urmet

Mod.
1099

DS1099-188

BUILDING&RETAIL H.265 IP Cameras

USER MANUAL

English

CONTENTS

1 Introduction 4
2 Product Description 5
2.1 Technical characteristics 5
2.2 Opening the Box 5
2.3 Warnings 6
3 Overview 8
3.1 Range of Application 8
3.2 Product description 8
3.3 Operating environment 8
3.4 IP Camera Connector Layout (Where Featured) 9
4 Operating instructions 10
4.1 Checking the Connection 10
4.2 Searching for the Device 10
4.3 Installation of Controls and Login to the System 11
5 Login 11
5.1 First Camera Login 11
5.2 Preview 13
5.3 Recovery password 13
5.3.1 Security Question Verification 14
5.3.2 Certificate of authorisation 14
5.3.3 Super code 14
6 Live 15
6.1 PTZ Control *(Only for certain models)* 16
7 Local settings 16
8 Playback 17
8.1 General 17
8.2 IA 17
8.3 Picture 18
8.4 Tag 18
8.5 Playback controls 18
9 Remote Setting 19
9.1 Display Configuration 19
9.1.1 Live 19
9.1.2 Image Control 20
9.1.3 Privacy Zone 21
9.1.4 Roi 22
9.2 Record 23
9.2.1 Encode 23
9.2.2 Record 24
9.2.3 Schedule 24
9.2.4 Capture 24
9.2.5 Capture Schedule 25
9.3 Event 25
9.3.1 Setup 25
9.3.1.1 Motion detection 25
9.3.1.2 Deterrence *Only for certain models* 26
9.3.1.3 Siren *Only for certain models* 26
9.3.1.4 Sound detection 27
9.3.2 Alarm output settings 28
9.3.2.1 Motion detection 28
9.3.2.2 I/O (Input/Output) [where featured] 29
9.3.2.3 Sound detection 30
9.3.3 Event push 31
9.4 IA (Intelligent Alarm) 32
9.4.1 Setup 32
9.4.1.1 FD: Face Detection 32

9.4.1.2 PD&VD: Pedestrian Detection & Vehicle Detection 33
9.4.1.3 PID: Perimeter Intrusion Detection 34
9.4.1.4 LCD: Line Crossing Detection 35
9.4.1.5 SOD: Stationary Object Detection 36
9.4.1.6 CC: Line Crossing Counter 37
9.4.1.7 HM: Heat Map 38
9.4.1.8 CD (Crowd Density Detection) 38
9.4.1.9 QD (Queue Length Detection) 39
9.4.1.10 LPD (License Plate Detection) 40
9.4.1.11 RSD (Rare Sound Detection) 41
9.4.1.12 IA Schedule 41
9.4.2 Recognition: face recognition *Only for certain models* 42
9.4.2.1 Face Recognition (FR) 42
9.4.2.2 License Plate Management *Only for certain models* 43
9.4.3 Alarms 45
9.4.3.1 FD: Face Detection 45
9.4.3.2 FR: Face Recognition *Only for certain models* 46
9.4.3.3 AD: Attribute detection *Only for certain models* 46
9.4.3.4 PD & VD: Person and vehicle detection 47
9.4.3.5 PID: Perimeter intrusion detection 47
9.4.3.6 LCD: Line crossing detection 48
9.4.3.7 SOD: Stationary object detection 49
9.4.3.8 CC: Crossing counting 49
9.4.3.9 FA: Face attendance *Only for certain models* 50
9.4.3.10 CD: Crowd Density Detection 50
9.4.3.11 QD: Queue Length Detection 51
9.4.3.12 LPD: License Plate Detection 52
9.4.3.13 RSD: Rare Sound Detection 53
9.4.4 Statistics 54
9.4.4.1 Face Detection *Only for certain models* 54
9.4.4.2 Human & Vehicle detection 54
9.4.4.3 Cross Counting Statistics 55
9.4.4.4 Heat Map Statistics 55
9.5 Network 57
9.5.1 General 57
9.5.1.1 General (Network) 57
9.5.1.2 PPPoE 57
9.5.1.3 SNMP 58
9.5.1.4 Port Configuration 58
9.5.2 E-Mail (E-Mail configuration) 59
9.5.3 FTP 60
9.5.4 RTSP 60
9.5.5 DDNS Configuration 61
9.5.6 HTTPS 62
9.5.7 IP Filter 62
9.6 Device 63
9.6.1 DISK 63
9.6.2 Audio 64
9.6.3 Cloud 65
9.7 System 66
9.7.1 General 66
9.7.1.1 Date and Time 66
9.7.1.2 Daylight Saving Time 66
9.7.2 Multi user 67
9.7.3 Maintenance 68
9.7.3.1 Log 68
9.7.3.2 Load Default: 69
9.7.3.3 Upgrade: 69
9.7.3.4 Parameter Management 70
9.7.3.5 Auto Reboot 70
9.7.4 Information 71
10 Maximum recording time with SD Card 72
11 Appendix 72
11.1 Router Port Forwarding 72
11.2 Installing ActiveX 73
11.3 Frequently Asked Questions 77

1 INTRODUCTION

Thank you for purchasing our integrated and developed network camera products for network video monitoring. Our range includes the following products: Storage Network Bullet, Wireless Storage Network Bullet, IR Network Dome, IR Network Weather-Proof and High-Speed Network Ball cameras. Individual high-performance SOC chips are used in the media processor for audio/video capture, compression and transmission/transfer. An h.265 standard encryption algorithm ensures clear and smooth video representation, as well as a high transfer capacity. The integrated Web server offers users access to real-time surveillance and remote control of the front-end camera through the Internet Explorer browser.
The network cameras are easy to install and operate. They are ideal for large and medium-sized companies, governmental projects, large malls, supermarket chains, intelligent buildings, hotels, hospitals, schools and other public places, as well as for applications that requiring remote network video transmission and monitoring.

Instructions:

- For the purpose of this manual, IP camera refers to a network camera.
- The default factory IP address for the IP camera is 192.168.1.168.
- The default factory administrator username for the IP camera is admin (in lowercase).
- The default Web port number is 80 and the default client port number is 9000.

Statement:
Some information contained in this manual may differ from the actual product. For any problems that cannot be solved with the help of this manual, please contact our technical support or an authorised dealer. This manual may be subject to change without prior notice.

2 PRODUCT DESCRIPTION

URMET S.p.A. proposes different ranges of cameras according to installation requirements and the locations to be video-surveilled. It currently has a range of cameras, in both bullet and dome versions, which support the main intelligent analysis algorithms, and a range of cameras, in both bullet and dome versions, which, in addition to intelligent analysis, is also equipped with the deterrence function via red/blue light LEDs, white light LEDs and integrated siren.

2.1 TECHNICAL CHARACTERISTICS

- Processor that ensures economic performance.
- CMOS progressive sensor
- Optimised H.265/H.264/H.265+/H.264+ video compression algorithms; multi-stream transmission ensures high definition images on both narrowband and wideband.
- Support simultaneous connection of up to 7 video streams (if the IP camera is connected to the NVR, the NVR will occupy 3 streams, leaving 4 free video streams. If the IP camera is connected to the Browser only, 7 streams will be available).
- SD card support up to 256GB
- The integrated Web server allows multi-browser use (Internet Explorer 10, 11, Edge V.79, Chrome 57/higher, Firefox 52/higher, Safari 11/higher) for real-time on-site monitoring, setup and management.
- Managed through Urmet UVS Pro client software.
- Mobile software for the following platforms: iOS and Android
- Remote system firmware updates.
- Support LAN and Internet.
- Support ONVIF and RSSP protocols.
- Support multiple network protocols, such as TCP/IP, UDP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, PPPoE, NTP, UPnP, SMTP, SNMP, IGMP, 802.1X, QoS and IPv6,
- Support motion detection alarm function (the user can set the area and sensitivity) and sensor/alarm out function (for camera models with motorised lenses and box cameras)
- Support privacy zone function.
- POE (optical) power supply function.
- Support snapshot. Image upload via FTP, Cloud or E-mail.
- Log Support: System logs, network logs, parameter logs, alarm logs, user logs, recording logs, storage logs and all logs
- Reset button supported
- Support automatic download recovery function. Automatic connection in the event of network interruption.

Note: The specifications of the different products may vary slightly.

2.2 OPENING THE BOX

Check that the packaging and the contents are not visibly damaged. Contact the retailer immediately if parts are either missing or damaged. Do not attempt to use the device in this case. Send the product back in its original packaging if damaged.

ACCESSORIES PROVIDED

- 1 IP camera unit
- 1 installation bag
- 1 Quick Guide containing instructions for proper installation
- 1 Addendum OSS Notice

※IMPORTANT NOTE: Keep the drilling template supplied with the product for future installations. Accessories may be changed without prior notice.

2.3 WARNINGS

Power supply

- Before connecting the equipment to the electrical outlet, ensure that the nameplate specifications match those of the mains power supply.
- It is advisable to install a suitable disconnection and protection switch upstream from the equipment.
- In the event of failure or malfunction, disconnect the power supply at the main switch.
- Use only the power supply unit provided with the product.

Safety precautions

- Keep the device away from rain and dampness to prevent the risk of fire and electrocution. Do not introduce any material (solid or liquid) inside it. If this should accidentally occur, disconnect the device from the mains and have it inspected by qualified personnel.
- Never open the device. In all cases, contact qualified personnel or an authorised service centre for repairs.
- Keep the device away from children, to prevent accidental damage.
- Do not touch the device with wet hands to prevent electrical shock or mechanical damage.
- Stop using the device if it falls or if the external casing is damaged. Continued use of the device in such conditions could cause an electric shock. In such cases, contact the retailer or authorised installer.

Installation precautions

- Do not install the camera in places exposed to rain or humidity. In these situations, use the special cases.
- Avoid pointing the camera directly towards sunlight or other intense sources of light, even when switched off; the subject to be filmed should not be against the light.
- Avoid pointing the camera towards reflecting objects.
- The presence of certain types of light (e.g. coloured fluorescent light) can distort the colours.
- Do not position this device on an unstable surface, such as a tottering or slanted table. The device could fall, causing injury or mechanical failures.
- Stop using the device if water or some other material penetrates inside it, to prevent risk of fire or electrocution. In such cases, contact the retailer or authorised installer.
- Do not cover the device with a cloth while it is running to prevent deformation of the external casing and overheating of internal parts, causing risk of fire, electrocution and mechanical failure.
- Keep magnets and magnetised objects away from the device to avoid malfunction.
- Do not use the device in the presence of smoke, vapour, humidity, dust or intense vibrations.
- Do not operate the device immediately after moving it from a cold place to a warm place or vice versa. Wait on average for three hours: this will allow it to adapt to the new environment (temperature, humidity, etc.).

Precautions for use

- Check that the device is not damaged after removing it from the packaging.
- Ensure that the working environment is not too humid and that the temperature is within the indicated range.
- Avoid pointing the camera towards sunlight to prevent damage to the sensor.

Cleaning the device

- Rub gently with a dry cloth to remove dust and dirt.
- Dip the cloth in a neutral detergent if dirt cannot be removed with a dry cloth alone.
- Do not use spray products to clean the device. Do not clean the device using volatile liquids (such a petrol, alcohol, solvents, etc.) or chemically treated cloths to prevent deformation, deterioration or scratches to the paint finish.
- Disconnect the device from the electrical outlet before any cleaning or maintenance operations.

Recording images

- This device is not designed as a burglar system but mainly to transmit and record video images. Urmet S.p.A. cannot be held liable for loss or damage due to theft from the user's premises.
- Make a test recording before using the device to ensure that is working correctly. Please note that Urmet S.p.A. is not liable for any loss of stored data or damage caused by incorrect installation, improper use or malfunctioning of the device.
- This device contains precision electronic components. Protect the device from bumps and jolts to ensure proper recording of images.

Privacy and Copyright

- The IP camera is designed for CCTV systems. The recording of images is subject to the laws in force in the country of use. Recording of images protected by copyright is forbidden.
- Product users are responsible for checking and complying with all local rules and regulations regarding monitoring and the recording of video signals. The manufacturer SHALL NOT BE LIABLE for any use of this product not in compliance with the laws currently in force. For more information go to http://www.garanteprivacy.it

Firmware upgrade

- You are advised to refer periodically to the Urmet website https://www.urmet.com to check the availability of firmware updates.

Network configuration

- The camera default setting is DHCP mode. If the installation network does not support dynamic addressing (DHCP), the device will automatically switch to the factory-set IP address 192.168.1.168. The Urmet "*Device Config Tool*" software can be used to change the IP address and other network settings to prevent conflict with other devices on the network.
- Once the camera is properly connected and configured on the IP network, its video and settings can be viewed from a PC or smartphone.

Network connections

- When connecting a remote PC (using client software or a browser), it should be borne in mind that any video channel used on the PC will have a "unicast" connection (TCP, RTP, UDP).
- The device can support up to 7 "unicast" connections, thus the video stream can be viewed from a maximum of 7 remote devices (PC or smartphone) at the same time, depending on the available bandwidth.

3 OVERVIEW

3.1 RANGE OF APPLICATION

These network cameras with their powerful image processing capacity can be used in various public places, such as malls, supermarkets, schools, factories and workshops, as well as in environments requiring HD images, such as banks and traffic control systems, as illustrated in the figure below:

3.2 PRODUCT DESCRIPTION

An IP camera is an online digital surveillance camera, equipped with a web server and capable of independent operation, providing the user with access to real-time monitoring from any location through a web browser or client software.

The IP camera features an integrated media processing platform for audio/video capture, compression and network transmission on a single board. It is compliant with High Profile H.264/ H265 coding standards. Remote users can have access to real-time monitoring by entering the IP address or domain name of the IP camera in the web browser. This network camera solution is suitable for residential or business environments, as well as a wide range of situations that require remote network video monitoring and transmission. The IP cameras are easy to install and operate.

The IP cameras can be controlled by several users with different levels of authorisation.

The IP cameras allow mobile detection and sending of e-mails and snapshots in cases of emergency; if an SD card is included, the image or video snapshots can be stored in the card for subsequent retrieval.

3.3 OPERATING ENVIRONMENT

Operating system: Windows 10/Windows 7/Windows 8/Windows 2008 (32/64-bit), Windows 2003/Windows XP/Windows 2000 (32-bit)

CPU: Intel Core Duo II processor or higher

Memory: 1G or higher

Video memory: 256M or higher

Display: 1024 × 768 or higher resolution

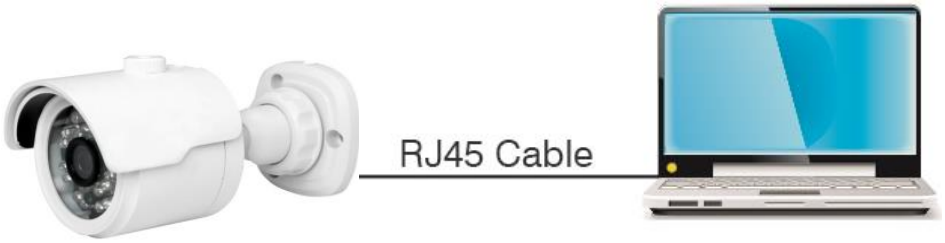
Internet Explorer 6.0 or later

Device Connection

The IP camera can be connected in two ways:

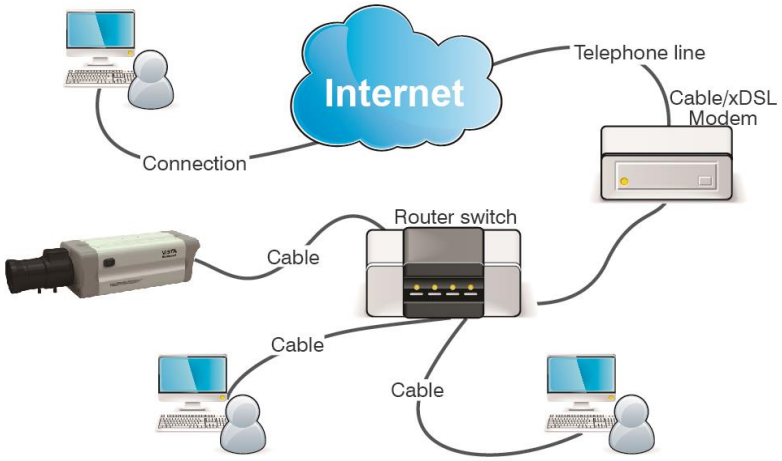
- Connection to a PC

  Connect the IP camera to the PC using a direct network cable, with the power input connected to a 12VDC adaptor, and enter the IP addresses of the PC and the camera in a network segment. The IP camera will communicate with the PC within one minute after being switched on if the network is working properly.

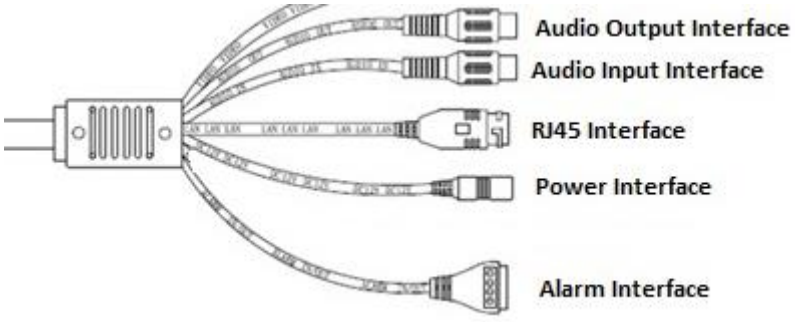


- Connection to a router/switch

  This solution is more commonly used to connect the IP camera to the Internet; in this case, the camera and the PC are connected to the LAN ports of a router/switch and the gateway of the camera is set to the IP address of the router.



3.4 IP CAMERA CONNECTOR LAYOUT (WHERE FEATURED)

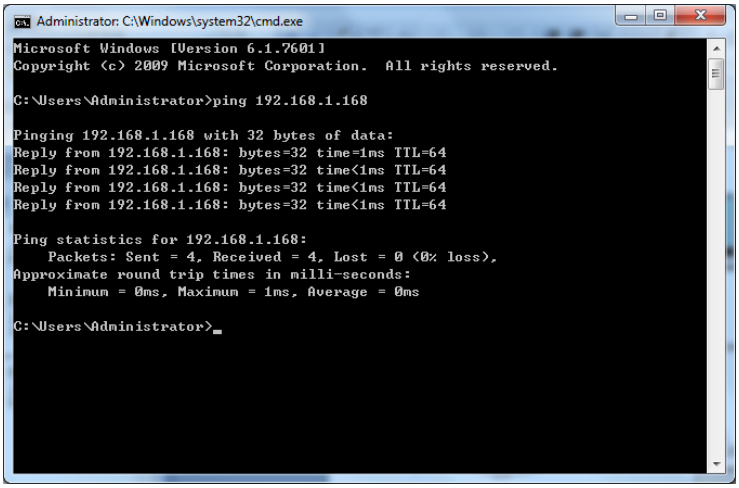


1. Audio Output Interface: RCA female connector (white), can connect with external devices, such as speakers.
2. Audio Input Interface: RCA female connector (red), can connect with input devices, such as a microphone.
3. RJ45 Interface (Network Interface): Connector for a RJ45 network cable.
4. Power Interface: DC 12V.
5. Alarm Interface: Including alarm input and output interface. ③, ④ (③COM and ④OUT) are alarm outputs; ① is the alarm input, and ② is used as Ground (GND).

4 OPERATING INSTRUCTIONS

4.1 CHECKING THE CONNECTION

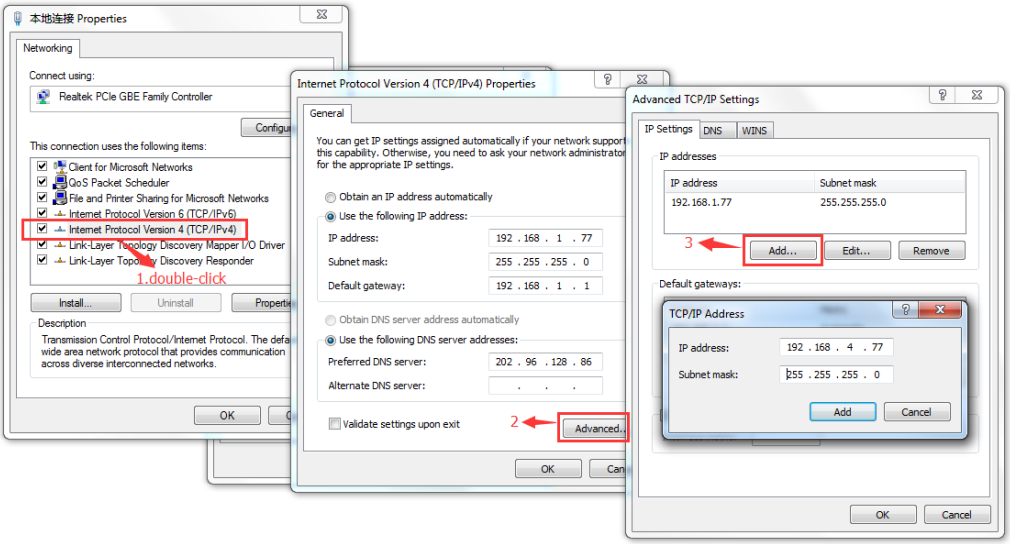
- The factory default IP address for the IP camera is 192.168.1.168 and the subnet mask is 255.255.255.0. Give your computer an IP address in the same network segment as the IP camera (e.g., 192.168.1.69) and the same subnet mask as that of the IP camera.
- Check whether the IP camera is connected and switches on properly by selecting Start > Run, entering “cmd” and pressing ENTER; then enter “ping 192.168.1.168” in the command line window.



- Check whether the IP camera is accessible. If the PING command is executed successfully, it means that the IP camera is operating normally and the network is connected properly. If the PING command fails, check the IP address and gateway settings of the PC, as well as the network connection.

4.2 SEARCHING FOR THE DEVICE

- Feedback: The Device Config Tool function may be used to search for the device across network segments. Before running the Device Config Tool, select the local connection icon at the bottom right corner of the desktop;
- Add the IP addresses of several network segments in the TCP/IP local area connection settings, as shown below. You can run this tool to search for any device with an IP address in the same network segment.



Note:

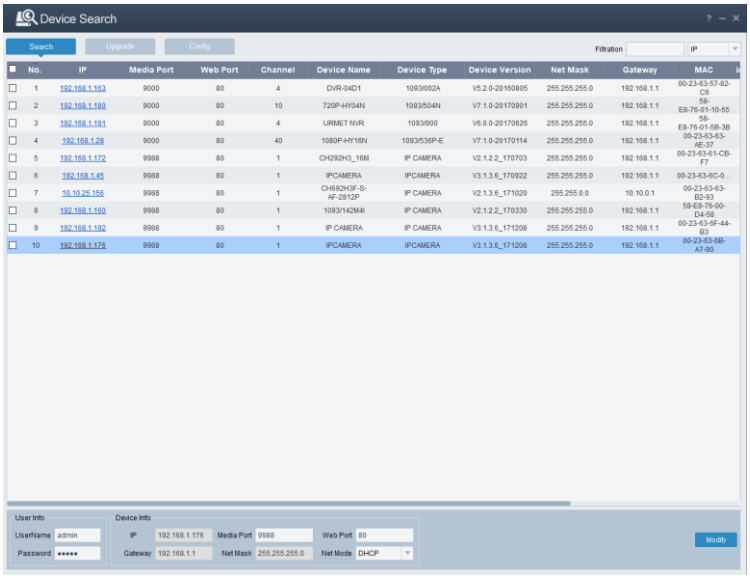
Device Config Tool uses the Multicast protocol to search for the device across the segments; however, since firewalls prevent multicast data packet traffic, they must be disabled so that the information on the device can be acquired.

Online device search procedure

1. Run Device Config Tool by double-clicking on the 

icon.

   It will search for and display any online device and its IP address, port number, web port number, number of channels, configured name, device type and version, subnet mask, gateway, MAC address, connection pattern and status.

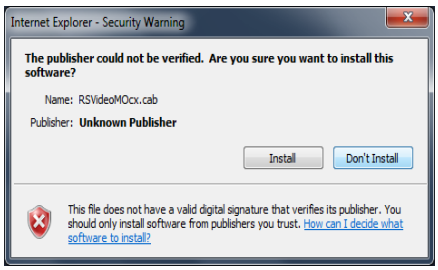


4.3 INSTALLATION OF CONTROLS AND LOGIN TO THE SYSTEM

Before using the Edge browser in IE mode (Internet Explorer mode) to access the IP camera for the first time, the plug-in components must first be installed, as follows:

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

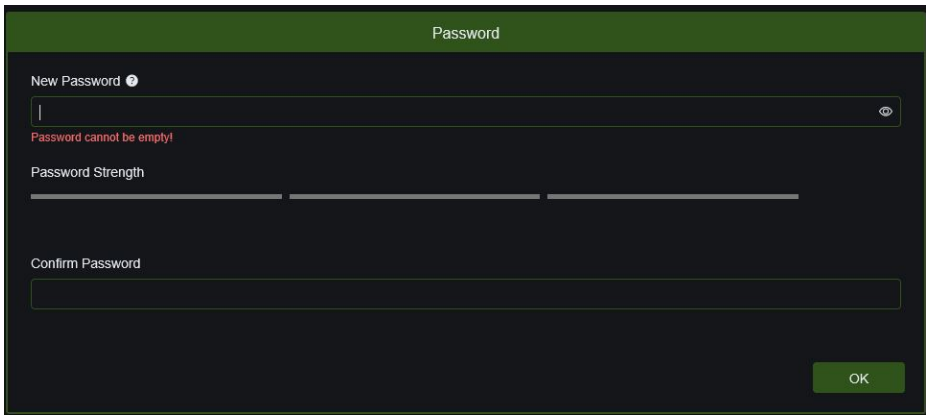
Select an option in the plug-in installation pop-up dialogue box to run the installation process.



5 LOGIN

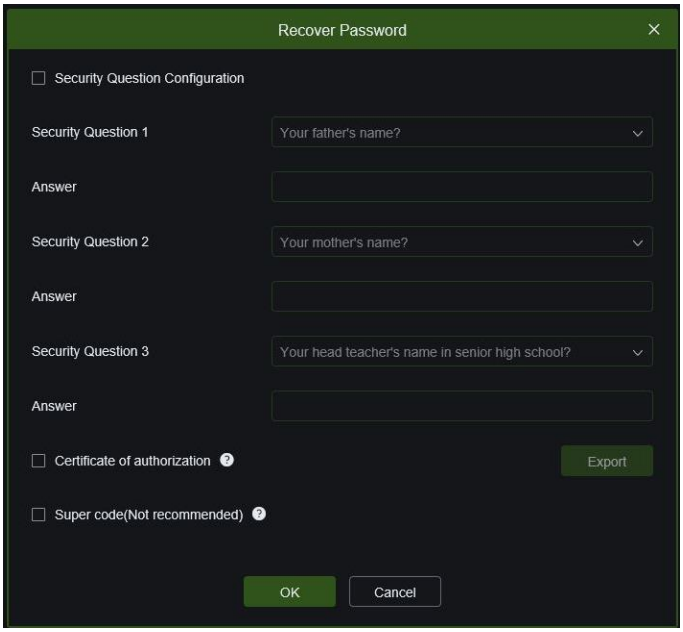
5.1 FIRST CAMERA LOGIN

Open a browser (all browsers for managing camera parameters from page [no video] or Edge in Internet Explorer mode for full camera management [parameters and video]) and enter the camera's IP address (http://192.168.1.168) to bring up the window for creating the Administrator password: you must set the password immediately to protect your privacy; the password should contain a combination of between 8 and 15 characters. Write down the password and keep it in a safe place.



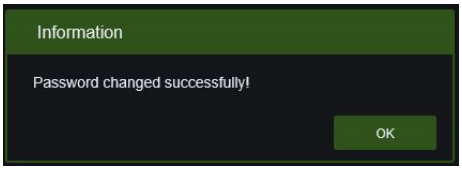
Click **OK** to confirm.

A window will then appear in which you can select and configure the password recovery modes in case the password is lost.



- **Security Question Configuration**: choose one of the suggested questions and enter the answer (if the function is enabled you must fill in all the security questions); if you lose your password, you can set a new one by using the **password recovery** function.
- **Certificate of authorisation**: you will be able to export a certificate (to be written down and kept in a safe place), which, if you lose your password, you can use to set it again using **the password recovery** function.
- **Super code**: by enabling this function, you can contact the Urmet Customer server to request a SUPER CODE that will allow you to set a new password using the **password recovery** function.

Once you have chosen the options, confirm with **the OK** button.
At the end of the password change process, the following window will appear:



Click the **OK** button to confirm.

*NOT*E: If no password recovery method is chosen, if you lose your password, you will have to activate the RESET button (on the camera), which restores the camera's default settings.

5.2 PREVIEW

Open IE and enter the camera's IP address (http://192.168.1.168) to bring up the login window shown below:

Login Interface for H.265 IP camera.

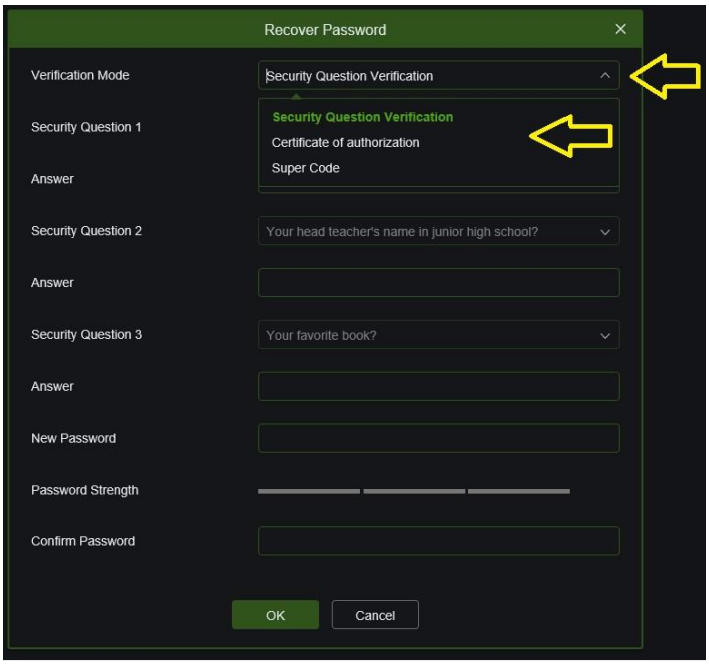
Figure 1

In the login window you can choose a language for the IE client. Enter your username (admin by default) and password (set previously) and then press **Login**.

5.3 RECOVERY PASSWORD

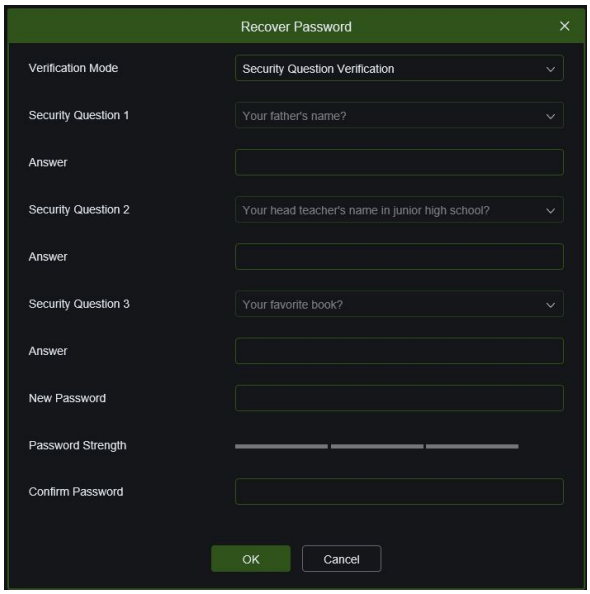
If you lose your password, you can simply click on the **Password Recovery** button and choose one of the modes set previously when changing your password.

In *Verification Mode*, select one of the three previously set password recovery modes:



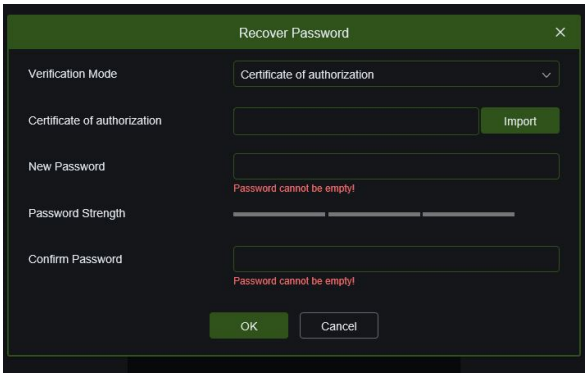
5.3.1 SECURITY QUESTION VERIFICATION

Give the correct answers to the previously selected questions, type the new password and confirm by clicking on the **OK** button.



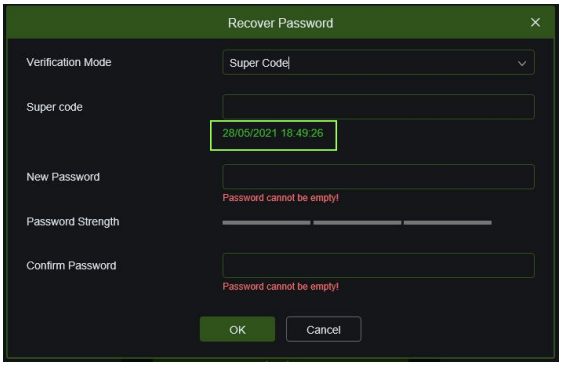
5.3.2 CERTIFICATE OF AUTHORISATION

Import the previously saved certificate (.txt file) and type the new password, then confirm by clicking on the **OK** button.

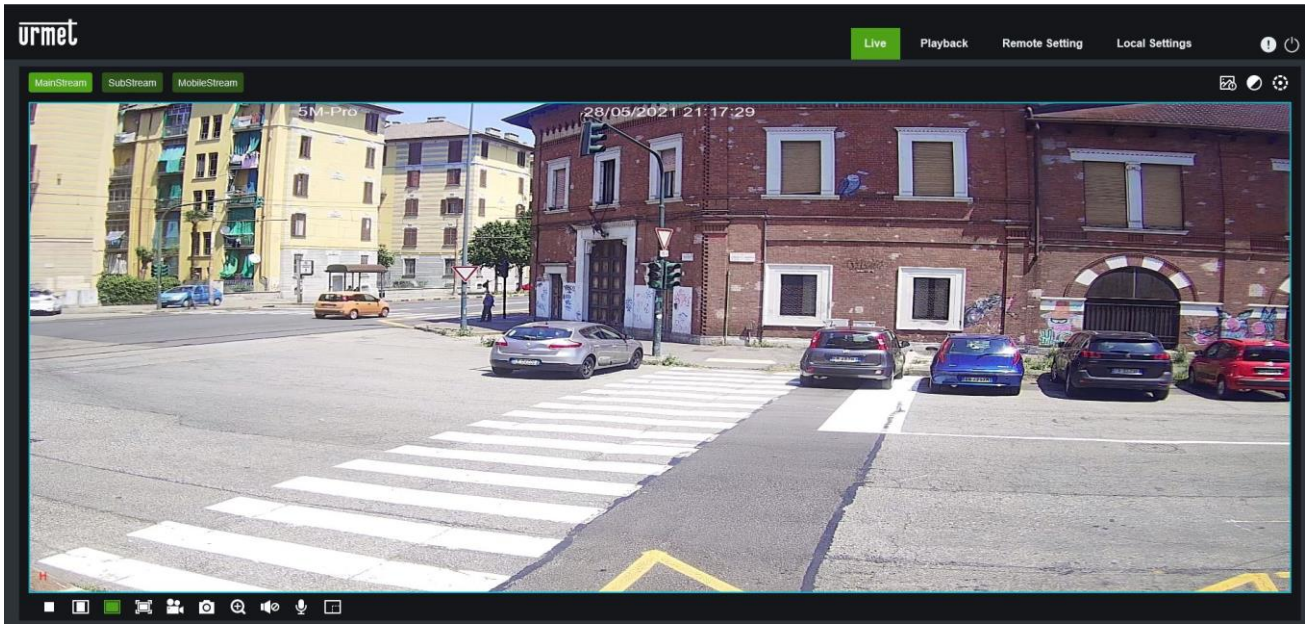


5.3.3 SUPER CODE

Contact Urmet Customer Service, having previously written down the date and time of the camera, and the MAC ADDRESS (which you can find with the **Device Config Tool**, available for download from the website www.urmet.com).



6 LIVE



Some of the buttons in the preview frame are described below.

 : (Colour) Button for setting the colour, brightness, contrast, saturation and sharpness of the frame.

 : (PTZ control) the PTZ interface appears when you click on the icon.

 : (IA Alarm) Button to open/close the window for alarms generated by intelligent video analysis.

Playback: Reads the recording file from the SD card and then plays it back through the browser.

Remote Setting: Access to the device settings menu to customise the settings of various parameters.

Local Settings: (Local setting) For snapshot, video file type and storage path settings.

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

 : Stop/Start Live video.

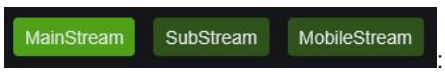
 : Preview frame ratio adjustment, toggling between Original Ratio, Automatic Ratio and Full Screen.

 : Preview control buttons - Open Video, Snap, Zoom-In/Out, Sound On/Off, Microphone (from left to right).

 : White light preview control button (only available on some models)

 : Preview control button for siren (only available on certain models).

 : Preview control button for deterrence light (only available on certain models).

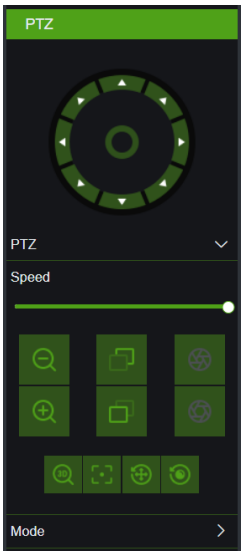


: Dynamic bitstream switching for the preview frame.

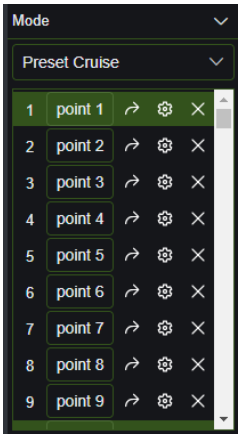
 : gives the number of pixels (W, H) of the selected portion of the screen.

6.1 PTZ CONTROL *(ONLY FOR CERTAIN MODELS)*

: (PTZ control) selecting this icon brings up the following window:



- **SPEED** increases or decreases the PAN/TILT speed
- **ZOOM** zooms in and out
- **FOCUS** increases or decreases FOCUS
- **3D Position:** allows to move the camera on an area of interest
- **Autofocus:** adjusts focus automatically
- **PTZ Reset**: resets the PTZ parameters to factory default
- **Lens Reset**: resets the lens to its centre position. Press on the FOCUS controls to refocus the camera.



Up to 255 preset points can be stored.

Preset programming procedure:

1 – Position the camera on the desired point using the directional buttons.

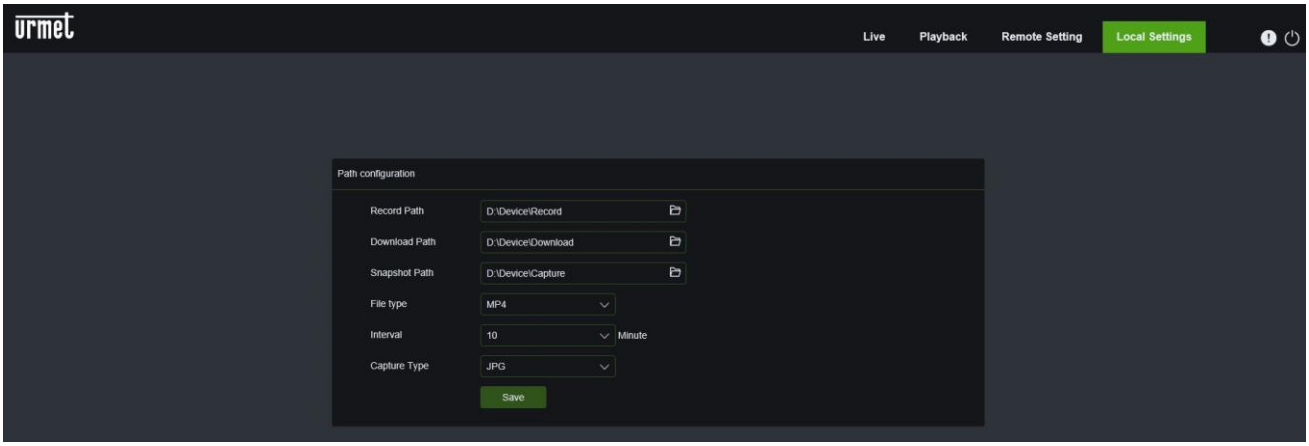
2 – Press on **Add preset** to store the preset point. The saved preset will be marked in green.

To recall a stored preset press **Go to**.

To delete a stored preset press **Delete preset**.

7 LOCAL SETTINGS

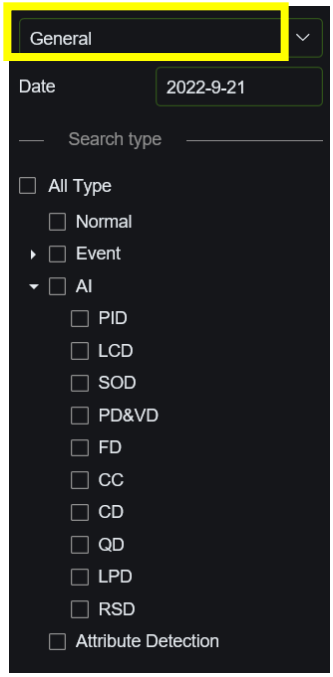
Select Local Settings to access the following dialogue window: here you can set the video storage location, paths for downloading remote files and storing snapshot images, the file type (MP4 by default, AVI or RF with H265 encryption), video recording duration and screen capture file type BMP, PNG or JPG.



8 PLAYBACK

Select Playback to access video search functions, choose the search type (General or AI), select the corresponding date, then click Search.

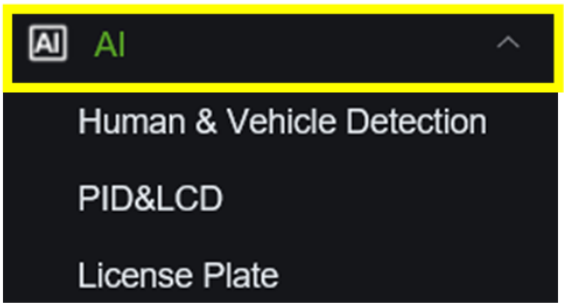
8.1 GENERAL



Select **the General** option to perform generic, NORMAL searches (24-HOUR recording), by type of EVENT (alarm input, sound detection, netbreak or motion events) or by type of Intelligent Video Analysis (IA) (PID, LCD, SOD, PD&VD, FD, CC, CD, QD, LPD, RSD) or ATTRIBUTE DETECTION, described in detail in the intelligence chapter.

8.2 IA

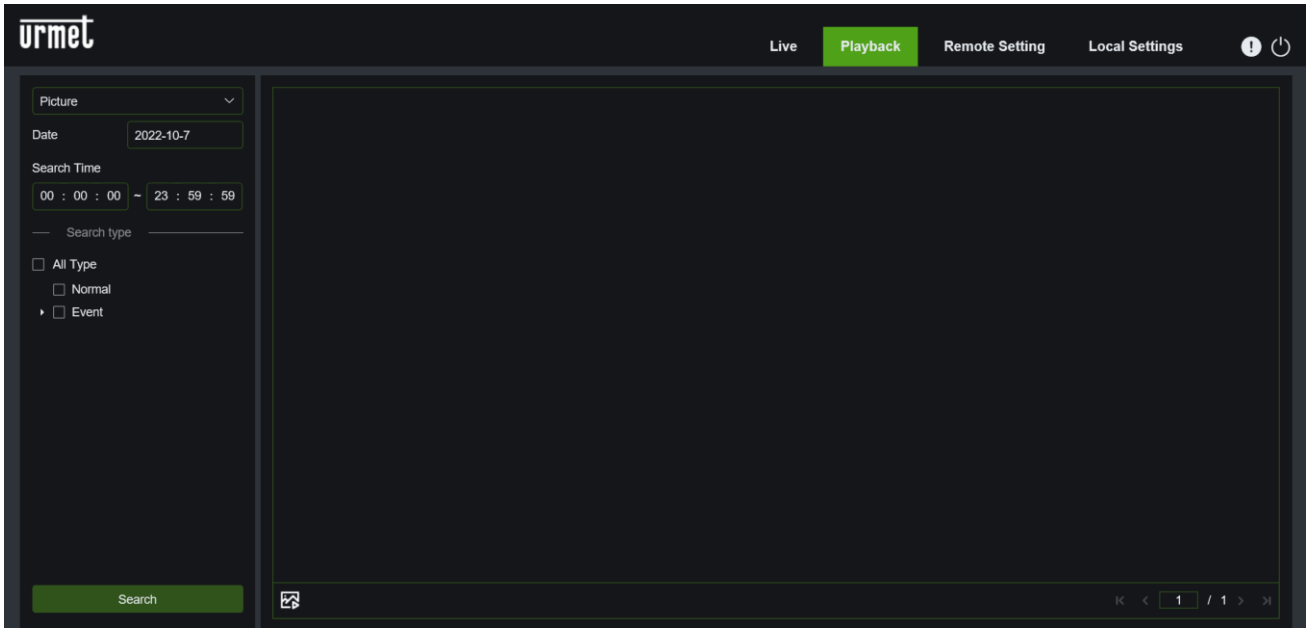
Select **the IA** option to perform thorough searches on recordings made with Intelligent Video Analytics for the following functions:



- Human & Vehicle Detection
- PID & LCD
- License Plate

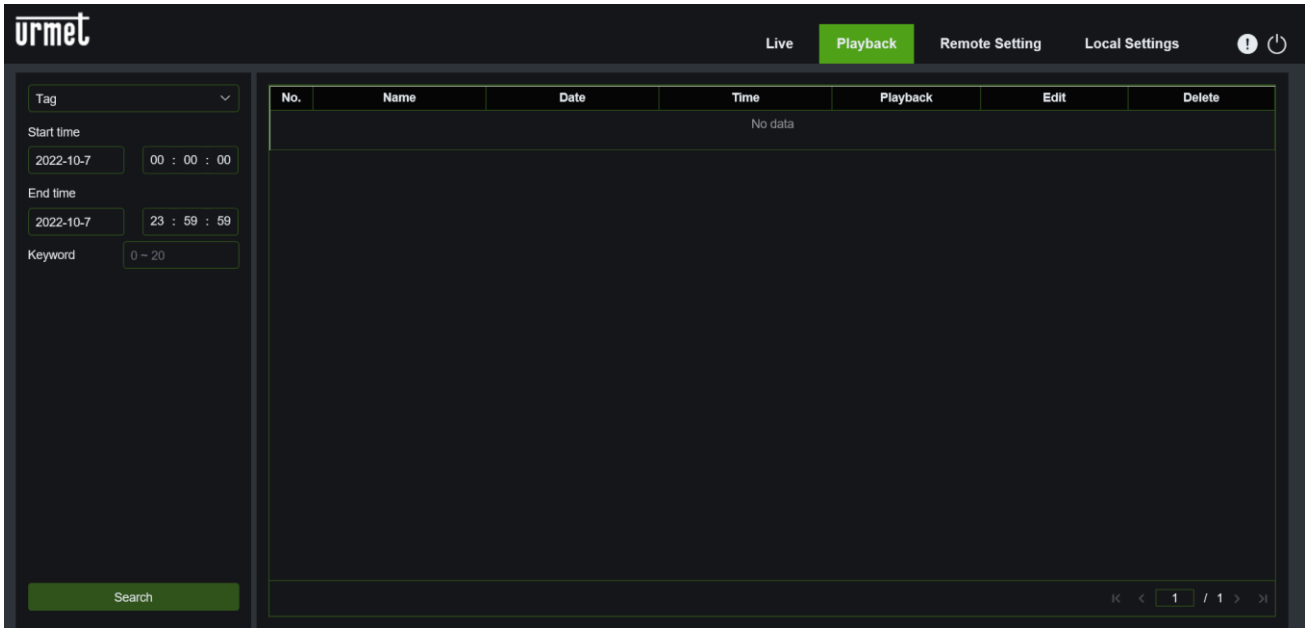
8.3 PICTURE

If you select the **Picture** option, it will be possible to search for saved pictures:

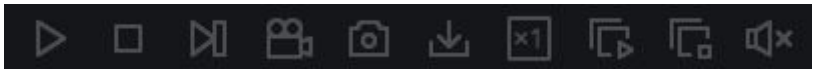


8.4 TAG

If you select the **Tag** option, it will be possible to search for saved tags:



8.5 PLAYBACK CONTROLS



: from left to right, Play/Pause, Stop, Next frame, (select once to play a frame), Record, Capture, Download, Zoom, Play all, Stop all, Audio control.

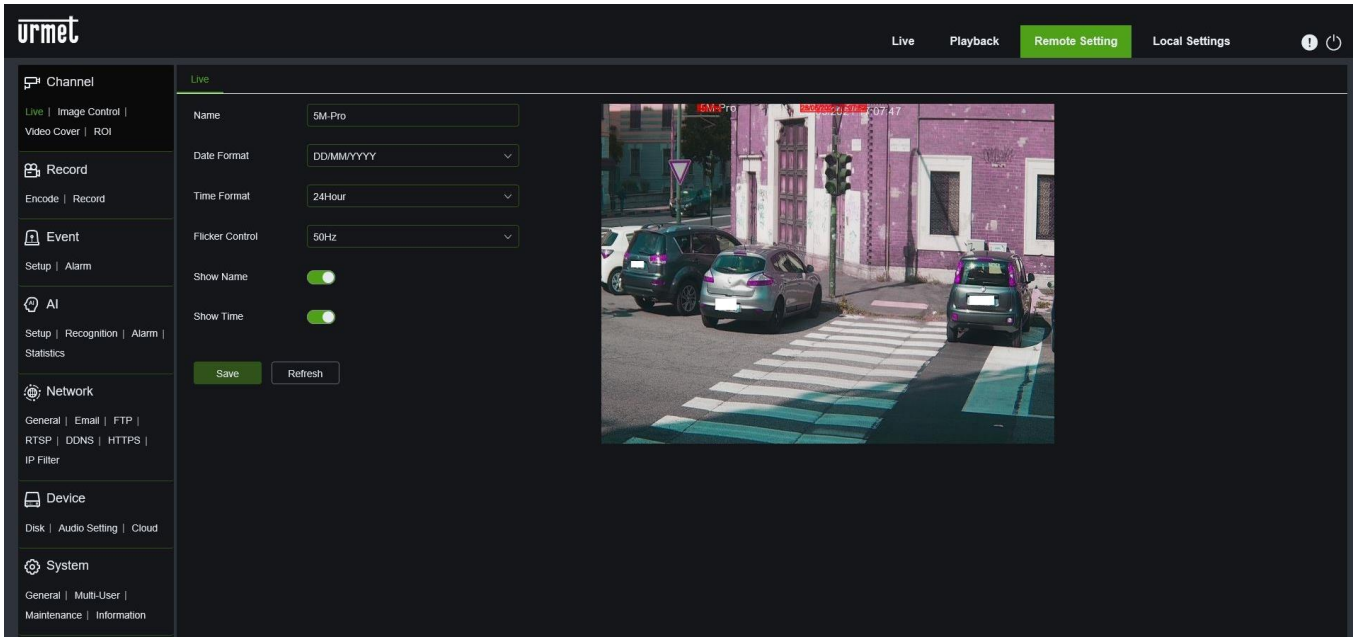
: from left to right, Zoom, Original proportions, Increase scale, Full screen.

9 REMOTE SETTING

9.1 DISPLAY CONFIGURATION

9.1.1 LIVE

Select Remote Settings to open the following page (default preview settings page):



Name: name of the IP camera.

Date Format: choose the format type for the date.

Time Format: Choose the format type for the time.

Flicker control: Choose 50Hz or 60Hz.

Show Name: the camera name is displayed.

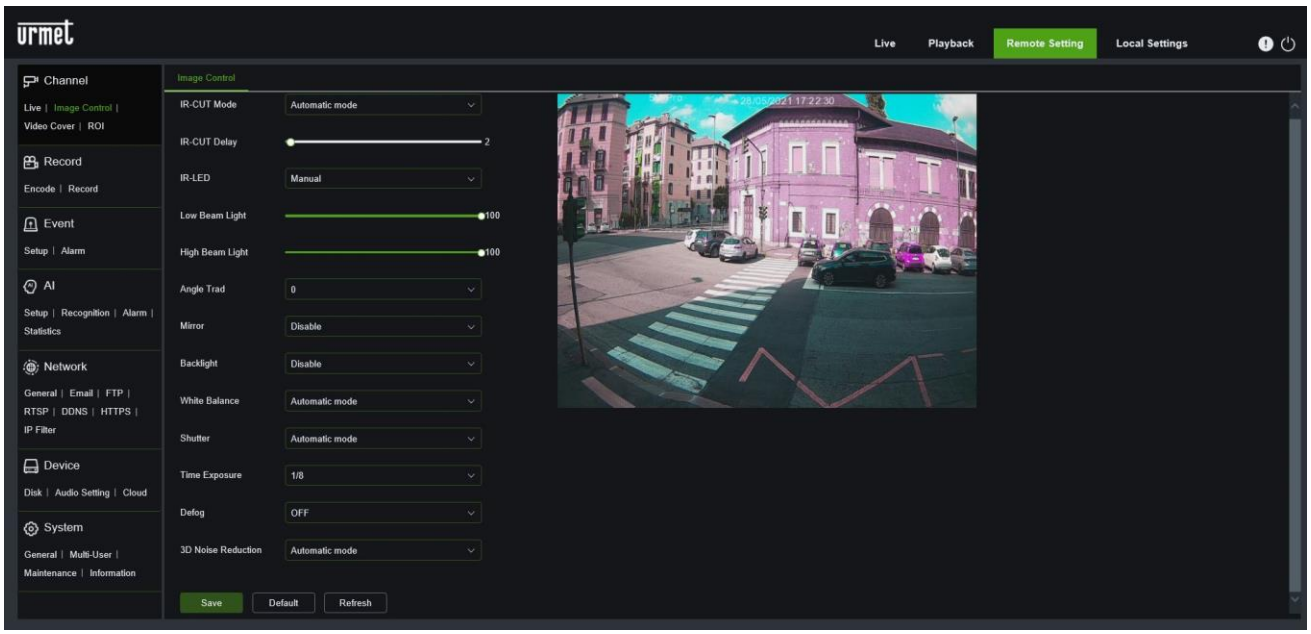
Show Time: the date and time are displayed.

OSD: the red text on the frame; the channel name and time display can be repositioned by dragging them in the preview frame.

After making your settings, confirm with the **Save** button

9.1.2 IMAGE CONTROL

Select Image Control in the Channel Menu to open the following page (for Varifocal cameras):



- **IR-CUT Mode**: Select the integrated IR-CUT filter mode to ensure that the camera functions properly in Day/Night: Automatic mode, Colour mode, Image mode, Day, Night, Schedule, where you have to indicate a time interval.

  By setting the automatic mode in the camera equipped with a light sensor (CDS), the changeover from colour (day) to black and white (night) of the image will take place as follows: the changeover from day to night will take place according to the brightness detected in the image, while the changeover from night to day will take place according to the brightness detected by the light sensor.
- **IR-CUT Delay**: Set the IR-Cut delay.
- **IR LED**: Manual mode (you can set the brightness of the LEDs) or SmartIR (automatic)
- **Low Beam Light** changes the infrared intensity of the low LEDs
- **Corridor Mode:** function that allows the camera to be used in portrait mode with the image in 9:16 format.
- **Angle Trad** (Lens Flip): Set to enable inversion of the image.
- **Mirror**: Set to enable horizontal, vertical or horizontal and vertical image inversion.
- **Exposure Compesation:** Menu where you can set some backlight functions (WDR, HLC, BLC) and levels
- **White Balance:** To set the white balance: Auto/Manual.
- **Shutter:** To set the shutter mode (Automatic, Manual)
- **Time Exposure**: Indicates the camera exposure time.
- **3D Noise Reduction:** To enable the function and choose automatic/manual mode

The following image control parameters are also available for panorama models:

- **Lens Distort Correct:** If enabled, allows correction of image distortion from its original version.
- **Fov Adjustment:** allows the field of view to be adjusted.

Press **Save** to save the desired setting.

The following image control parameters are also available for full colour models:

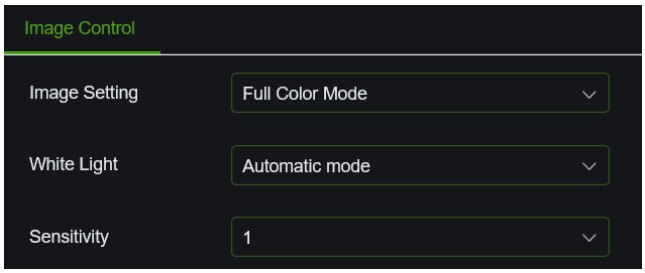
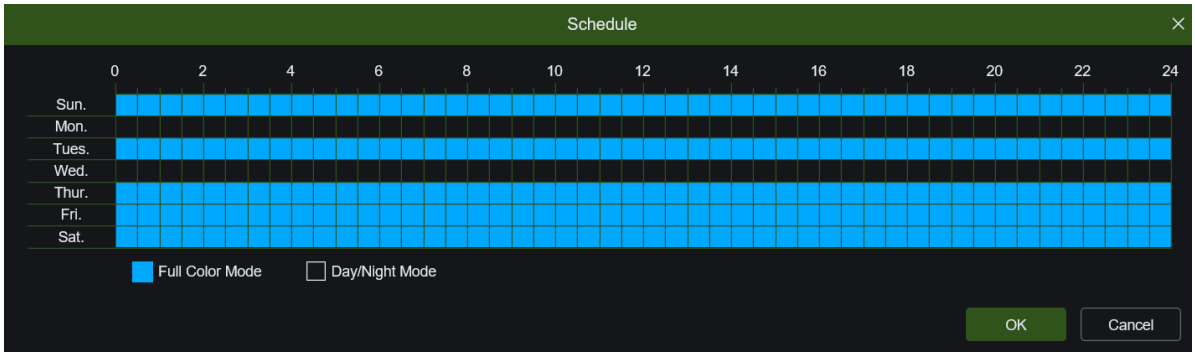
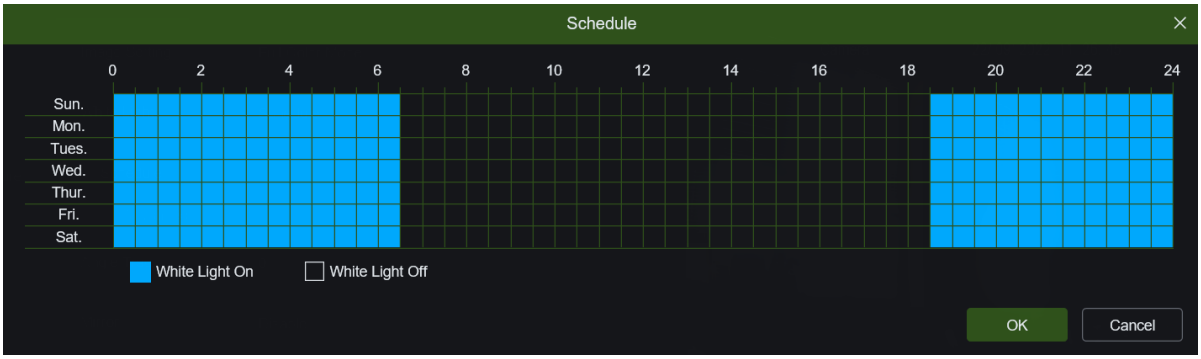


Image setting: Three modes can be chosen, **full colour mode**, **day/night mode** and **schedule mode** (hybrid full colour + day/night).

- **Full colour mode:** If set, images can be displayed in colour even in low light.
- **Day/night mode:** If set, this allows the camera to switch from colour to black and white according to ambient light conditions (colour during the day/black and white at night).
- **Schedule mode:** If set, allows you to schedule full colour and day/night modes on time slots as shown below.



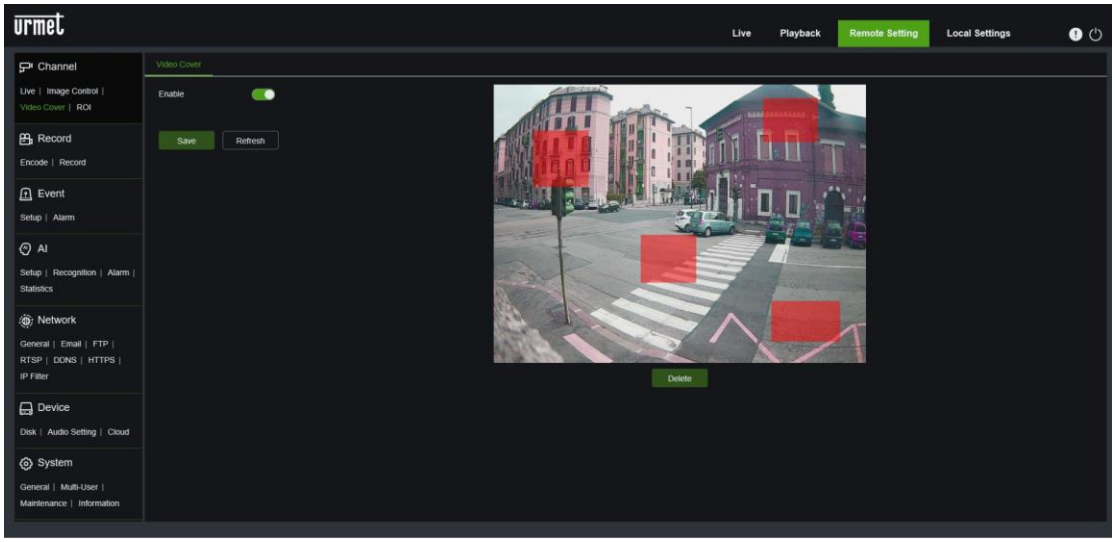
By choosing full colour mode, only the red/blue deterrence LEDs on the camera can be set to function. The white light will instead be activated as auxiliary lighting when the light of the image framed by the camera becomes poor. It is possible to choose between **OFF**, **manual mode**, **automatic mode** and **schedule mode**.
The automatic mode also includes the adjustment of the sensitivity (0 to 3) of detection by the sensor.



By choosing **day/night mode** instead, the manual white light control is also enabled.

9.1.3 PRIVACY ZONE

Select Video Cover under Channel to open the following page:

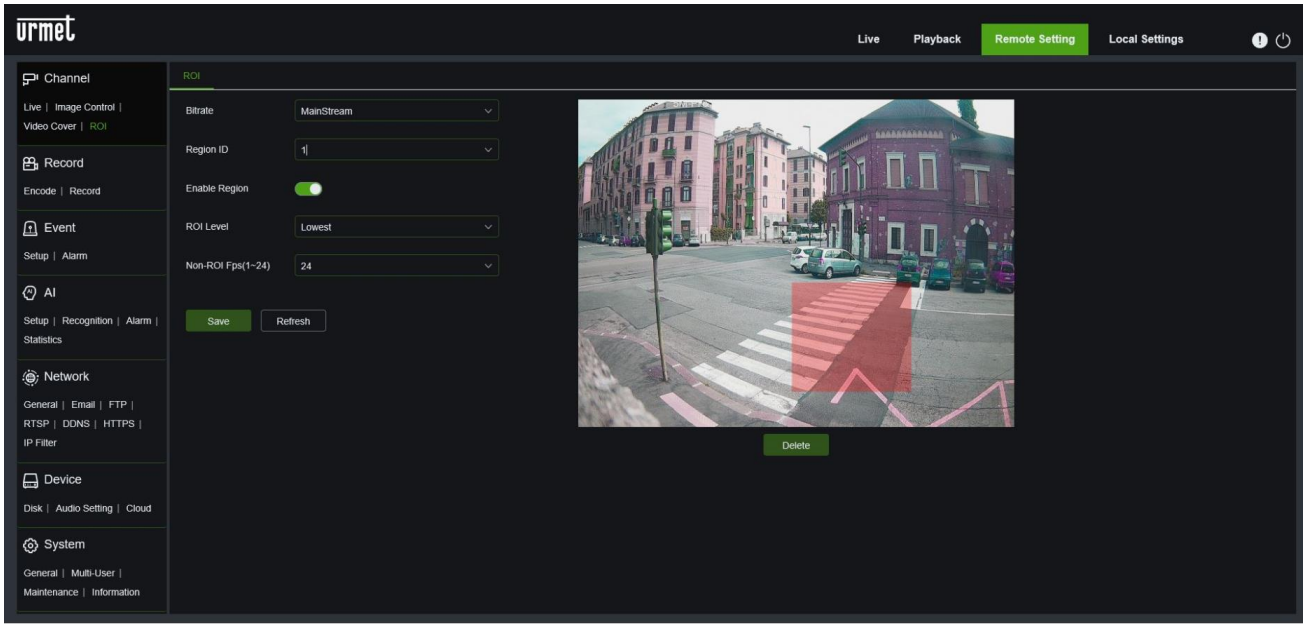


Enable Video Cover, and then use the left mouse button to trace rectangles around areas not to be displayed during recording, in screenshots and in Live viewing. Save when done to keep the settings.

Press **Save** to save the desired setting.

9.1.4 ROI

Select Channel → **ROI** to open the following page:



ROI setting procedure:

1. Choose a region of application,
2. Press and hold the left mouse button and drag out a ROI (only one ROI can be set for each zone),
3. Select Save to apply the ROI.

The following is a description of the configuration parameters:

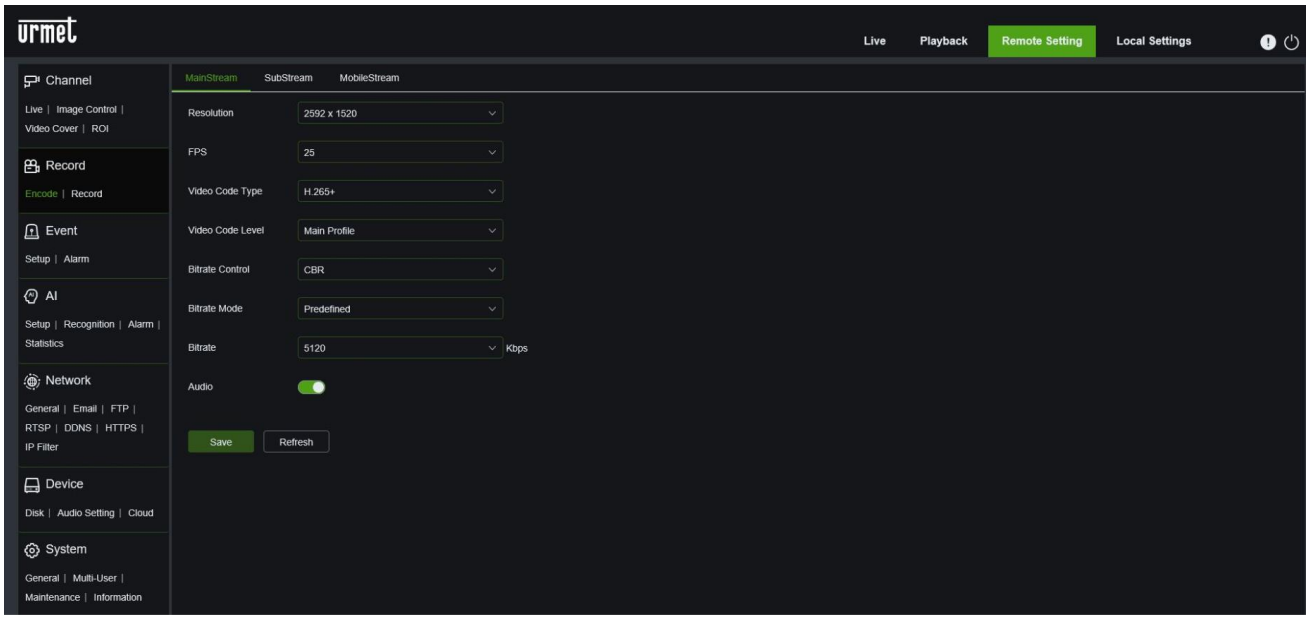
- **Bitrate:** Select the type of Stream on which you want to set the ROI
- **Region ID:** Up to 8 ROI zones can be set in a single bit stream.
- **Enable Region:** Enable or disable the ROI.
- **ROI level:** Select a bit stream for the ROI from Lowest, Lower, Low, Medium, Higher and Highest.
- **Non-ROI frame rate Fps:** Set the frame rate outside of the ROI; the smaller the value, the higher the image quality in the ROI. The frame rate range depends on the video standard and the resolution. It varies from 1 to 25 Fps. (Note: Different non-ROI frame rates may be given to different ROIs, but the lowest value among them will be used as the frame rate applied to the non-ROI area on the preview frame).

Press **Save** to save the desired setting.

9.2 RECORD

9.2.1 ENCODE

Select Encode in the Record menu to access the page below.



The following bit streams are available by default:

- **Main stream**, **Substream** and **Mobile Stream**: The resolution, frame rate, video code, encryption level, bitrate control, bitrate modality, bitrate frequency, audio and frame interval can be set for the main stream, the substream and the stream for mobile devices respectively.
- **Resolution:** Sets the resolutions for the respective bit streams. The maximum resolution for the main stream is 2592x1944(for Tc 5MPro) and 3840x2160 (for Tc 4K). The maximum resolution for the substream is 1920x1080. The resolutions for mobile devices are 640x480, 320×480.
- **FPS:** When the refresh rate is 50Hz, the maximum available FPS is 25 fps. When the refresh rate is 60Hz, the maximum available FPS is 30 fps.
- **Video Code Type:** Sets the video encoding (H265/H264) for each bit stream.
- **Video Code Level:** Main Profile
- **Bitrate control:** Sets the constant (CBR) or variable (VBR) bitrate for the stream.
- **Bitrate Mode:** User-defined or Predefined.
- **Bitrate:** To set the Bitrate level

Note:

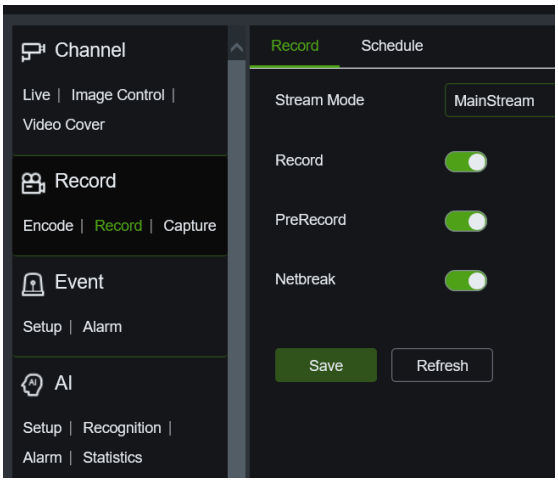
  - The range of the main bit stream is 256-12288.
  - The range of the substream is 64-2048.
  - The mobile flow range is 64-2048.

- **I Frame Interval:** is an interval to improve image quality. The selectable range is from 1 to 100 for the Main stream, 1 to 40 for the Sub stream and 1 to 12 for the Mobile stream.
- **Audio:** Enables audio for each bit stream.

Press **Save** to save the desired setting.

9.2.2 RECORD

This function allows you to enable recording to an SD card (if present):



- *Stream mode*: recording mode (main stream or substream)
- *PreRecord*: pre-recording
- *Netbreak*: If you have no connectivity, use your SD as a backup recording until connectivity is restored

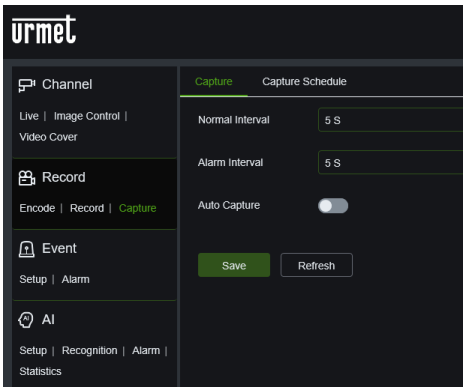
9.2.3 SCHEDULE

Select Schedule in the menu Record to access the page below.

Example: a grid in the table is equivalent to 30 minutes; green indicates continuous recording.

9.2.4 CAPTURE

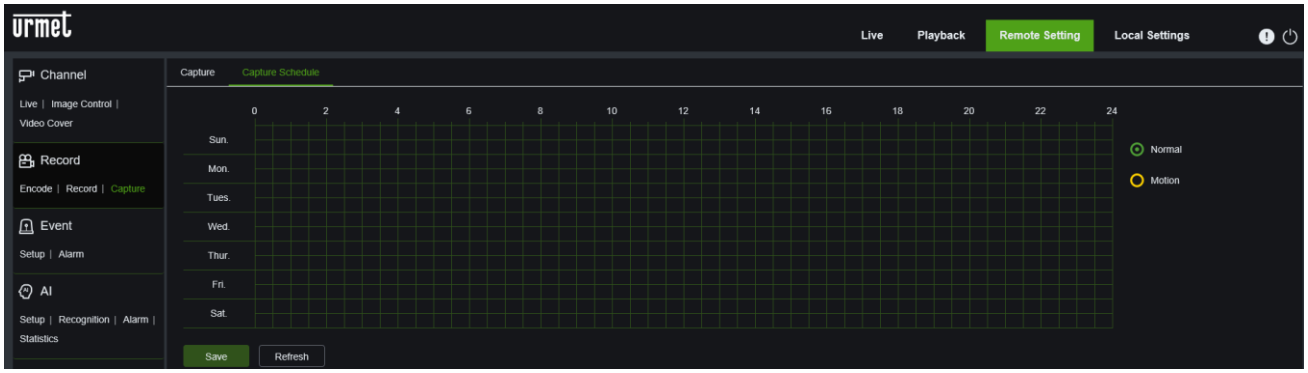
This subsection allows you to configure the parameters dedicated to capturing images in alarm conditions and programming the time slots within which the function is to be active.



- **Normal Interval:** interval between the capture of two images.
- **Alarm Interval:** Time interval for capturing an image in the event of a motion or I/O alarm.
- **Auto Capture**: Enable or disable automatic capture on the camera

9.2.5 CAPTURE SCHEDULE

This item allows you to configure the time slots and days of the week when the capture function is to be operational.

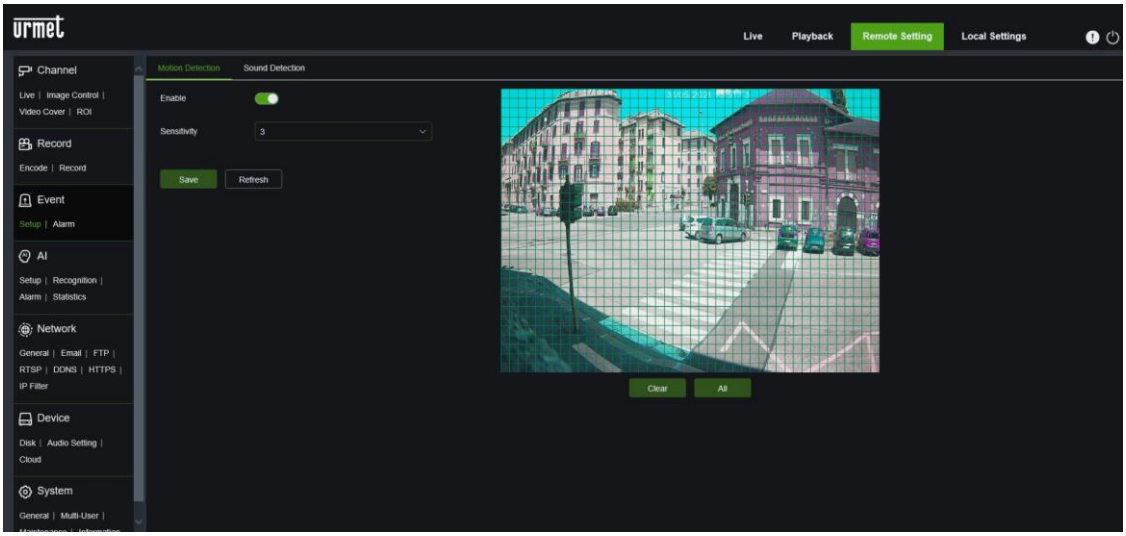


Normal: When the time slot is marked in green, this indicates that the channel performs normal recording in that time slot.
Motion: When the time slot is marked in yellow, this indicates that the channel only performs recording if motion is detected in that time slot.
No Record: A time slot marked in black indicates no scheduled recordings.
Once the programme is complete, press the **Save** button.
Press the **Refresh** button to update the parameters.

9.3 EVENT

9.3.1 SETUP

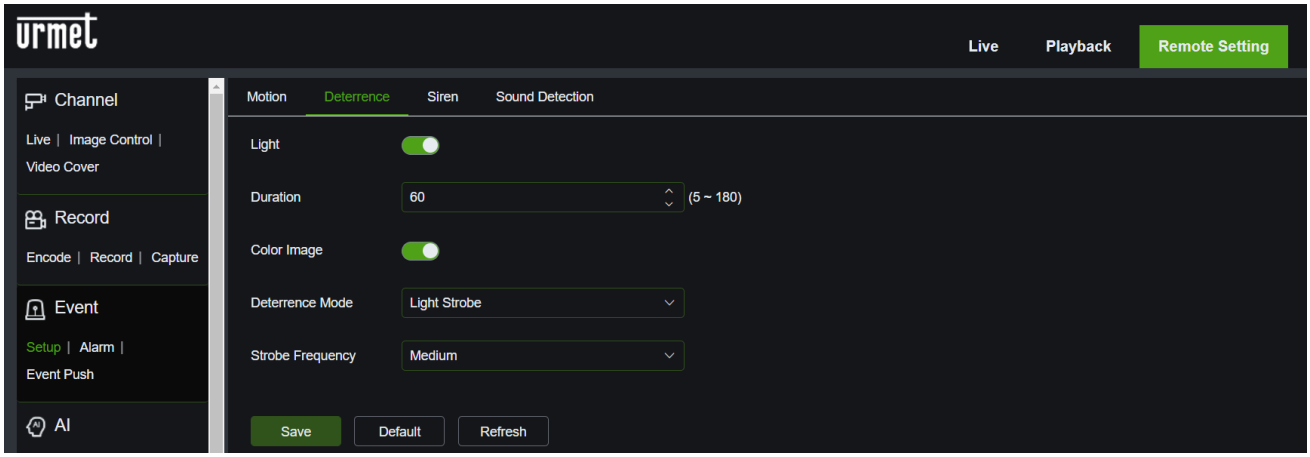
9.3.1.1 Motion detection



Motion detection setting procedure:

- Select Enable
- Click and hold the left mouse button on the image and drag out an area for motion detection.
- Set the motion detection sensitivity (from 1 to 8; the higher the value, the greater the sensitivity).

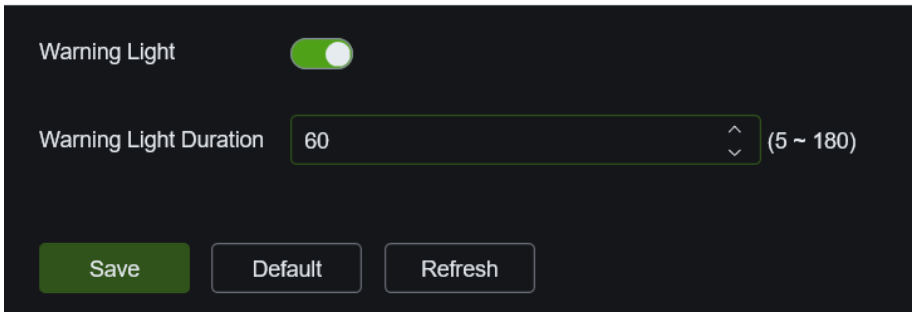
9.3.1.2 **Deterrence** *Only for certain models*



- **Light:** if enabled, it allows to turn on the white light for deterrence event.
- **Duration:** it's possible to setup the duration (in seconds) of the light after a deterrence event with a range from 5 to 180.
- **Color image:** if enabled (green), when the camera is on alarm, it switches to colors. If disabled (grey), the camera only switches to colour when in alarm if it detects sufficient light.
- **Deterrence mode:** Light warning (white lights are used steady on in case of deterrence. Light strobe (white lights are used flashing in case of deterrence).
- **Strobe frequency:** High, medium and low can be selected.

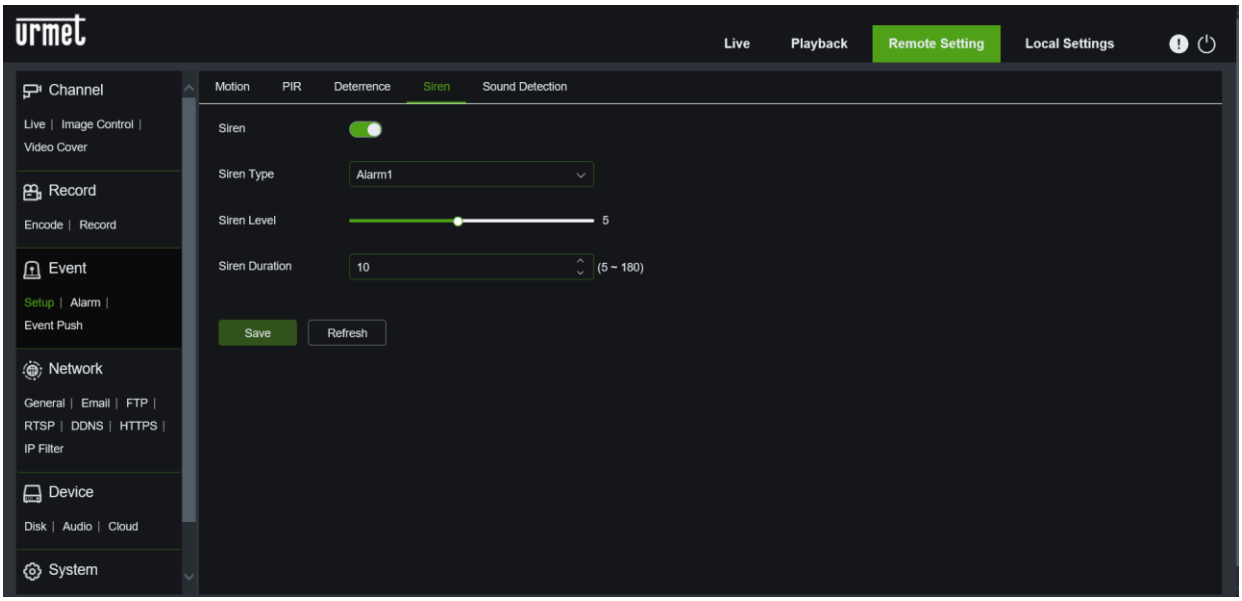
Press **Save** to save changes.

In some models there is a deterrence light configuration (red/blue light):



- **Warning Light**: if enabled (green) allows the red/blue light to come on in the event of a deterrence event.
- **Warning Light Duration**: The duration (in seconds) of the light in the event of an event can be set on a scale from 5 to 180.

9.3.1.3 **Siren** *Only for certain models*

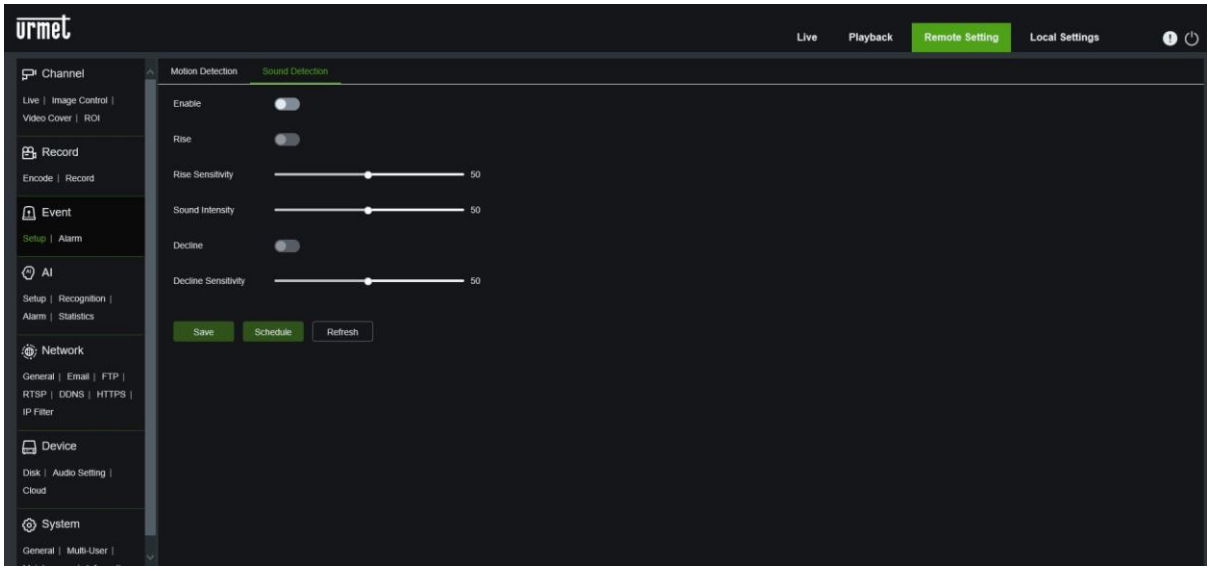


- **Siren:** allows to enable the siren with a detected event.
- **Siren Type:** choose between Alarm1, Alarm2 or User-defined1/2/3.
- **Siren Level:** it's possible to setup the volume of the sound of the siren with a range from 1 to 10.
- **Siren Duration:** it's possible to setup the duration (in seconds) the sound of the siren after the alarm event with a range from 5 to 180.

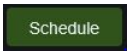
Press **Save** to save the changes.

9.3.1.4 Sound detection

This function allows you to detect sound in the external environment if the IP camera model has an audio microphone connection.



- **Enable**: enable or exclude the Sound Detection function.
- **Rise**: enable or exclude the sound detection Rise function
- **Rise Sensitivity**: set to between 0 and 100; the default value is 50.
- **Sound intensity**: set to between 0 and 100; the default value is 50.
- **Decline**: enable or exclude the sound detection Decline function.
- **Decline Sensitivity**: set to between 0 and 100; the default value is 50.

By clicking on the 

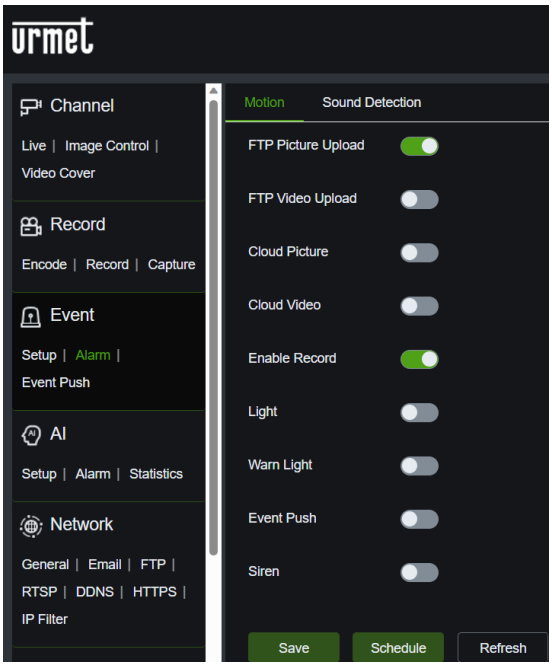
button, you can schedule the activation of the sound detection function.

IMPORTANT NOTE:

- Sending push notifications is not available for **the sound detection** event using the connected Camera alone. If you want to receive push notifications on the App regarding this type of event, you must associate and connect the IP Camera to NVR/HVR.

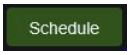
9.3.2 ALARM OUTPUT SETTINGS

9.3.2.1 Motion detection



- **Latch Time**: To set the alarm output time (5S,10S, 20S, 30S). [for models where featured]
- **Post Recording**: When Enable Record is enabled, the recording delay can then be set (5S, 10S, 20S, 30S).
- **Send Mail**: a function used with SMTP to enable the sending of e-mail.
- **FTP Picture Upload:** enables or disables sending images to an FTP server
- **FTP Video Upload:** enables o disables sending videos to an FTP server.
- **Cloud Picture:** enables or disables sending images to a cloud Dropbox.
- **Cloud Video:** enables or disables sending videos to cloud Dropbox.
- **Alarm Out**: enables or disables the alarm output.
- **Enable Record:** enables or disables the record.
- **Light:** enables or disables the white light.
- **Warn Light:** enables or disables the deterrence light.
- **Event Push:** enables or disables the push notification.
- **Siren:** enables or disables the siren.

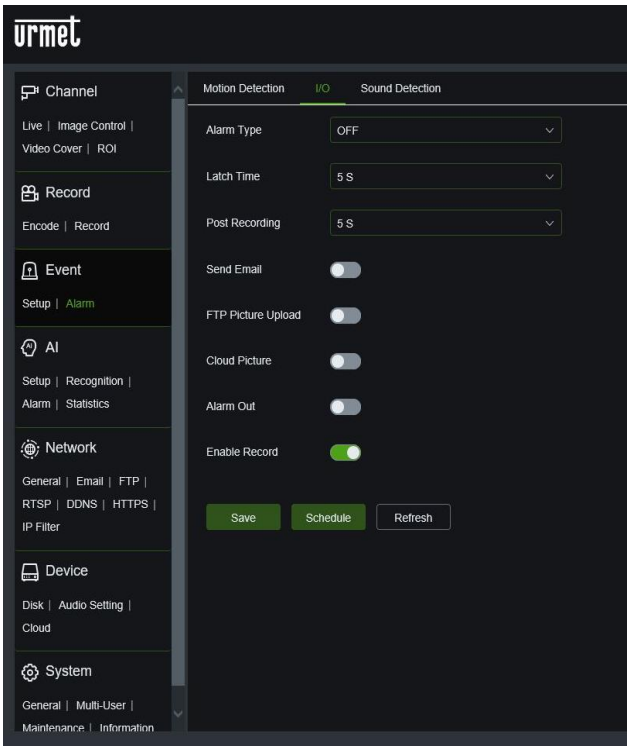
(Note: When any object moves within the target area, a green letter “M” is displayed in the preview frame).

Click on  the buttons to schedule the output actions for a Motion event:

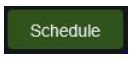
Send an email, switch the alarm output (if provided), send an image to an FTP Server, send an image to the cloud (Dropbox) or enable recording on an SD card.

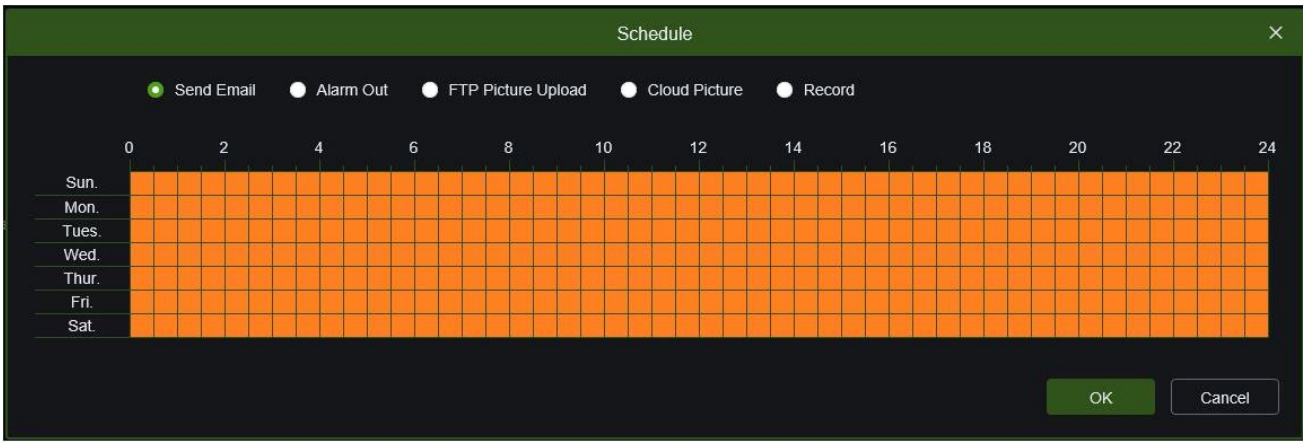
Press **Save** to save the desired setting.

9.3.2.2 I/O (Input/Output) [where featured]



- **Alarm Type**: Available values: OFF, Normally-Open, Normally-Closed.
- **Latch Time**: Set the alarm output time (5S,10S, 20S or 30S). [for models where featured]
- **Post Recording**: When Enable Record is selected, the recording delay can then be set (5S, 10S, 20S or 30S).
- **Send Mail**: a function used with SMTP to enable the sending of e-mail.
- **FTP Picture Upload:** enables or disables sending images to an FTP Server
- **Cloud Picture:** enables or disables sending images to a Cloud Dropbox
- **Alarm Out**: enables or disables the alarm output.
- **Enable Record**

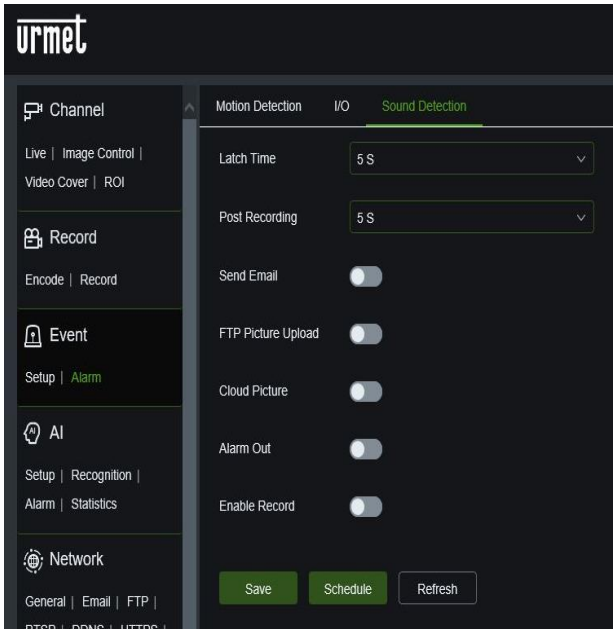
Click on the  button to schedule the output actions for an Alarm Input (if included):



Send an email, switch the alarm output (if included), send an image to an FTP Server, send an image to the cloud (Dropbox) or enable recording on an SD card.

Press **Save** to save the desired setting.

9.3.2.3 Sound detection



- **Latch Time**: To set the alarm output time (5S,10S, 20S, 30S). [for models where featured]
- **Post Recording**: When Enable Record is selected, the recording delay can then be set (5S, 10S, 20S or 30S).
- **Send Mail**: a function used with SMTP to enable the sending of e-mail.
- **FTP Picture Upload:** enables or disables sending images to an FTP Server
- **FTP Video Upload:** enables o disables sending videos to an FTP server.
- **Cloud Picture:** enables or disables sending images to a Cloud Dropbox
- **Cloud Video:** enables or disables sending videos to cloud Dropbox.
- **Alarm Out**: enables or disables the alarm output.
- **Enable Record:** enables or disables the record.
- **Event Push:** enables or disables the push notification.

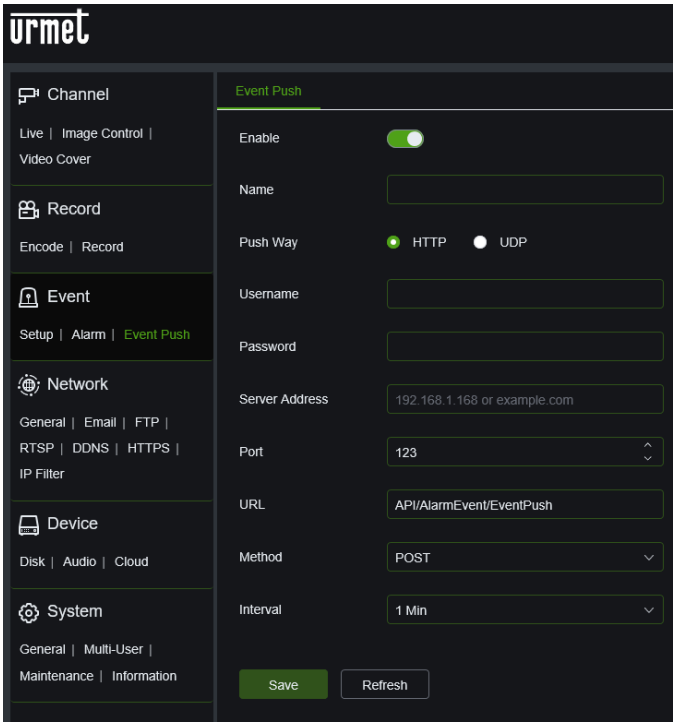
Click on Schedule the button to schedule the output actions for a sound detection:

Send an email, switch the alarm output (if included), send an image to an FTP Server, send an image to the cloud (Dropbox) or enable recording on an SD card.

Press **Save** to save the desired setting.

9.3.3 EVENT PUSH

In this section, you can enter the server on which to receive Push notifications.



- **Enable:** Enables the functionality of sending PUSH to an HTTP or UDP server.
- **Name:** Enter the name of the server.
- **Push Way:** Choose the server type between HTTP and UDP server.
- **Username:** To be filled in if the HTTP or UDP server requires authentication.
- **Password:** To be filled in if the HTTP or UDP server requires authentication.
- **Server Address:** Enter the server address.
- **Port:** Enter the server port number.
- **URL:** You can use the default URL or change it.
- **Method:** Select the method of transmitting the notification between POST and GET.
- **Interval:** Set the interval, in minutes, of the sending to the server. You can choose between OFF, 1 min, 5 min and 10 min.

- Press **Save** to save the desired setting.

9.4 IA (INTELLIGENT ALARM)

This section briefly describes the intelligent video analysis functions capable of generating specific events that can also be recorded on a remote NVR.

IMPORTANT:

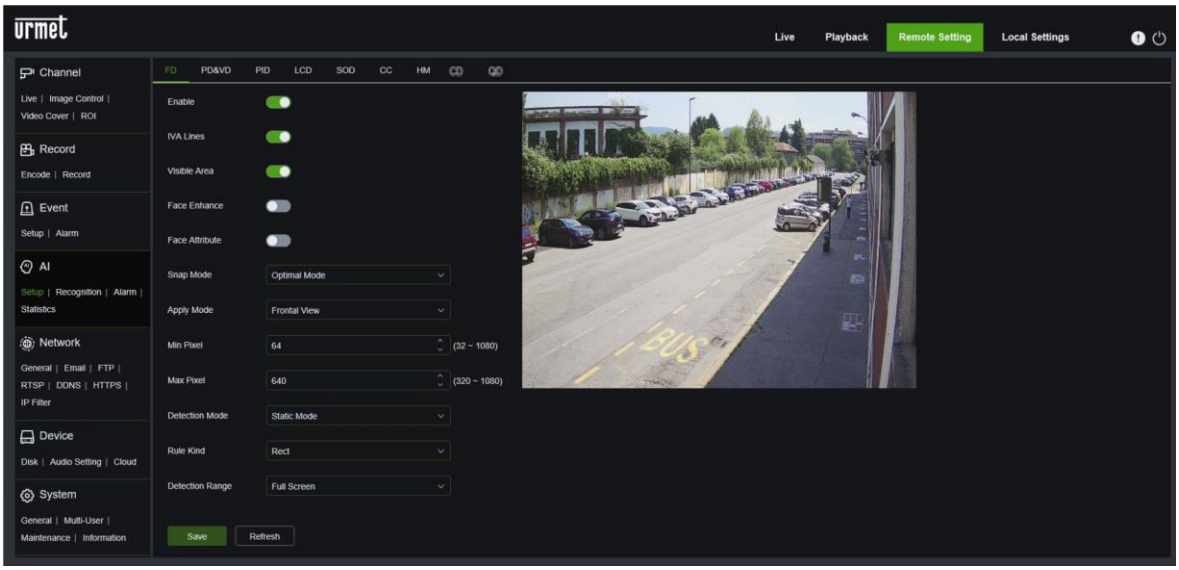
1) The video content analysis algorithms described in this section are based on an automatic analysis of the scene filmed by the camera device, which is capable of automatically processing the images. The algorithms may, in some conditions, generate false alarms or fail to detect certain events.
   In this sense, therefore, they cannot be considered zero-error-rate analysis systems.
2) The efficiency of the video analysis algorithms strictly depends on the level of quality of the image filmed by the camera.
3) After activation of any video analysis algorithm, you must wait for a period of 30-60 seconds for initialisation of the function. During this period, the video analysis algorithm is not operational.
4) To enable recordings, set the programming in the Schedule menu and ensure that there is available free space in the memory drive.
5) The letter **S** (in green) at the bottom centre of the image indicates an intelligent analysis event in progress without video recording. If recording is enabled and the Schedule has been programmed, the letter **S** (in red) will appear at the bottom centre of the image for all intelligent analysis events.
6) The following two groups of algorithms: PID / LCD / SOD and PD / FD / CC are mutually exclusive and cannot be activated at the same time.
7) When the three algorithms PID / LCD / SOD are activated at the same time, the most recently configured scene has validity.
8) Dates and times can be programmed for intelligent video analysis.

9.4.1 SETUP

The following intelligent video analysis algorithms are available for this series of IP cameras: Face Detection (FD), Pedestrian & Vehicle Detection (PD&VD), Perimeter Intrusion Detection (PID), Line Crossing Detection (LCD), Stationary Object Detection (SOD), Line Crossing Counter (CC), Heat Map (HM), Crowd Density Detection (CD), Queue Length Detection (QD), Face Recognition (FR), License Plate Detection (LPD), Rare Sound Detection (RSD) and AI Schedule.

9.4.1.1 **FD:** Face Detection

This feature allows faces to be detected within a specific predefined area of the image.
The function also allows alarms to be generated if one or more faces are detected.

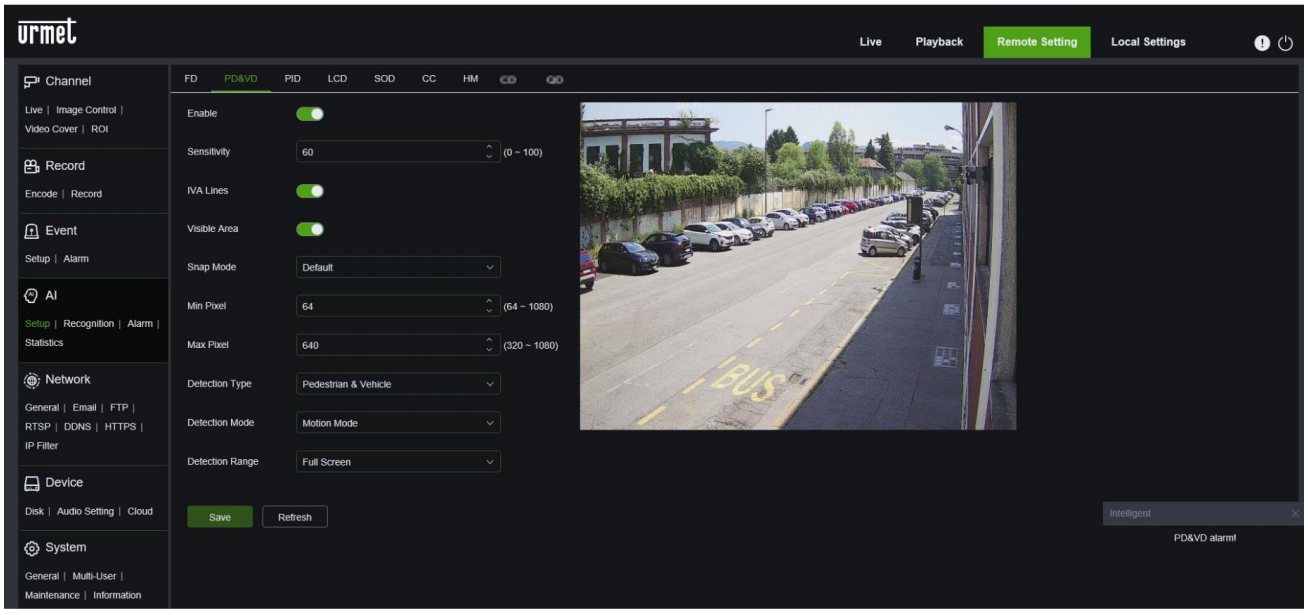


Enable: enables or disables the face detection function (FD).
IVA Lines: allows you to choose whether or not to show the face detection box.
Visible Area: allows you to choose whether or not to show the sensitive face detection area.

Face Enhance: enables the face enhancement function. By enhancing the effect of the face image, its capture during movement is improved. Activating this parameter requires more camera resources causing an inevitable loss of overall effect on the screen.
Face Attribute: if activated, faces can be discriminated on the basis of desired attributes (glasses, hat, mask, etc.).
Snap Mode: there are three recognition modes, optimal mode, real-time mode and interval mode.
- **Optimal Mode:** when the person enters the monitoring area, the camera will always detect. After the person has left the monitoring area, the best and clearest of the images captured during this time will be sent to the device.
- **Realtime Mode:** an image will be sent to the device at the moment the person enters the monitoring area and a second image will be sent to the NVR when the person has left the monitoring area.
- **Interval Mode:** the maximum number of times and the interval at which each image is sent to the device can be set.
Snap number: The number of push images per face detection can be set from 1, 2, 3 up to unlimited, i.e. send images to the device one, two, three or infinite times. (Note: this function is available in interval mode)
Snap Frequency: n s / pic (n can be set to 1-255), chooses the best snapshot every N seconds and sends it to the device.
Apply Mode: there are three apply modes, frontal view, multi-angle and customise.
- Frontal View: images only in frontal view
- Multi angle: captures images from multiple perspectives
- Customise: customised detection angle
Roll Range: face capture roll range can be set from 0 to 180.
Pitch Range: the face capture pitch range can be set from 0 to 180.
Yaw Range: the YAW range of face capture can be set from 0 to 180.
Picture Quality: the picture quality of face capture can be set from 0 to 180.
Min Pixel: lowest pixel setting of the person. No alarm is generated when the recognised person is smaller than the set pixel. Can be set to 64-1080. Note: The figure recognition function sees the entire image as a 1080p image.
Max Pixel: highest pixel setting of persons. No alarm is generated when the recognised person is larger than the set pixel. Can be set to 32-1080. Note: The figure recognition function sees the entire image as a 1080p image.
Detection Mode: there are two types of detection, static mode and motion mode.
- Motion Mode: captures the face and person in motion.
- Static Mode: captures the person and their face when stationary.
Rule Kind: there are two rules, rectangular and linear.
- Rectangular: there are two modes for setting the rectangular detection area.
Full screen: the detection area coincides with the camera's coverage area.
Customise: if this mode is selected a region box will appear in the right-hand window. Select the small red box next to the region's digital ID box to change the area itself.
- Linear: there are two types of rules, A→ B and B → A.
Rule Type: there are two types, A→ B and B → A. Draws a regular line from A to B (or B to A) on the area. When the face moves from A to B (or B to A), the rule will be activated to capture the human face.
Save: to save the set parameters.
Refresh: to refresh the parameters.
(Note: 'S' will appear on the channel and a pop-up window will appear in the bottom left corner of the screen. PID / LCD and PD & VD / FD are mutually exclusive and cannot be enabled simultaneously).

9.4.1.2 **PD&VD:** Pedestrian Detection & Vehicle Detection

This feature allows automatic detection of people/vehicles passing across the image or a portion/area of it.
The function allows alarms to be generated when a person/vehicle in transit is detected.

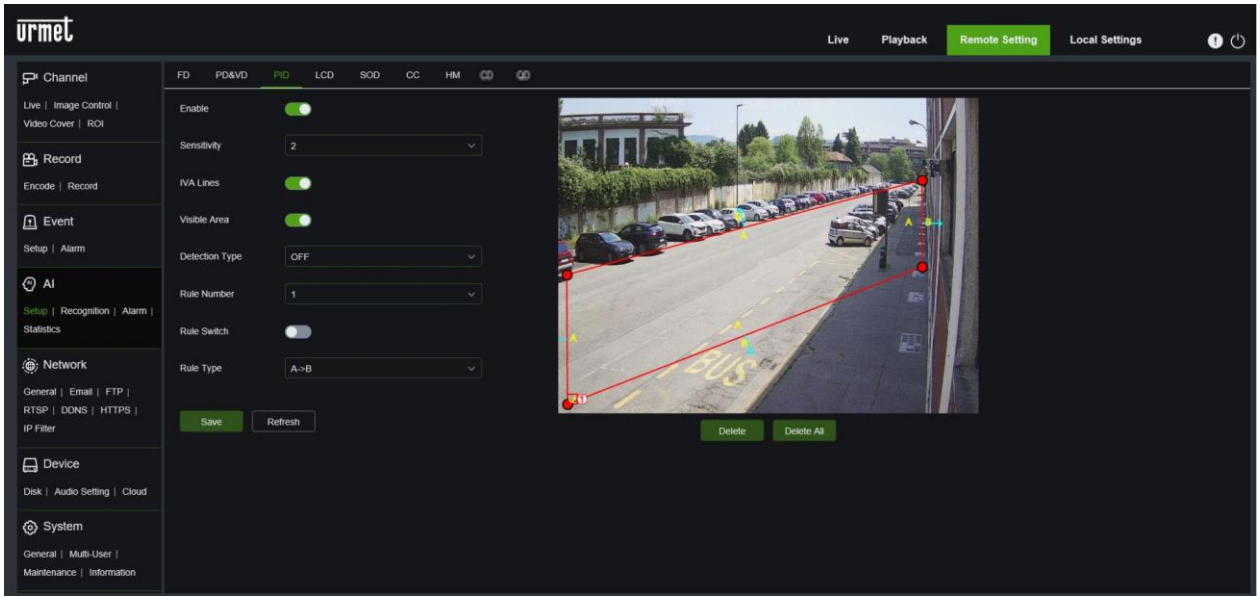


Enable: enables or disables the pedestrian and vehicle detection function (PD & VD)
Sensitivity: can be a value from 0 to 100. The larger the value, the more accurate and similar the detection will be to the set pedestrian and vehicle shape. The default value is 60.
IVA Lines: allows you to choose whether or not to show the pedestrian and vehicle detection box.
Visible Area: allows you to choose whether or not to show the sensitive pedestrian and vehicle detection area.
Snap Mode: there are three detection modes, default mode, real-time mode and interval mode.
- Default Mode: when the person or vehicle enters the monitoring area, the camera will always detect. After the person or vehicle has left the monitoring area, the best and clearest of the images captured during this time will be sent to the device.

- Realtime Mode: one image will be sent to the device when the person or vehicle enters the monitoring area and a second image will be sent to the NVR when the person or vehicle has left the monitoring area.
- Interval Mode: the maximum number of times and the interval for sending each image to the device can be set.
Snap number: the number of push images for each person/vehicle detection can be set from 1, 2, 3 up to unlimited, i.e. send the images to the device one, two, three or infinite times. (Note: this function is available in interval mode)
Snap Frequency: n s / pic (n can be set to 1-255), chooses the best snapshot every N seconds and sends it to the device.
Min Pixel: lowest pixel setting of person and vehicle. No alarm is generated when the recognised human or vehicle is smaller than the set pixel. Can be set to 64-1080. Note: The figure recognition function sees the entire image as a 1080p image.
Max Pixel: highest pixel setting of the person and vehicle. No alarm is generated when the recognised human or vehicle is larger than the set pixel. Can be set to 32-1080. Note: The figure recognition function sees the entire image as a 1080p image.
Detection Type: can be set to pedestrians only, vehicles only or pedestrians and vehicles.
Detection Mode: there are two types of detection, static mode and motion mode.
- Motion Mode: captures the person or vehicle in motion.
- Static Mode: captures the person or vehicle stationary.
Detection Range: sets the detection area. It is possible to choose between two modes: full screen and customise.
- Full screen: the detection area coincides with the coverage area of the camera.
- **Customise**: if this mode is selected a region box will appear in the right-hand window. Select the small red box next to the region's digital ID box to change the region itself.
Save: to save the set parameters.
Refresh: to refresh the parameters.
(Note: 'S' will appear on the channel and a pop-up window will appear in the bottom left corner of the screen. PID / LCD and PD & VD / FD are mutually exclusive and cannot be enabled simultaneously).

9.4.1.3 **PID:** Perimeter Intrusion Detection

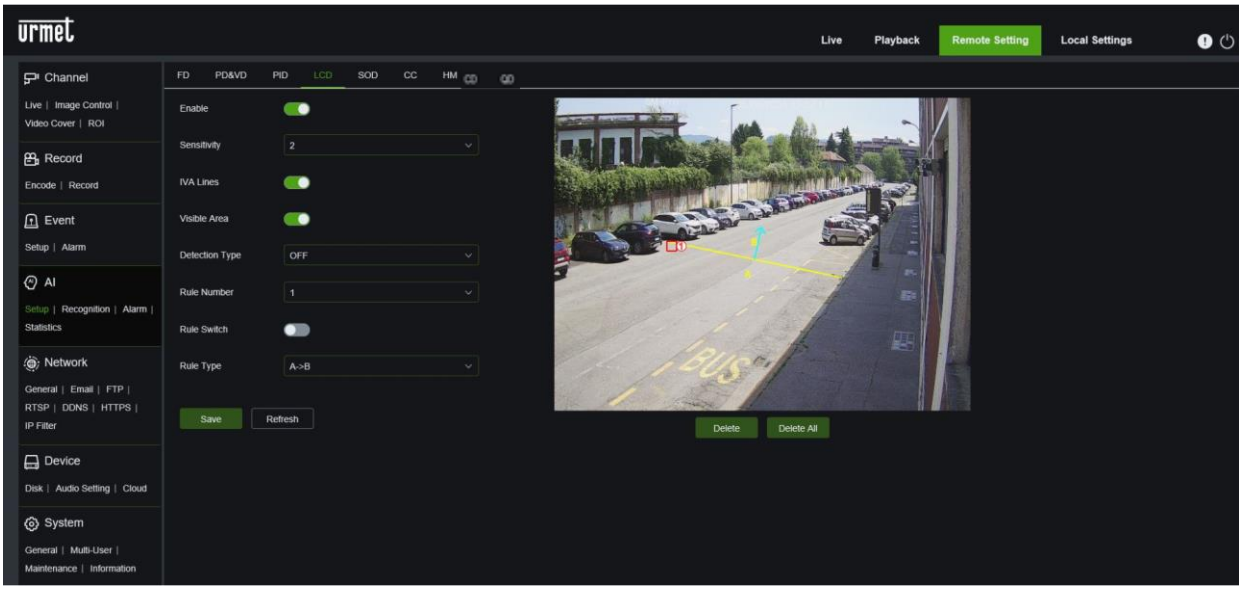
Automatic detection of entry or exit of an object/person in a specific area of the image, delimited by a manually defined box. Press on the area and draw a zone with four points and set it as a perimeter intrusion detection rule. Up to four rule areas can be created and each rule corresponds to a digital ID. Select the red box next to the rule ID to drag and drop the perimeter intrusion detection rule area.



Enable: enables or disables the detection of an object/person entering and leaving a defined area (PID).
Sensitivity: sensitive level, the range is 1 to 4 and the default setting is 3. If the sensitivity is higher, the moving object can be detected easily. At the same time, the probability of false alarms being detected is increased.
IVA Lines: allows you to choose whether or not to show the detection frame.
Visible Area: allows you to choose whether or not to show the sensitive detection area.
Detection Type: the selectable detection types are pedestrian and vehicle. If not activated, any type of object/person crossing the line will be detected.
Rule Number: up to 4 rules can be set. Draw a rule area on the image and select the next number to continue drawing more rules. Each rule type is independent and can be set separately.
Rule Switch: allows the rule to be activated.
Rule Type: can be set for each rule. A->B: movements in the direction from A to B can be detected.
B->A: movements in the direction B to A can be detected. A ⟷B can detect movements in both directions.
Save: to save the set parameters.
Refresh: to refresh the parameters.
(Note: 'S' will appear on the channel and a pop-up window will appear in the bottom left corner of the screen. PID / LCD and PD & VD / FD are mutually exclusive and cannot be enabled simultaneously).

9.4.1.4 **LCD:** Line Crossing Detection

This feature allows automatic detection of the crossing (in both directions) of a preset line by a moving object/person.
The function is used to generate alarms when the algorithm traces the movement of an object that crosses a line previously defined by the user.

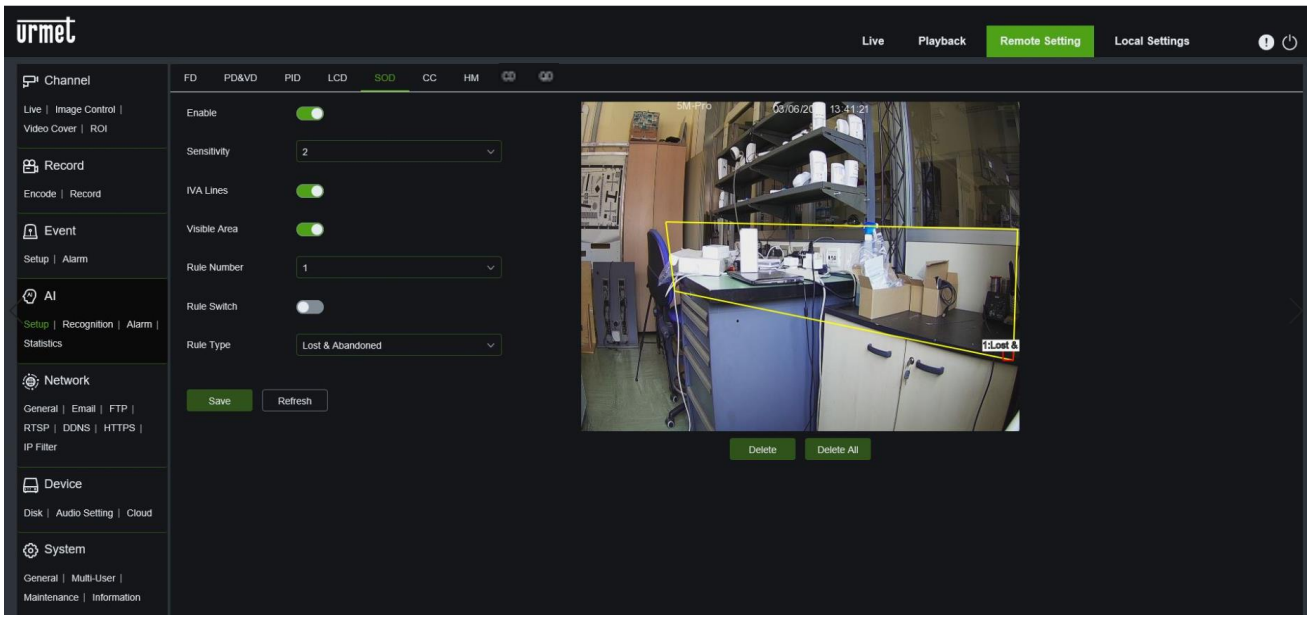


Enable: enables or disables line crossing detection (LCD).
Sensitivity: sensitive level, the range is 1 to 4 and the default setting is 2. If the sensitivity is higher, the moving object can be detected easily. At the same time, the probability of false alarms being detected is increased.
IVA Lines: allows you to choose whether or not to show the detection frame.
Visible Area: allows you to choose whether or not to show the sensitive detection area.
Detection Type: the selectable detection types are pedestrian and vehicle. If not activated, any type of object/person crossing the line will be detected.
Rule Number: up to 4 rules can be set. Draw a rule line on the image and select the next number to continue drawing more rules. Each rule type is independent and can be set separately.
Rule Switch: allows the rule to be activated.
Rule Type: can be set for each rule. A->B: movements in the direction from A to B can be detected.
B->A: movements in the direction B to A can be detected. A ⟷B can detect movements in both directions.
Save: to save the set parameters.
Refresh: to refresh the parameters.

(Note: 'S' will appear on the channel and a pop-up window will appear in the bottom left corner of the screen. PID / LCD and PD & VD / FD are mutually exclusive and cannot be enabled simultaneously).

9.4.1.5 **SOD:** Stationary Object Detection

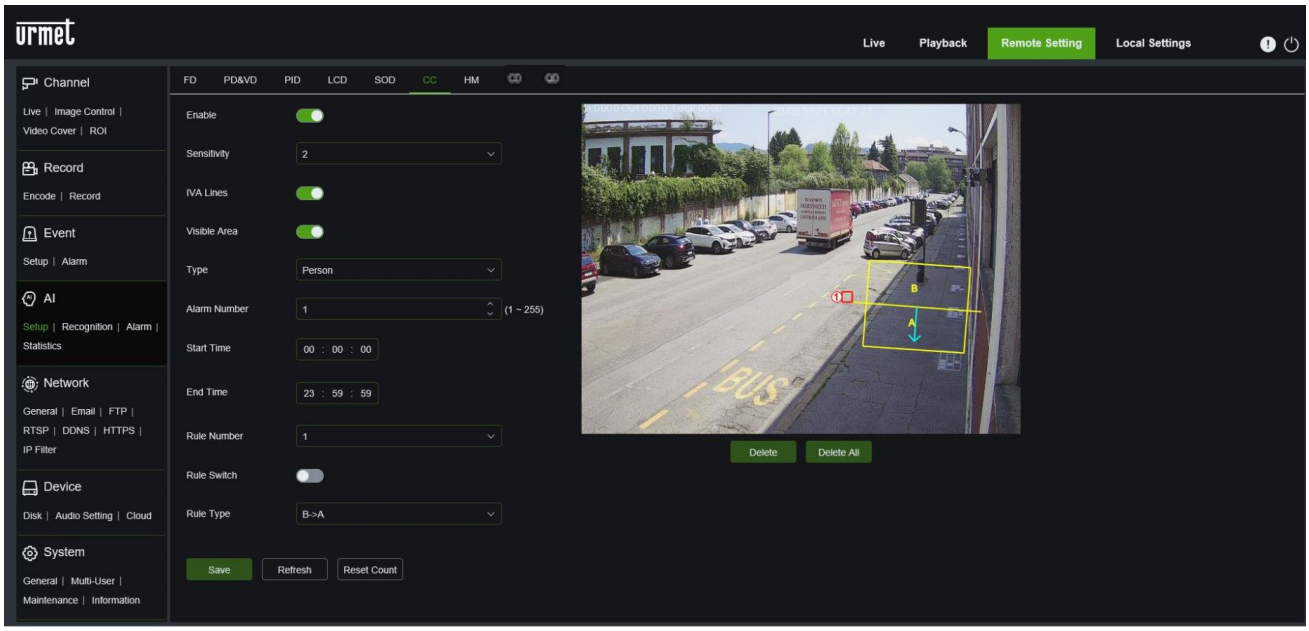
This feature allows automatic detection of a change regarding the presence of an object within a preset area.
The function is used to generate alarms in response to the “presence” or “removal” of an object in a previously defined area.



Enable: enables or disables the detection of a stationary object (SOD).
Sensitivity: sensitive level, the range is 1 to 4 and the default setting is 3. The higher the value, the more sensitive the SOD alarm.
IVA Lines: allows you to choose whether or not to show the detection box.
Visible Area: allows you to choose whether or not to show the sensitive detection area.
Rule Number: up to 4 rules can be set. Draw a rule area on the image and select the next number to continue drawing more rules. Each rule type is independent and can be set separately.
Rule Switch: allows the rule to be activated.
Rule Type: can be set for each rule. Lost means that something can be detected as missing. Abandoned means that abandoned objects can be detected. Lost & Abandoned means that lost and abandoned objects can be detected.
Save: to save the set parameters.
Refresh: to refresh the parameters.

9.4.1.6 **CC:** Line Crossing Counter

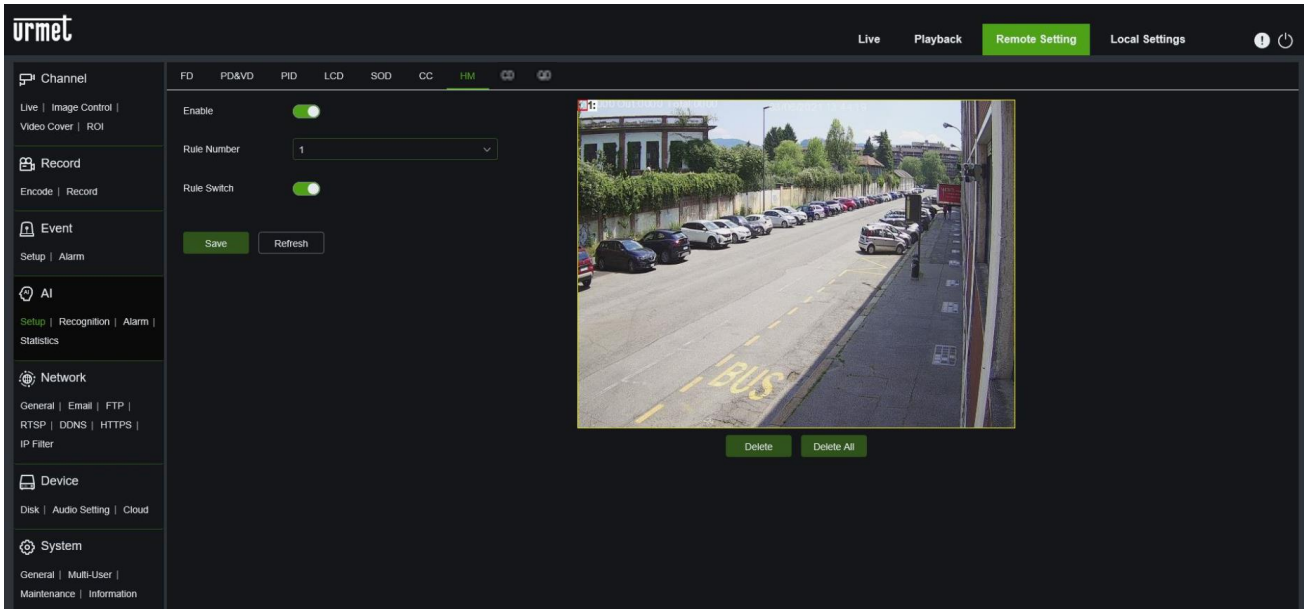
This feature allows automatic detection and counting of objects passing through the image if they cross a specific line in a given direction.
The function also allows alarms to be generated if the count increases.



Enable: enables or disables the detection and counting of objects passing through a line (CC).
Sensitivity: sensitive level, the range is 1 to 4 and the default setting is 2. The higher the value, the more sensitive the CC alarm.
IVA Lines: allows you to choose whether or not to show the detection box.
Visible Area: allows you to choose whether or not to show the sensitive detection area.
Type: Three types can be selected, person, vehicle, motion.
Alarm Number: Set the alarm number count. The value ranges from 1 to 255.
Start Time: Set the start time of detection.
End Time: Set the end time of detection.
Rule Number: Set the rule number.
Rule Switch: Set the rule to be activated.
Rule Type: A->B: Movement in the direction from A to B can be detected.
B->A: movements in the direction B to A can be detected. A ⟷B can detect movements in both directions.
Save: to save the set parameters.
Refresh: to refresh the parameters.
Reset Count: to reset the counter.

9.4.1.7 **HM:** Heat Map

The **Heat Map** function allows you to identify areas with the highest movement flows by colour overlay.
Warmer colours (orange, red) indicate the areas with the most activity.

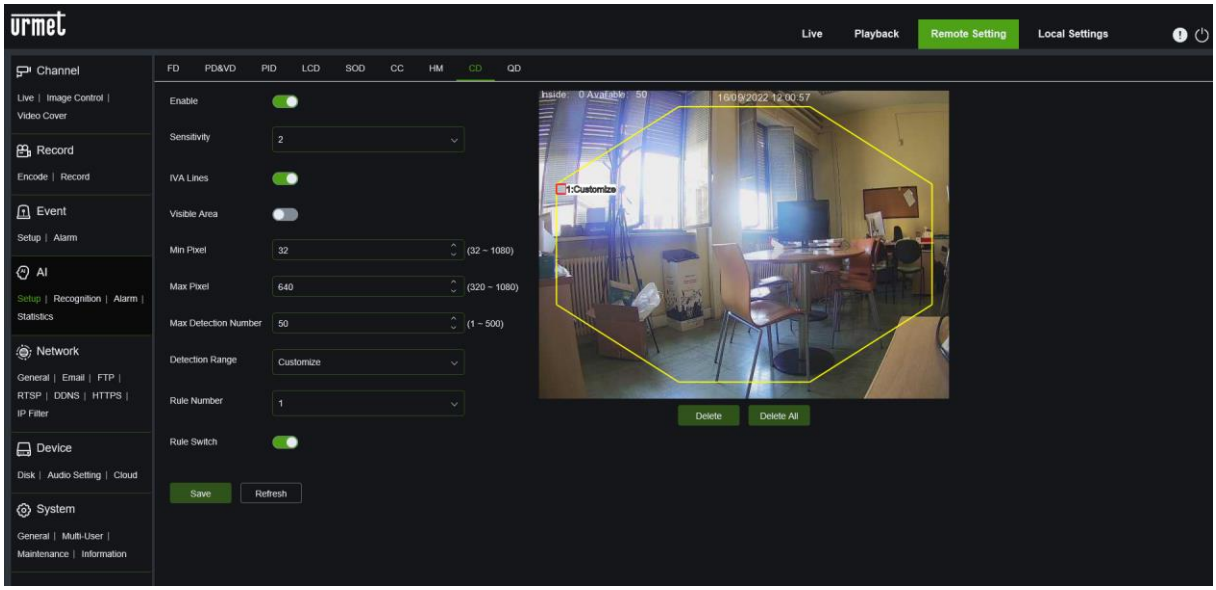


Enable: enables or disables the Heat Map (HM) function.
Rule Number: only one rule can be activated. The entire screen is selected as the default area. If you need to customise the area, check the box in the top left corner of the screen and drag the dots in the four corners of the screen to change the detection area.
Rule Switch: to activate the rule.

Save: to save the set parameters.
Refresh: to refresh the parameters.

9.4.1.8 **CD (Crowd Density Detection)**

The Crowd Density Detection function makes it possible to identify the presence of crowding in a specific area.



Enable: enables or disables the Crowd Density Detection (CD) function.
Sensitivity: sensitive level, the range is 1 to 4 and the default setting is 2. The higher the value, the more sensitive the CD alarm.
IVA Lines: allows you to choose whether or not to show the detection box.
Visible Area: allows you to choose whether or not to show the sensitive detection area.
Min Pixel: lowest pixel setting of the person. No alarm is generated when detected humans are smaller than the set pixel. Can be set to 32-1080. Note: The figure recognition function sees the entire image as a 1080p image.
Max Pixel: highest pixel setting of the person. No alarm is generated when recognised humans are larger than the set pixel. Can be set to 320-1080. Note: The figure recognition function sees the entire image as a 1080p image.
Max Detection Number: a value from 1 to 500 can be set.
Detection Range: there are two detection modes, full screen and customise.

- Full Screen: the detection area coincides with the camera's coverage area.
- Customise: if this mode is selected a region box will appear in the right window. Select the small red box next to the digital region ID box to change the region.

Rule Number: only one rule can be activated. The entire screen has been selected as the default area. If you need to customise the area, check the box in the top left corner of the screen and drag the dots in the four corners of the screen to change the detection area.

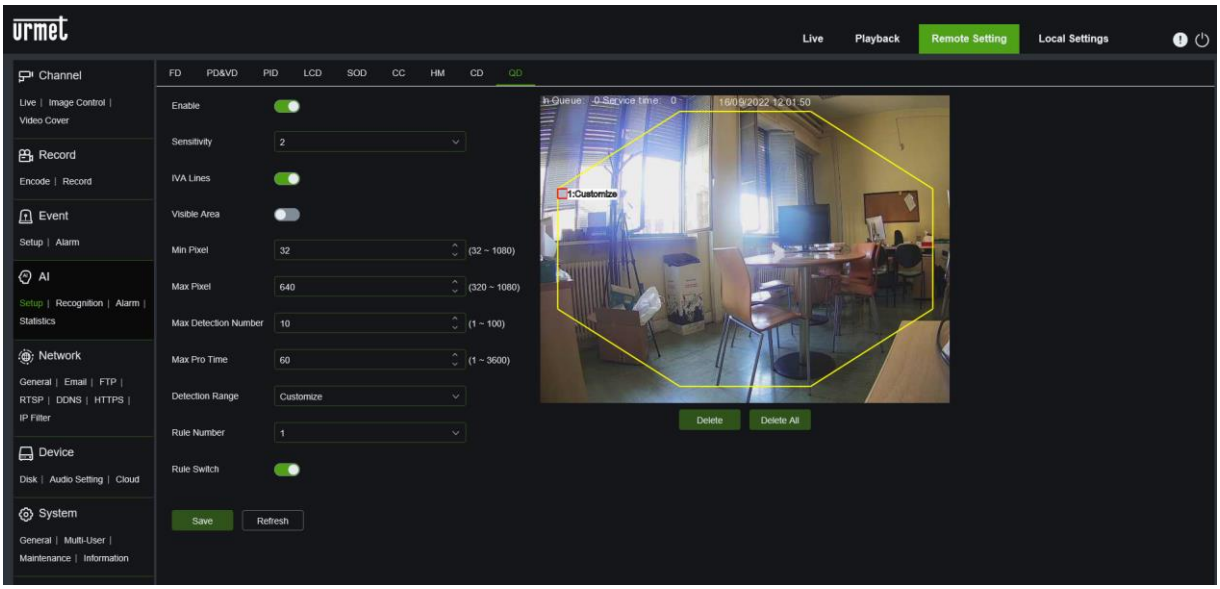
Rule Switch: to activate the rule.

Save: to save the set parameters.

Refresh: to refresh the parameters.

9.4.1.9 QD (Queue Length Detection)

The Queue Length Detection function makes it possible to detect several people queuing in a specific area.



Enable: enables or disables the Queue Length Detection (QD) function.

Sensitivity: sensitive level, the range is 1 to 4 and the default setting is 2. The higher the value, the more sensitive the QD alarm.

IVA Lines: allows you to choose whether or not to show the detection box.

Visible Area: allows you to choose whether or not to show the sensitive detection area.

Min Pixel: lowest pixel setting of the person. No alarm is generated when detected humans are smaller than the set pixel. Can be set to 32-1080. Note: The figure recognition function sees the entire image as a 1080p image.

Max Pixel: highest pixel setting of the person. No alarm is generated when recognised humans are larger than the set pixel. Can be set to 320-1080. Note: The figure recognition function sees the entire image as a 1080p image.

Max Detection Number: the maximum number of human detection can be set by choosing a value from 1 to 100.

Max Pro Time: the alarm will be activated if no-one has left the monitoring area for longer than the set time. A value from 1 to 3600 can be set.

Detection Range: there are two detection modes, full screen and customise.

- Full screen: the detection area coincides with the camera's coverage area.

- Customise: if this mode is selected a region box will appear in the right window. Select the small red box next to the digital region ID box to change the region.

Rule Number: only one rule can be activated. The entire screen has been selected as the default area. If you need to customise the area, check the box in the top left corner of the screen and drag the dots in the four corners of the screen to change the detection area.

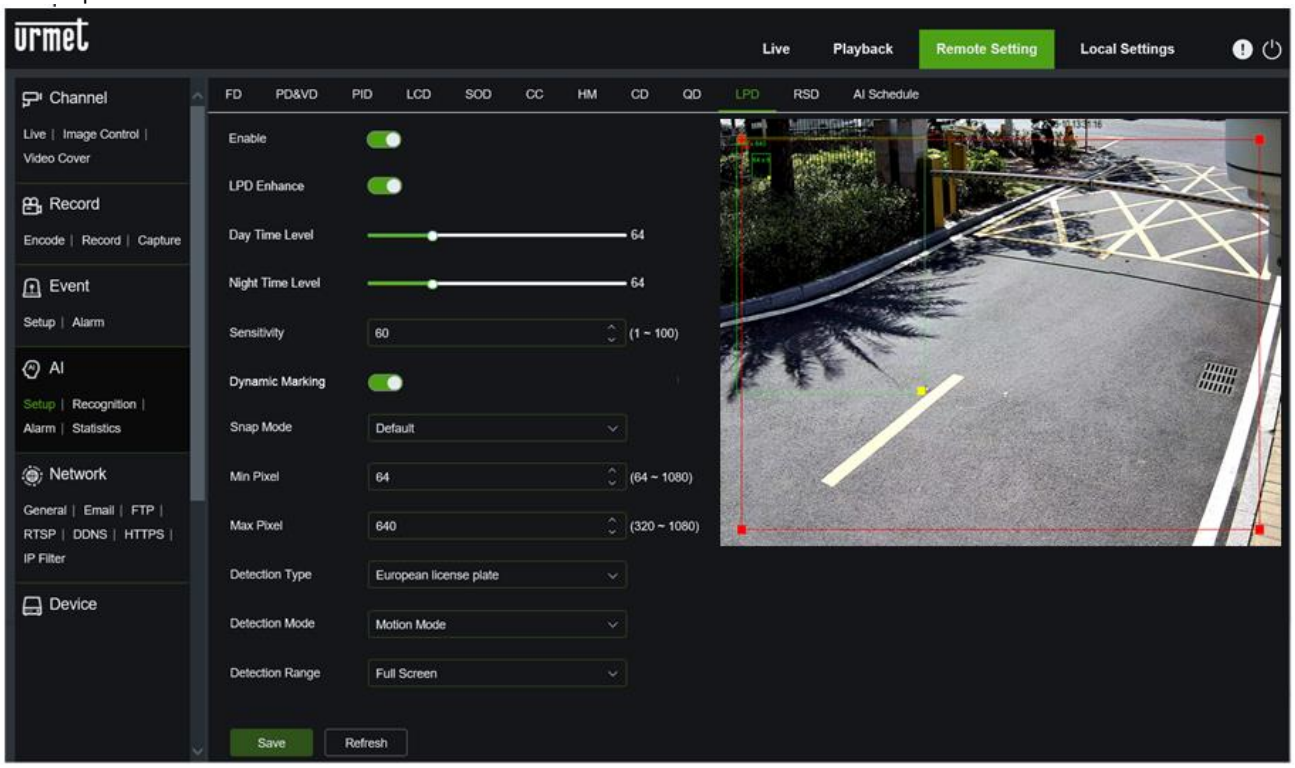
Rule Switch: to activate the rule.

Save: to save the set parameters.

Refresh: to refresh the parameters.

9.4.1.10 LPD (License Plate Detection)

This function allows the registration number of unknown vehicles or vehicles entered in the database to be recorded. Effective detection requires that the vehicle is not moving and that the positioning of the camera complies with certain requirements such as a certain distance from the number plate to be detected, a specific side angle and certain installation height. A backup of vehicle number plate information can also be performed. Currently, number plate detection supports European and American number plates.



Enable: Enables or disables the License Plate Detection (LPD) function.
LPD Enhance: If enabled, allows the performance of the licence plate reading algorithm to be improved.
Day Time Level: Allows you to set the level of HLC (High Light Compensation) during daylight hours.
Night Time Level: Allows you to set the level of HLC during night hours.
Sensitivity: The higher the value, the more sensitive the detection.
Dynamic Marking: If enabled, allows the motion detection frame to be displayed.
Snap Mode: There are three detection modes, default mode, real-time mode and interval mode.

- **Default Mode:** When the vehicle licence plate enters the monitoring area, the camera will always detect. After the vehicle licence plate has left the monitoring area, the best and clearest of the images captured during this time will be sent to the device.
- **Realtime Mode:** One image will be sent to the device at the moment the vehicle's licence plate enters the monitoring area and a second image will be sent to the NVR when the vehicle's licence plate has left the monitoring area.
- **Interval Mode:** The maximum number of times and the interval at which each image is sent to the device can be set.
  - **Snap number:** the number of push images per number plate detection can be set from 1, 2, 3 up to unlimited, i.e. send images to the device once, twice, three times or infinitely. (Note: this parameter is available in interval mode).
  - **Snap Frequency:** n s / pic (n can be set to 1-255), chooses the best snapshot every N seconds and sends it to the device. (Note: this parameter is available in interval mode).

Min Pixel: Setting the minimum pixel for number plate recognition. The licence plate must be larger than the set minimum pixel in order to be recognised. The value can be set from 64 to 1080.
Max Pixel: setting of the maximum number plate recognition pixel. The licence plate must be smaller than the set maximum pixel in order to be recognised. The settable value ranges from 320 to 1080.
Detection Type: Two types of number plate can be chosen: European number plate or American number plate.
Detection Mode: Two detection modes can be chosen, static mode or motion mode.

- **Motion Mode:** Captures the number plate of moving vehicles.
- **Static Mode:** Captures the number plate of stationary vehicles.

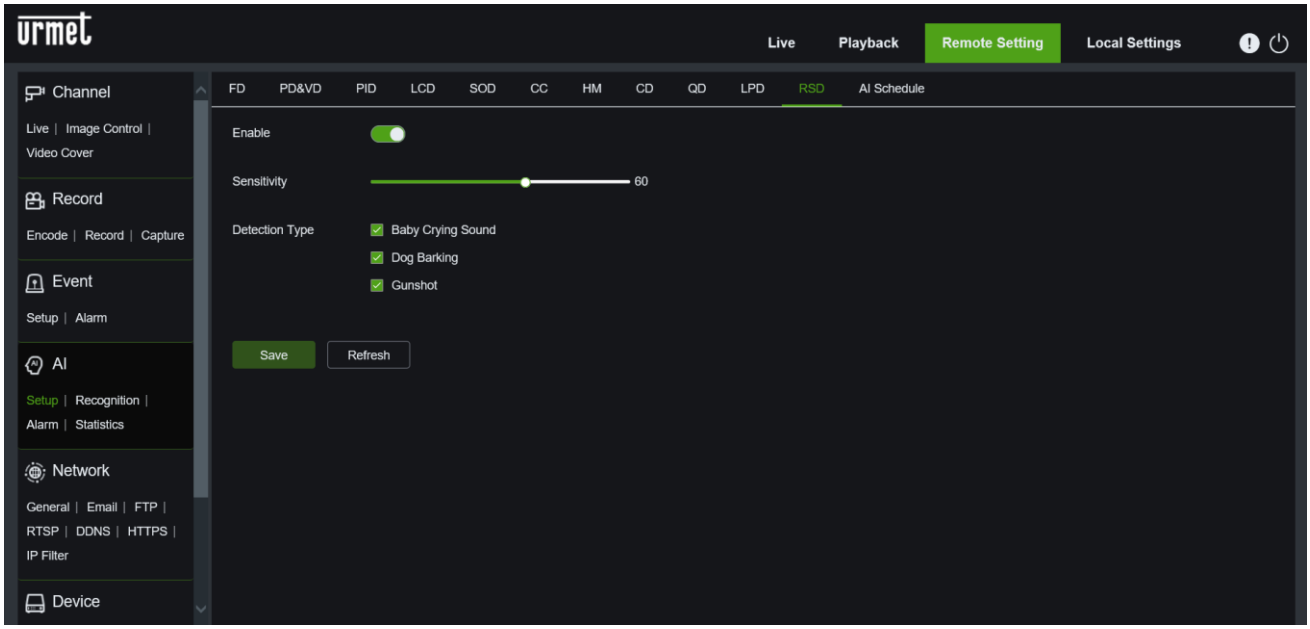
Detection Range: It is possible to choose between two detection ranges, full screen or customised.

- **Full Screen:** The detection area coincides with the coverage area of the camera.
- **Customize:** if this mode is selected a region box will appear in the right-hand window. Select the small red box next to the region's digital ID box to change the area itself.

Save: To save the set parameters.
Refresh: To refresh parameters.

9.4.1.11 RSD (Rare Sound Detection)

This function allows the camera to detect specific background noises, dog barking, a child crying and/or gunshot.



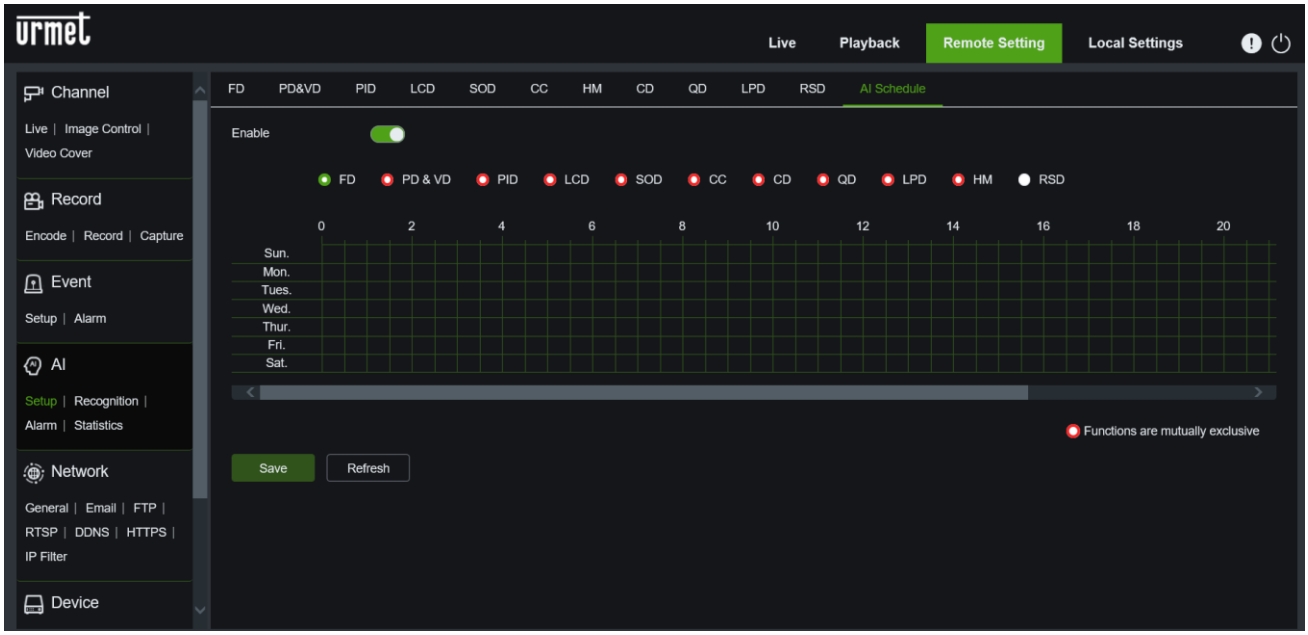
Enable: Enables or disables the Rare Sound (RSD) function.
Sensitivity: The higher the value, the more sensitive the detection. The value can be set from 1 to 100.
Detection Type: Three types of sounds can be chosen: baby crying, dog barking and gunshot.

- **Baby Crying Sound**: Check the box to activate cry detection.
- **Dog Barking:** Check the box to activate the barking dog detection.
- **Gunshot:** Check the box to activate gunshot detection.

Save: To save the set parameters.
Refresh: To refresh parameters.

9.4.1.12 IA Schedule

In this section it is possible to program for each type of AI alarm at which time slots the intelligent function algorithms are active.



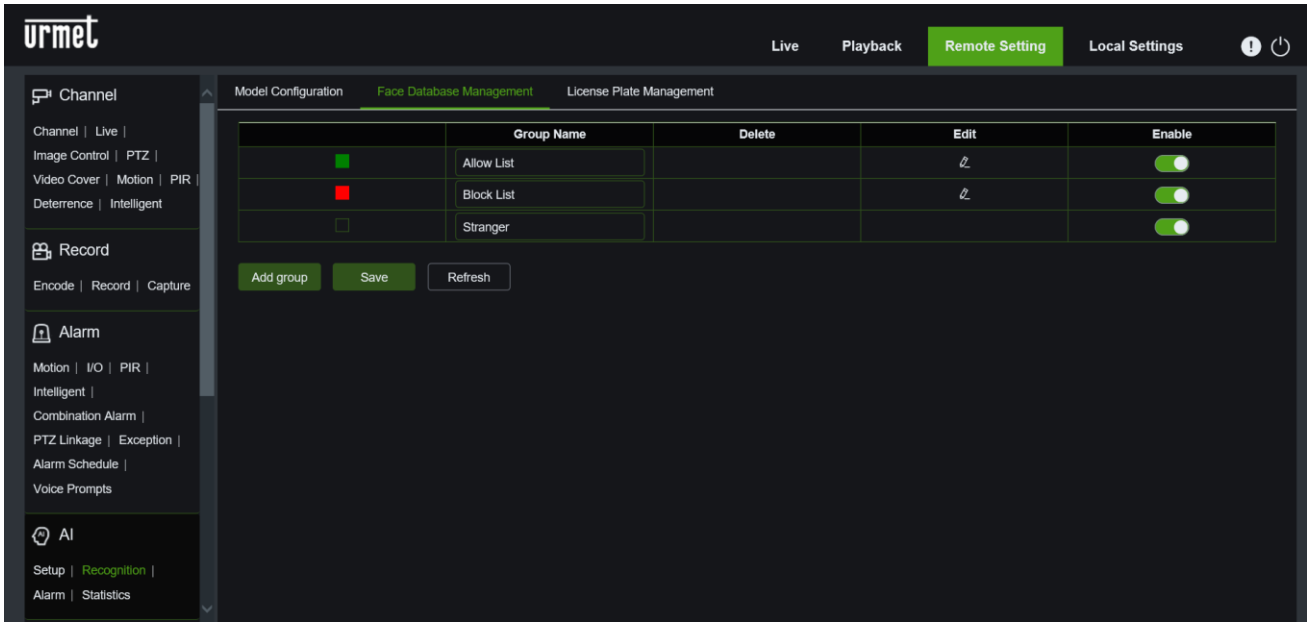
Enable: Enables or disables the schedule table.
Select the AI function and left-click the boxes in the table where you want to activate the function.
The functions are mutually exclusive.

Save: To save the set parameters.
Refresh: To refresh parameters.

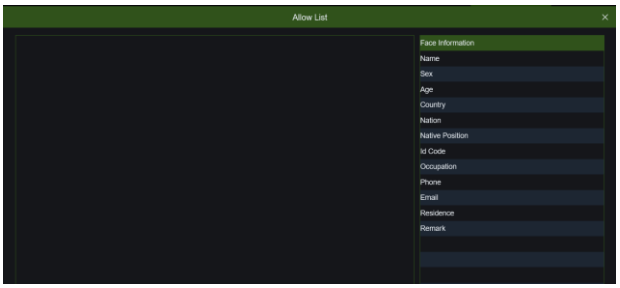
9.4.2 **RECOGNITION:** FACE RECOGNITION *ONLY FOR CERTAIN MODELS*

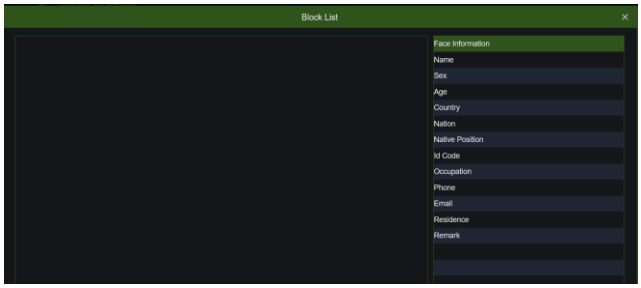
9.4.2.1 Face Recognition (FR)

This feature allows you to detect the human faces filmed in the scene, and then perform automatic comparisons to check the similarity between them. This specific feature can be configured and used from the Camera and from the NVR on which the camera has been set for recording.



Enable: enables the list of allowed/ banned/unknown faces.
Allow List Edit: imports face images into the allowed list.
Block List Edit: imports images of faces in the banned list.



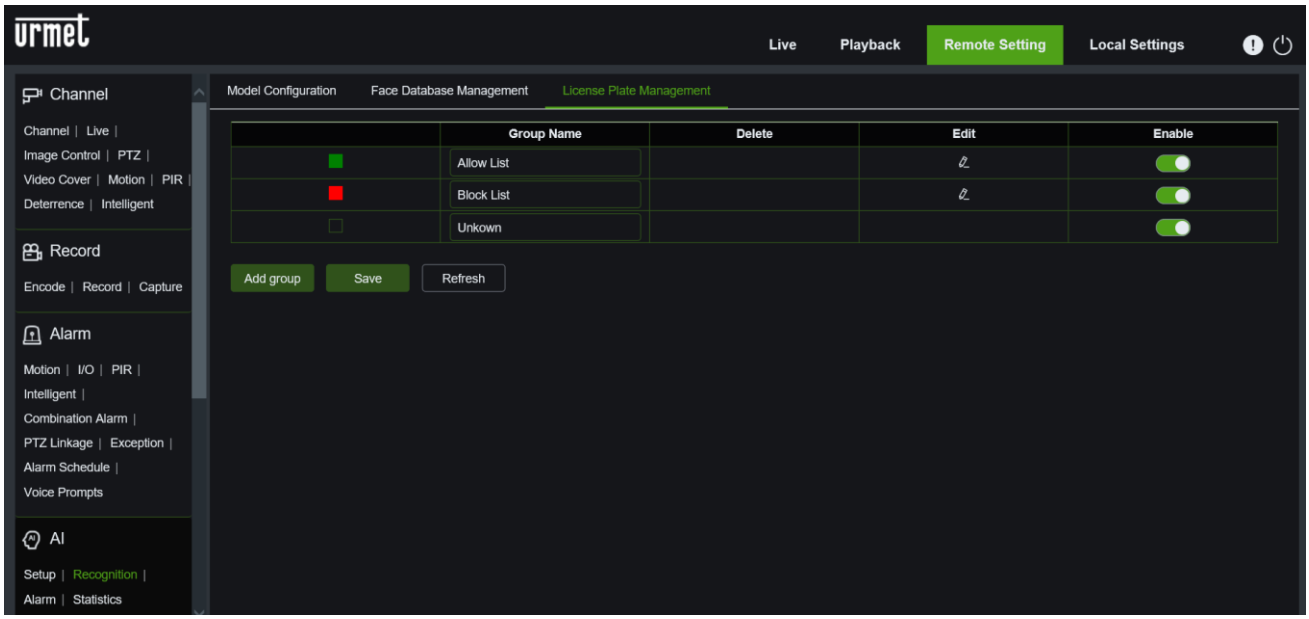


IMPORTANT NOTE:

- To use the RECOGNITION function, you must install an SD card in the camera to which you can upload the face databases. The capacity of the card must be at least 4GB. If the capacity is less than 4GB, the AI Recognition/statistics option will not be displayed after formatting.

9.4.2.2 **License Plate Management** *Only for certain models*

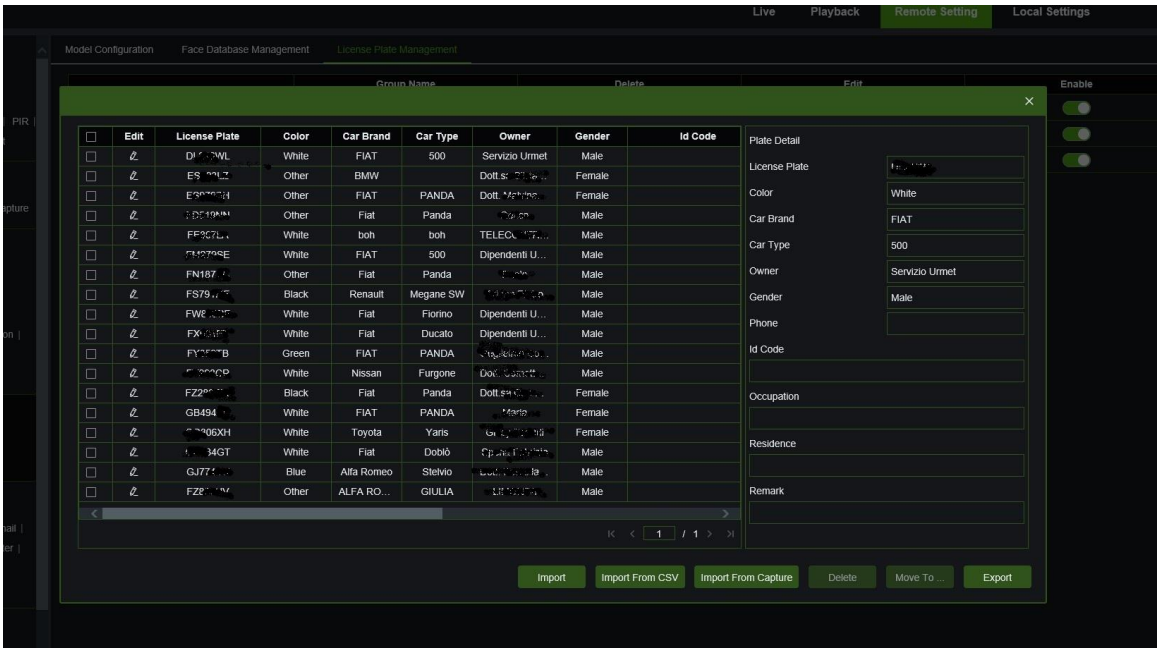
This menu provides a database of licence plate information.



Enable: enables the desired LPD list.

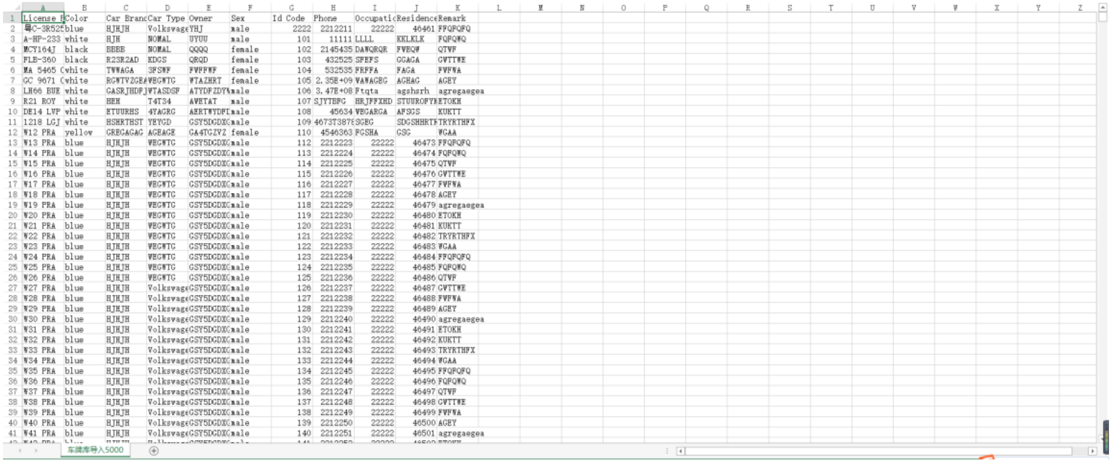
Group Name: allows you to set the database group name, Allow List , Block List and Stranger group . Up to 61 custom groups can be added, for a total of 64 groups. Each group can contain up to 5000 number plates, the entire database can contain 10000 number plates.
Add Group: allows you to add a new group of number plates
Edit: allows access to the management interface of the desired group.

Press on to edit licence plate data. Three types of licence plate import can be used: **Import (manual addition), Import from CSV** and **Import from capture**.



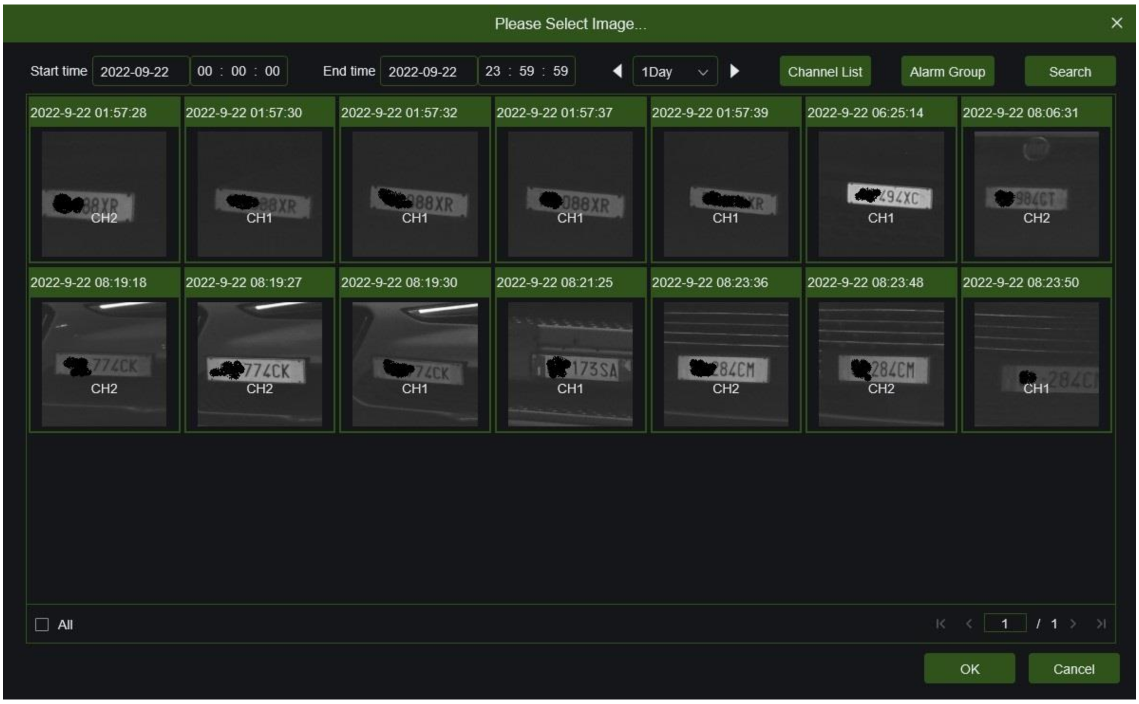
Press the **Import** button to manually enter the data for the individual number plate.

Press the **Export** button to export the entire group data to an external drive.
Press the **Move To...** button to check the plate data box and transfer it to another group.
Press the **Delete** button to select the licence plate data box and delete it from the group.
Press the **Import from CSV** button to import one or more data. The format of the CSV table is shown below:



Press the **Import/Modify** button to add a group and edit the licence plate data. When more than 5000 data are added, the message **Add data has reached the upper limit of the group is displayed**.

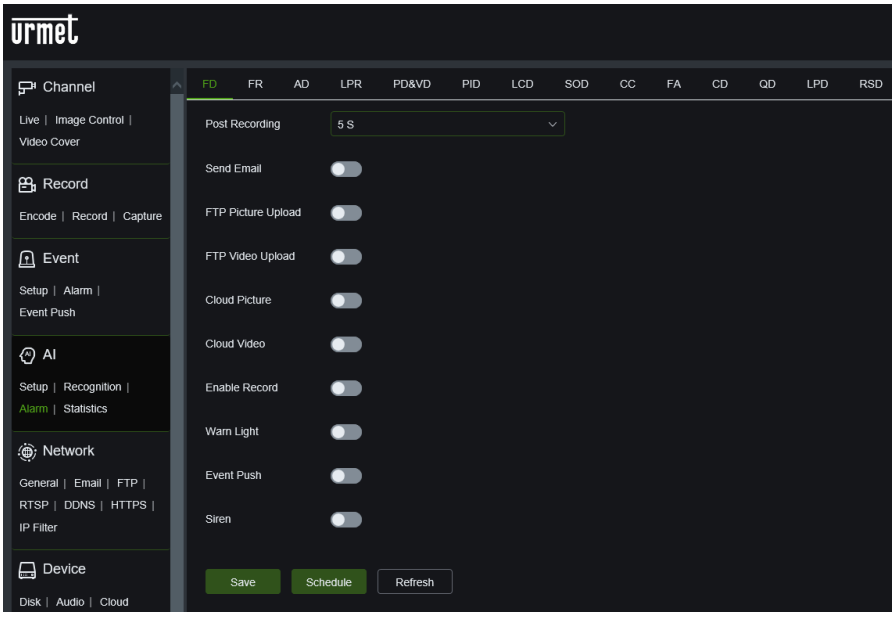
Press the **Import from capture** button to locally import licence plate data from the capture database.
Select date, duration and channels and press on **Search** to search for plates saved by the device in that time period.



9.4.3 ALARMS

In this section you can configure all the actions that can be implemented by the system in response to an Intelligent alarm.
In the **FD**, **FR**, **AD**, **PD&VD**, **PID**, **LCD**, **SOD**, **CC, FA, CD, QD, LPD** e **RSD** function menus, you can also schedule the actions generated by these alarms, by accessing **the schedule** section of each menu.

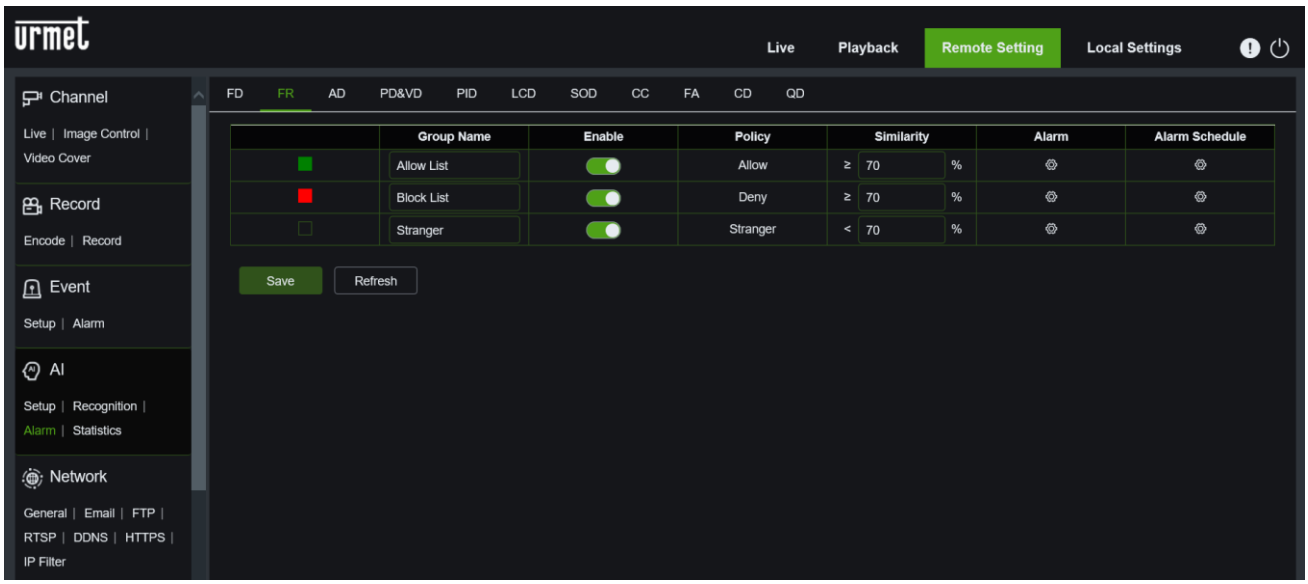
9.4.3.1 **FD:** Face Detection



Latch Time: set the alarm time, a time period of 5s, 10s, 20s and 30s is allowed.
Post Recording: set the recording time after the alarm is triggered. OFF, 5s, 10s, 20s and 30s can be selected.
Send Email: if enabled, allows an email notification to be sent after the alarm has been triggered. It is necessary to configure the e-mail data in the Remote Setup menu under E-mail Network.
FTP Picture Upload: if enabled, allows the alarm picture to be uploaded to the FTP server after the alarm has been triggered.
FTP Video Upload: If enabled, allows you to upload the alarm video to the FTP server after the alarm has been triggered.
Cloud Picture: if enabled, this allows the alarm picture to be uploaded to the cloud after the alarm has been triggered.
Cloud Video: If enabled, this allows you to upload the alarm video to the cloud after the alarm has been triggered.
Alarm Out: if enabled, allows the camera's alarm output to be switched after the alarm has been triggered.
Enable Record: if enabled, allows you to enable recording in the event of an alarm.
Warn Light*: If enabled, allows you to activate the warn light in the event of an alarm.
Event Push: If enabled, enables push notifications in the event of an alarm.
Siren*: if enabled, enables the siren in the event of an alarm.
*Functions only available for models equipped with deterrence.

Save: saves the set parameters.
Schedule: allows you to schedule set actions on an hourly/daily basis.
Refresh: to refresh the parameters.

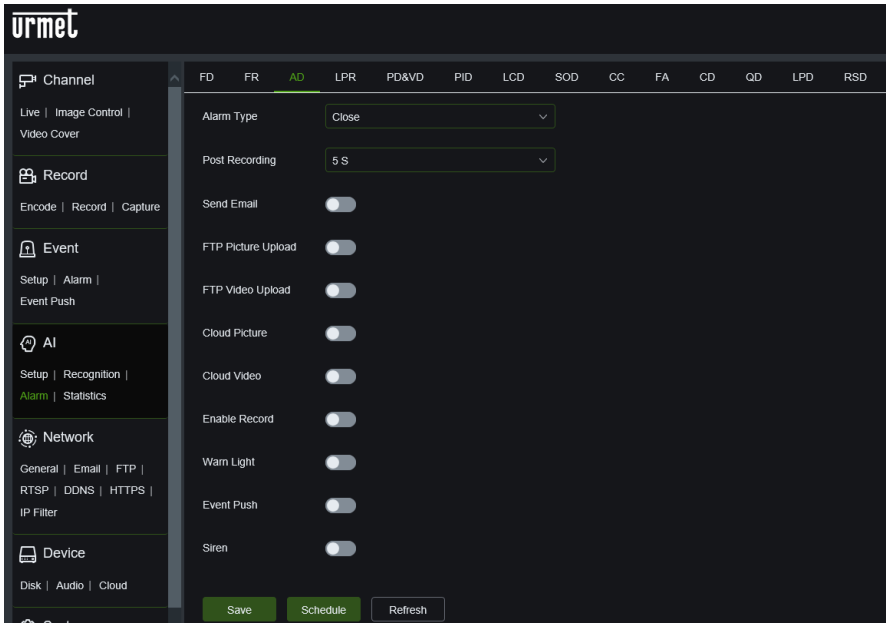
9.4.3.2 **FR:** Face Recognition *Only for certain models*



Enable: enables or disables the relevant list.
Similarity: if the similarity is greater than the set percentage the alarm will be generated.
Latch Time: set the alarm time, a time period of 0-5s, 10s, 20s, 40s and 60s is allowed.
Alarm Out: if enabled, allows the camera's alarm output to be switched after the alarm has been triggered.
Save Picture: if enabled, enables the saving of the alarm picture.
Send Email: if enabled, this allows an email notification to be sent after the alarm has been triggered. It is necessary to configure the e-mail data in the Remote Setup menu under E-mail Network.
FTP Picture Upload: if enabled, allows the alarm picture to be uploaded to the FTP server after the alarm has been triggered.
Cloud Picture: if enabled, this allows the alarm picture to be uploaded to the cloud after the alarm has been triggered.
Alarm Schedule: the schedule consists of a grid of 30-minute boxes. You can hold down the left mouse button to scroll through the time table and select/deselect fields.
Save: to save the set parameters.
Refresh: to refresh the parameters.

9.4.3.3 **AD:** Attribute detection *Only for certain models*

In this section you can configure the possible actions related to the recognition of some facial characteristics (e.g. presence or absence of a mask).

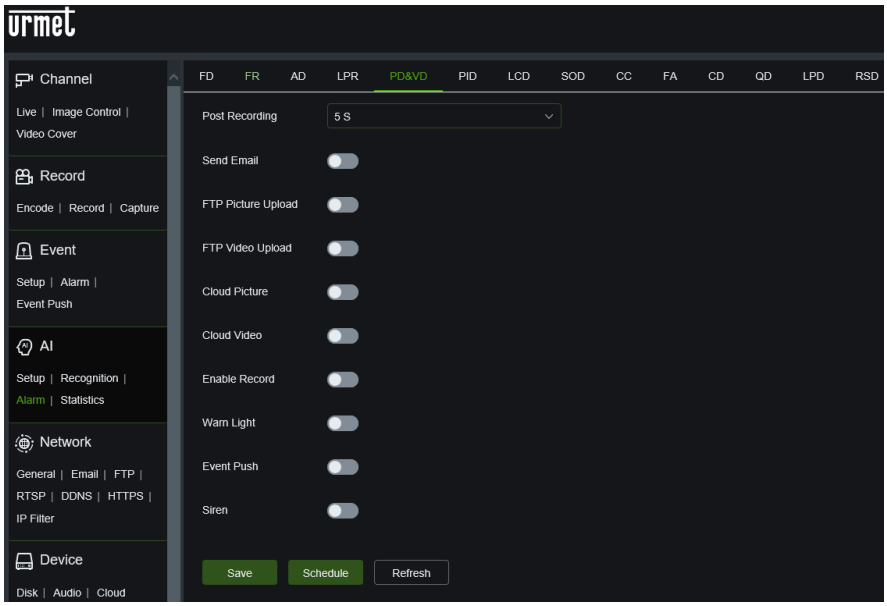


Alarm Type: there are three types of alarm, close, no mask, with mask.
Latch Time: set the alarm time, a time period of 5s, 10s, 20s and 30s is allowed.
Post Recording: set the recording time after the alarm is triggered. OFF, 5s, 10s, 20s and 30s can be selected.
Send Email: if enabled, allows an email notification to be sent after the alarm has been triggered. It is necessary to configure the e-mail data in the Remote Setup menu under E-mail Network.
FTP Picture Upload: if enabled, allows the alarm picture to be uploaded to the FTP server after the alarm has been triggered.
FTP Video Upload: If enabled, allows you to upload the alarm video to the FTP server after the alarm has been triggered.
Cloud Picture: if enabled, this allows the alarm picture to be uploaded to the cloud after the alarm has been triggered.

Cloud Video: If enabled, this allows you to upload the alarm video to the cloud after the alarm has been triggered.
Alarm Out: if enabled, allows the camera's alarm output to be switched after the alarm has been triggered.
Enable Record: if enabled, allows you to enable recording in the event of an alarm.
Warn Light*: If enabled, allows you to activate the warn light in the event of an alarm.
Event Push: If enabled, enables push notifications in the event of an alarm.
Siren*: if enabled, enables the siren in the event of an alarm.
*Functions only available for models equipped with deterrence.

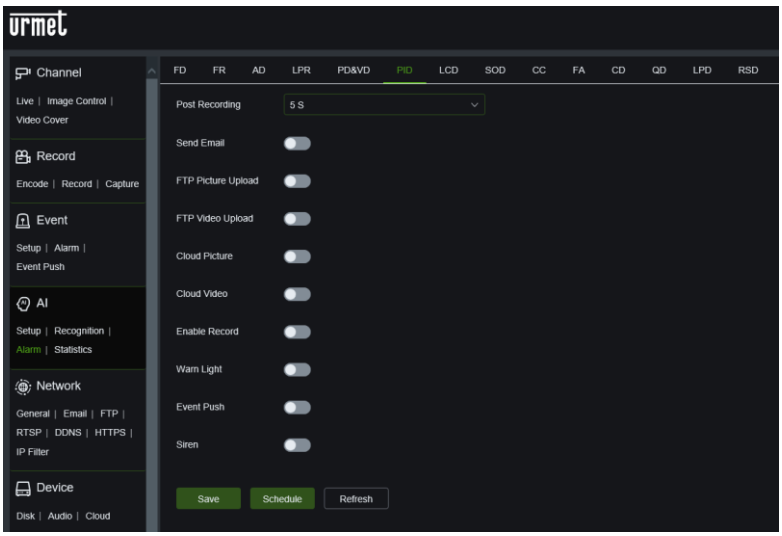
Save: to save the set parameters.
Schedule: allows set actions to be scheduled on an hourly/daily basis
Refresh: to refresh the parameters.

9.4.3.4 **PD & VD:** Person and vehicle detection



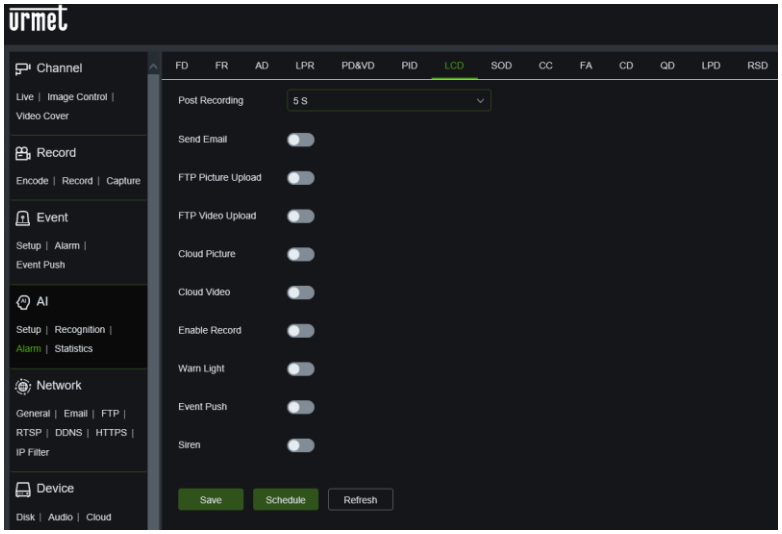
Latch Time: set the alarm time, a time period of 5s, 10s, 20s and 30s is allowed.
Post Recording: set the recording time after the alarm is triggered. OFF, 5s, 10s, 20s and 30s can be selected.
Send Email: if enabled, allows an email notification to be sent after the alarm has been triggered. It is necessary to configure the e-mail data in the Remote Setup menu under E-mail Network.
FTP Picture Upload: if enabled, allows the alarm picture to be uploaded to the FTP server after the alarm has been triggered.
FTP Video Upload: If enabled, allows you to upload the alarm video to the FTP server after the alarm has been triggered.
Cloud Picture: if enabled, this allows the alarm picture to be uploaded to the cloud after the alarm has been triggered.
Cloud Video: If enabled, this allows you to upload the alarm video to the cloud after the alarm has been triggered.
Alarm Out: if enabled, allows the camera's alarm output to be switched after the alarm has been triggered.
Enable Record: if enabled, allows you to enable recording in the event of an alarm.
Warn Light*: If enabled, allows you to activate the warn light in the event of an alarm.
Event Push: If enabled, enables push notifications in the event of an alarm.
Siren*: if enabled, enables the siren in the event of an alarm.
*Functions only available for models equipped with deterrence.
Save: to save the set parameters.
Schedule: allows set actions to be scheduled on an hourly/daily basis
Refresh: to refresh the parameters.

9.4.3.5 **PID:** Perimeter intrusion detection



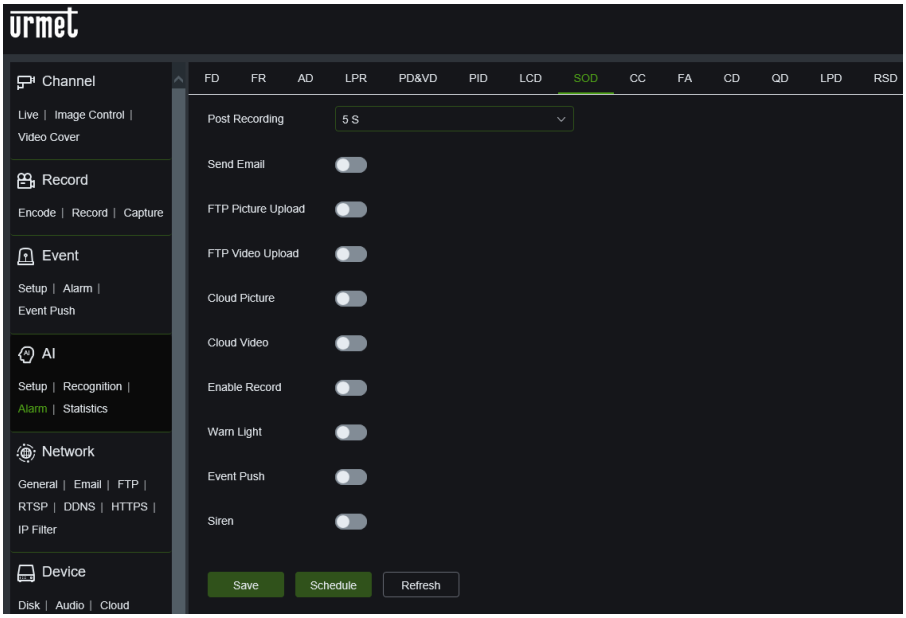
Latch Time: set the alarm time, a time period of 5s, 10s, 20s and 30s is allowed.
Post Recording: set the recording time after the alarm is triggered. OFF, 5s, 10s, 20s and 30s can be selected.
Send Email: if enabled, allows an email notification to be sent after the alarm has been triggered. It is necessary to configure the e-mail data in the Remote Setup menu under E-mail Network.
FTP Picture Upload: if enabled, allows the alarm picture to be uploaded to the FTP server after the alarm has been triggered.
FTP Video Upload: If enabled, allows you to upload the alarm video to the FTP server after the alarm has been triggered.
Cloud Picture: if enabled, this allows the alarm picture to be uploaded to the cloud after the alarm has been triggered.
Cloud Video: If enabled, this allows you to upload the alarm video to the cloud after the alarm has been triggered.
Alarm Out: if enabled, allows the camera's alarm output to be switched after the alarm has been triggered.
Enable Record: if enabled, allows you to enable recording in the event of an alarm.
Warn Light*: If enabled, allows you to activate the warn light in the event of an alarm.
Event Push: If enabled, enables push notifications in the event of an alarm.
Siren*: if enabled, enables the siren in the event of an alarm.
*Functions only available for models equipped with deterrence.
Save: to save the set parameters.
Schedule: allows set actions to be scheduled on an hourly/daily basis
Refresh: to refresh the parameters.

9.4.3.6 **LCD:** Line crossing detection



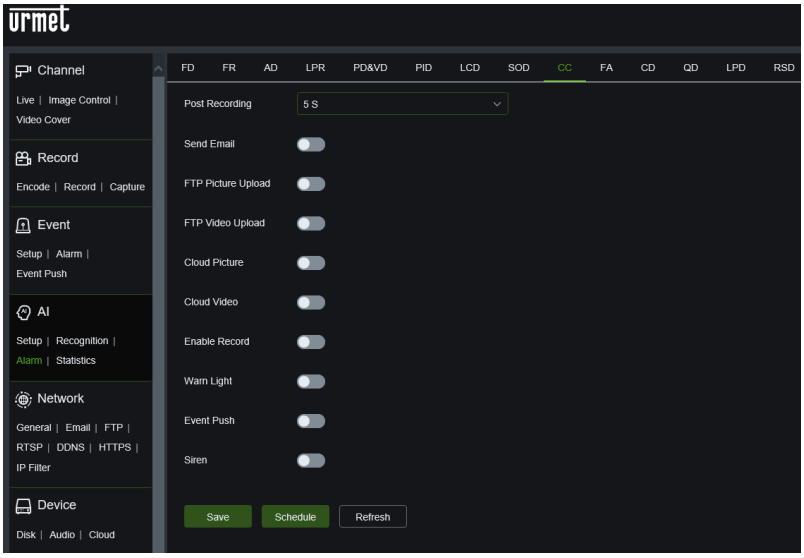
Latch Time: set the alarm time, a time period of 5s, 10s, 20s and 30s is allowed.
Post Recording: set the recording time after the alarm is triggered. OFF, 5s, 10s, 20s and 30s can be selected.
Send Email: if enabled, allows an email notification to be sent after the alarm has been triggered. It is necessary to configure the e-mail data in the Remote Setup menu under E-mail Network.
FTP Picture Upload: if enabled, allows the alarm picture to be uploaded to the FTP server after the alarm has been triggered.
FTP Video Upload: If enabled, allows you to upload the alarm video to the FTP server after the alarm has been triggered.
Cloud Picture: if enabled, this allows the alarm picture to be uploaded to the cloud after the alarm has been triggered.
Cloud Video: If enabled, this allows you to upload the alarm video to the cloud after the alarm has been triggered.
Alarm Out: if enabled, allows the camera's alarm output to be switched after the alarm has been triggered.
Enable Record: if enabled, allows you to enable recording in the event of an alarm.
Warn Light*: If enabled, allows you to activate the warn light in the event of an alarm.
Event Push: If enabled, enables push notifications in the event of an alarm.
Siren*: if enabled, enables the siren in the event of an alarm.
*Functions only available for models equipped with deterrence.
Save: to save the set parameters.
Schedule: allows set actions to be scheduled on an hourly/daily basis
Refresh: to refresh the parameters.

9.4.3.7 **SOD:** Stationary object detection



Latch Time: set the alarm time, a time period of 5s, 10s, 20s and 30s is allowed.
Post Recording: set the recording time after the alarm is triggered. OFF, 5s, 10s, 20s and 30s can be selected.
Send Email: if enabled, allows an email notification to be sent after the alarm has been triggered. It is necessary to configure the e-mail data in the Remote Setup menu under E-mail Network.
FTP Picture Upload: if enabled, allows the alarm picture to be uploaded to the FTP server after the alarm has been triggered.
FTP Video Upload: If enabled, allows you to upload the alarm video to the FTP server after the alarm has been triggered.
Cloud Picture: if enabled, this allows the alarm picture to be uploaded to the cloud after the alarm has been triggered.
Cloud Video: If enabled, this allows you to upload the alarm video to the cloud after the alarm has been triggered.
Alarm Out: if enabled, allows the camera's alarm output to be switched after the alarm has been triggered.
Enable Record: if enabled, allows you to enable recording in the event of an alarm.
Warn Light*: If enabled, allows you to activate the warn light in the event of an alarm.
Event Push: If enabled, enables push notifications in the event of an alarm.
Siren*: if enabled, enables the siren in the event of an alarm.
*Functions only available for models equipped with deterrence.
Save: to save the set parameters.
Schedule: allows set actions to be scheduled on an hourly/daily basis
Refresh: to refresh the parameters.

9.4.3.8 **CC:** Crossing counting

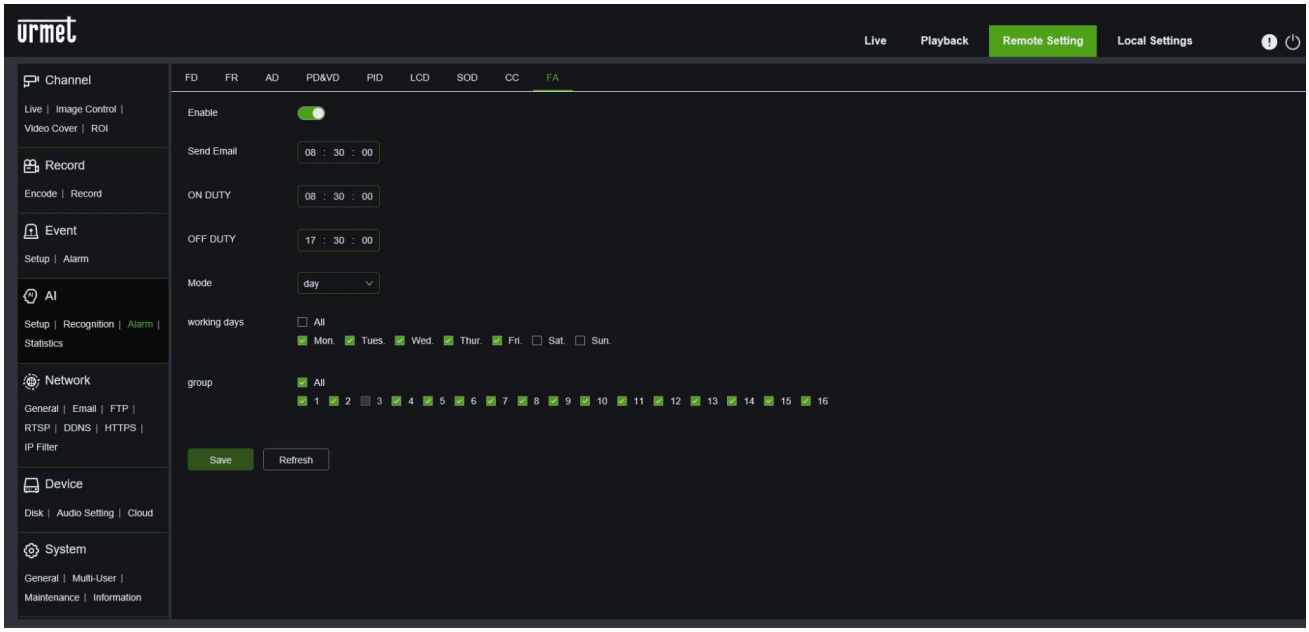


Latch Time: set the alarm time, a time period of 5s, 10s, 20s and 30s is allowed.
Post Recording: set the recording time after the alarm is triggered. OFF, 5s, 10s, 20s and 30s can be selected.
Send Email: if enabled, allows an email notification to be sent after the alarm has been triggered. It is necessary to configure the e-mail data in the Remote Setup menu under E-mail Network.
FTP Picture Upload: if enabled, allows the alarm picture to be uploaded to the FTP server after the alarm has been triggered.
FTP Video Upload: If enabled, allows you to upload the alarm video to the FTP server after the alarm has been triggered.
Cloud Picture: if enabled, this allows the alarm picture to be uploaded to the cloud after the alarm has been triggered.
Cloud Video: If enabled, this allows you to upload the alarm video to the cloud after the alarm has been triggered.

Alarm Out: if enabled, allows the camera's alarm output to be switched after the alarm has been triggered.
Enable Record: if enabled, allows you to enable recording in the event of an alarm.
Warn Light*: If enabled, allows you to activate the warn light in the event of an alarm.
Event Push: If enabled, enables push notifications in the event of an alarm.
Siren*: if enabled, enables the siren in the event of an alarm.
*Functions only available for models equipped with deterrence.
Save: to save the set parameters.
Schedule: allows set actions to be scheduled on an hourly/daily basis
Refresh: to refresh the parameters.

9.4.3.9 **FA**: Face attendance *Only for certain models*

Allows you to manage the presence/absence of certain faces on days and time slots that can be set.

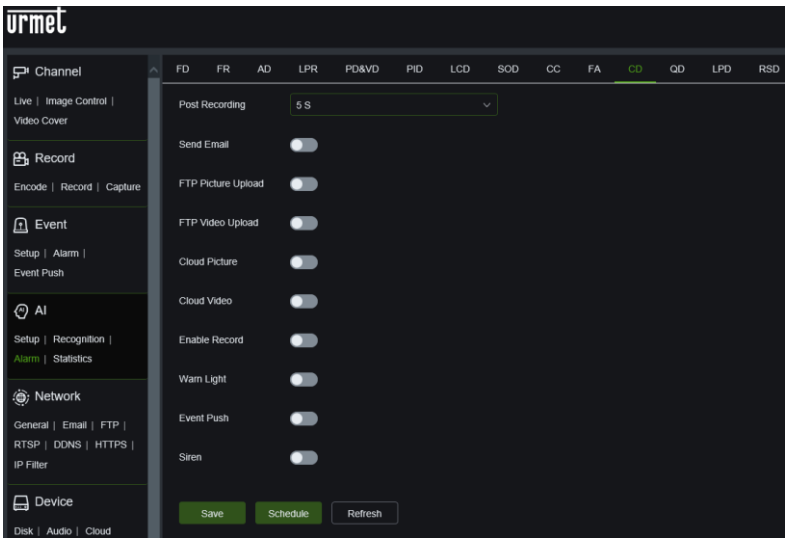


Enable: enables the face presence/absence (FA) function.
Send Email: if enabled, allows an email notification to be sent at the set time. It is necessary to configure the e-mail data in the Remote Setup menu under E-mail Network.
ON DUTY: sets the start time of the FA function.
OFF DUTY: sets the end time of the FA function.
Mode: Sets the mode of sending the e-mail on a day, week, month basis.
Working days: sets the days that require attendance.
Group: sets the corresponding group

Note: the data sent will be the data before the day of sending. For example, if you set monthly sending mode and the sending date is the 15th, the sent data range is from the 15th of the previous month to the 14th of this month. If there is no check-in data during the time period set for sending, no file will be generated and an e-mail will be sent)

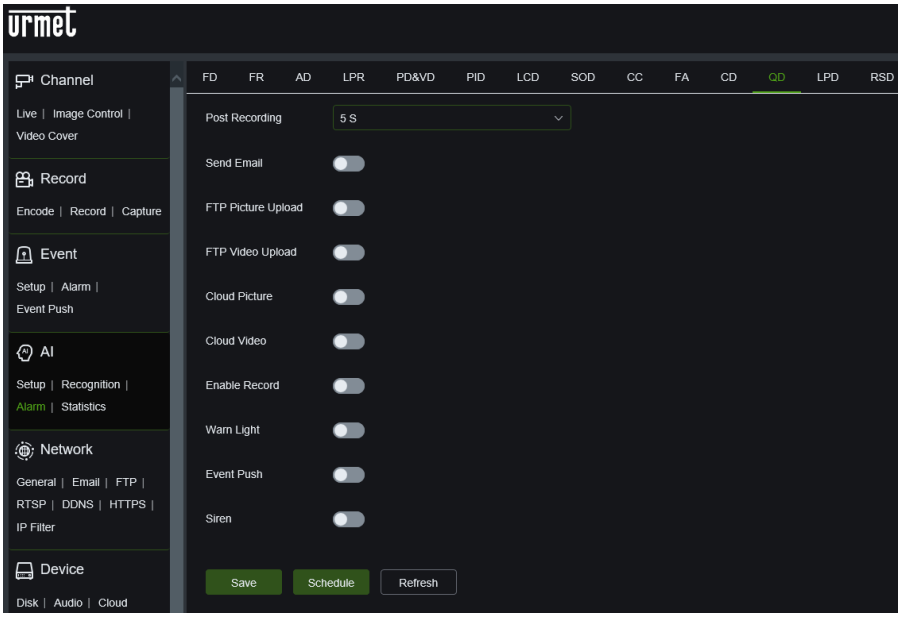
Save: to save the set parameters.
Refresh: to refresh the parameters.

9.4.3.10 **CD:** Crowd Density Detection



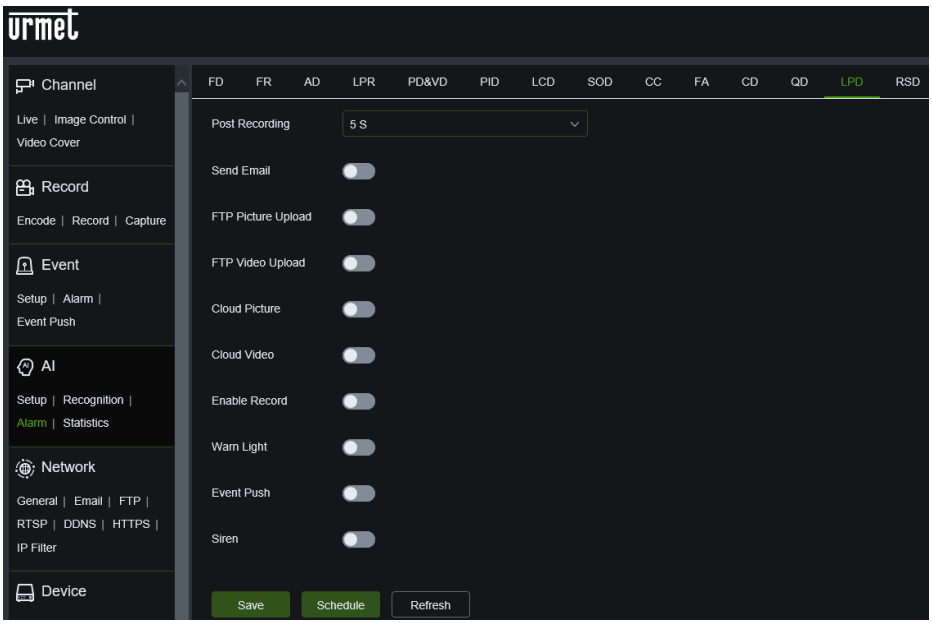
Latch Time: set the alarm time, a time period of 5s, 10s, 20s and 30s is allowed.
Post Recording: set the recording time after the alarm is triggered. OFF, 5s, 10s, 20s and 30s can be selected.
Send Email: if enabled, allows an email notification to be sent after the alarm has been triggered. It is necessary to configure the e-mail data in the Remote Setup menu under E-mail Network.
FTP Picture Upload: if enabled, allows the alarm picture to be uploaded to the FTP server after the alarm has been triggered.
FTP Video Upload: If enabled, allows you to upload the alarm video to the FTP server after the alarm has been triggered.
Cloud Picture: if enabled, this allows the alarm picture to be uploaded to the cloud after the alarm has been triggered.
Cloud Video: If enabled, this allows you to upload the alarm video to the cloud after the alarm has been triggered.
Alarm Out: if enabled, allows the camera's alarm output to be switched after the alarm has been triggered.
Enable Record: if enabled, allows you to enable recording in the event of an alarm.
Warn Light*: If enabled, allows you to activate the warn light in the event of an alarm.
Event Push: If enabled, enables push notifications in the event of an alarm.
Siren*: if enabled, enables the siren in the event of an alarm.
*Functions only available for models equipped with deterrence.
Save: to save the set parameters.
Schedule: allows set actions to be scheduled on an hourly/daily basis
Refresh: to refresh the parameters.

9.4.3.11 **QD:** Queue Length Detection



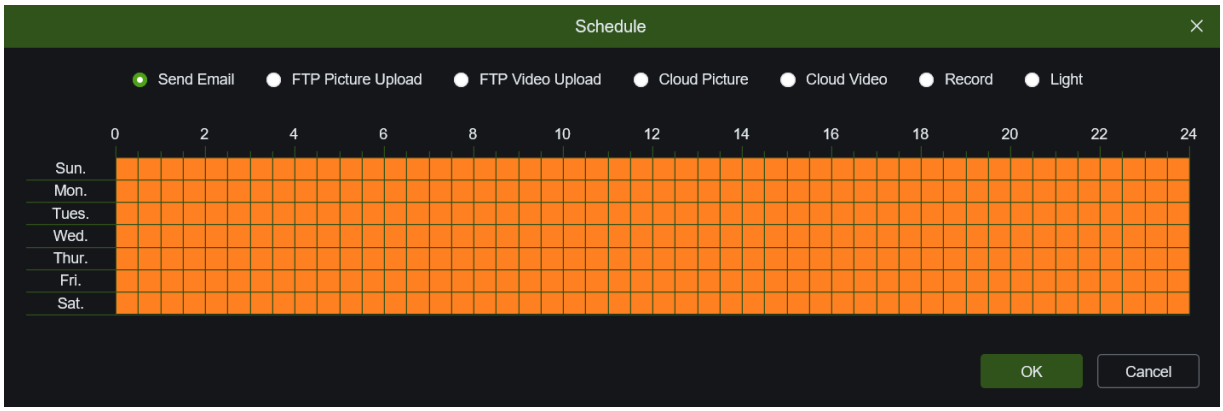
Latch Time: set the alarm time, a time period of 5s, 10s, 20s and 30s is allowed.
Post Recording: set the recording time after the alarm is triggered. OFF, 5s, 10s, 20s and 30s can be selected.
Send Email: if enabled, allows an email notification to be sent after the alarm has been triggered. It is necessary to configure the e-mail data in the Remote Setup menu under E-mail Network.
FTP Picture Upload: if enabled, allows the alarm picture to be uploaded to the FTP server after the alarm has been triggered.
FTP Video Upload: If enabled, allows you to upload the alarm video to the FTP server after the alarm has been triggered.
Cloud Picture: if enabled, this allows the alarm picture to be uploaded to the cloud after the alarm has been triggered.
Cloud Video: If enabled, this allows you to upload the alarm video to the cloud after the alarm has been triggered.
Alarm Out: if enabled, allows the camera's alarm output to be switched after the alarm has been triggered.
Enable Record: if enabled, allows you to enable recording in the event of an alarm.
Warn Light*: If enabled, allows you to activate the warn light in the event of an alarm.
Event Push: If enabled, enables push notifications in the event of an alarm.
Siren*: if enabled, enables the siren in the event of an alarm.
*Functions only available for models equipped with deterrence.
Save: to save the set parameters.
Schedule: allows set actions to be scheduled on an hourly/daily basis
Refresh: to refresh parameters.

9.4.3.12 **LPD:** License Plate Detection



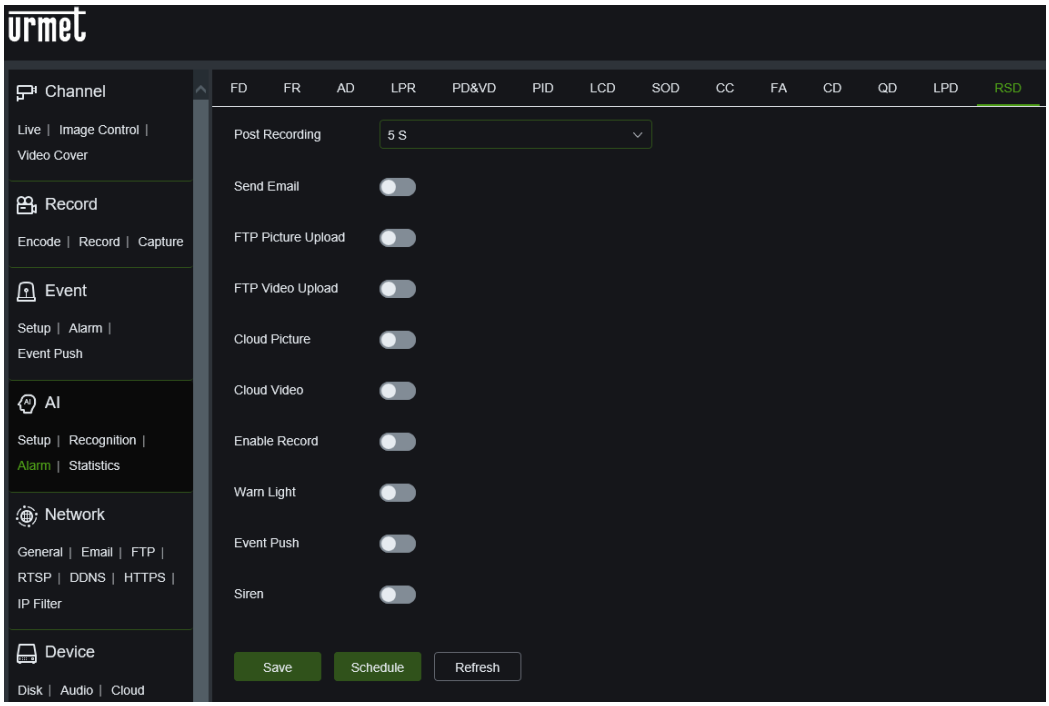
Post Recording: set the recording time after the licence plate reading alarm is activated. OFF, 5s, 10s, 20s and 30s can be selected.
Send Email: if enabled, allows an email notification to be sent after the licence plate reading alarm has been triggered. Email data must be configured in the Remote Setup menu under E-mail Network.
FTP Picture Upload: If enabled, allows the alarm picture to be uploaded to the FTP server after the licence plate reading alarm has been triggered.
FTP Video Upload: If enabled, this allows the alarm video to be uploaded to the FTP server after the licence plate reading alarm has been triggered.
Cloud Picture: if enabled, allows the licence plate image to be uploaded to the cloud after the alarm has been triggered.
Cloud Video: if enabled, allows the licence plate image to be uploaded to the cloud after the alarm has been triggered.
Enable Record: If enabled, this allows you to activate recording in the event of a licence plate reading alarm.
Warn Light*: If enabled, allows you to activate the warn light in the event of an alarm.
Event Push: If enabled, enables push notifications in the event of an alarm.
Siren*: if enabled, enables the siren in the event of an alarm.
*Functions only available for models equipped with deterrence.

Schedule: allows you to schedule set actions on an hourly/daily basis



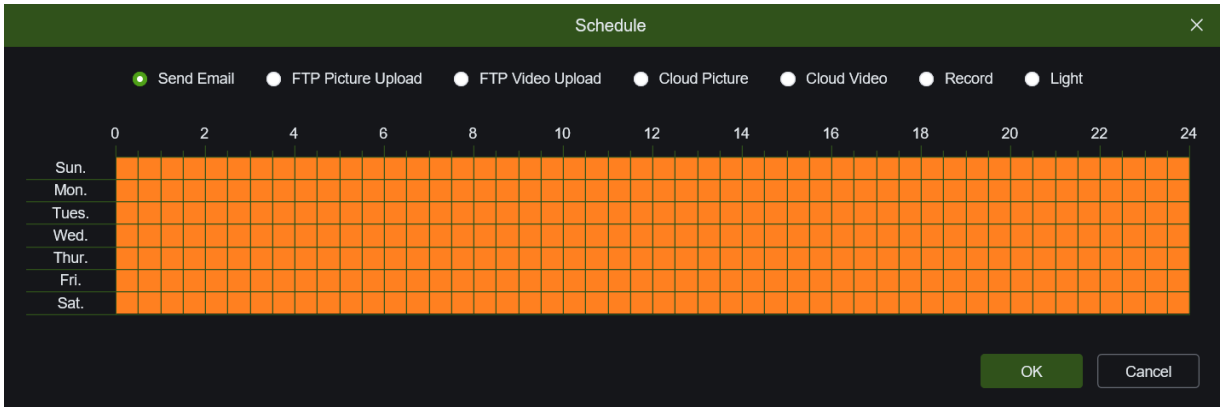
Save: To save the set parameters.
Refresh: To refresh parameters.

9.4.3.13 **RSD:** Rare Sound Detection



Post Recording: Set the recording time after the noise detection alarm is activated. It is possible to select OFF, 5s, 10s, 20s and 30s.
Send Email: If enabled, allows a notification email to be sent after the noise detection alarm has been triggered. It is necessary to configure the e-mail data in the Remote Setup menu under E-mail Network.
FTP Picture Upload: If enabled, allows the alarm picture to be uploaded to the FTP server after the noise detection alarm has been triggered.
FTP Video Upload: If enabled, this allows you to upload an alarm video to the FTP server after the noise detection alarm has been triggered.
Cloud Picture: If enabled, allows you to upload a picture to the cloud after the alarm has been triggered.
Cloud Video: If enabled, allows you to upload a video to the cloud after the alarm has been triggered.
Enable Record: if enabled allows you to activate recording in the event of a noise detection alarm
Warn Light*: If enabled, allows you to activate the warn light in the event of an alarm.
Event Push: If enabled, enables push notifications in the event of an alarm.
Siren*: if enabled, enables the siren in the event of an alarm.
*Functions only available for models equipped with deterrence.

Schedule: allows you to schedule set actions on an hourly/daily basis



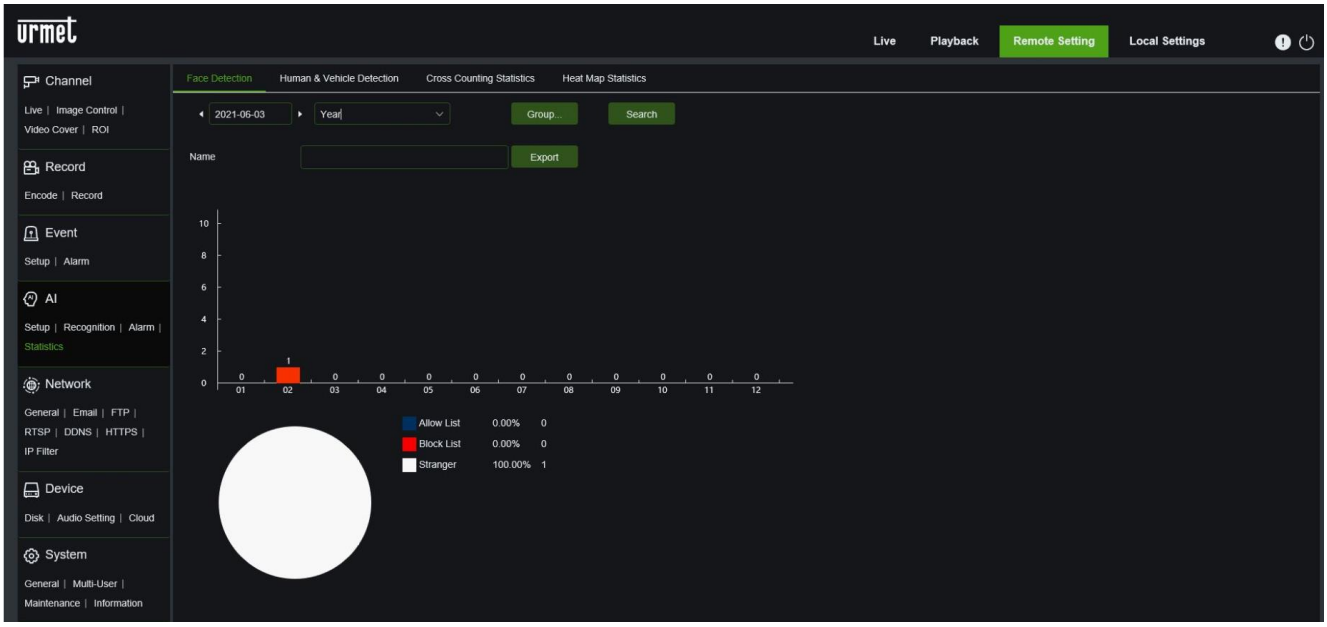
Save: To save the set parameters.
Refresh: To refresh parameters.

9.4.4 STATISTICS

From this section of the menu you can produce statistics for the **Face Detection**, **Human& Vehicle Detection**, **Cross Counting** and **Heat Map** functions.

9.4.4.1 Face Detection *Only for certain models*

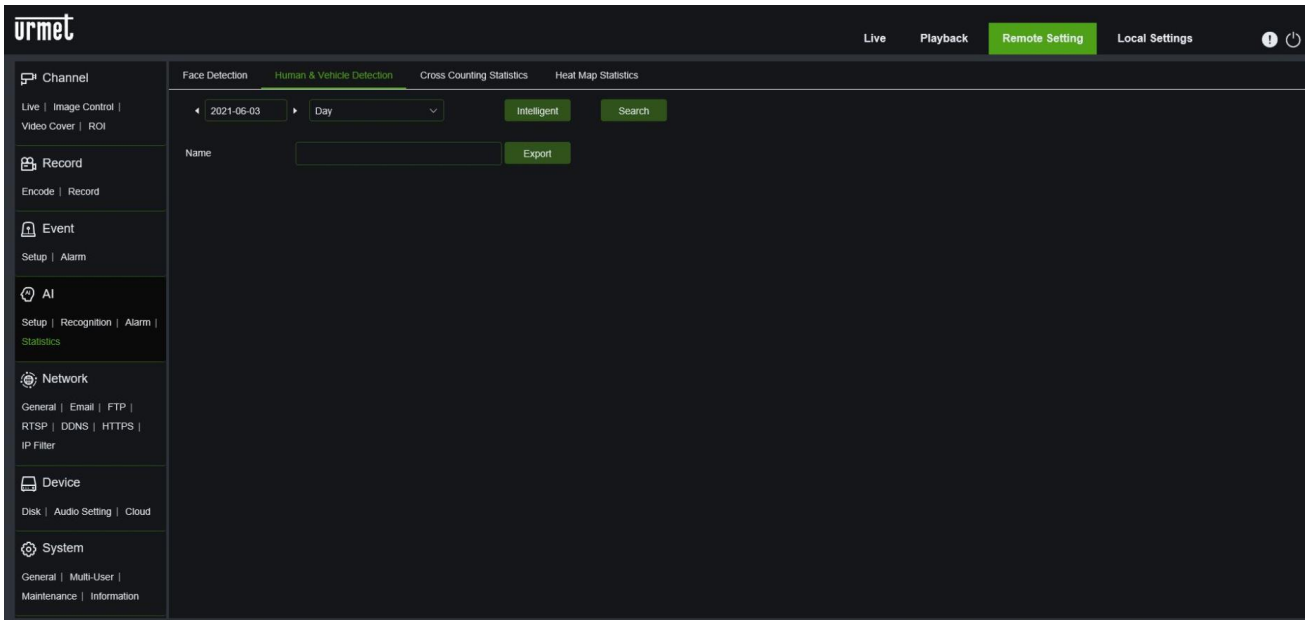
This section allows you to view and export statistics related to the face detection function.



Date: select a specific date
Report type: include daily/weekly/monthly/quarterly/yearly
Group: select the specific list from All/Allow List/Block List/Stranger List
Export: Press on Search and then on Export to export statistics in .CSV file format.

9.4.4.2 Human & Vehicle detection

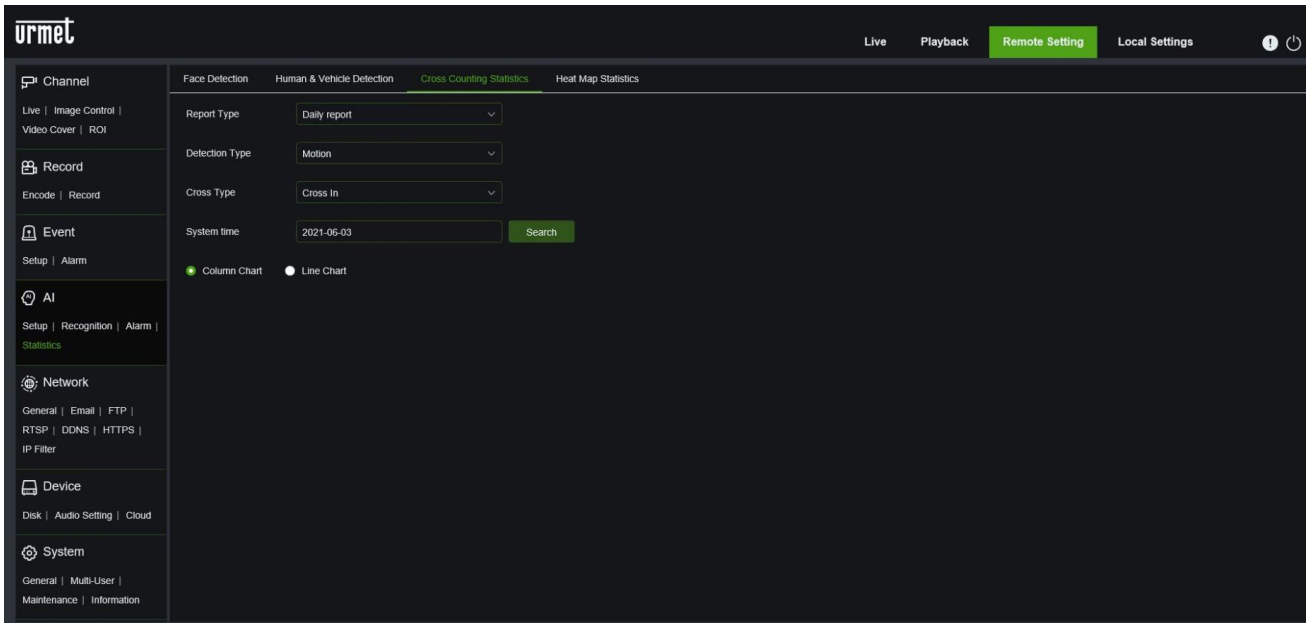
This section allows you to view and export statistics related to the pedestrian and vehicle detection function.



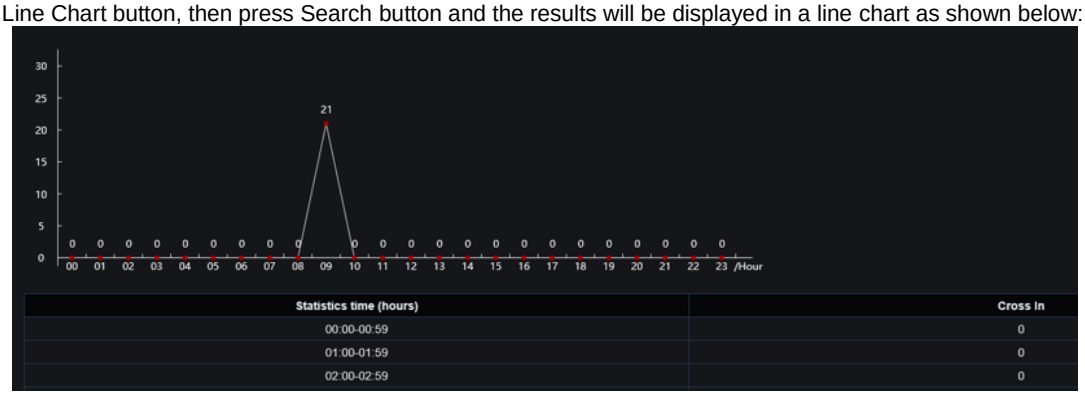
Date: select a specific date
Report type: include daily/weekly/monthly/quarterly/yearly
Group: select the specific list from All/PID(People)/PID(Vehicles)/LCD(People)/LCD(Vehicles)/People/Vehicles
Export: Press on Search and then on Export to export the statistics in the .CSV file format.

9.4.4.3 Cross Counting Statistics

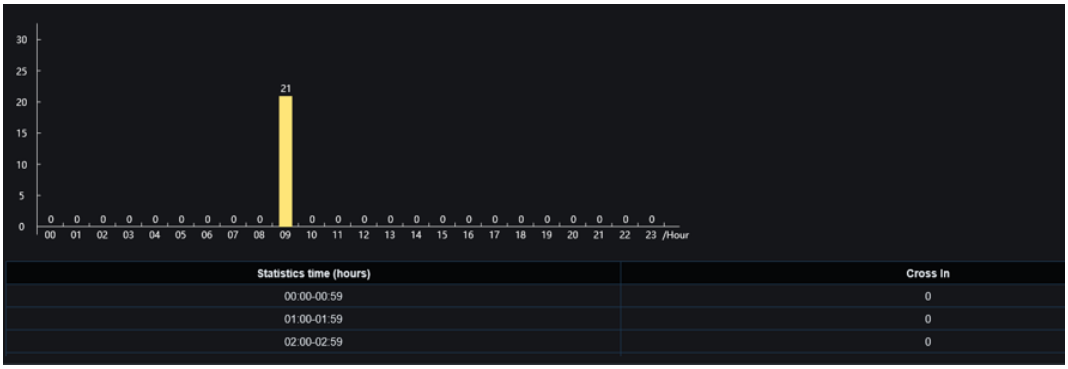
This section allows you to display in graphs the statistics for the type of crossing counting chosen



Report Type: includes daily/weekly/monthly/yearly
Detection Type: includes motion/person/vehicle
Cross Type: include cross in/cross out
Export: Press on Search and then on Export to export statistics in .CSV file format.
System Time: select a specific time
Select the Line Chart button, then press Search button and the results will be displayed in a line chart as shown below:

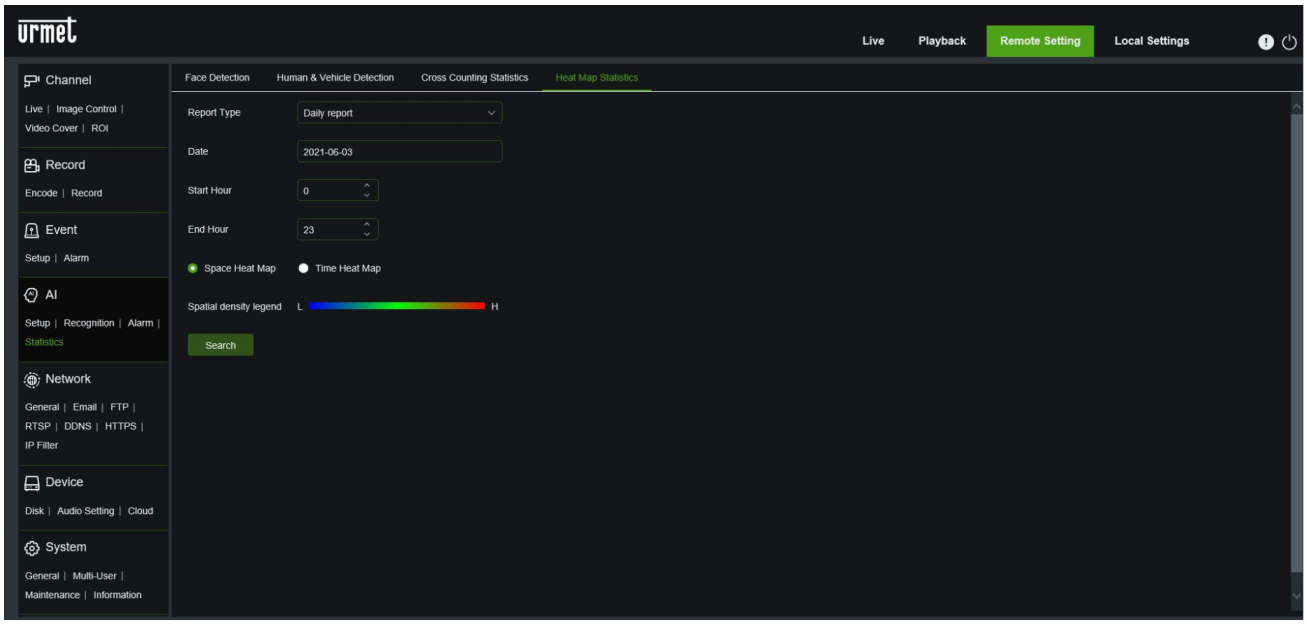


Select the Column Chart button, then press Search button and the results will be displayed in a column chart as shown below:

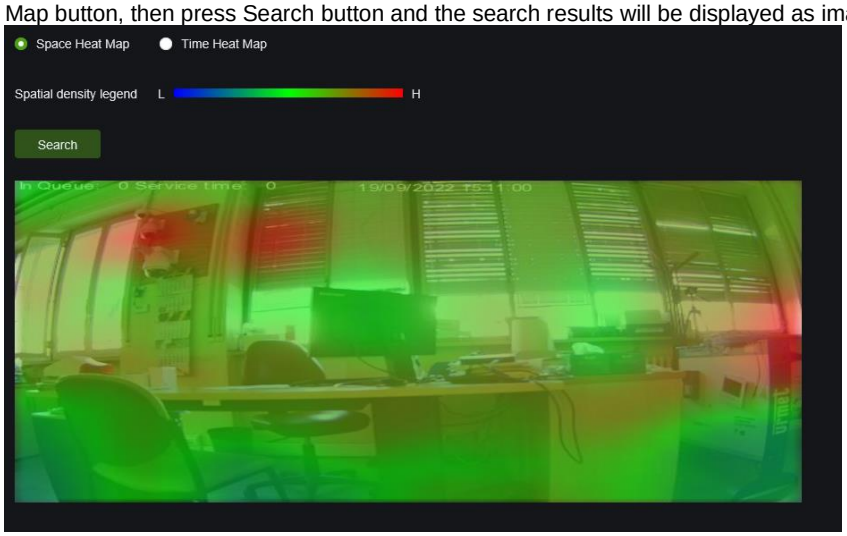


9.4.4.4 Heat Map Statistics

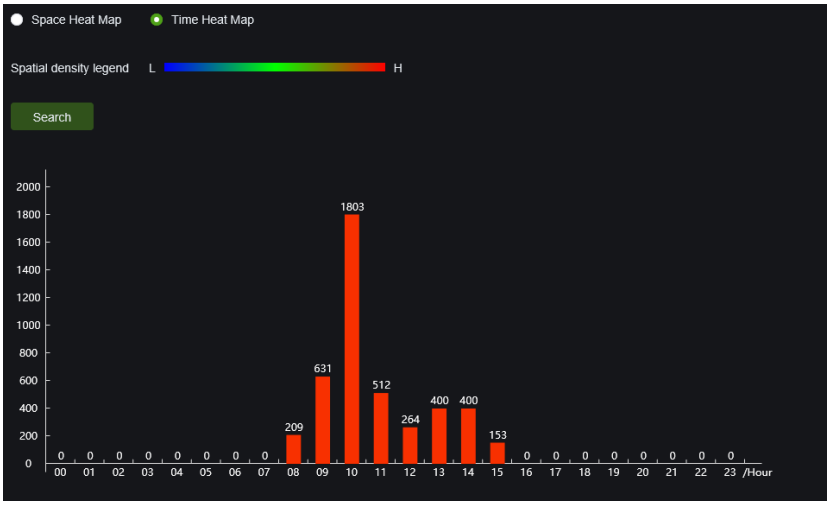
This section allows the heat map to be displayed according to the movement detected in a specific monitoring area. The more the area is affected by movement, the darker the colour displayed. Blue represents a low level of movement while red represents a high level of movement.



Report Type: include daily/weekly/monthly/annual
Date: select a specific date
Start/End Hour: set the start and end time period for the search
Select the Space Heat Map button, then press Search button and the search results will be displayed as images as shown below:



Select the Time Heat Map button, then press Search button and the search results will be displayed as a column chart as shown below:



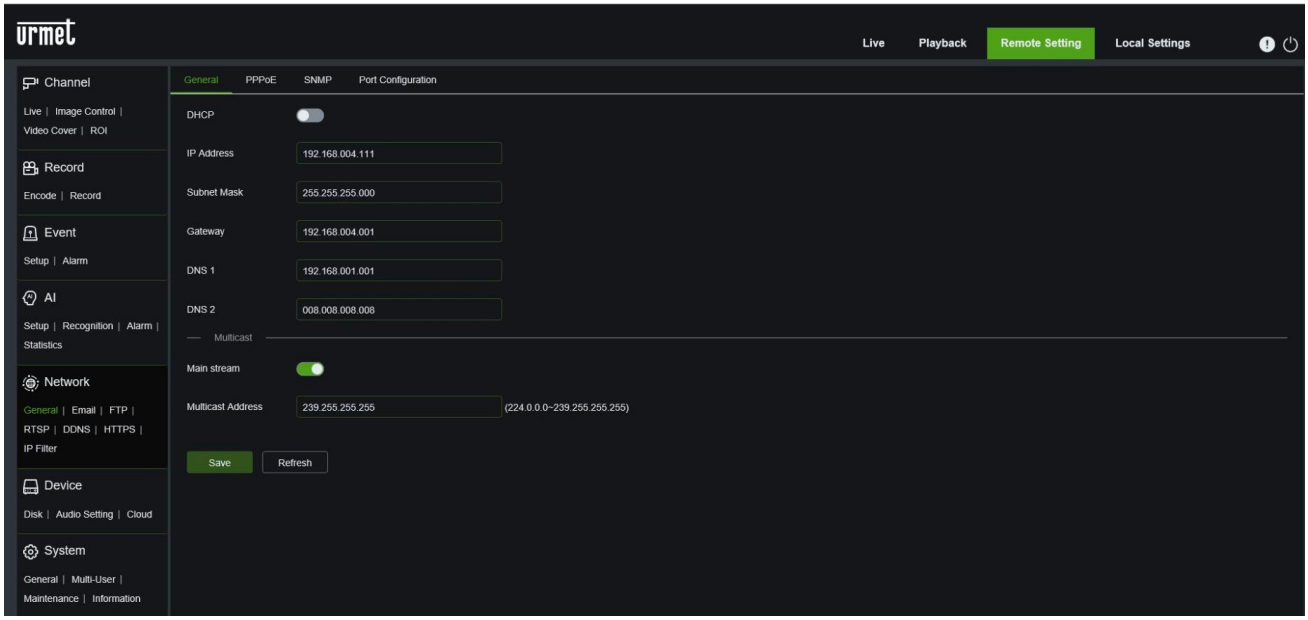
Note: If the search were to be carried out in the current time frame, the value displayed in the columns would not correspond to the actual data as the detection count is calculated on each frame of processed data and as the movement reading progresses the NVR will update the statistics accordingly.

9.5 NETWORK

9.5.1 GENERAL

9.5.1.1 General (Network)

Click on General in the Network menu to open the following page:



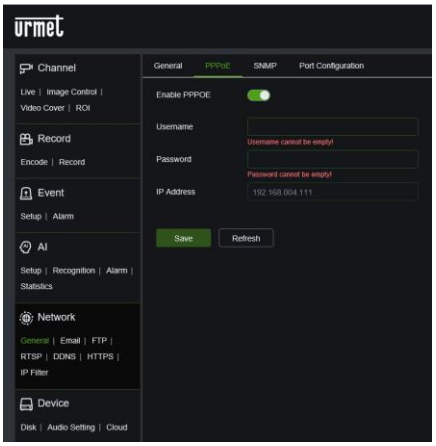
If you connect the camera to a router to use DHCP, enable the DHCP button. The router will automatically assign all network parameters for the camera. Unless the network is addressed manually, the parameters are as follows:

- **IP Address**: the IP address identifies the camera on the network. It consists of four groups of digits between 0 and 255, separated by full stops, e.g., “192.168.001.168”.
- **Subnet Mask**: this is a network parameter that defines a range of IP addresses that can be used on a network. If we compare the IP address to the street where you live, the subnet mask would be your neighbourhood. The subnet address also consists of four groups of digits, separated by full stops, e.g., “255.255.000.000”.
- **Gateway**: this address allows the camera to access the Internet. The Gateway address format is identical to that of the IP address, e.g., “192.168.001.001”.
- **IPv6 DHCP**: Enables IPv6 automatic addressing.
- **IPv6 Address**: Enables manual entry of IPv6 address.
- **IPv6 Gateway**: Enables manual input of the IPv6 gateway.
- **DNS1/DNS2**: DNS1 is the primary DNS server, DNS2 is the backup DNS server. As a rule, it is sufficient to enter the address of the DNS1 server.
- **IPv6 DNS1/IPv6 DNS2**: DNS1 IPv6 is the primary IPv6 DNS server, while DNS2 is the backup IPv6 DNS server. As a rule, it is sufficient to enter the address of the DNS1 IPv6 server.
- **Main stream**: Enables the entry of Multicast addresses.
- **Multicast Address**: range of multicast addresses.
- **Video Encryption Transmission**: If enabled, enables encrypted transmission of information.

Press **Save** to save the desired setting

9.5.1.2 PPPoE

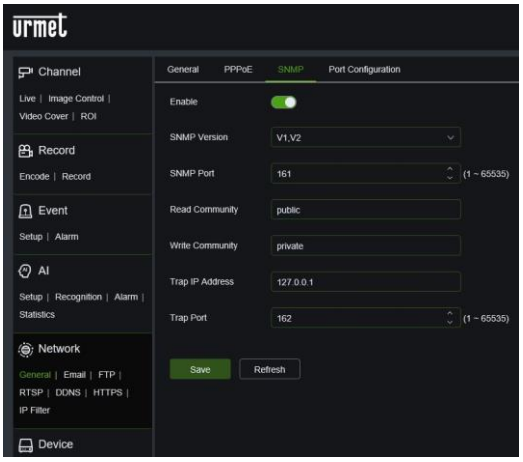
This is an advanced protocol that allows the NVR to connect to the network more directly, via a DSL modem.
Enable the “Enable PPPOE” switch, then enter the username and password for the PPPoE.



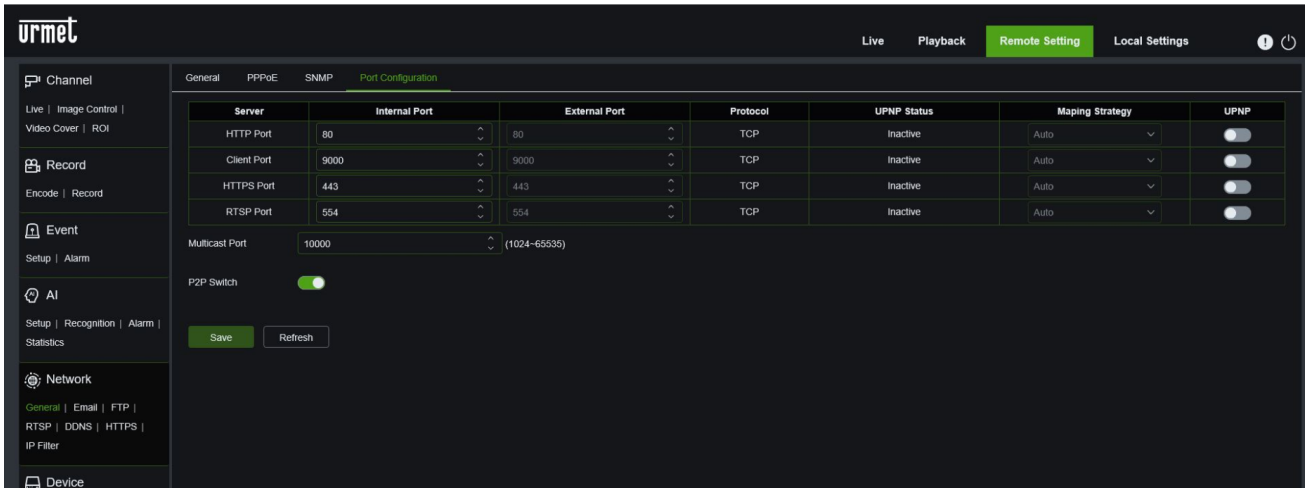
Click **Save**; the camera will be restarted to activate the PPPoE setting.

9.5.1.3 SNMP

(For future use) SNMP: Simple Network Management Protocol, an opensource protocol. SNMP can verify basic device parameters such as IP, hardware information and software information.



9.5.1.4 Port Configuration

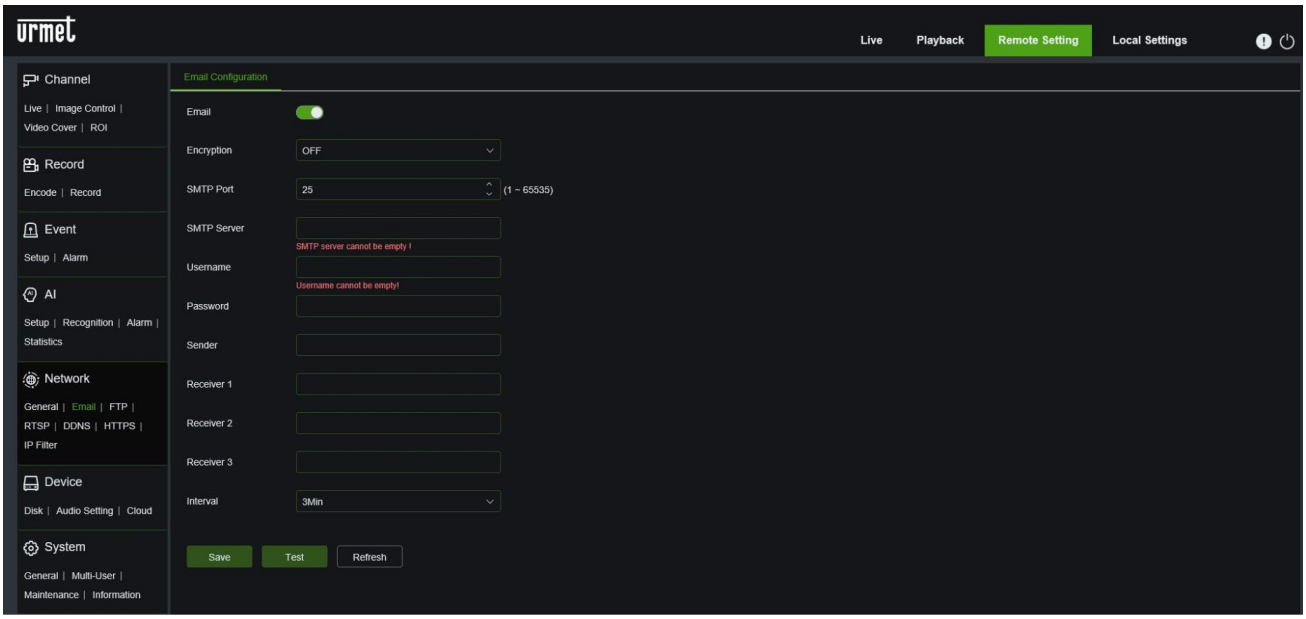


- **HTTP Port**: this is the port that will be used to connect remotely with the camera (i.e. via the Web Client). If the default port 80 is already in use by other applications, you must change it.
- **Client Port**: this is the port that the camera will use to send information. If the default port 9000 is already in use by other applications, you must change it.
- **Https Port:** this is the port that will be used to connect remotely with the camera in encrypted mode (i.e. via the Web Client).
- **RTSP Port: the default port is 554;** if the default port 554 is already in use by other applications, you must change it.
- **Multicast port:** select a Multicast port between 1024 and 65535.

- **P2P Switch:** P2P address can be disabled (enable by default).

9.5.2 E-MAIL (E-MAIL CONFIGURATION)

The e-mail menu allows you to access the configuration of the parameters for alarm notifications via e-mail.

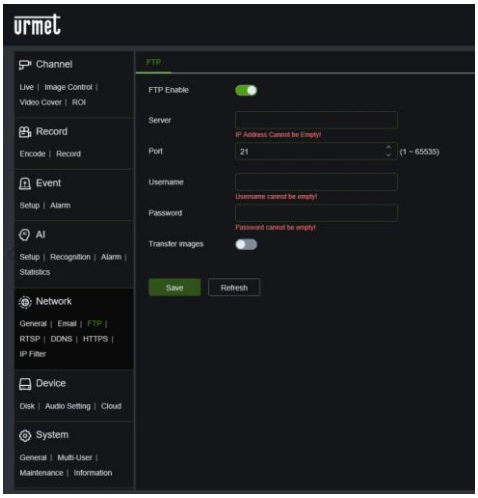


- **Email:** allows you to enable or disable the configuration of the email parameters.
- **Encryption:** allows you to specify whether or not communication with the mail server will be encrypted; the use of a secure transfer protocol using data encryption allows you to encrypt the information communicated (including your email) to prevent hackers from monitoring email, transmitted data and the password. It is recommended to enable an encryption option, if possible. For further information, contact your email provider. Possible values: Disable, SSL, TLS and Auto
- **SMTP Port:** this indicates a port type for email transmission via Simple Message Transfer Protocol (SMTP). The port number for most emails is 25[1].
- **SMTP server:** this indicates the address of the server used.
- **Username:** sets the user name used for authentication on the SMTP server.
- **Password:** sets the password assigned to the email account by the sender.
- **Sender:** indicates the sender's Email address. The email address must be consistent with the server used. In other words, if the email address – aaa@gmail.com is used, the server must be smtp.gmail.com.
- **Receiver 1**: Indicates the e-mail address of the first recipient. The email address is used to receive the image transmitted by the NVR alarm. Delete all the received images as soon as possible to prevent overloading your email account.
- **Receiver2, Receiver3**: you can specify a second and third email address to which to send the images transmitted by the NVR.
- **Interval:** If there are attachments in the notification email (images taken during an alarm), it will take longer to send the email to the recipients. During this time, no further reports may be sent. This option allows you to set this time interval; possible values: 1 min, 3 min, 5 min, 10 min.
- **Test Email:** click the TEST Email button to check that the configuration is working.
- The **Refresh, Save and Delete** buttons are functions to update the page, save it or delete the data entered.

[1] If using Gmail, set the SMTP port to 465 and enable the Encryption option

9.5.3 FTP

This menu allows you to enable the FTP function to view and load snapshots captured by the camera into the storage device on FTP.

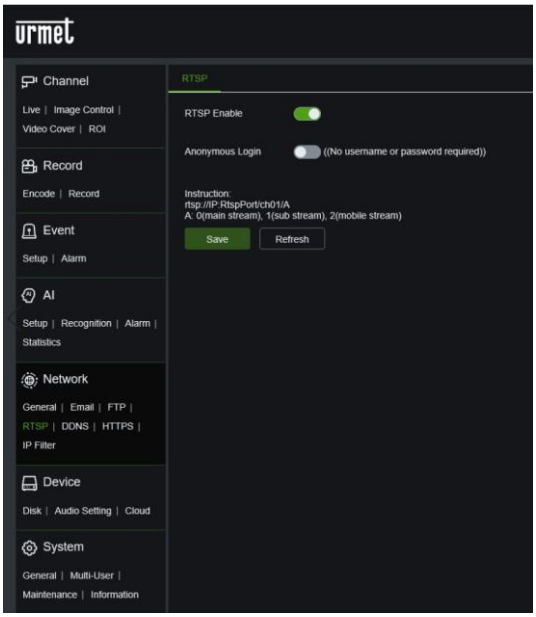


- **FTP Enable:** select the desired option to enable or disable operation.
- **IP Server**: enter the address or name of the FTP server.
- **Port:** FTP service port. Default value: 21.
- **Username**: the username to access the FTP server
- Password: the password to access the FTP server.
- **Transfer images:** select the option to enable or disable image transfer.

Press **Save** to save the desired setting.

9.5.4 RTSP

The Real Time Streaming Protocol (RTSP) function is used to display the main/secondary video streams of an IP camera, for example from a Web page on a PC, through the RTSP port. This function is useful for managing the live stream of an IP camera from a non-proprietary system.



- **RTSP Enable:** select the desired option to enable or disable operation.
- **Anonymous Login:** If not selected, no credentials are required for authentication.

Instructions:

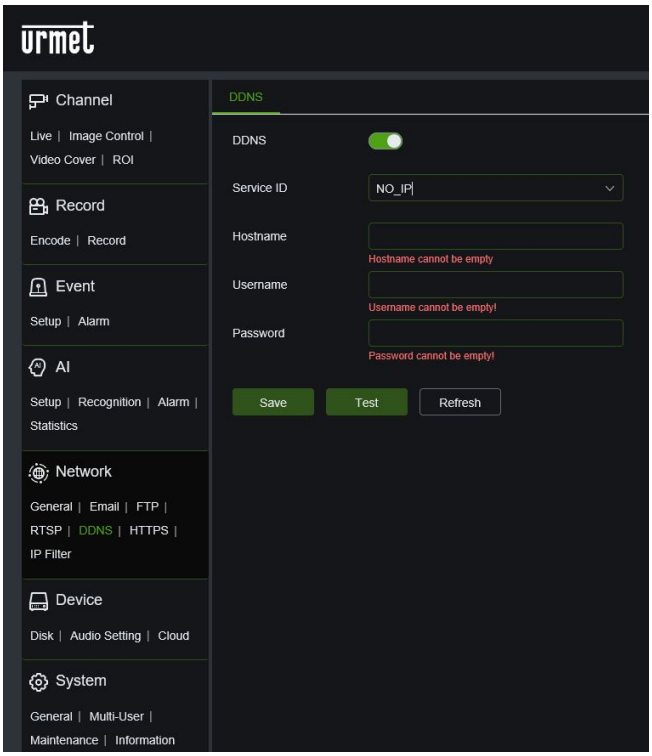
rtsp://IP:RtspPort/ch01/A

A = 0 (main stream), 1 (substream), 2 (mobile stream)

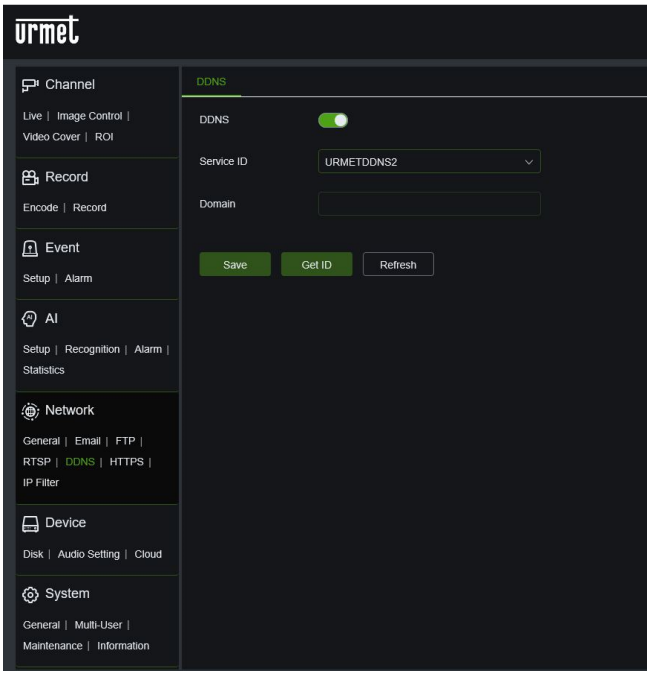
9.5.5 DDNS CONFIGURATION

Select DDNS in the Network menu to open the following page:

DDNS (Dynamic DNS) is a service used to record a domain name and floating IP address with the DDNS server so that the domain name can be routed towards the IP address even if it is changed in a dynamic IP system. The user can access a remote camera using DDNS on the three previous types (Static, DHCP and PPPoE).



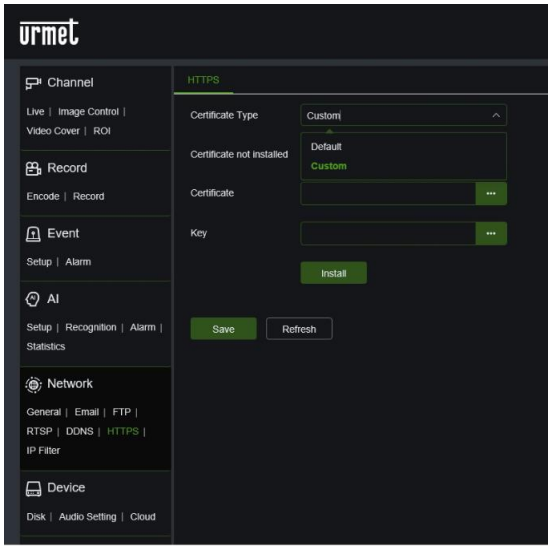
- **DDNS:** Enable or disable the function.
- **SERVIDCE id (Server):** Server options are *URMET DDNS*/*URMET DDNS2*/*DynDNS*/*NO-IP*/*DDNS_332*. Choose the Server address. For **URMET DDNS/DDNS2** accounts you can generate the ID.
- **Hostname:** Enter the name of the active server.
- **User Name:** Name of the user.
- **Password:** User's password



- If you are using one of the Urmet DDNS services, after selecting **the Server ID**, click the **Get ID** button and wait approximately 10 seconds for the Domain ID to be generated. Once the ID has been generated, enter it into the app or the Client software for remote connection.

9.5.6 HTTPS

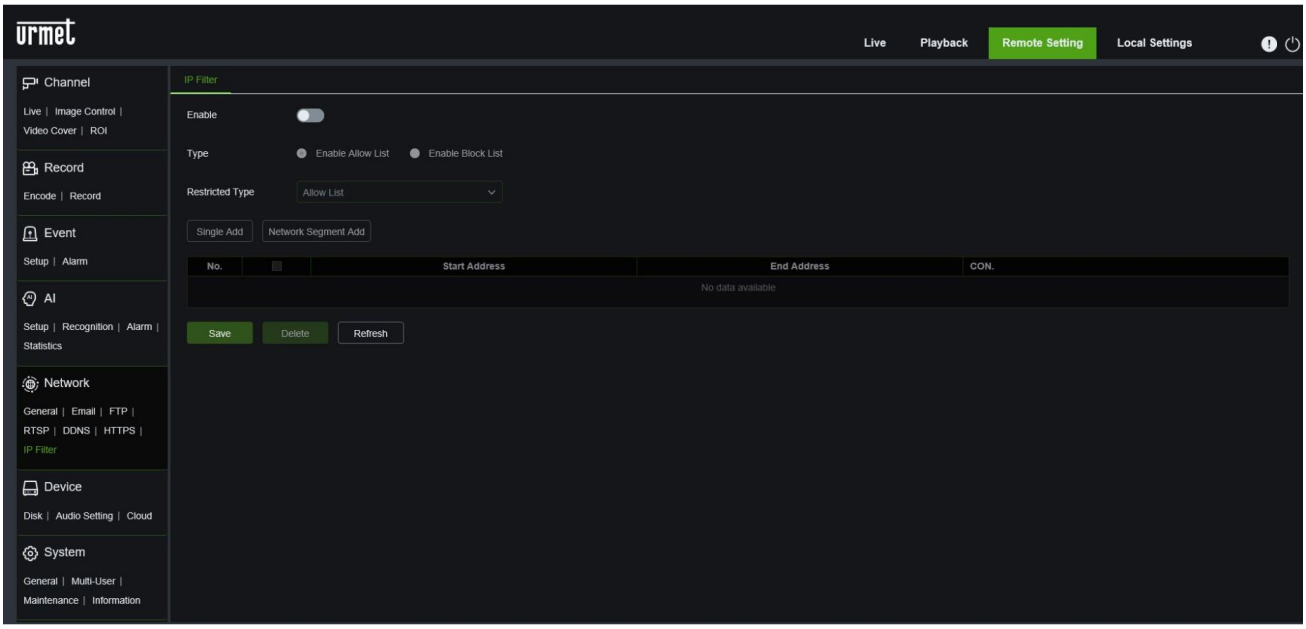
In this menu you can set the security encryption protocol.



- **Certificate Type:** Default or Custom

9.5.7 IP FILTER

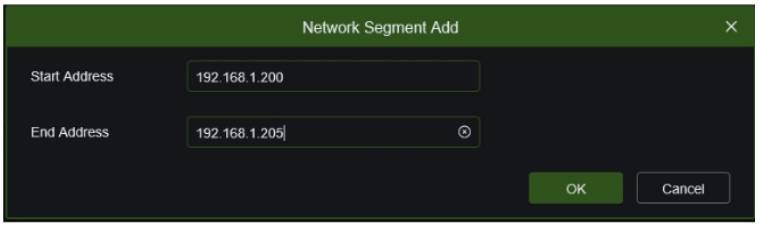
Select IP Filter in the Network menu to open the following page:



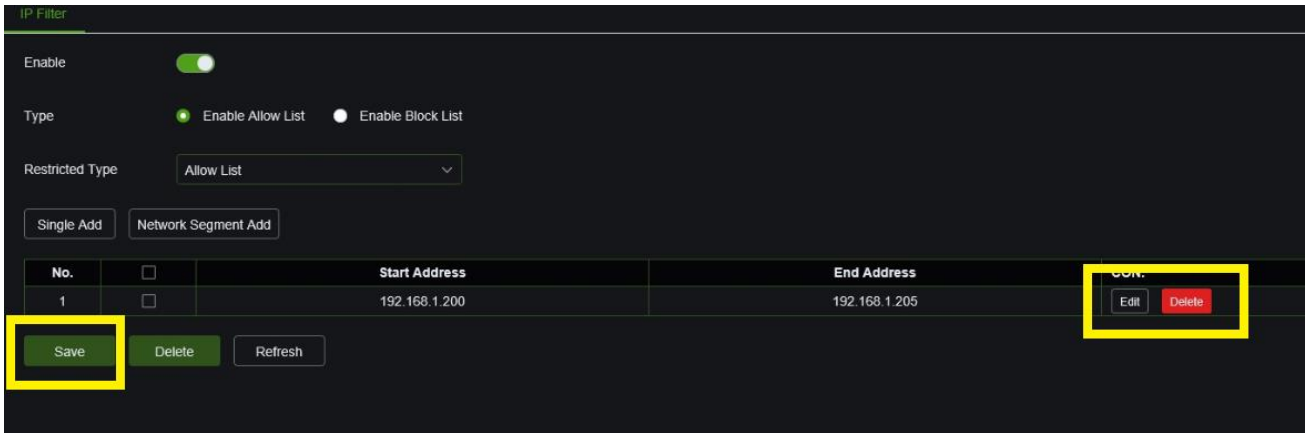
- **Enable:** if **Enable** is selected, the Whitelist and Blacklist can be configured.
- **Type:** Enable Allow List or Enable Block List.
- **Restricted Type:** Select the type of restriction to configure.

For both lists, you can add one address, **Single Add,** or an address list.

Network Segment Add



Once the choice of address or address class has been confirmed, confirm with **OK**; the setting will be displayed in the menu below:



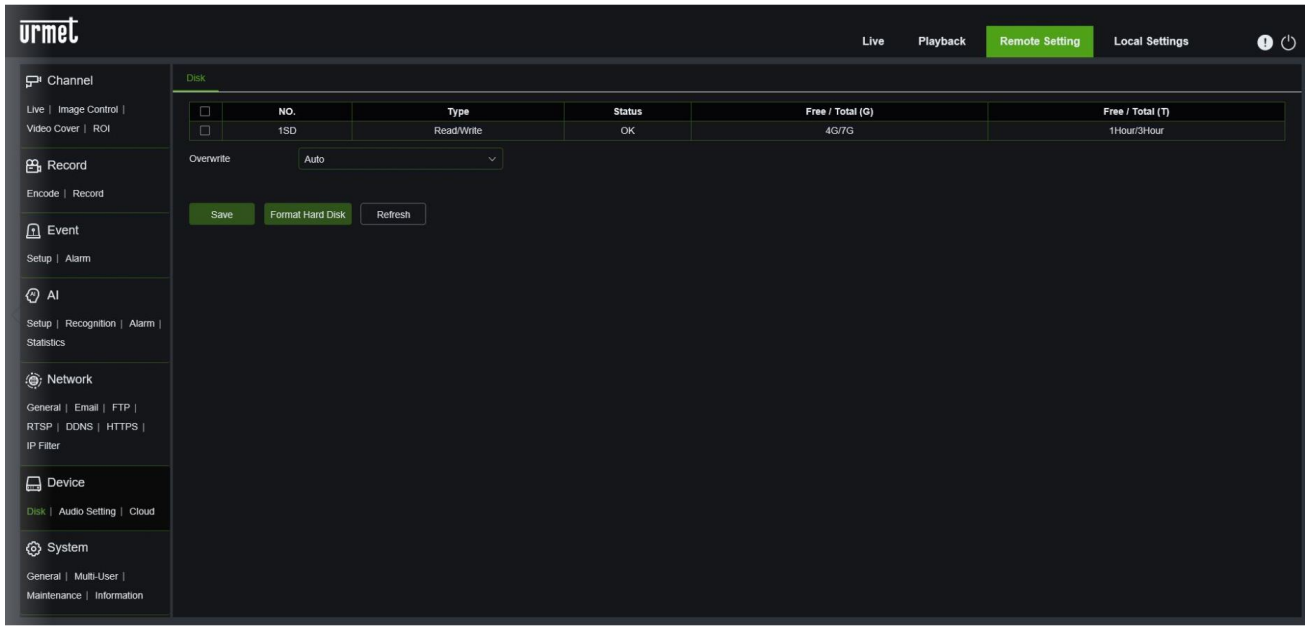
You can edit the address list with the **Edit** button or delete the list with the **Delete** button.
Press **Save** to save the desired setting.

9.6 DEVICE

Includes Disk, Audio Setting and Cloud. The various interfaces and functions are described below.

9.6.1 DISK

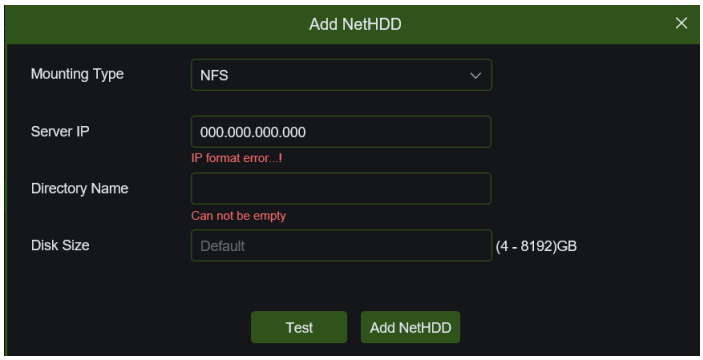
Select Disk in the Device menu to access the page below.

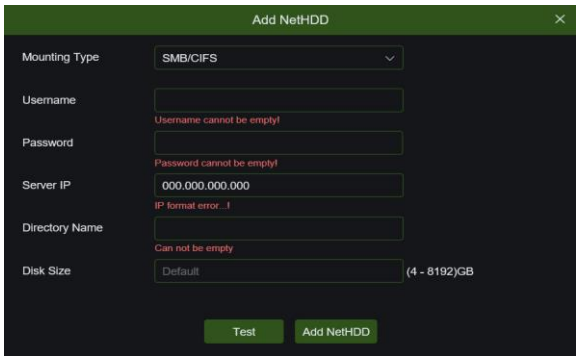


With the device disconnected, insert the SD card in the appropriate slot; when the device is powered, it will automatically detect the total capacity and provide information on the remaining recording time.

- Overwrite: when the capacity of SD card is 0, new records will overlap previous records (this function is on by default).
- HD Format: Formats the SD card.

Add NetHDD: by selecting this button, NAS-type storage can be set up for the NFS or SMB/CFS protocols.

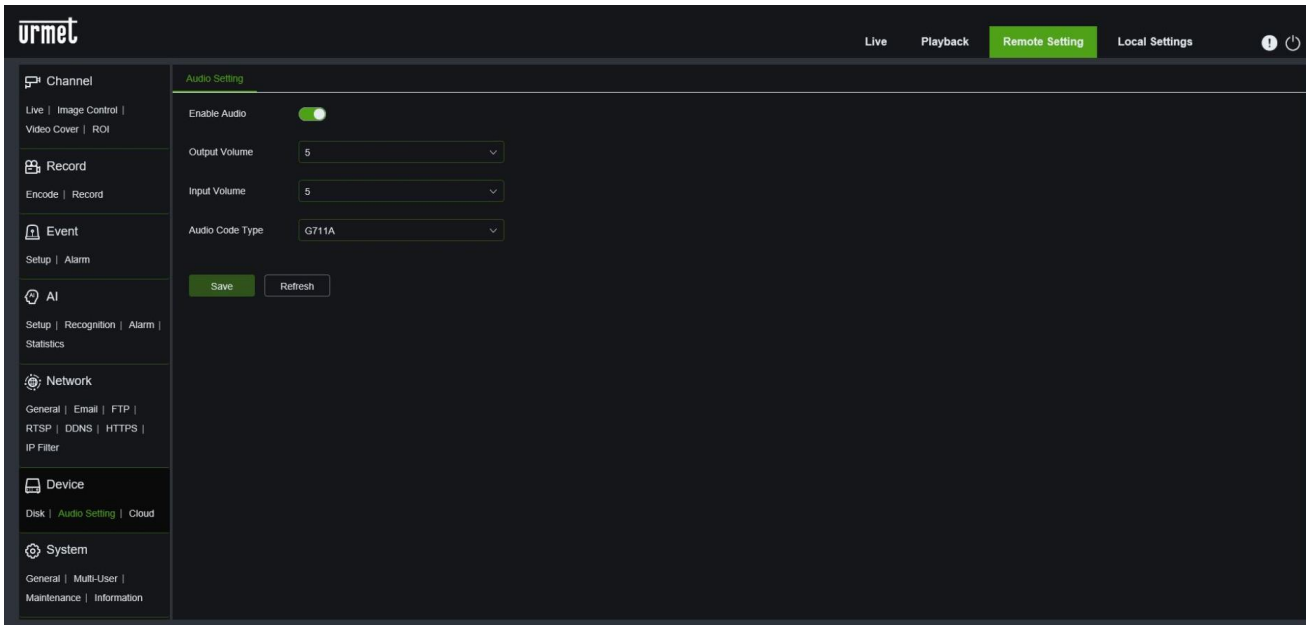




Press **Save** to save the desired setting.

9.6.2 AUDIO

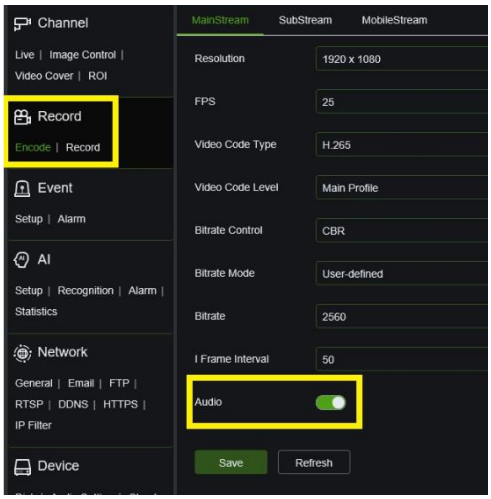
Click on Audio in the Device menu to open the following page:



Audio setup procedure:

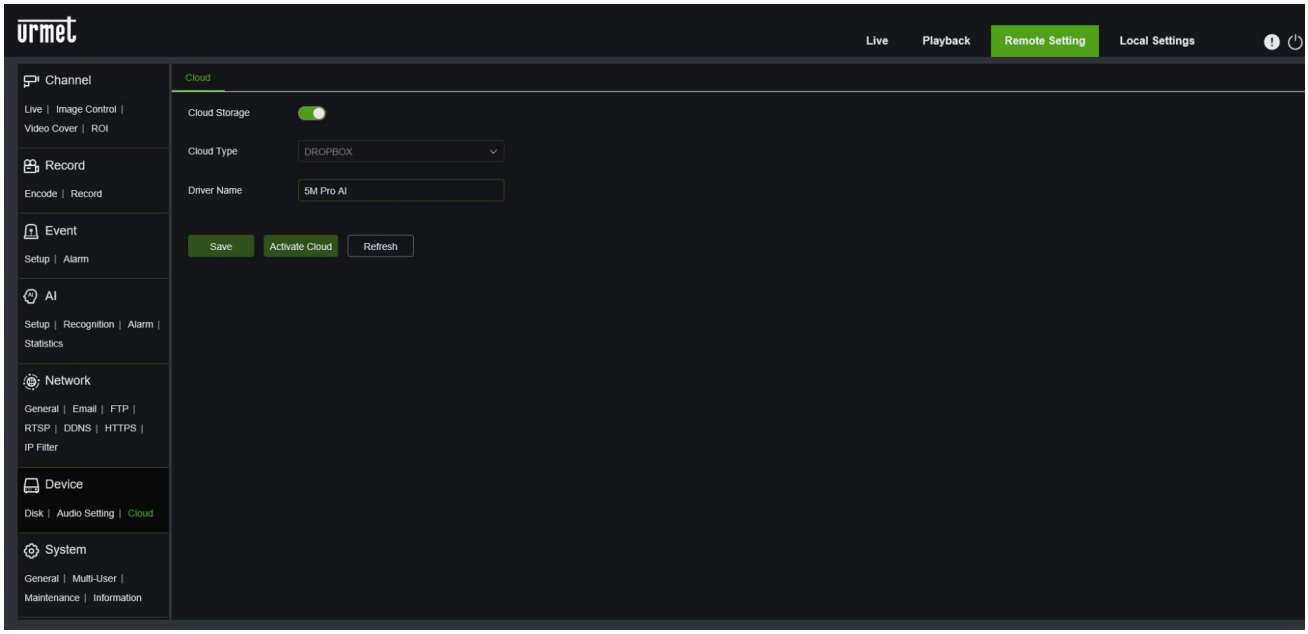
- Select the **Enable Audio** option to access the audio parameters.
- set **Output Volume** and **Input Volume** (0~10)
- **Audio Code Type:** Choose the audio encoding between G711A (default) and G711U
- Select **Save** to save the settings.

Note: In order to use the audio function, the audio option in **Record/Encode** must be enabled, for each desired type of Stream.



9.6.3 CLOUD

In the event of an alarm, the IP camera is capable of sending images and video to a Cloud storage service via Dropbox, a free service that allows you to easily store and share snapshots and always have them on hand when needed. The configuration can be accessed under **Cloud** in the **DEVICE** menu.
Before activating the Cloud function, it is recommended to create a Dropbox account using the e-mail address and password chosen for the HVR. Enter your email address and password on the main Dropbox site, accept the terms and conditions, then click the Sign-up button.



- **Cloud Storage**: the Cloud storage function can be activated.
- **Cloud Type (Tipo di Cloud)**: you can select the type of Cloud; DROPBOX.
- **Cloud Overwrite**: you can setup the number of the days for overwrite the data over the cloud.
- **Video Type**: you can select the video type saved over the cloud between RF, AVI or MP4.
- **Driver name**: the driver name can be changed.

Press **Save** to save the desired setting.

Activate Cloud: click on this button to activate the Cloud storage function.

The System will prompt you to confirm the local IP of the camera and then return to the Cloud DROPBOX login page to complete the device registration.

Note: to set the send function on Dropbox, it is recommended that you access your camera's Remote Settings using a browser other than Internet Explorer (e.g. Edge, Firefox or Google Chrome).

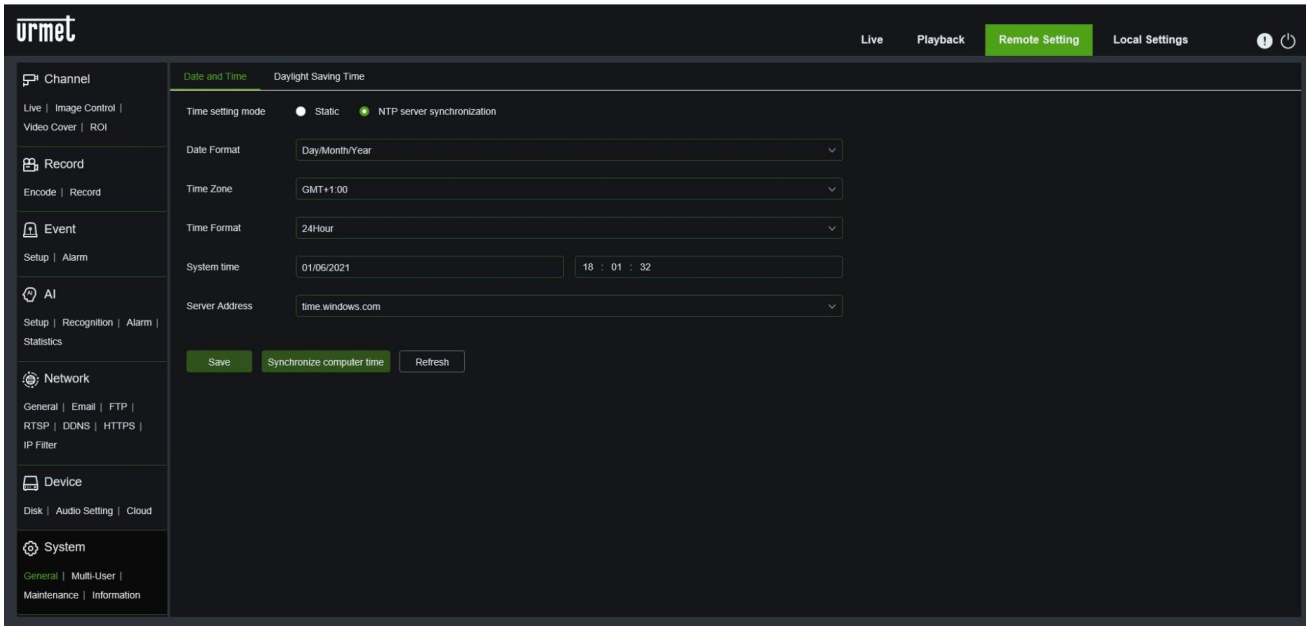
9.7 SYSTEM

System parameters include: General, Multi-User, Maintenance and Information. The various interfaces and functions are described below.

9.7.1 GENERAL

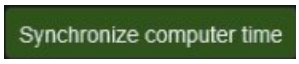
9.7.1.1 Date and Time

Select General in the System menu to open the following page

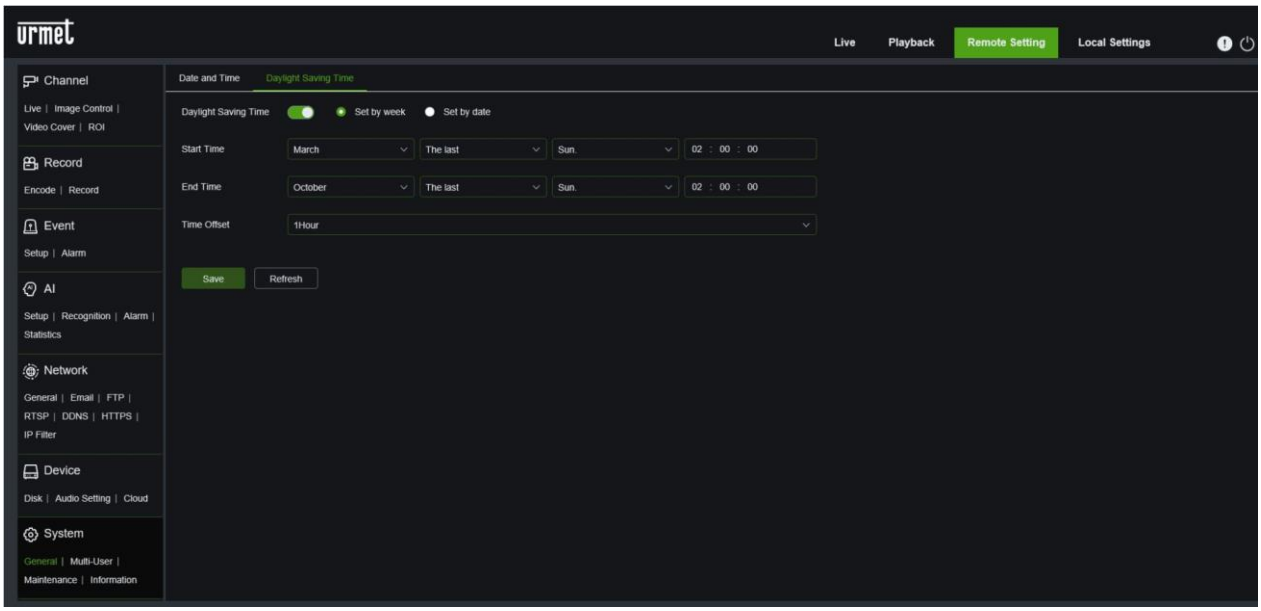


- **Time setting mode:** Select the time setting mode, whether **Static** or **NTP Server Synchronisation**
- **Date Format**: Select the preferred date format.
- **Time Zone**: Select the time zone for your region or city.
- **System time:** Manually select the correct date and time if you have chosen static mode
- **Server Address:** Choose the reference server for automatic time setting if you have selected the **NTP Server Synchronisation** setting.

Press **Save** to save the desired setting.

Click the button  to set the date and time of the PC on the camera.

9.7.1.2 Daylight Saving Time



- **DST:** Select the Daylight Savings Time (DST) option to enable DST correction.
- **Daylight Saving Time:**

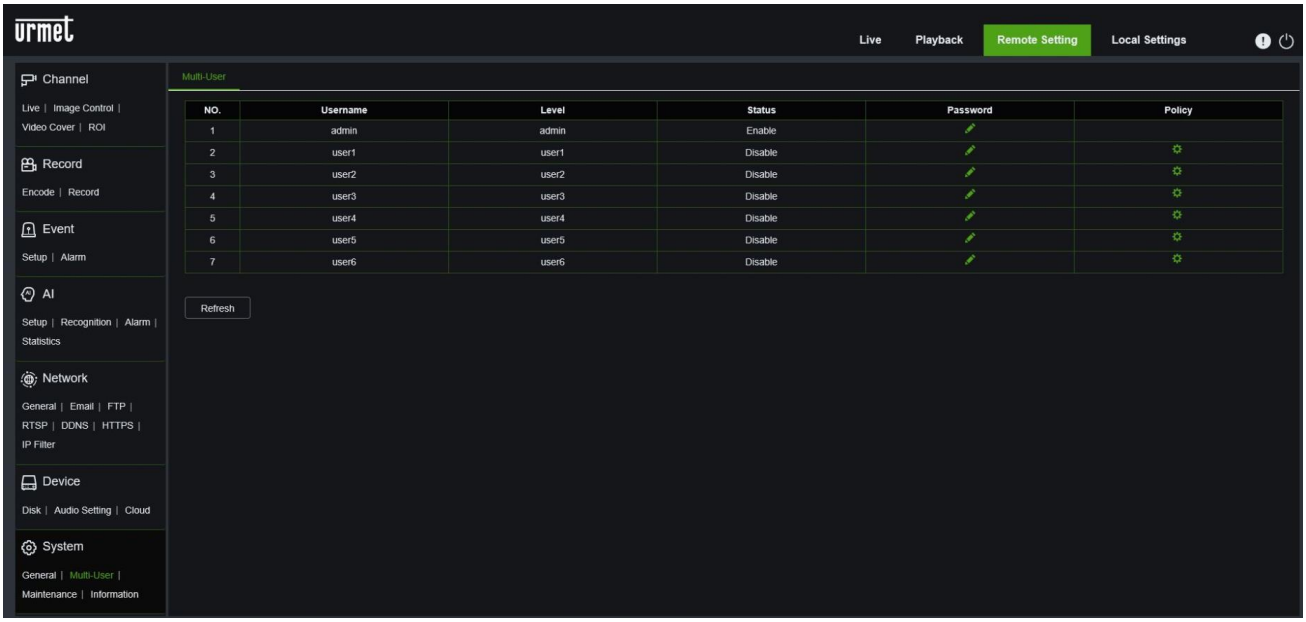
- **Set by week**: Select the month, day and time for the start and end time of daylight saving time. For example, 2: 00 a.m. on the first Sunday of a certain month.
- **Set by date**: select the start date (click the calendar icon), end date and time for activation of daylight saving time.
- **Start Time / End Time**: Set the start and end time for daylight saving time.

- **Time Offset**: Select the time difference due to daylight saving time in the local time zone. This is the difference in minutes between Coordinated Universal Time (UTC) and local time.

Press **Save** to save the desired setting.

9.7.2 MULTI USER

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

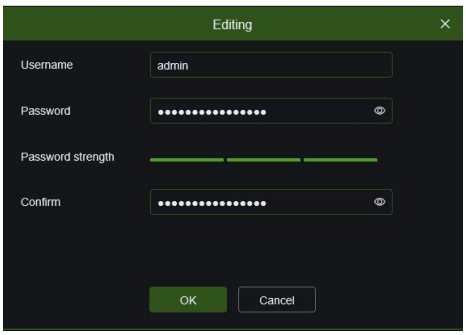


In this section you can set the user access authority and login password.

The system supports the following types of accounts:
- ADMIN — System Administrator: the administrator has complete control of the system and can change the administrator and user(s) passwords, as well as enable/exclude password protection.
- USER — Normal user: users can only access live viewing, search, playback, etc. You can set up multiple user accounts with different levels of system access.

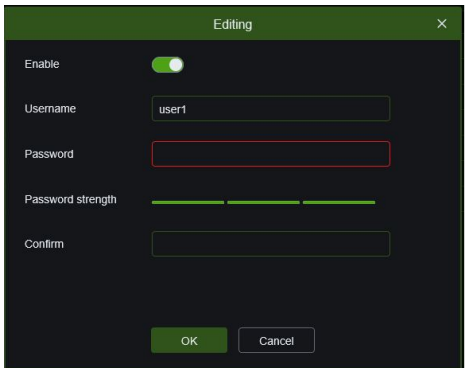
1. Password

To change the administrator account password, click the Password icon. The password must be at least eight characters long and can contain a series of digits and letters. Enter the new password a second time to confirm it, then click **Save** to save it.



2. Add New Users

From the same menu you can also enable other users by clicking on the  icon for the user to be enabled.

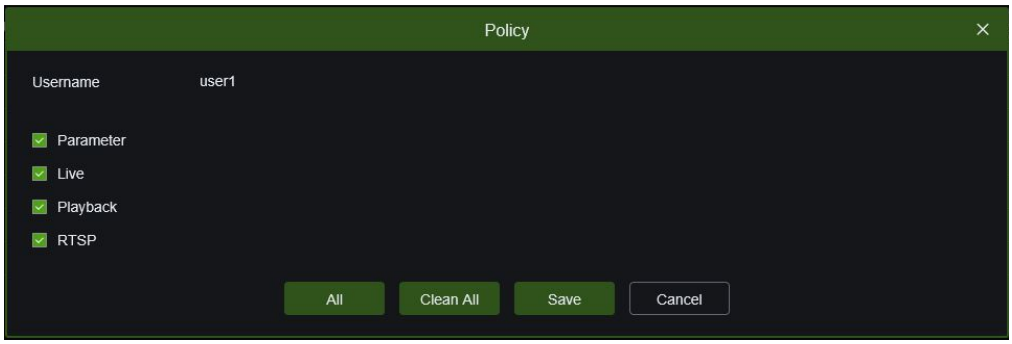


- Select **Enable**
- Click the field next to **Username** to change the user name of the account.
- Click the field next **to Password** to enter the desired password.
- Click the field next **to Confirm** to re-enter the password.
- Click **OK**. You will need to enter the Administrator password for authentication.

3. Policy: Setting user prerogatives

The administrator account is the only one with full control of all system functions. You can enable/exclude access to certain menus and features for each user account.

- Click the icon below **the Policy** tab; the following configuration window will appear:

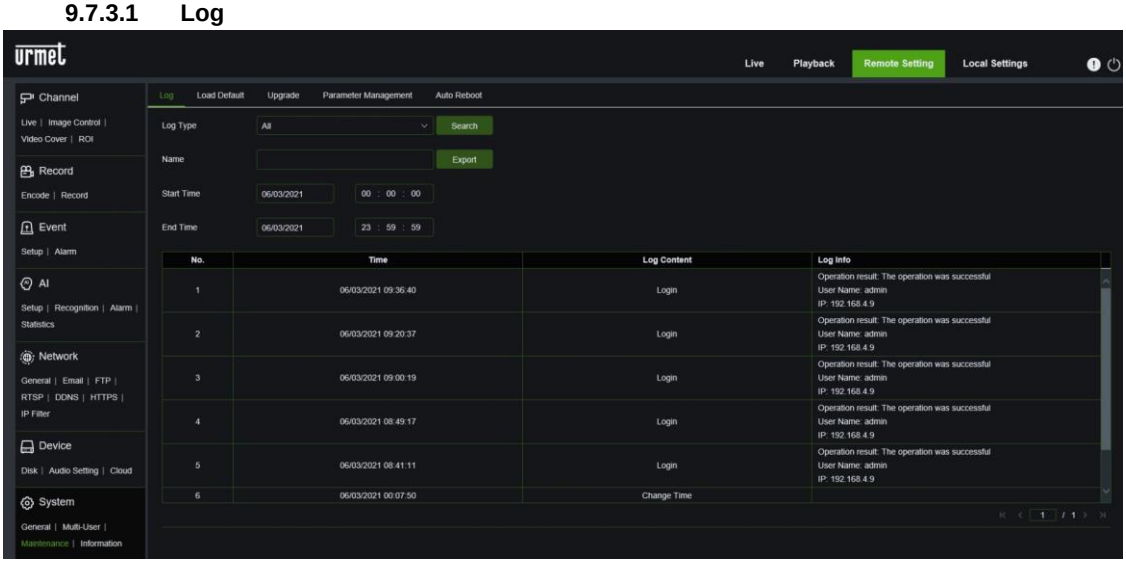


- Tick the boxes next to the menus and system capabilities that the user can access. Click **All** to tick all the boxes. Click **Clean all** to tick no boxes.
- Click **Save** to save the settings made.

9.7.3 MAINTENANCE

In this section, you can search and view the system log, load defaults, update the system, export/import system parameters and manage automatic system restart.

9.7.3.1 Log



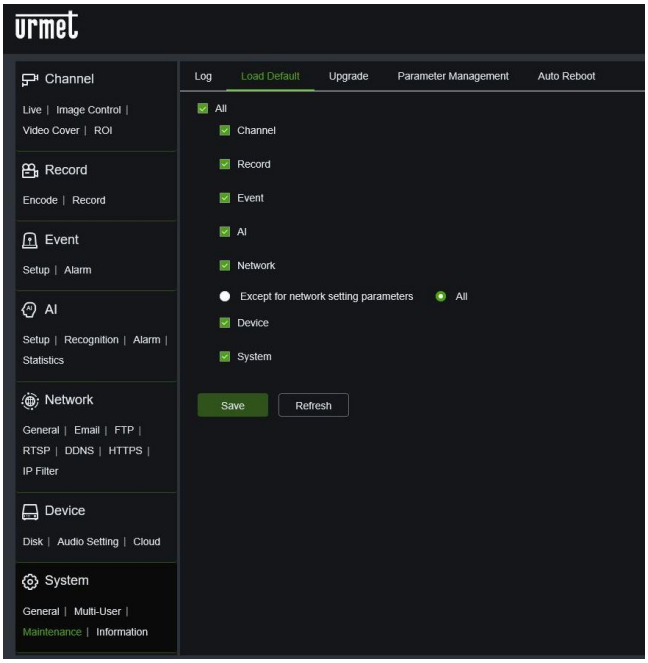
Log Search and Back up:

- Select the type of events you are looking for from the drop-down menu next **to Log Type** or select **All** to view the entire system log for the selected period.
- Click the field next **to Start Date** & **Start Time** to select the search start date and time from the displayed calendar.
- Click the field next **to End Date** & **End Time** to select the search end date and time from the displayed calendar.
- Click **Search.**
- Browse system log events by search period.

- Click **Export** to create a backup of the system log for the period searched, after naming the file, which will be saved in a system folder in .csv format

9.7.3.2 Load Default:

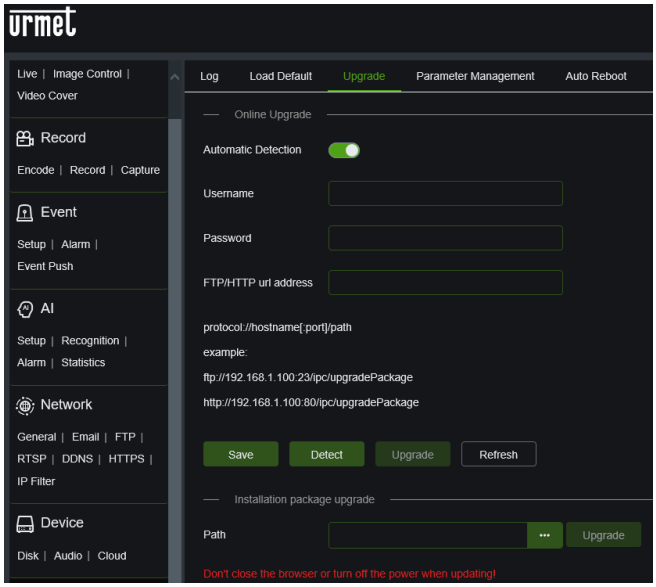
Through this menu you can reset the camera's factory settings. You can choose to reset all settings at once or only specific menu settings. Restoring the default settings will not erase recordings and snapshots saved on a SD card.



Select all the items to reset or select **All** to select all items. Click **Save** to load the default settings for the selected items.

9.7.3.3 Upgrade:

This feature allows you to update the NVR firmware.

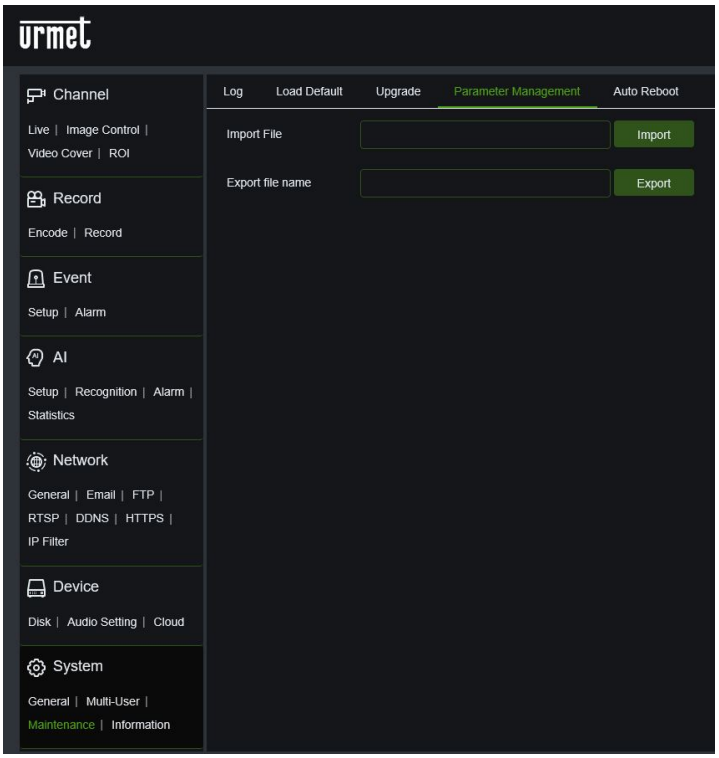


Click the **Select File** button  to select the firmware file (.sw file), and then click OK.
Click **the Upgrade** button to start the system update. The system update will take about 5-10 minutes: **DO NOT turn off the camera during the firmware update.**

In the near future, **automatic update detection** via a URL address and protected by user name and password will be possible.

9.7.3.4 Parameter Management

This menu allows you to *export/import* the main camera settings.

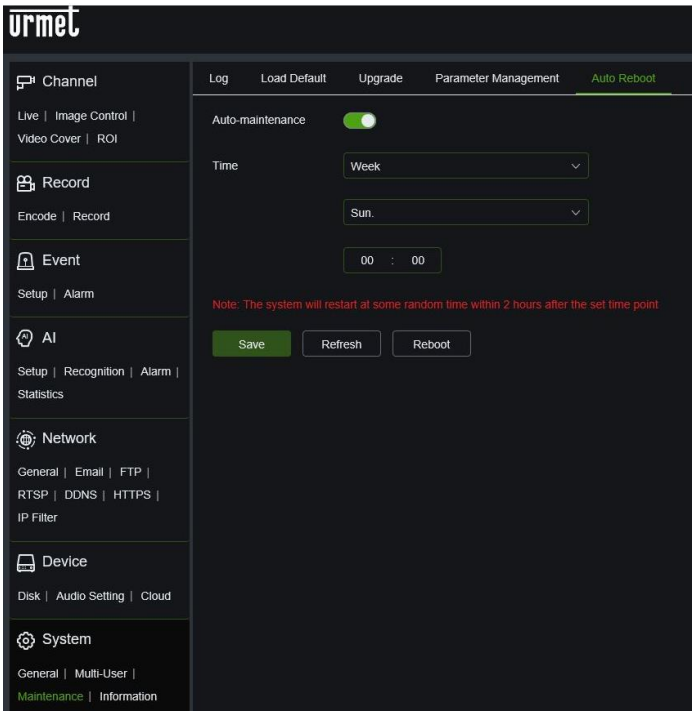


- Click in the **Import file** window to open the dialogue where you can select the backup file to import, and confirm by clicking on the **Import** button.
- Type the name of the backup file you want to export in the **export file name** window, then click on the **Export** button to complete the operation.

Note: You must provide Administration credentials in order to complete both operations

9.7.3.5 Auto Reboot

This menu allows the system to automatically restart the camera periodically.

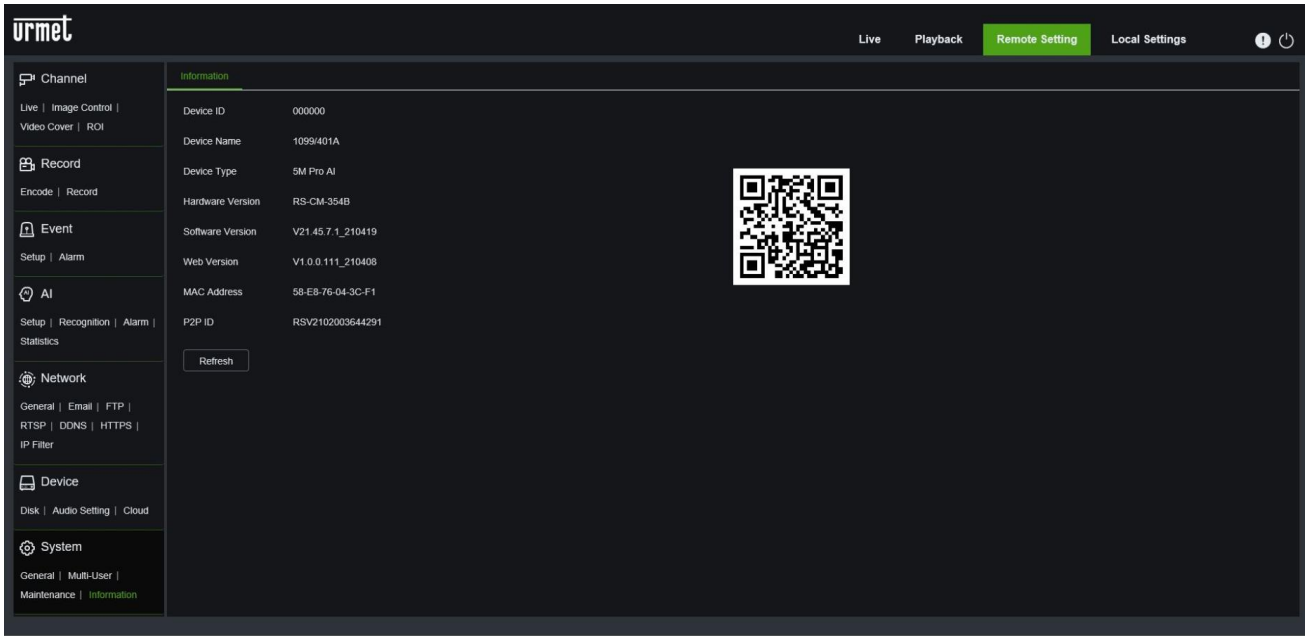


- **Auto Reboot:** click to enable feature
- **Time:** You can set the day, week, or month the camera is restarted.

Press **Save** to save the desired setting.

9.7.4 INFORMATION

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



Some system information on the device is displayed in this section, including device type, MAC address and software version. The QR Code is the P2P ID that can be used via APP or UVS Pro Client for remote connection to the device.

10 MAXIMUM RECORDING TIME WITH SD CARD

The following resolution options can be selected for Main Stream recording:

- "**8Mpx**", "**5Mpx**", "**4Mpx**", "**3Mpx**", "**1080P**", "**960P**" for IP camera with **H.265/ H.265+/ H.264/H264+** codec

※IMPORTANT NOTES

- The following tables show the approximate time needed to fill the SD Card when the IP channel records with the selected Bitrate to an SD card with a 256GB capacity.

SD 256GB	
Bitrate (Kbps)	**Days of recording**
10240	2.18
8192	2.73
7168	3.12
6144	3.6
5376	4.17
5120	4.37
4608	4.86
4096	5.47
3840	5.83
3328	6.75
3072	7.29
2560	8.75
2304	9.72
2048	10.94
1792	12.5
1664	13.46
1536	14.59
1280	17.51
1024	21.88
896	25
768	29.18
640	35
512	43.77
384	58.36
256	87.54
192	116.72
96	233.45

NOTE: To find out the Bitrate of the stream used in recording, see the Web page under **REMOTE SETTING, RECORD, ENCODE**

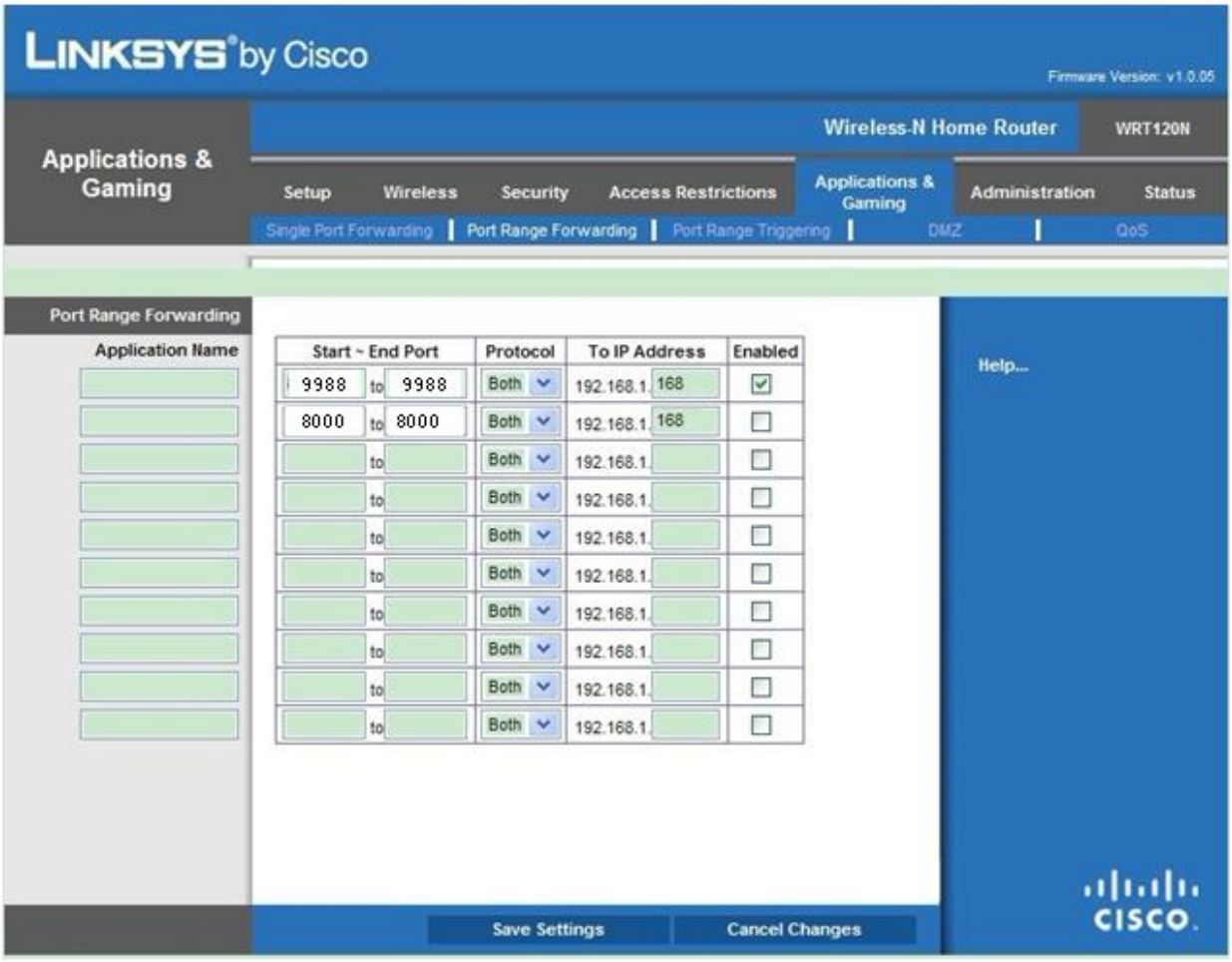
11 APPENDIX

11.1 ROUTER PORT FORWARDING

To remotely view the IP Camera via the Internet, you must first set the web port and client port of the IP Camera.

Taking a Cisco router as an example:

The IP address of the IP camera is 192.168.1.168, the web port is 8000 and the client port is 9988.

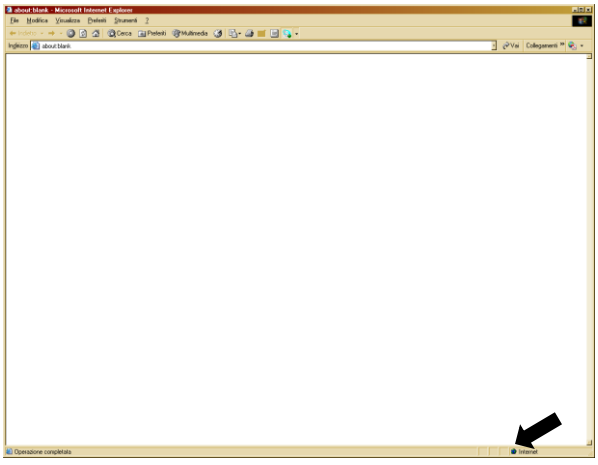


11.2 INSTALLING ACTIVEX

If you need to install an ActiveX component, you may do so as follows.
Before connecting the PC, activate the IE protection settings, as shown below:

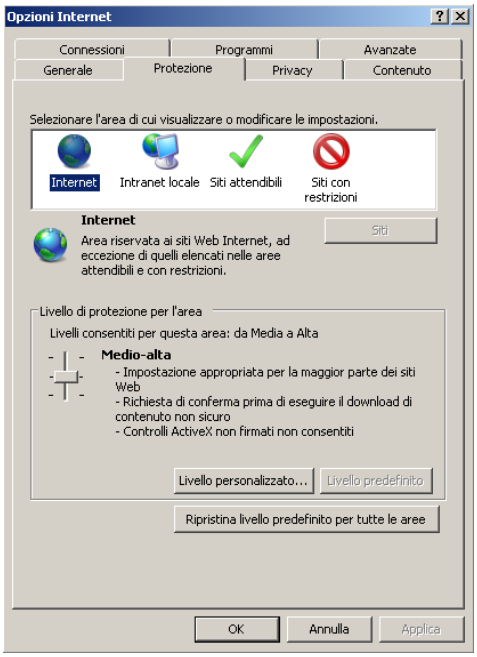
Double click on the  icon to open Internet Explorer.

- The following window will appear (or the default page).



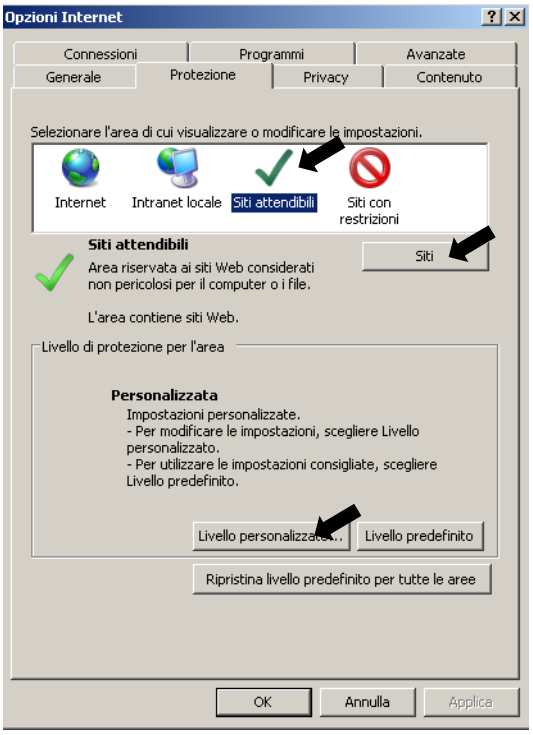
- Double click on the 

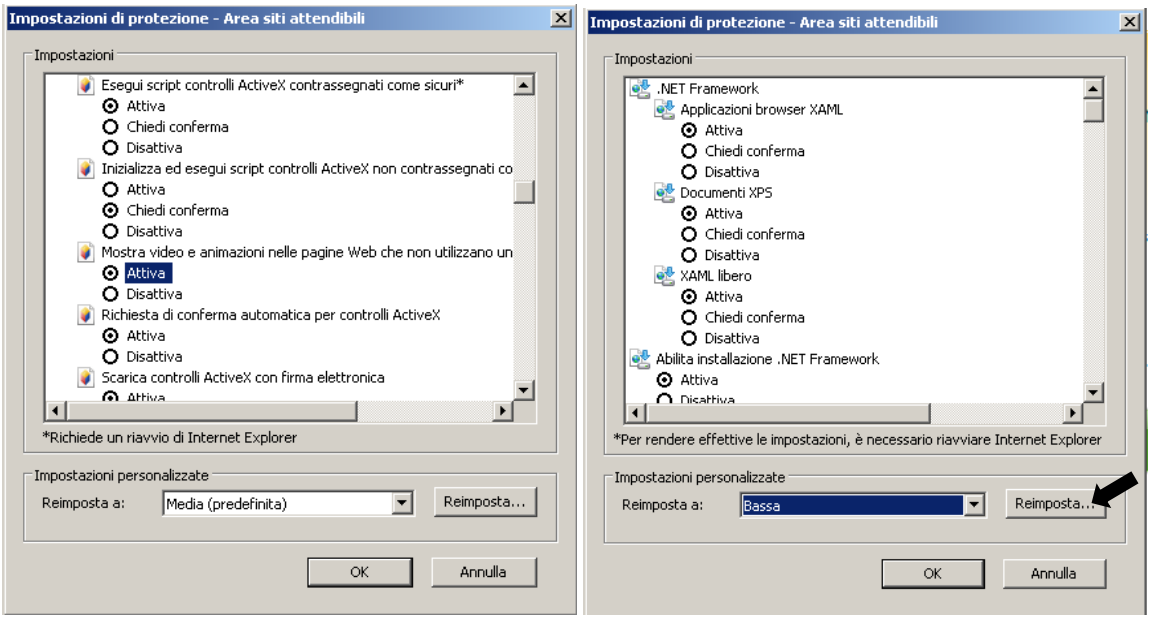
icon to open Internet Explorer.
- The “Internet Options” window will appear.


Opzioni Internet
Connessioni
Programmi
Avanzate
Generale
Protezione
Privacy
Contenuto
Selezionare l'area di cui visualizzare o modificare le impostazioni.
Internet
Intranet locale
Siti attendibili
Siti con restrizioni
Internet
Area riservata ai siti Web Internet, ad eccezione di quelli elencati nelle aree attendibili e con restrizioni.
Siti
Livello di protezione per l'area
Livelli consentiti per questa area: da Media a Alta
Medio-alta
- Impostazione appropriata per la maggior parte dei siti Web
- Richiesta di conferma prima di eseguire il download di contenuto non sicuro
- Controlli ActiveX non firmati non consentiti
Livello personalizzato...
Livello predefinito
Ripristina livello predefinito per tutte le aree
OK
Annulla
Applica

- Select the “**Trusted Sites**” area.
- Click “**Custom Level**” and check that:
    - “Initialise and script ActiveX controls not marked as safe” is set to “Enable” or “Prompt”.
    - “Download signed ActiveX controls” is set to “Enable” or “Prompt”.

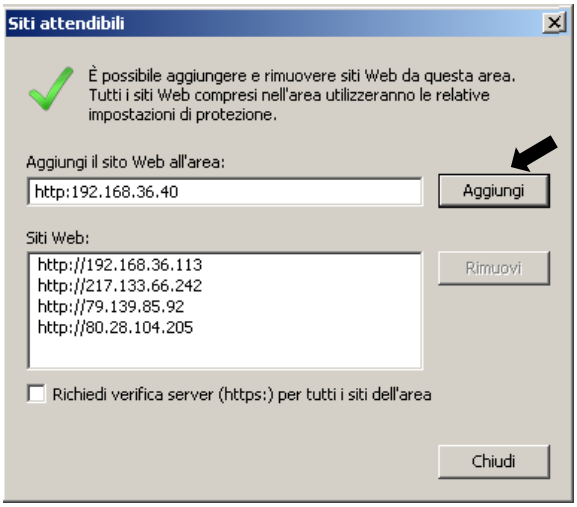
Check that the Security Level is set to “**Low**”. If the Security Level is not set, set it to “Low” and click “Reset”. Confirm by clicking OK.





- Click on **“Sites”**.

- The following screen will be displayed: You will need to add the IP address of the device (example: http://192.168.36.40) in the "*Add the website to the zone*" field.



- Add the IP address of the device in the field and click "**Add**".

※ NOTE

Do not select the item: "Require server verification (https:) for all sites in this zone"

- Click on "**Close**" to close the window
- Confirm by clicking "**Apply**" and "**OK**"
- Close the Internet Explorer interface and launch your browser again to install the new Active X.

11.3 FREQUENTLY ASKED QUESTIONS

- **Internet Explorer cannot load and install plug-ins.**
  1. Possible cause: IE security level is set too high.
     Solution: Set IE security level to the minimum level.

- **After updating, I cannot access the IP Camera through Internet Explorer.**
  1. Solution: Clear the IE cache as follows: open IE Tools, select Internet Options, select the 2nd option under “Delete Files” (Temporary Internet Files), click “Delete all offline content” and click OK. Access the camera once again.

- **Why am I unable to access the IP Camera through IE?**
  1. Possible cause 1: network fault.
     Solution: connect the PC to the Internet and check whether network access is normal. Check that there are no problems with cable connection or network problems so that the two devices can ping each other.
  2. Possible cause 2: the IP address is occupied by other devices.
     Solution: Disconnect the IP camera from the network, connect the IP camera directly to the PC and set the device IP address.
  3. Possible cause 3: the IP address belongs to a different mask.
     Solution: check the settings of the IP address, the subnet mask address, and the gateway.
  4. Possible cause 4: the physical address of the network conflicts with that of the IP camera.
     Solution: change the physical address of the IP camera.
  5. Possible cause 5: the web port has changed.
     Solution: contact the network operator to obtain the port information.

- **The PC client cannot connect to the front-end video**
  1. Solution: check that the IP camera video can be normally viewed in IE, that the device can be accessed by the PC client software and that the device parameters on the client PC are set correctly.

- **The mobile client cannot connect to the front-end video**
  1. Possible cause 1: mobile stream is not enabled.
     Solution: Enable Sub Stream (Mobile Stream not available).
  2. Possible cause 2: the mobile port number was not entered correctly.
     Solution: the mobile client software port number is 9988 and that of the third-party client is 8800.
  3. Possible cause 3: the video streams connections exceed the maximum limit.
     Solution: reduce the video stream connections on the device.

DS1099-188

URMET S.p.A.
10154 TURIN (ITALY)
VIA BOLOGNA 188/C
Tel. +39 011.24.00.000 (AUTO)
Fax +39 011.24.00.300 - 323

urmet

CE

Technical area
customer service
+39 011.23.39.810
http://www.urmet.com
e-mail: info@urmet.com
MADE IN CHINA