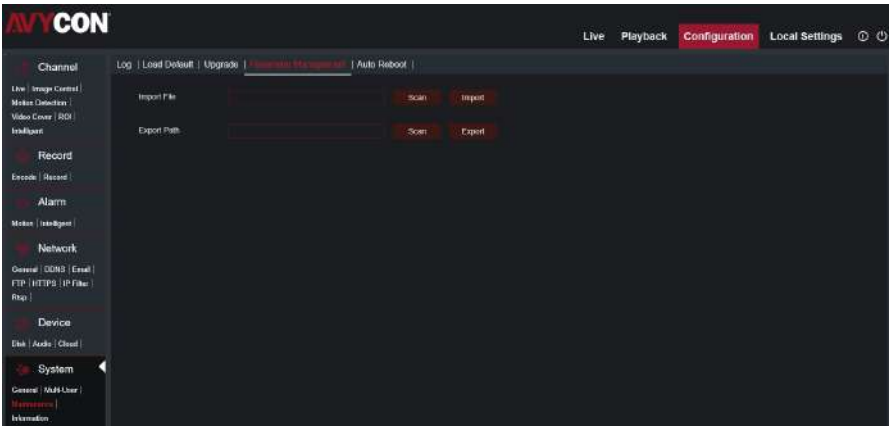
Picture 10-8 Upgrade interface

Click “Scan” choose the upgrade firmware, click “Start” and upgrade. Update will be unavailable if the update files do not match the target device.

Note: During the upgrade process, please do not close Internet Explorer or power off.

10.3.4 Parameter Management

Click【System】--【Maintenance】—>【Parameter management】column, to shows Picture 10-9【Parameter management】interface:



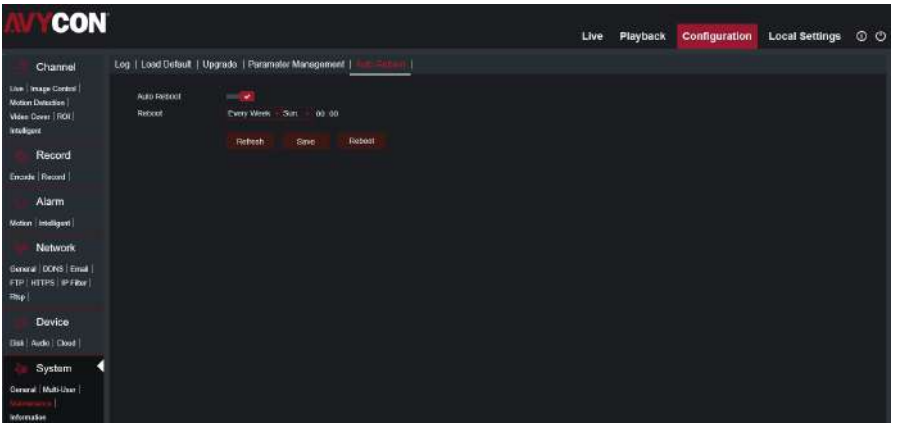
Picture 10-9 Parameter Management interface

- **Import File:** Click the Scan button, select the parameters to be imported, and click the Import button. The parameters will be imported into IP CAMERA and will take effect after restart. Note: The parameters derived from products of the same model must be available first.

- **Export File (Export parameter file path):** Click the Scan button, select the path to export the parameters, and click the Export button. The parameters will be exported to the specified path.

10.3.5 Auto Reboot

Click【System】--【Maintenance】—>【Auto reboot】column, to show Picture 10-10 【Auto reboot】interface:



Picture 10-10 Auto Reboot interface

Here you can set regular restart or manual restart of the device.

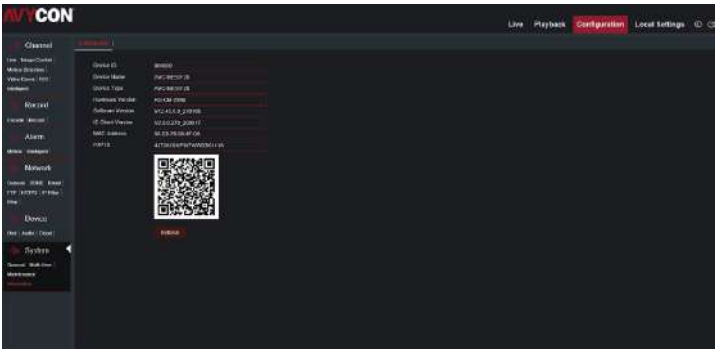
- **Auto Reboot:** Enable or disable Auto reboot function.
- **Reboot:** Restart time setting, you can restart the device on time according to three options: the day of the month, the day of the week, and the time of day.

Click the Reboot button and enter the device password to restart the device manually.

After modifying the parameters, click the "Save" button to save the settings.

10.4 Information

Click【System】--【Information】column, shows Pic 10-11【Information】interface:



Picture 10-11 Information Interface

Here some system information on the device will be displayed, including Device ID,Device Name,Device Type,Hardware Version,Software Version,IE Client Version, MAC Address, and P2P ID (You can visit mobile app or Netview through P2P QR code directly).

System Information:
Click on System Information in System Parameters menu to open the following page:

Picture 10-12 System Information interface

Here some system information on the device will be displayed, including device type, MAC address and software version.

You can visit mobile app through P2P QR code directly.

10.5 Log

10.5.1 Log Review

The log can record the time and log content of system, video, alarm, network and other key operations, which is convenient for users to query the historical operation time and status. Logs are divided into system logs, parameter logs, alarm logs, user logs, recording logs, storage logs, and network logs. Each type of log is subdivided into multiple subtypes. Users can query the logs according to different types and starting time conditions. Can be exported to .xlsx file for viewing, the log is written directly in flash memory.

10.5.2 Log Description

System logs: sub-types include system startup, system restart, system restore defaults, system upgrades, automatic system maintenance, and system time changes.

Sub type	Operation	Log content
System reboot	System setting	User name: current user Start time: The start time of the execution End time: The end time of the execution operation IP address: The IP address of the computer used to perform the operation
System reboot	System reboot	
System restore	System restore	
System upgrade	System upgrade	
System auto maintain	System maintain	
System time change	System time change	

Parameter log: subtypes include preview, video settings, video occlusion, recording parameters, recording plan, main stream, network settings, substream, Email configuration, DDNS configuration, color, motion detection, SD card, user configuration, system Maintenance, image control, RTSP, IP filtering, video occlusion, date / time, silent parameters, ROI, audio.

Sub type	Operation	Log content
Live view	Live view changes	User name: current user IP address: The IP address of the computer used to perform the operation
Video setting	Video setting changes	
Video cover	Video covert changes	
Recording Parameters	Recording parameters change	
Record schedule	Record schedule	
Mainstream	Mainstream changes	
Network setting	Network setting changes	
Sub stream	Sub stream changes	
Email configuration	Email changes	
DDNS configuration	DDNS changes	
Color	Color changes	
Motion detection	Motion detection changes	
SD card	SD card changes	
User configuration	User configuration changes	
System maintenance	System maintenance changes	

Sub type	Operation	Log content
Image control	Image control changes	User name: current user IP address: The IP address of the computer used to perform the operation
RTSP	RTSP changes	
IP filter	IP filter changes	
Video covert	Video covert changes	
Date/time	System time changes	
Default parameter	Default parameter changes	
ROI	ROI changes	
Audio	Audio changes	

Alarm log: Sub-types include motion detection alarm start, motion detection alarm end, lens block alarm start, and lens block alarm end.

Sub type	Operation	Log content
Motion detection alarm started	Motion detection alarm started	Video: Is there a video
Motion detection alarm ended	Motion detection alarm ended	
Camera blocking alarm started	Camera blocking alarm started	
Camera blocking alarm ended	Camera blocking alarm ended	

User logs: subtypes include user login, logout

Sub type	Operation	Log content
User login	Admin login successfully	User name: current user Operation user: Perform operation user IP address: The IP address of the computer used to perform the operation
User logout	Admin logout	

Video log: subtypes include video query, video playback, and video backup.

Sub type	Operation	Log content
Record query	Record query	User name: current user Start time: The start time of the execution End time: The end time of the execution operation IP address: The IP address of the computer used to perform the operation
Record playback	Record playback	
Record backup	Record backup	

Store logs: Subtype includes formatting.

Sub type	Operation	Log content
Format	SD card format	User name: current user Serial number: SD card serial number IP address: The IP address of the computer used to perform the operation

Network logs: sub-types include network disconnection, network connection, network abnormality, and changes in networking mode.

Sub type	Operation	Log content
Network disconnected	Network disconnected	User name: current user IP address: The IP address of the computer used to perform the operation
Network connected	Network connected	
Network anomaly	Network anomaly	
Networking changes	Networking changes	

CAUTION

RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS

Scan the following QR Code with your smart phone to visit our website and learn more.

AVYCON
16682 Millikan Ave
Irvine, CA 92606
Email: info@avycon.com
Website: avycon.com
Tel: 949-752-7606
Toll Free: 888-8334611 (Canada)
Fax: 949-250-7076