

H.265 5M ECO 2 IP Camera

Bullet Camera IP Sch. 1099/500A



Bullet Camera IP Varifocal Sch. 1099/501A



Bullet Camera IP Varifocal Sch.1099/502A



Camera IP 1099/550A



Dome Camera IP Varifocal 1099/551A



Vandal Dome IP Sch. 1099/552A



H.265 5M ECO 2 IP Camera

Bullet Camera IP Deterrence Sch. 1099/208A



Cube Camera IP WIFI 2M 1099/210



USER MANUAL

CONTENTS

1	Introduction.....	5
2	Product Description	6
2.1	Technical characteristics	6
2.2	Opening the Box	6
2.3	Warnings	7
3	Overview.....	9
3.1	Range of Application	9
3.2	Product description	9
3.3	Operating environment	9
3.4	IP Camera Connector Layout (Where FEATURED)	10
4	Operating instructions	11
4.1	Checking the Connection	11
4.2	Searching for the Device	11
4.3	Installation of Controls and Login to the System	12
5	Login.....	12
5.1	First Camera Login	12
5.2	Preview	13
5.3	Recovery password	14
5.3.1	Security Question Verification	14
5.3.2	Certificate of authorisation	15
5.3.3	Super code	15
6	Live	15
6.1	PTZ Control	16
7	Local settings	17
8	Playback.....	17
8.1	General	17
8.2	Playback controls	18
8.3	TAG	18
9	Remote Setting	18
9.1	Display Configuration	18
9.1.1	Live	18
9.1.2	Image Control	19
9.1.3	Privacy Zone	20
9.2	Record	20
9.2.1	Encode.....	20
9.2.2	Record	21
9.2.3	Schedule	22
9.3	Event.....	22
9.3.1	Setup	22
9.3.1.1	MOTION DETECTION	22
9.3.1.2	PIR (Only for some models)	23
9.3.1.3	Deterrence (Only for some models)	23
9.3.1.4	Siren (Only for some models).....	24
9.3.1.5	SOUND DETECTION	24
9.3.2	Alarm output settings	25
9.3.2.1	Motion detection.....	25
9.3.2.2	I/O (INPUT/OUTPUT) [where featured]	26
9.3.2.3	PIR (Only for some models)	27
9.3.2.4	Sound detection.....	28
9.3.3	Event Push	29
9.4	Network	29
9.4.1	General	29
9.4.1.1	General (Network).....	29
9.4.1.2	PPPoE	30
9.4.1.3	Wireless (Only available on some models).....	30
9.4.1.4	SNMP	31
9.4.1.5	Port Configuration	32
9.4.2	E-Mail (E-Mail configuration)	32

9.4.3	FTP	33
9.4.4	RTSP	33
9.4.5	DDNS Configuration	34
9.4.6	HTTPS	35
9.4.7	IP Filter	35
9.5	Device	36
9.5.1	DISK	36
9.5.2	Audio.....	37
9.5.3	Cloud	38
9.6	System.....	39
9.6.1	General	39
9.6.1.1	Date and Time	39
9.6.1.2	Daylight Saving Time	39
9.6.2	MULTI USER	40
9.6.3	MAINTENANCE.....	41
9.6.3.1	Log	41
9.6.3.2	Load Default:	42
9.6.3.3	Upgrade:	42
9.6.3.4	Parameter Management	43
9.6.3.5	Auto Reboot.....	43
9.6.4	Information	44
10	Technical Specifications for the Bullet 5M ECO 2 ip cameras	45
11	Technical Specifications for the dome 5M ECO 2 ip cameras.....	47
12	Technical Specifications for the Bullet DETERRENCE ECO 2 IP Cameras.....	49
13	Technical Specifications for cube Camera IP WiFi 2M.....	51
14	LED, I/O INTERFACE AND MICRO SD CARD SLOT DESCRIPTION FOR 1099/210	52
15	Maximum recording time with SD Card	53
15.1	Ref. 1099/500A – 1099/501A – 1099/502A – 1099/550A – 1099/551A – 1099/552A – 1099/208A.	53
16	Appendix	53
16.1	Router Port Forwarding	53
16.2	Installing ActiveX	54
16.3	Frequently Asked Questions	58

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) and the password 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. Ref. 1099/500A, Ref. 1099/501A, Ref. 1099/502A, Ref. 1099/550A, Ref. 1099/551A, Ref. 1099/552A and Ref. 1099/208A, are Eco 2 Series 5 Megapixel IP cameras, which can be controlled by a TCP/IP network connection. URMET S.p.A. Ref. 1099/210 is instead a Wi-Fi IP Camera 2MegaPixel.

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 8, 9, 10, 11, Edge, Chrome 44/lower, Firefox 51/lower, Safari 11/lower) for real-time on-site monitoring, setup and management.
- Managed through Urmnet 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 in paper format

※IMPORTANT NOTE:

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.

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 as 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 it 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

- It is advisable to periodically check the Urmet website in the product-specific section for software and/or firmware updates (go to www.urmet.com in the Products section "VIDEOSORVEGLIANZA AREA", type the reference product code in the search field and move to DOCUMENTATION AND RESOURCES).

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

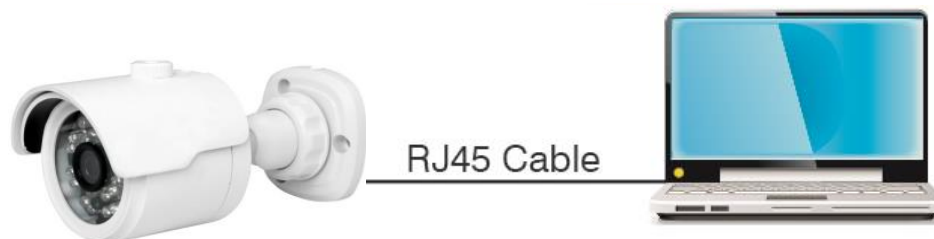
Internet Explorer 6.0 or later

Device Connection

The IP camera can be connected in two ways:

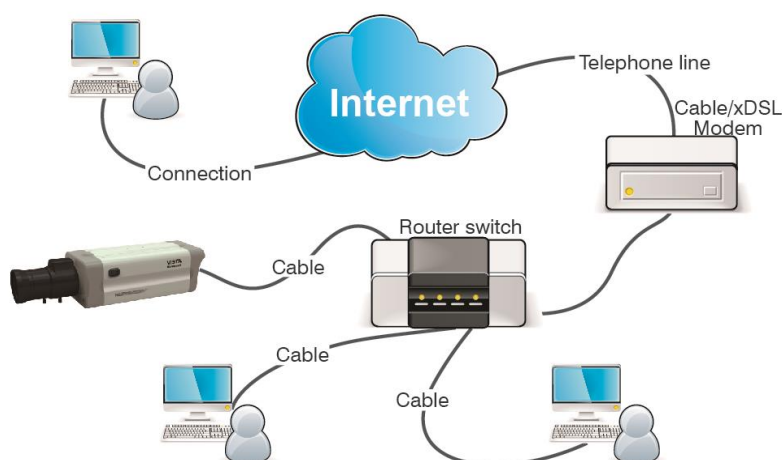
- Connection to a PC

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.

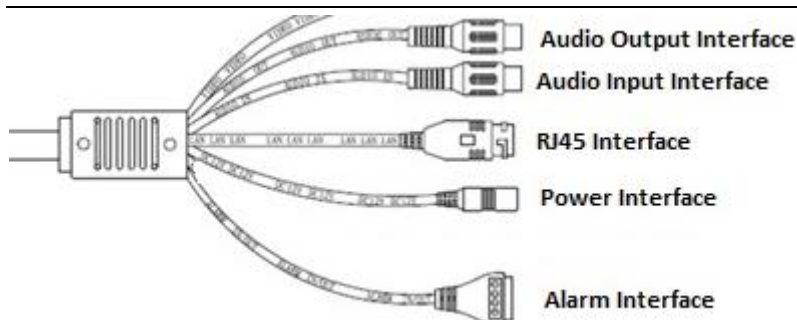


- Connection to a router/switch

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)

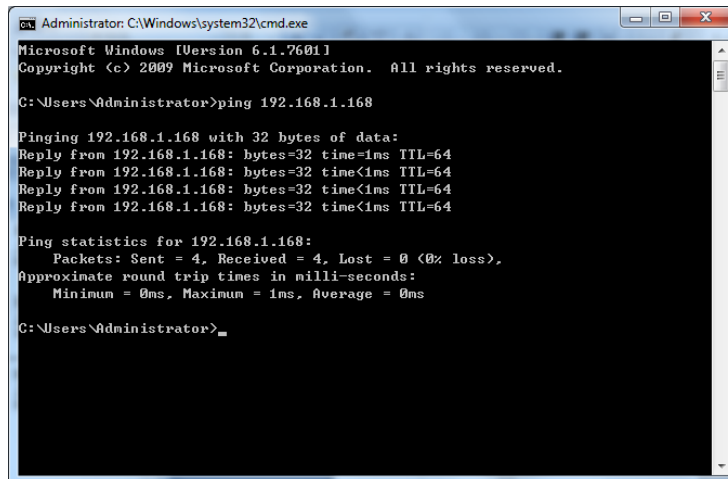


1. Audio Output Interface: RCA female connector (white), can connect with external devices, such as speakers.
2. Audio Input Interface: RCA female connector (red), can connect with input devices, such as a microphone.
3. RJ45 Interface (Network Interface): Connector for a RJ45 network cable.
4. Power 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

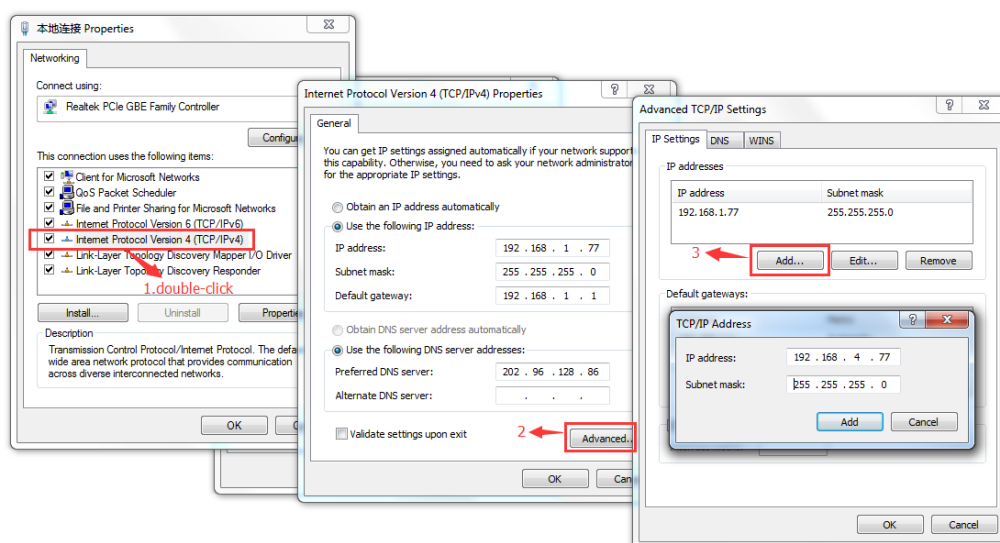
- The factory default IP address for the IP camera is 192.168.1.168 and the subnet mask is 255.255.255.0. Give your computer an IP address in the same network segment as the IP camera (e.g., 192.168.1.69) and the same subnet mask as that of the IP camera.
- Check whether the IP camera is connected and 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.



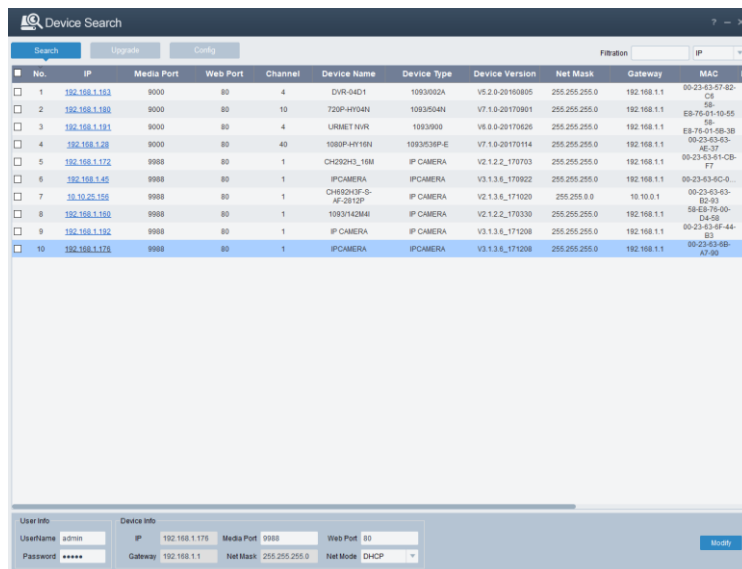
Note:

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.



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 (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.

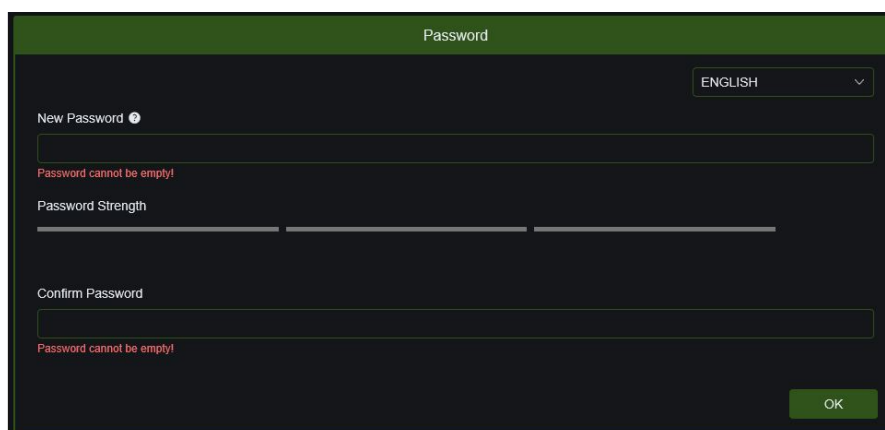
Select an option in the plug-in installation pop-up dialogue box to run the installation process.



5 LOGIN

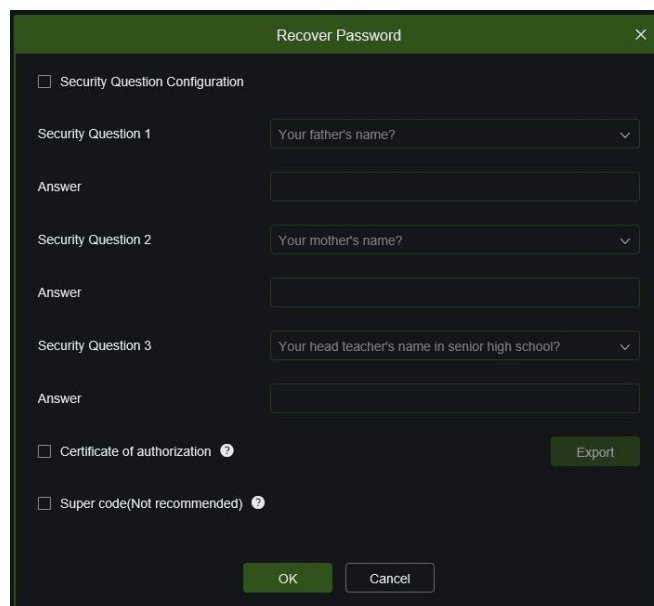
5.1 FIRST CAMERA LOGIN

Open a browser (all browsers for managing camera parameters from page [no video] or Edge in IE 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. (It is possible, at this stage, to choose the language)

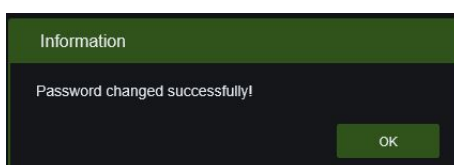
A window will then appear in which you can select and configure the password recovery modes in case the password is lost.

A screenshot of the 'Recover Password' window. It has a dark green header with the title 'Recover Password' and a close button. Below the header, there is a checkbox for 'Security Question Configuration'. If checked, it shows three security questions with dropdown menus for selection and text input fields for answers. The questions are: 'Your father's name?', 'Your mother's name?', and 'Your head teacher's name in senior high school?'. Below the questions, there are checkboxes for 'Certificate of authorization' and 'Super code(Not recommended)', each with a help icon. An 'Export' button is next to the 'Certificate of authorization' checkbox. At the bottom, there are 'OK' and 'Cancel' buttons.

- **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 Service 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:

A screenshot of an 'Information' window. It has a dark green header with the title 'Information'. Below the header, the text 'Password changed successfully!' is displayed. At the bottom right, there is an 'OK' button.

Click the **OK** button to confirm.

NOTE: 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 Edge in IE mode and enter the camera's IP address (<http://192.168.1.168>) to bring up the login window shown below:

Login Interface for Fish Eye IP camera.

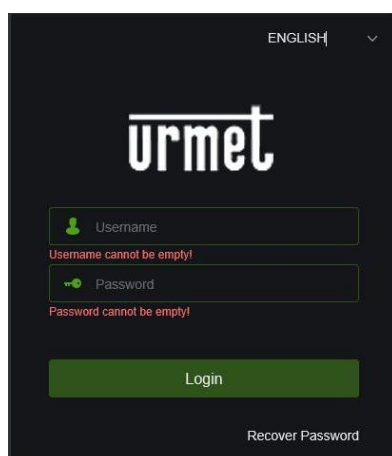
A screenshot of the login interface for a Fish Eye IP camera. It has a dark background with the 'urmet' logo in white. At the top right, there is a language selector set to 'ENGLISH'. Below the logo, there are two input fields: 'Username' and 'Password'. Below the 'Username' field, there is a red error message 'Username cannot be empty!'. Below the 'Password' field, there is a red error message 'Password cannot be empty!'. At the bottom, there is a large green 'Login' button. In the bottom right corner, there is a link that says 'Recover Password'.

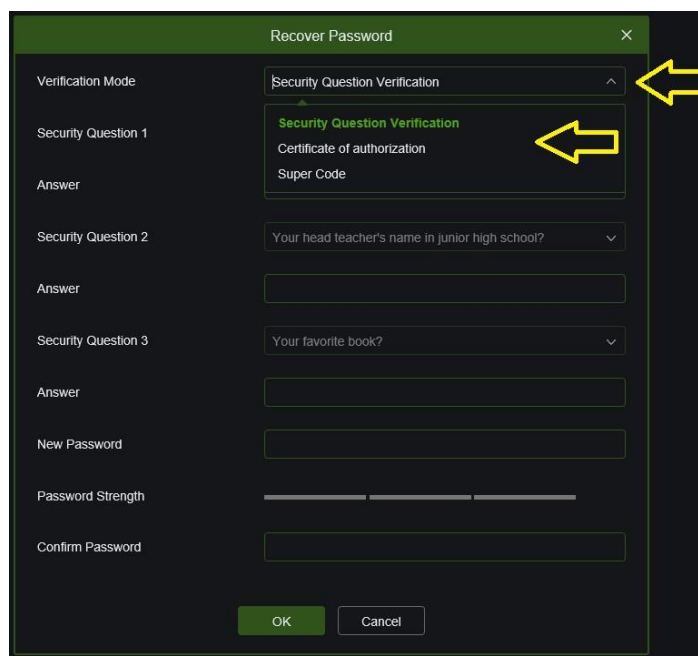
Figure 1

In the login window you can choose a language. 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.

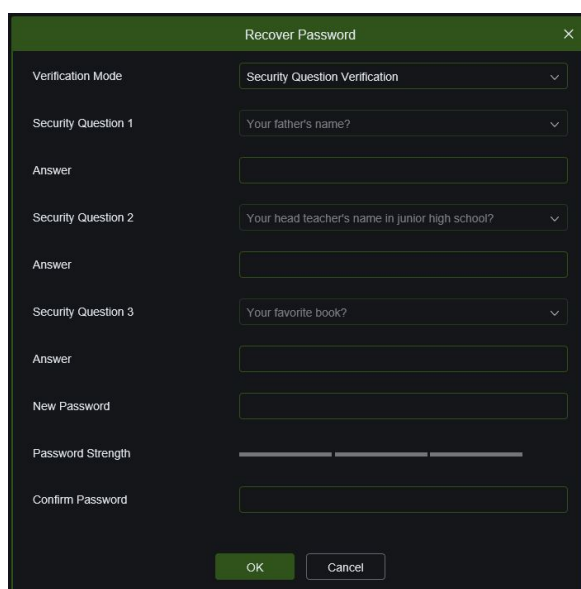
In Verification Mode, select one of the three previously set password recovery modes:



The screenshot shows a 'Recover Password' dialog box with a dark theme. At the top, the title is 'Recover Password'. Below it, there's a 'Verification Mode' dropdown menu currently set to 'Security Question Verification'. To the right of this dropdown, a list of three modes is displayed: 'Security Question Verification' (highlighted in green), 'Certificate of authorization', and 'Super Code'. Two yellow arrows point to the 'Security Question Verification' mode in the list and the 'Verification Mode' dropdown menu. Below the list, there are three security questions with their respective answers: 'Security Question 1' (Your father's name?), 'Security Question 2' (Your head teacher's name in junior high school?), and 'Security Question 3' (Your favorite book?). Each question has a corresponding text input field for the answer. Below these, there are fields for 'New Password', 'Password Strength' (a progress bar), and 'Confirm Password'. At the bottom, there are 'OK' and 'Cancel' buttons.

5.3.1 SECURITY QUESTION VERIFICATION

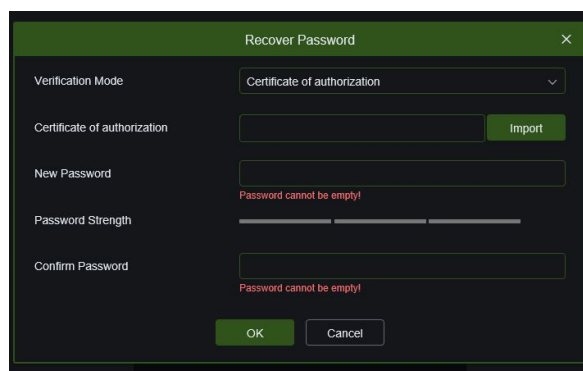
Give the correct answers to the previously selected questions, type the new password and confirm by clicking on the **OK** button.



The screenshot shows the same 'Recover Password' dialog box, but now the 'Security Question Verification' mode is selected. The 'Security Question 1' dropdown is set to 'Your father's name?', 'Security Question 2' is set to 'Your head teacher's name in junior high school?', and 'Security Question 3' is set to 'Your favorite book?'. Each question has a corresponding text input field for the answer. Below these, there are fields for 'New Password', 'Password Strength' (a progress bar), and 'Confirm Password'. At the bottom, there are 'OK' and 'Cancel' buttons. The 'OK' button is highlighted.

5.3.2 CERTIFICATE OF AUTHORISATION

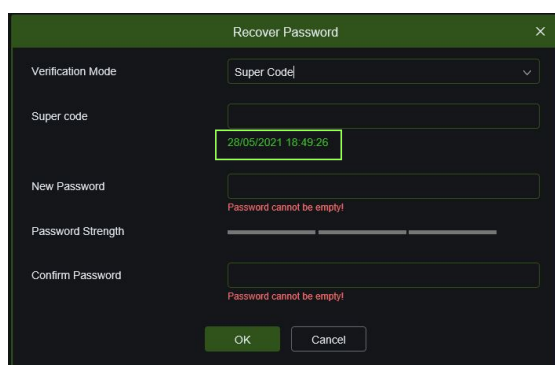
Import the previously saved certificate (.txt file) and type the new password, then confirm by clicking on the **OK** button.



The 'Recover Password' dialog box shows the 'Verification Mode' set to 'Certificate of authorization'. It includes an 'Import' button next to the 'Certificate of authorization' field. The 'New Password' and 'Confirm Password' fields are empty, with red error messages 'Password cannot be empty!' below them. A 'Password Strength' progress bar is also visible. 'OK' and 'Cancel' buttons are at the bottom.

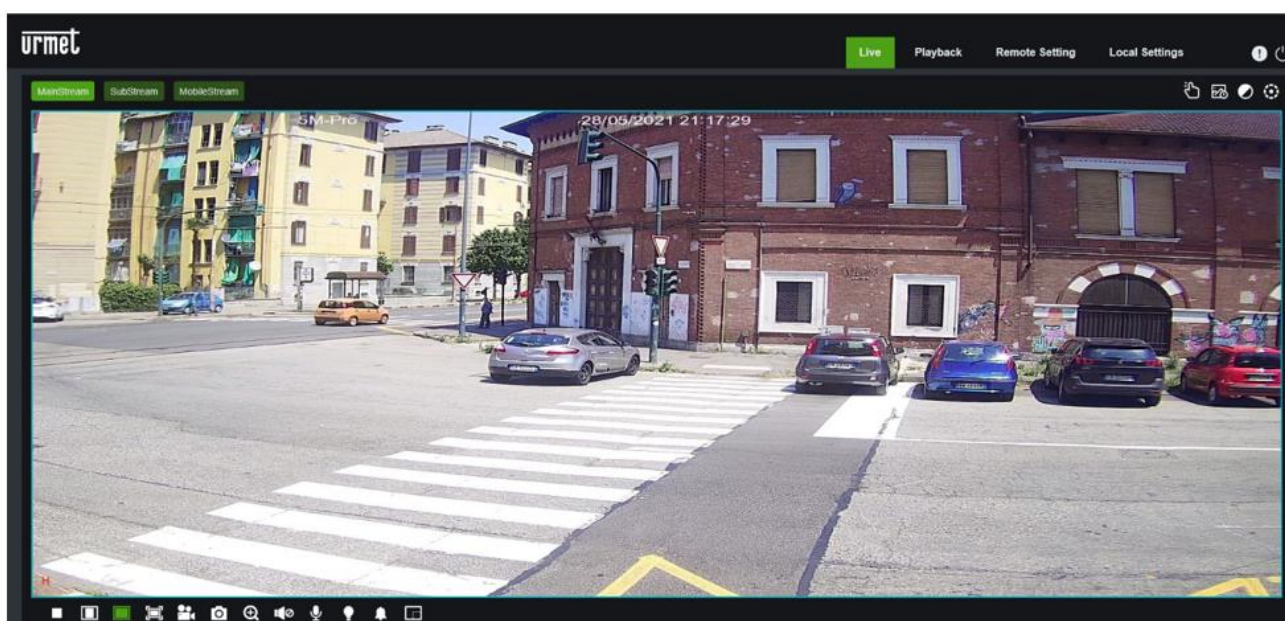
5.3.3 SUPER CODE

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).



The 'Recover Password' dialog box shows the 'Verification Mode' set to 'Super Code'. The 'Super code' field contains the text '28/05/2021 18:49:26', which is highlighted with a green box. The 'New Password' and 'Confirm Password' fields are empty, with red error messages 'Password cannot be empty!' below them. A 'Password Strength' progress bar is also visible. 'OK' and 'Cancel' buttons are at the bottom.

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.



: (Manual Alarm): Button to manually activate the camera's alarm output.

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.



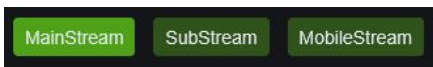
: Stop/Start Live video.



: 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, Light, Siren (from left to right).



: Dynamic bitstream switching for the preview frame.

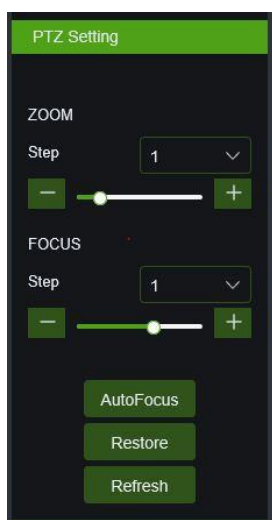


: this icon allows you to show the number of pixels (W, H) of the selected portion of the screen.

6.1 PTZ CONTROL



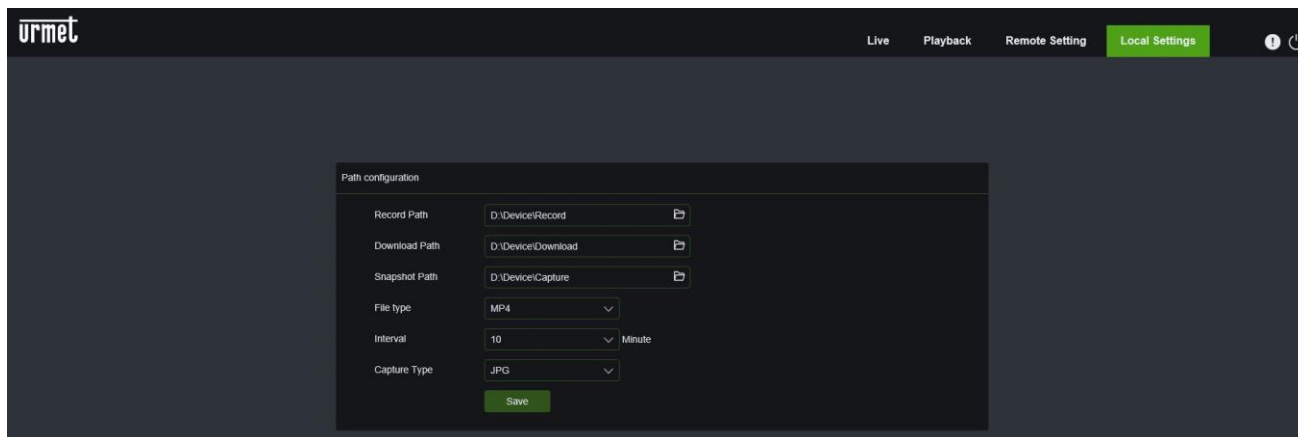
: (PTZ control) selecting this icon brings up the following window:



- **ZOOM** zooms in and out
- **FOCUS** increases or decreases FOCUS
- **Autofocus:** Adjusts focus automatically
- **Restore:** moves the optics to the maximum zoom point. If the image is not in focus at the end of the RESTORE operation, you can press the AUTOFOCUS button
- **Refresh:** updates the ZOOM and FOCUS values after requesting them from the camera

7 LOCAL SETTINGS

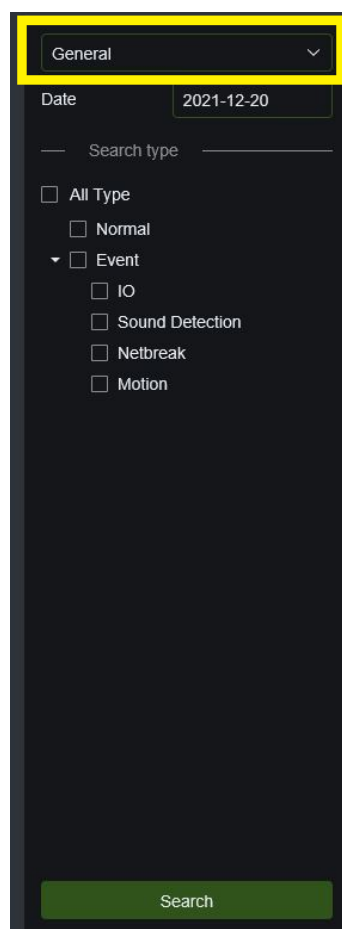
Select Local Settings to access the following dialogue window: here you can set the video storage location, paths for downloading remote files and storing snapshot images, the file type (MP4 by default, AVI or RF with H265 encryption), video recording duration and screen capture file type BMP, PNG or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

8.2 PLAYBACK CONTROLS

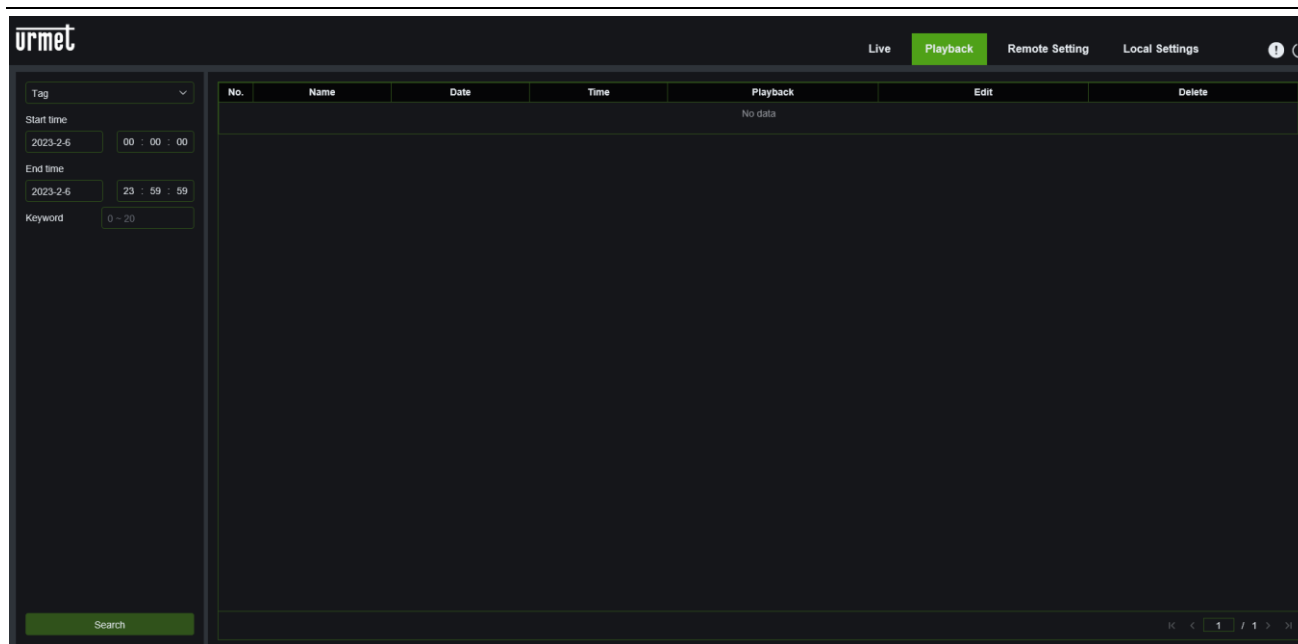


: from left to right, Play/Pause, Stop, Next frame, (select once to play a frame), Record, Capture, Download, Zoom, Play all, Stop all, Audio control.



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

8.3 TAG



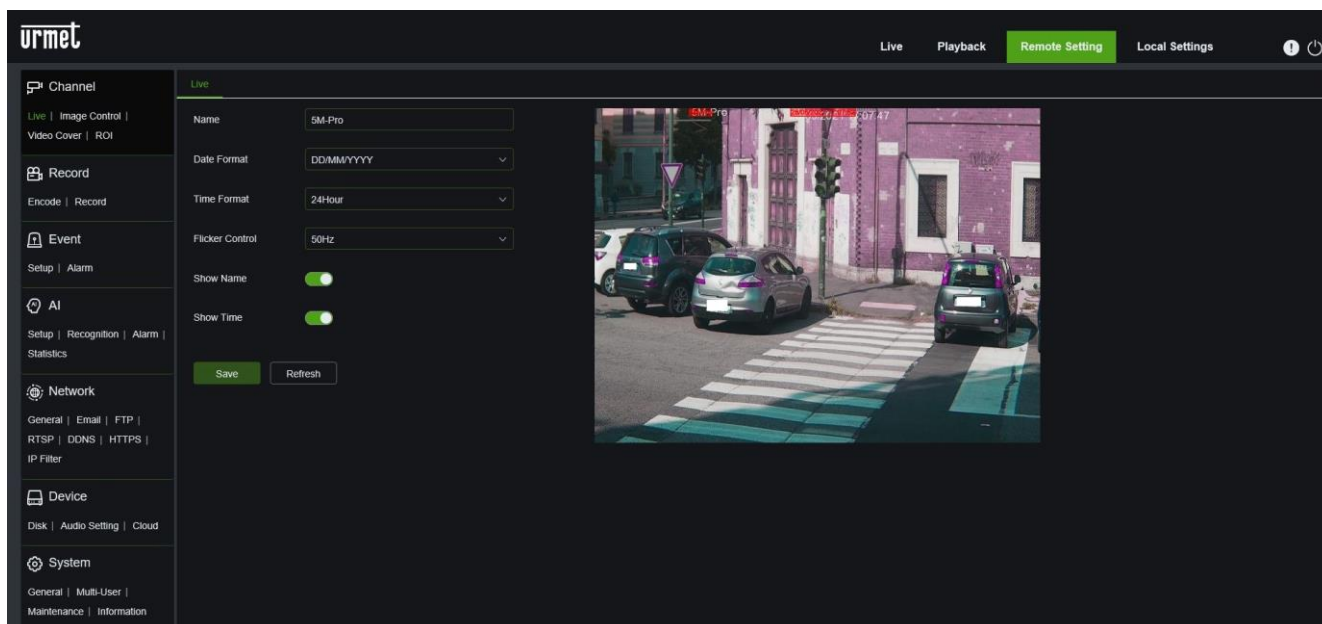
With Tag option, it will be possible to search on the basis of saved tags.

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.

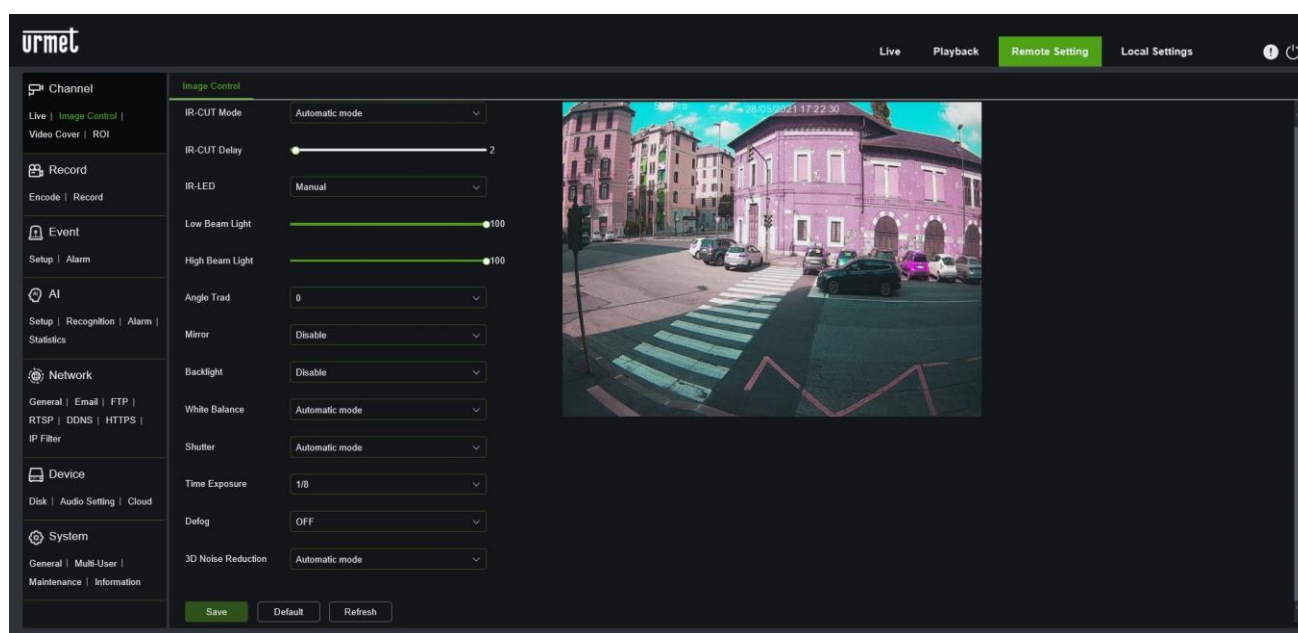
Show Time: the date and time are displayed.

OSD Self-adaptive: 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):

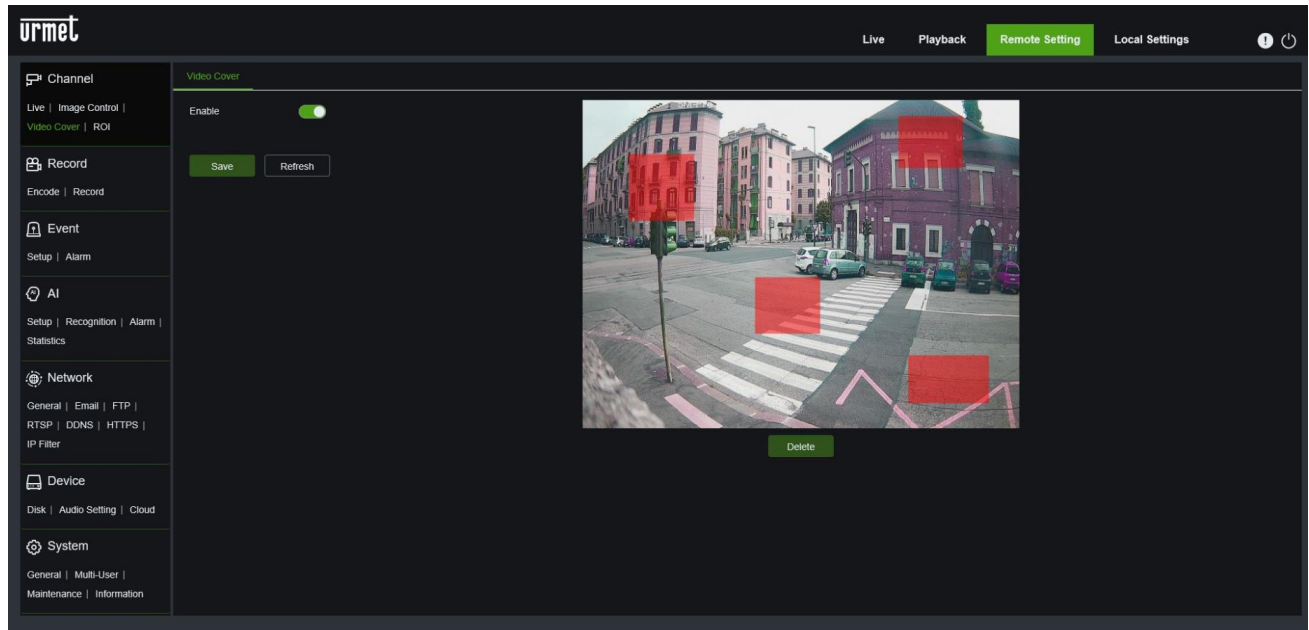


- **IR-CUT Mode:** Select the integrated IR-CUT filter mode to ensure that the camera functions properly in Day/Night: GPIO Automatic, Colour, Black and White and Schedule, where you have to indicate a time interval.
- **IR-CUT Delay:** Set the IR-Cut delay.
- **IR LED:** Manual mode (you can set the brightness of the LEDs) or SmartIR (automatic)
- **Low Beam Light** changes the infrared intensity of the low LEDs
- **High Beam Light** changes the infrared intensity of the high LEDs
- **Angle Trad** (Lens Flip): Set to enable inversion of the image.
- **Mirror:** Set to enable horizontal, vertical or horizontal and vertical image inversion.
- **Backlight:** Menu where you can set some backlight functions (WDR, HLC, Backlight) 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.
- **Defog Mode:** To set Defog mode: Disable/Auto/Manual mode, if Defog mode is set to Manual, adjust the level to improve video quality.
- **3D Noise Reduction:** To enable the function and choose automatic/manual mode

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

9.1.3 PRIVACY ZONE

Select Video Cover under Channel to open the following page:



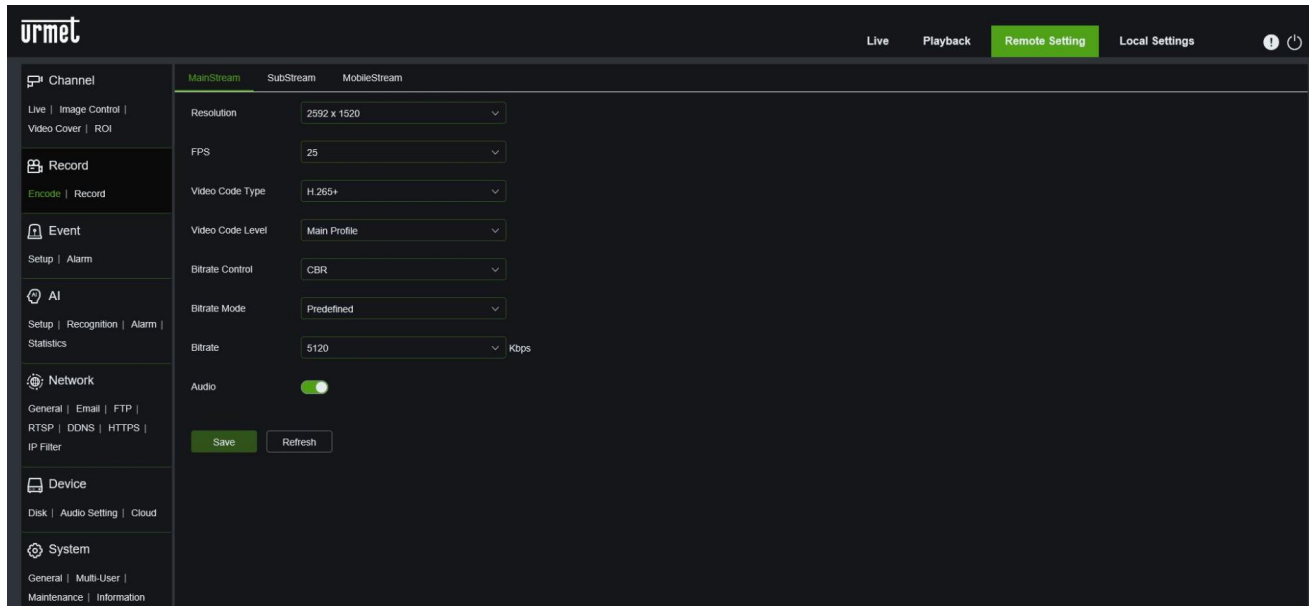
Enable Video Cover, and then use the left mouse button to trace rectangles around areas not to be displayed during recording, in screenshots and in Live viewing. Save when done to keep the settings.

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

9.2 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 2592x1520. The maximum resolution for the substream is 1280x720. The resolution for mobile devices is 640x480. (For 2MP models the maximum resolution selectable is 1920x1080).
- **FPS:** The maximum available FPS is 25 fps.

- **Video Code Type:** Sets the video encoding (H265/H264/H265+/H264+) for each bit stream.
- **Video Code Level:** Main Profile
- **Bitrate control:** Sets the constant or variable bitrate for the stream.
- **Bitrate Mode:** User-defined or Predefined.
- **Bitrate:** To set the Bitrate level

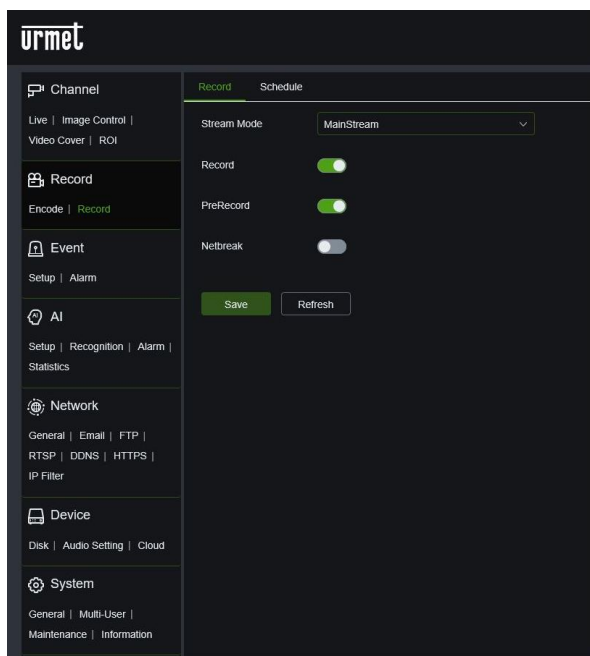
Note:

- 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.
- **Audio:** Enables audio for each bit stream.
- **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.

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

9.2.2 RECORD

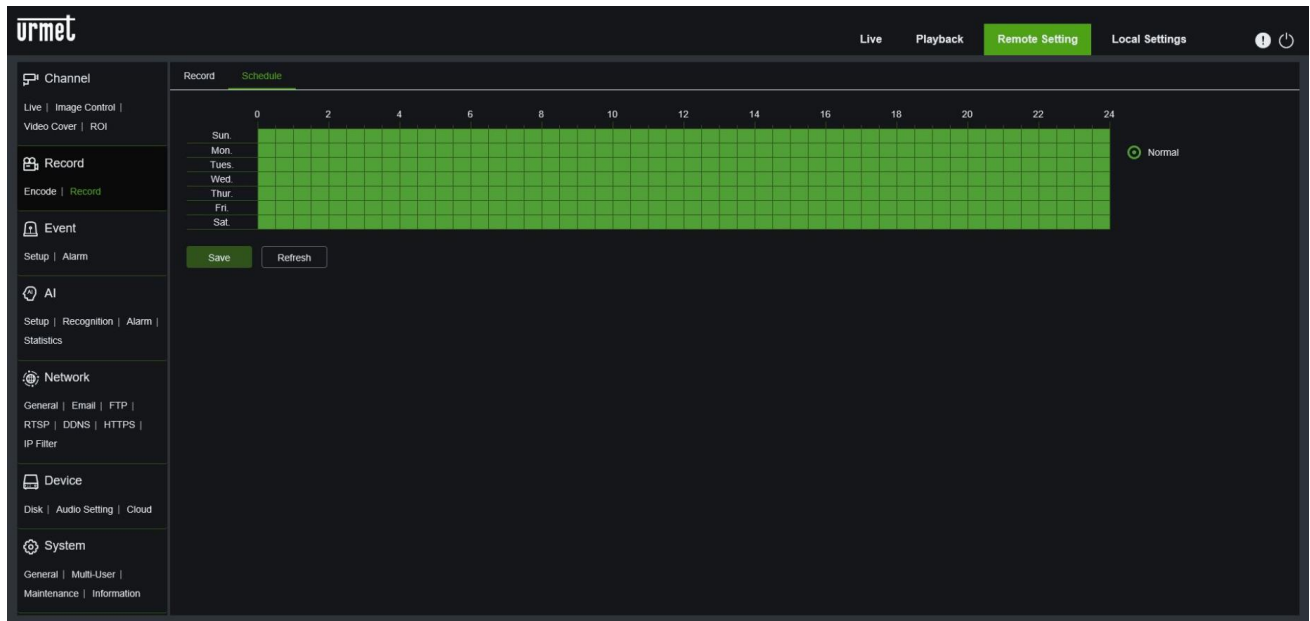
This function allows you to enable recording to an SD card (if present):



- *Stream mode:* recording mode (main stream or substream)
- *Record:* enable the recording
- *PreRecord:* enable the 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.

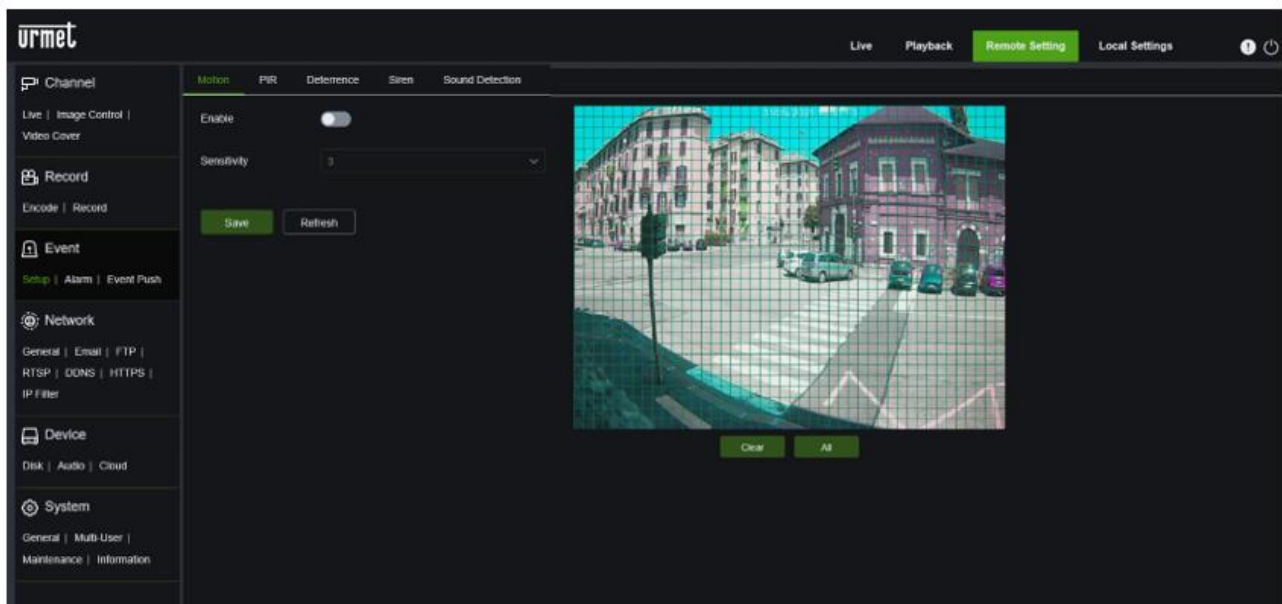


Example: a box in the table is equivalent to 30 minutes; green indicates continuous recording.

9.3 EVENT

9.3.1 SETUP

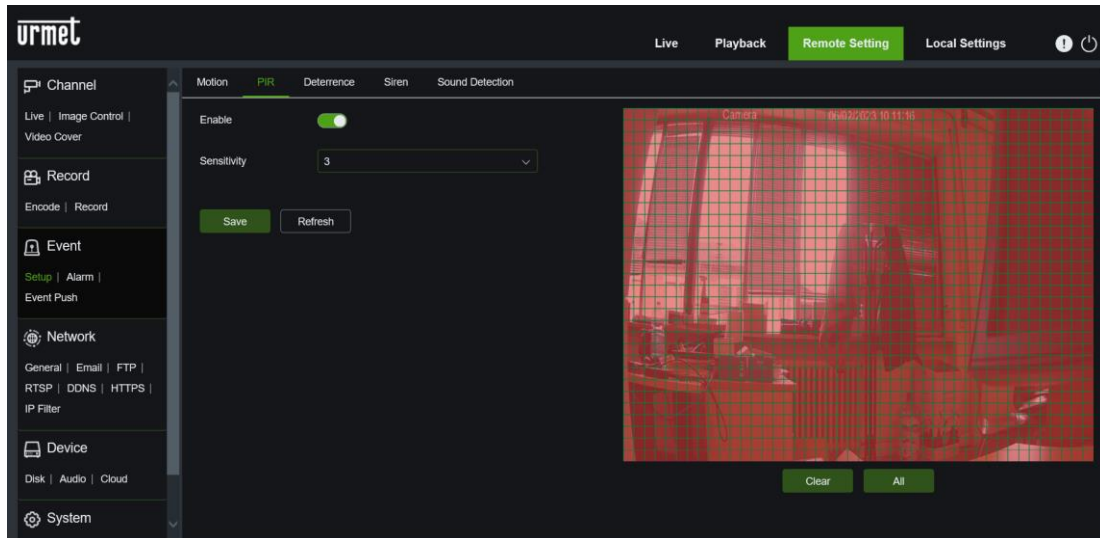
9.3.1.1 MOTION DETECTION



Motion detection setting procedure:

- Select Enable
- Hold down the left mouse button and drag over the image to colour (red) an area in which to define the motion detection area.
- **Clear/All:** Allows you to select or deselect the entire displayed area.
- 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).
- Press **Save** to save changes.

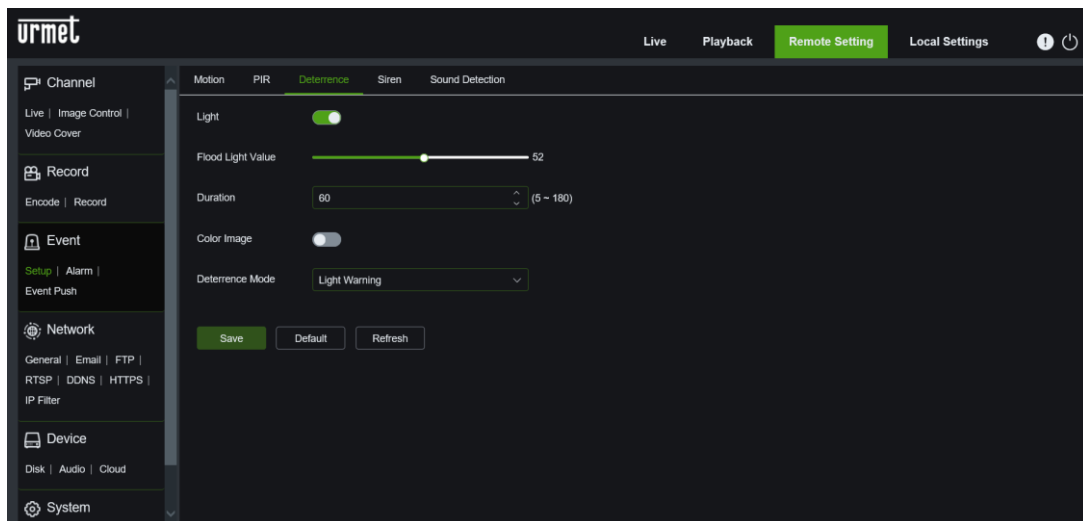
9.3.1.2 PIR (Only for some models)



PIR detection setting procedure:

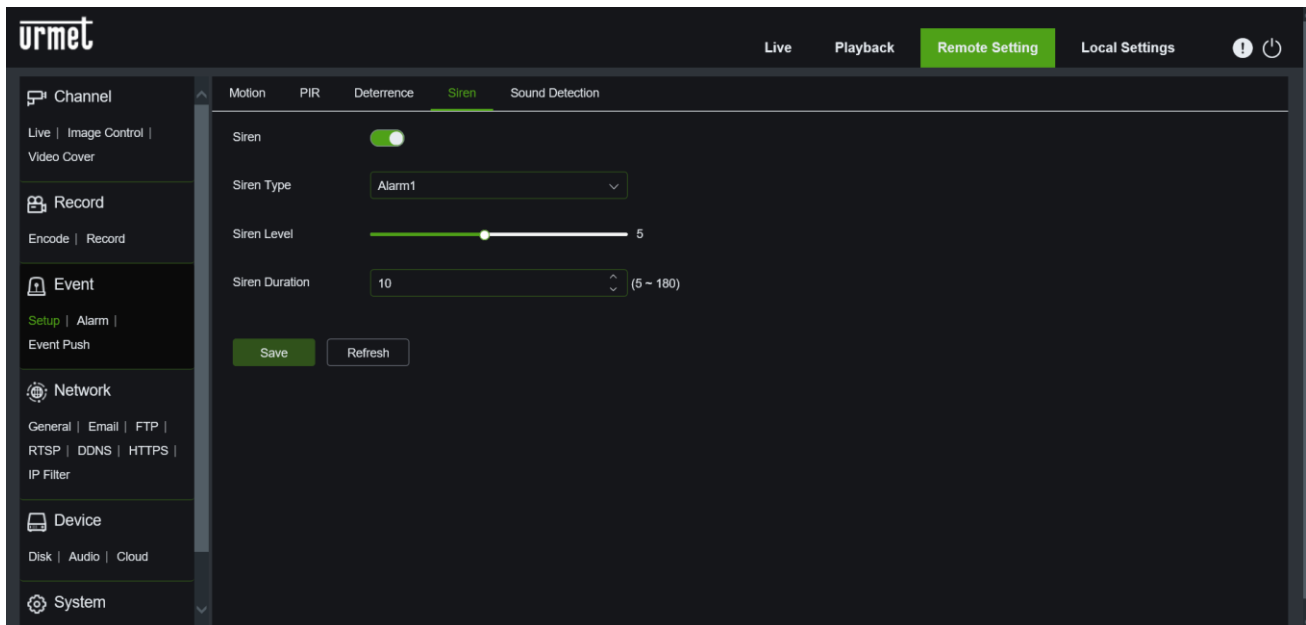
- Select **Enable**.
- Hold down the left mouse button and drag over the image to colour (red) an area in which to define the PIR detection area.
- **Clear/All**: Allows you to select or deselect the entire displayed area.
- Set the motion detection sensitivity (between 1 and 8; the higher the value, the greater the sensitivity).
- Press **Save** to save changes.

9.3.1.3 Deterrence (Only for some models)



- **Light**: Enables the white light to be switched on in the event of a deterrence event.
- **Flood Light Value**: You can set the intensity of the light on a scale from 1 to 100.
- **Duration**: The duration (in seconds) of the light in the event of an event can be set on a scale from 5 to 180.
- **Colour image**: If enabled (green) the camera immediately switches to colour when in alarm. 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 permanently on in case of deterrence. Light strobe (white lights are used flashing in case of deterrence).
- Press **Save** to save the changes.

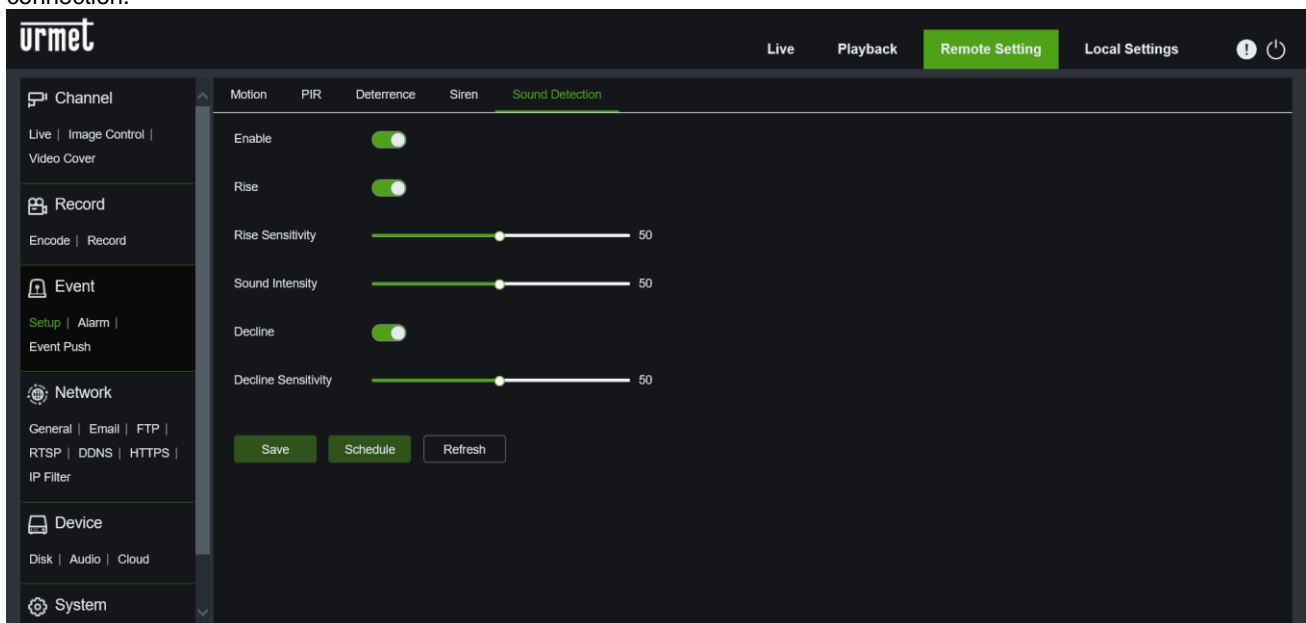
9.3.1.4 Siren (Only for some models)



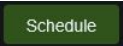
- **Siren:** enables the siren in the event of an event detected.
- **Siren Type:** Alarm1 type.
- **Siren Level:** You can set the intensity of the siren sound on a scale from 1 to 10.
- **Siren Duration:** You can set the duration (in seconds) of the siren sound in case of an event on a scale from 5 to 180.
- Press **Save** to save changes.

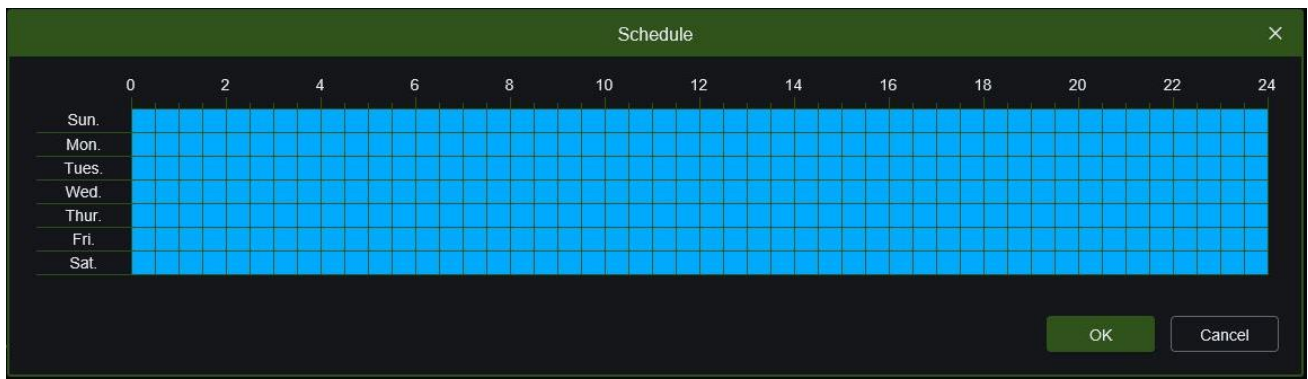
9.3.1.5 SOUND DETECTION

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.

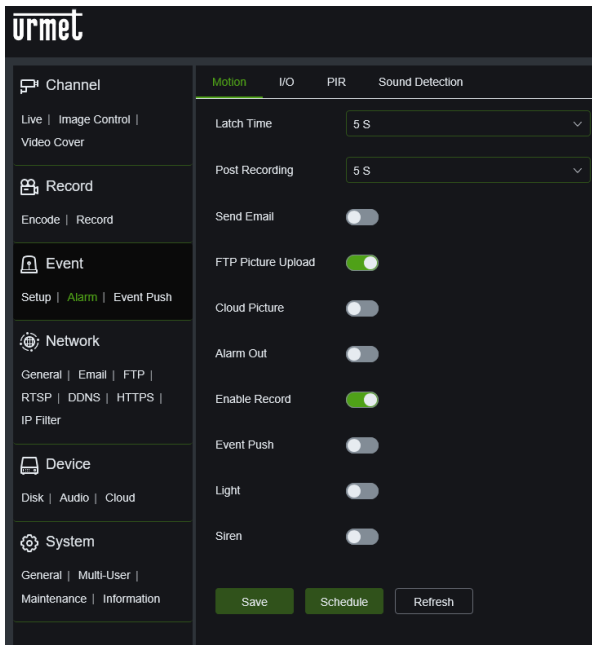


IMPORTANT NOTE:

- 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

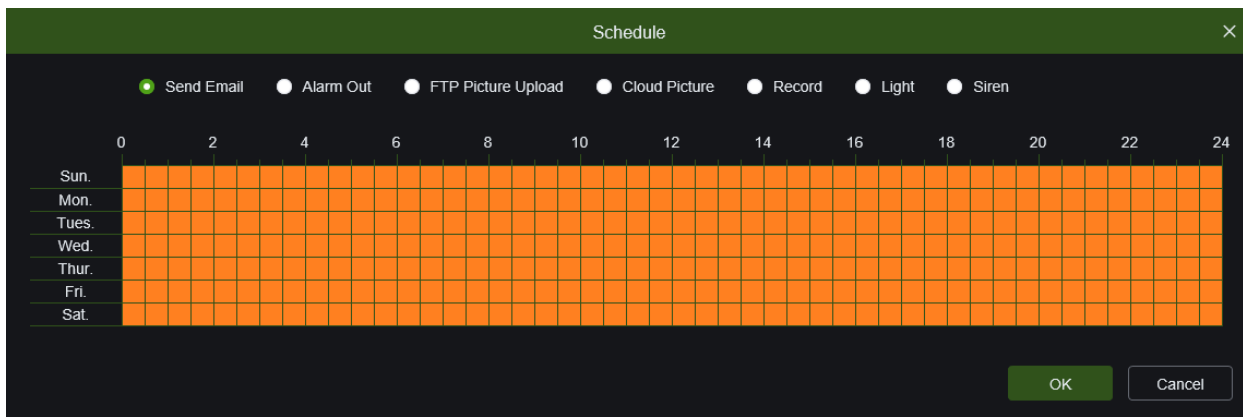


- **Latch Time:** To set the alarm output time (5S, 10S, 20S, 30S). [for models where featured]
- **Post Recording:** When Enable Record is enabled, the recording delay can then be set (5S, 10S, 20S, 30S).
- **Send Mail:** a function used with SMTP to enable the sending of e-mail.
- **FTP Picture Upload:**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

- **Light: [where available]:** enables or disables the activation of the white light in the event of a motion detection alarm.
- **Siren: [where available]:** enables or disables the activation of the siren in the event of a motion detection alarm.

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

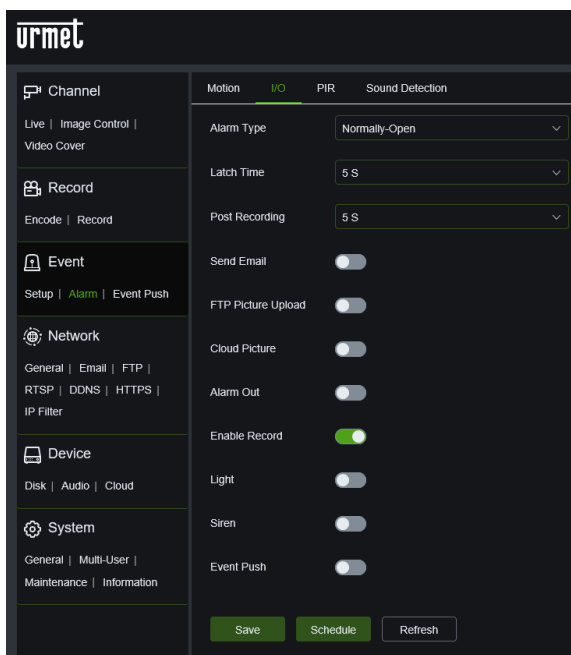
Click on the  buttons to schedule the output actions for a Motion event:



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

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

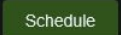
9.3.2.2 I/O (INPUT/OUTPUT) [where featured]

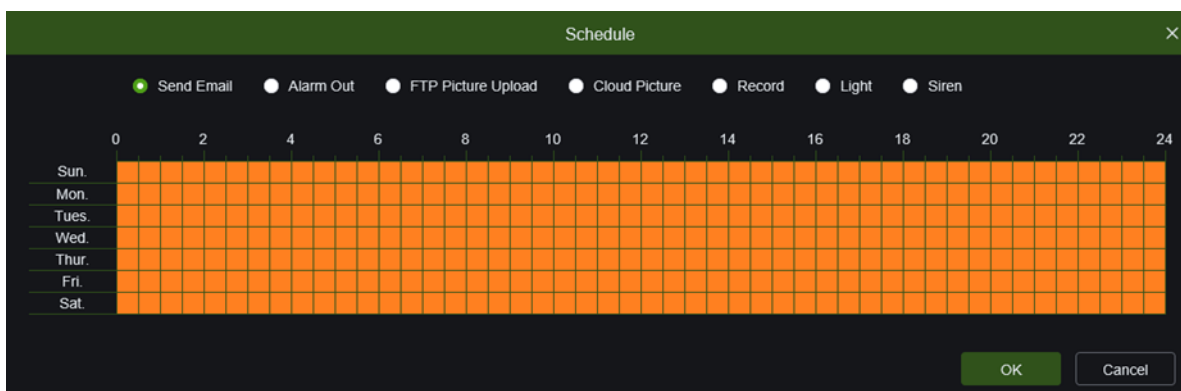


- **Alarm Type:** Available values: OFF, Normally-Open, Normally-Closed.
- **Latch Time:** Set the alarm output time (5S, 10S, 20S or 30S). [for models where featured]
- **Post Recording:** When Enable Record is selected, the recording delay can then be set (5S, 10S, 20S or 30S).
- **Send Mail:** a function 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:** enables or disables the recording for

I/O alarm.

- **Event Push:** enables or disables the sending of the push notification on the app for I/O alarm.
- **Light: [where available]:** enables or disables the activation of the white light in the event of an I/O alarm.
- **Siren: [where available]:** enables or disables the activation of the siren in the event of an I/O alarm.

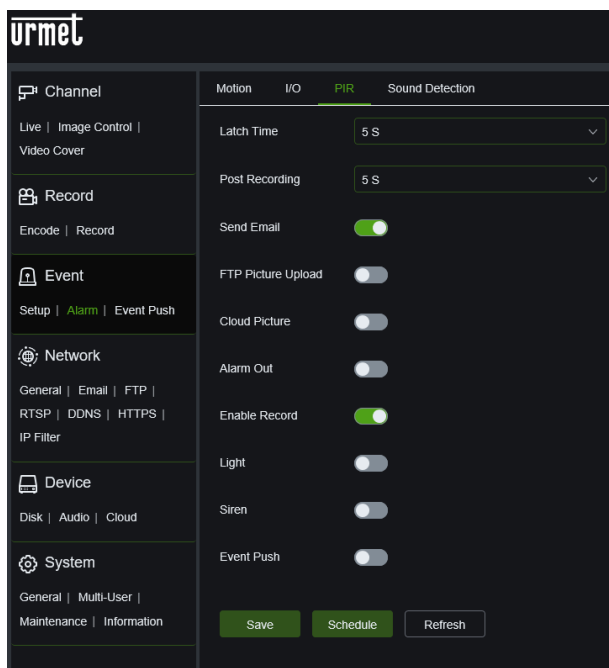
Click on the  button to schedule the output actions for an Alarm Input (if included):



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

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

9.3.2.3 PIR (Only for some models)

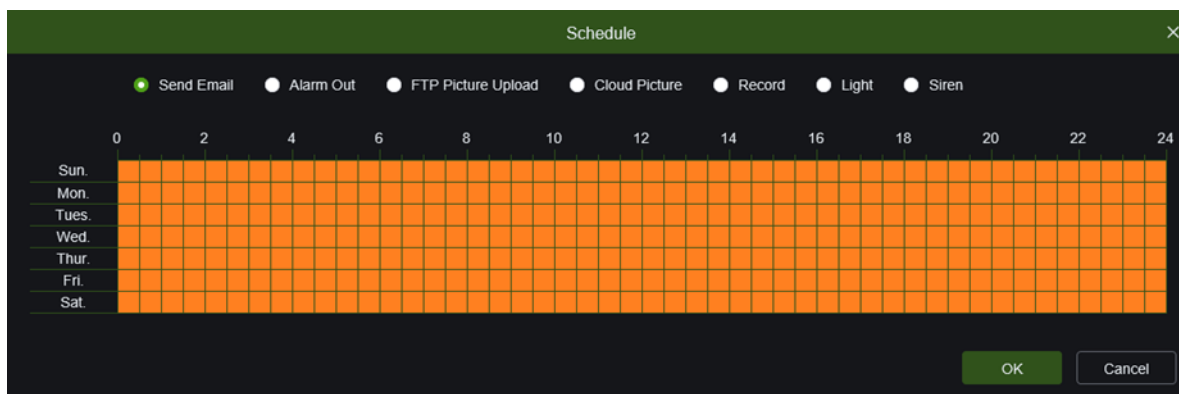


- **Latch Time:** Set the alarm output time (5S,10S, 20S or 30S). [for models where featured]
- **Post Recording:** When Enable Record is selected, the recording delay can then be set (5S, 10S, 20S or 30S).
- **Send Mail:** a function used with SMTP to enable the sending of e-mail.
- **FTP Picture Upload:** 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:** enables or disables the recording for PIR alarm.
- **Event Push:** enables or disables the sending of the

push notification on the app for PIR alarm.

- **Light: [where available]:** enables or disables the activation of the white light in the event of PIR alarm.
- **Siren: [where available]:** enables or disables the activation of the siren in the event of PIR alarm.

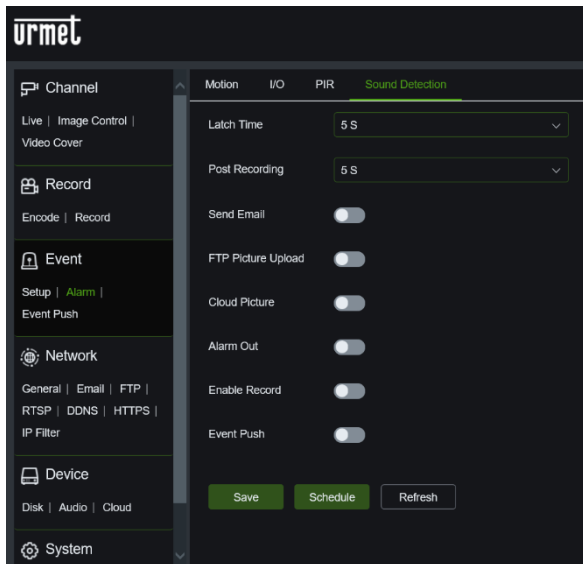
Click on the **Schedule** button to schedule the output actions for an Alarm Input (if included):



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

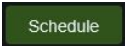
Press **Save** to save the desired setting.

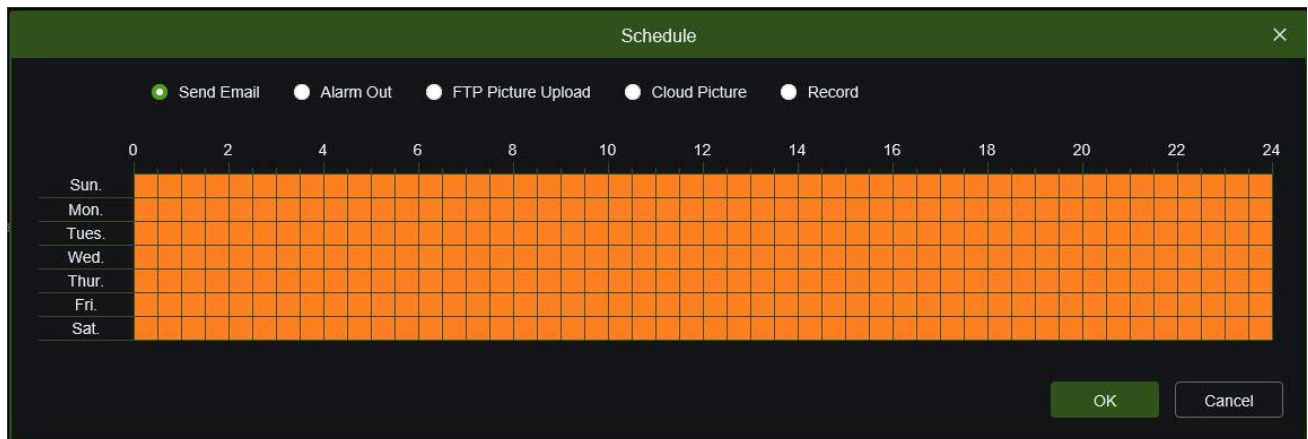
9.3.2.4 Sound detection



- **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
- **Cloud Picture:** enables or disables sending images to a Cloud Dropbox
- **Alarm Out:** enables or disables the alarm output.
- **Enable Record:** enables or disables the recording for sound detection alarm.

- **Event Push:** enables or disables the sending of the push notification on the app for sound detection alarm.

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

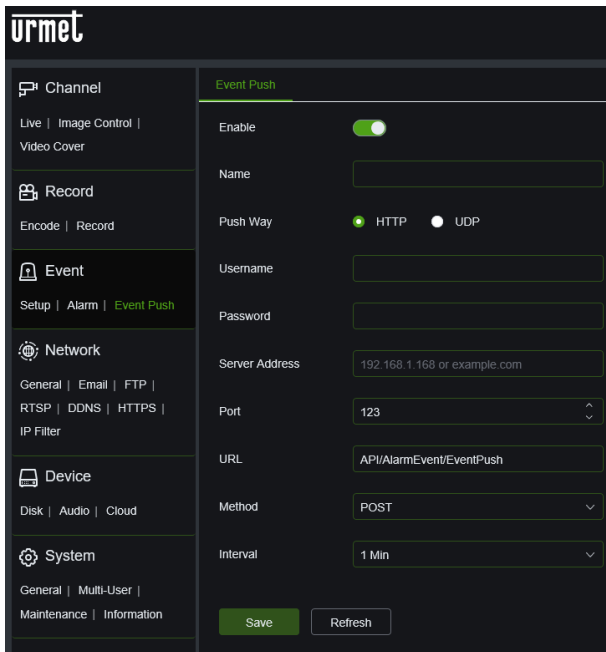


Send an email, switch the alarm output (if included), send an image to an FTP Server, send an image to the cloud (Dropbox) or enable recording on an SD card.

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 notification transmission method 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.

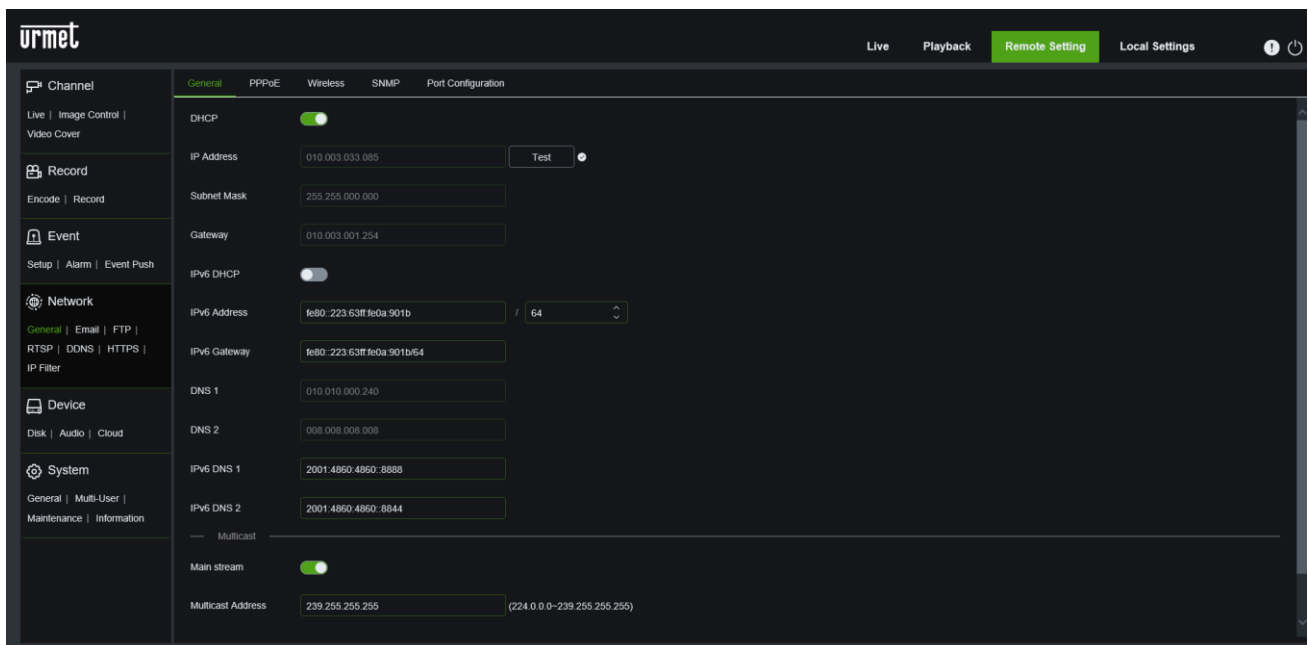
Press **Save** to save the desired setting.

9.4 NETWORK

9.4.1 GENERAL

9.4.1.1 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:

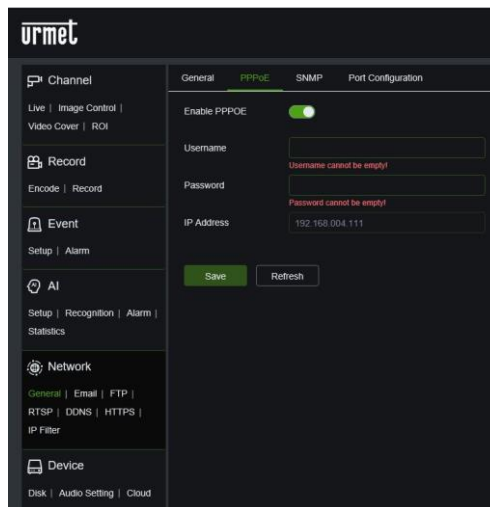
- **IP Address:** the IP address identifies the camera on the network. It consists of four groups of digits between 0 and 255, separated by full stops, e.g., "192.168.001.168".
- **Test:** the Test button allows a check to be made that the device is correctly addressed on the network.
- **Subnet Mask:** 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 automatic IPv6 addressing.
- **IPv6 Address:** enables manual entry of IPv6 address.
- **IPv6 Gateway:** enables manual entry of the IPv6 gateway.
- **DNS1/DNS2:** DNS1 is the primary DNS server and DNS2 is the backup DNS server. As a rule, simply 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:** Multicast address range.
- **Video Encryption Transmission:** if enabled, allows encrypted transmission of information.

Press **Save** to save the desired setting

9.4.1.2 PPPoE

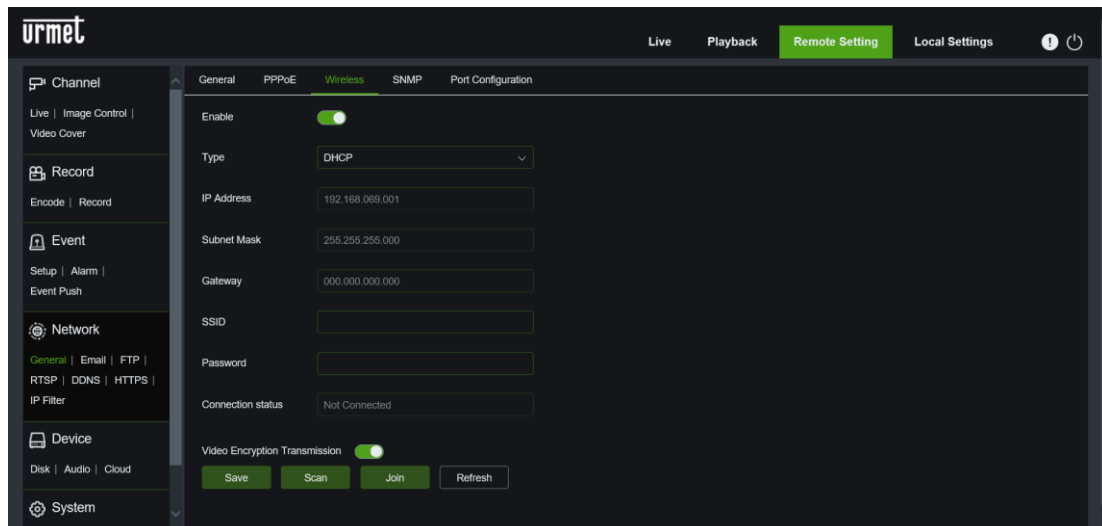
This is an advanced protocol that allows to connect to the network more directly, via a DSL modem. Enable the "Enable PPPOE" switch, then enter the user name and password for the PPPoE.



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

9.4.1.3 Wireless (Only available on some models)

This section is only present on wireless cameras and allows the device to be configured to the desired Wi-Fi network (e.g. home router).



- **Enable:** Enables the device's wireless network configuration.
- **Type:** You can choose between automatic (DHCP) and manual (Static) addressing of the device.
- **IP Address:** Displays the IP address currently assigned to the camera. If addressing is STATIC, you can edit and then save the address you wish to assign to the camera.
- **Subnet Mask:** This is a network parameter that defines a range of IP addresses that can be used on a network. Assuming that the IP address represents the street where you live, the subnet mask is the neighbourhood. The

subnetwork address also consists of four groups of digits, separated by dots. For example, '255.255.000.000'. It is possible to enter the subnet mask in the case of STATE IP addressing.

- **Gateway:** This address allows the camera to access the Internet. The format of the Gateway address is identical to that of the IP address. For example, "192.168.001.001".
- **SSID (Service Set Identifier):** this is the name of the Wi-Fi network that users identify.

Scan

positioned at the bottom, it is possible to scan the wireless networks detected by the camera.

List		
SSID	Level	Securi
TVCClabfast	<div><div></div><div></div><div></div><div></div><div></div></div>	[WPA-PSK-CCMP+TKIP][WPA2 SS]
UFFTVCCext	<div><div></div><div></div><div></div><div></div><div></div></div>	[WPA-PSK-CCMP+TKIP][WPA2 SS]
RS08B0D9	<div><div></div><div></div><div></div><div></div><div></div></div>	[WPA-PSK-CCMP][WPA2 SS]
MobileTVCC	<div><div></div><div></div><div></div><div></div><div></div></div>	[WPA-PSK-CCMP+TKIP][WPA2 SS]
NVR083a2f1aeecd	<div><div></div><div></div><div></div><div></div><div></div></div>	[WPA2-PSK-CCMP][WPA2 SS]
TP-LINK_CSAT2	<div><div></div><div></div><div></div><div></div><div></div></div>	[WPA-PSK-CCMP][WPA2-F
UDOMUS	<div><div></div><div></div><div></div><div></div><div></div></div>	[WPA-PSK-CCMP][WPA2-F

Select the wireless network (e.g. the Wi-Fi network of your home router) to which you want to connect the camera and press **OK**. In the **Password** field enter the password of the selected wireless network. Finally, press on **Join** to establish the connection between the two wireless devices.

In **Connection status** (Connection Status) you can see if the connection between the two wireless devices will be established (**Connected**) or failed (**NOT connected**).

- **Video Encryption Transmission:** If enabled, allows encrypted transmission of information.

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

9.4.1.4 SNMP

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

9.4.1.5 Port Configuration

Server	Internal Port	External Port	Protocol	UPNP Status	Port forwarding	UPNP
HTTP Port	80	80	TCP	Inactive	Auto	<input type="checkbox"/>
Client Port	9000	9000	TCP	Inactive	Auto	<input type="checkbox"/>
HTTPS Port	443	443	TCP	Inactive	Auto	<input type="checkbox"/>
RTSP Port	554	554	TCP	Inactive	Auto	<input type="checkbox"/>

Multicast Port: 10000 (1024-65535)

P2P Switch: ☒

Save Refresh

- **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).

9.4.2 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 Configuration

Email: ☒

Encryption: OFF

SMTP Port: 25 (1 ~ 65535)

SMTP Server:

Username:

Password:

Sender:

Receiver 1:

Receiver 2:

Receiver 3:

Interval: 3Min

Save Test Refresh

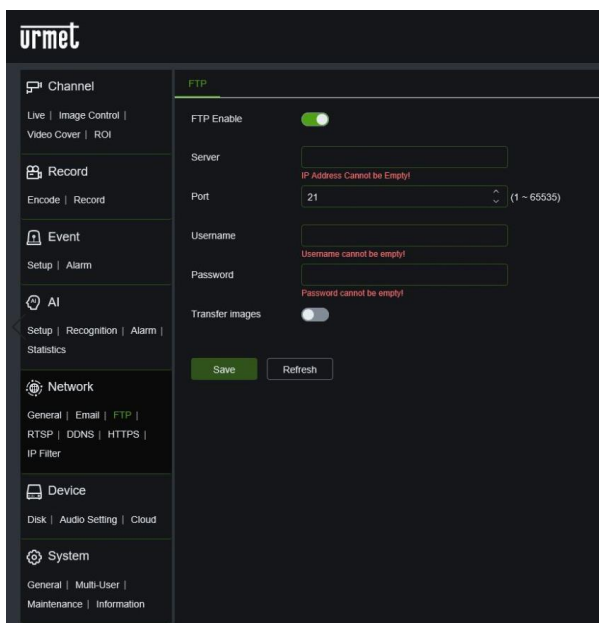
- **Email:** allows you to enable or disable the configuration of the email parameters.
- **Encryption:** allows you to specify whether or not communication with the mail server will be encrypted; the use of a secure transfer protocol using data encryption allows you to encrypt the information communicated (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 25¹.
- **SMTP server:** this indicates the address of the server used.

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

- **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.

9.4.3 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.

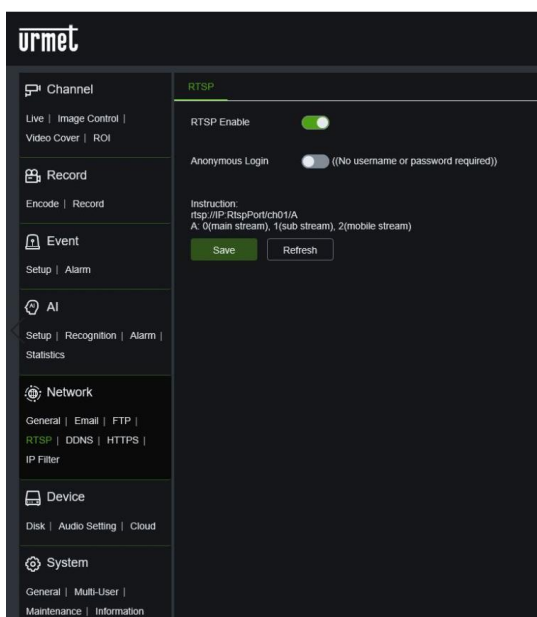


- **FTP Enable:** select the desired option to enable or disable operation.
- **IP Server:** enter the address or name of the FTP server.
- **Port:** FTP service port. Default value: 21.
- **Username:** the username to access the FTP server
- **Password:** the password to access the FTP server.
- **Transfer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

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

9.4.4 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:

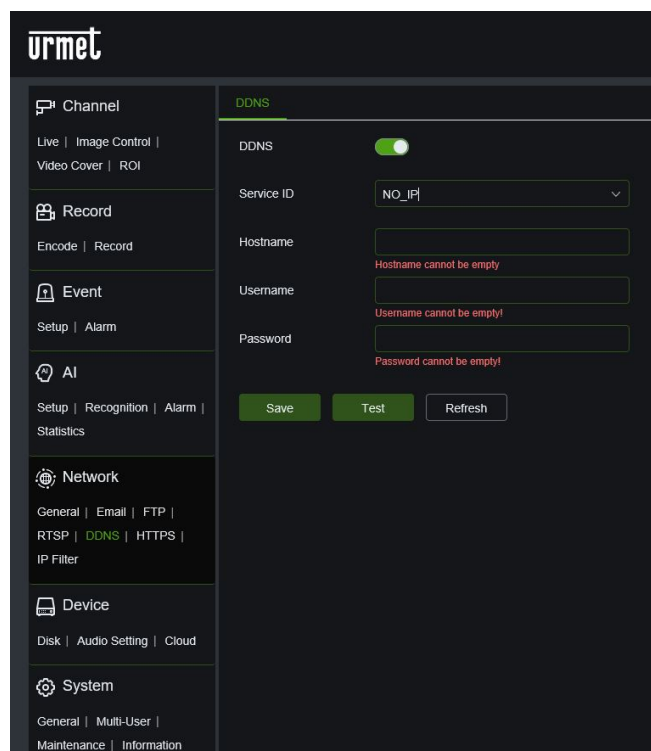
rtsp://IP:RtspPort/ch01/A

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

9.4.5 DDNS CONFIGURATION

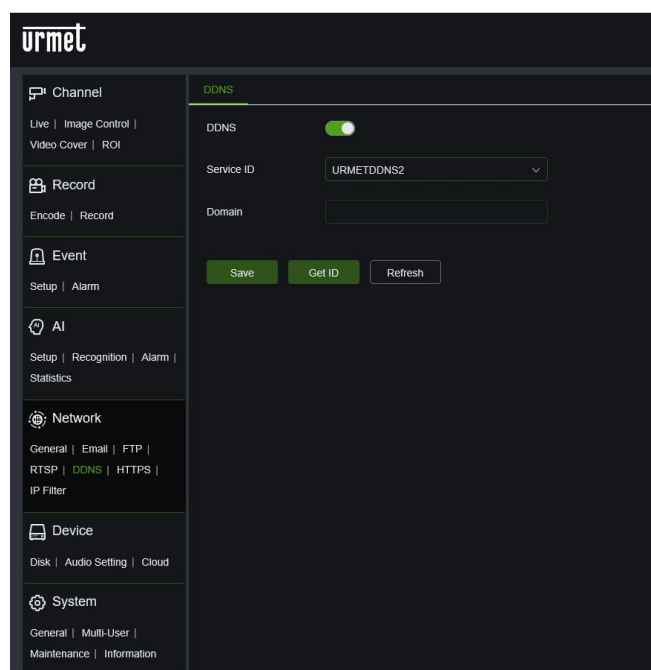
Select DDNS in the Network menu to open the following page:

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

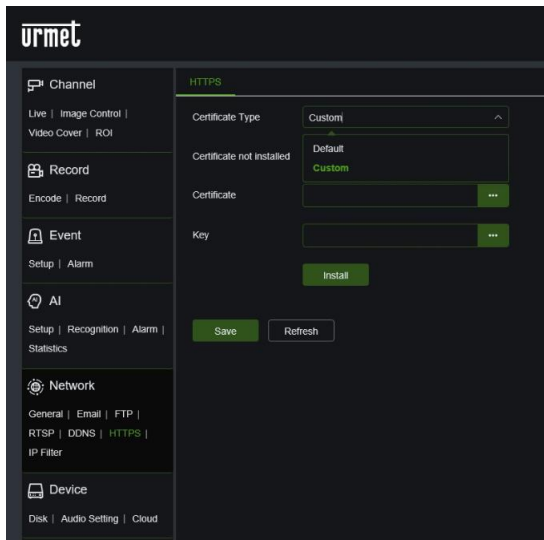
Test : Pressing the Test button verifies the correct connection to the DDNS Server set up.



- If you are using one of the Urmnet 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.

9.4.6 HTTPS

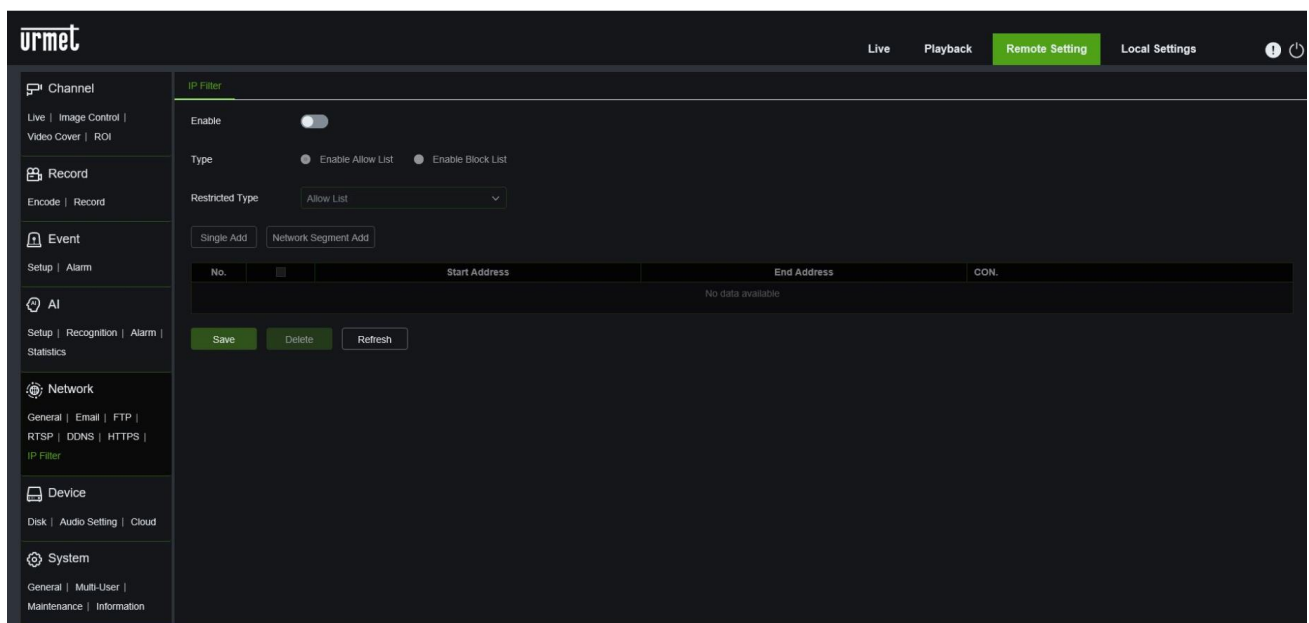
In this menu you can set the security encryption protocol.



- **Certificate Type:** Default or Custom

9.4.7 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:

IP Filter

Enable ☒

Type ☒ Enable Allow List ☐ Enable Block List

Restricted Type Allow List

Single Add Network Segment Add

No.	<input type="checkbox"/>	Start Address	End Address	OK
1	<input type="checkbox"/>	192.168.1.200	192.168.1.205	Edit Delete

Save Delete Refresh

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.

9.5 DEVICE

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

9.5.1 DISK

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

urmet

Live Playback **Remote Setting** Local Settings

Channel
Live | Image Control | Video Cover | ROI

Record
Encode | Record

Event
Setup | Alarm

AI
Setup | Recognition | Alarm | Statistics

Network
General | Email | FTP | RTSP | DDNS | HTTPS | IP Filter

Device
Disk | Audio Setting | Cloud

System
General | Multi-User | Maintenance | Information

Disk

<input type="checkbox"/>	NO.	Type	Status	Free / Total (G)	Free / Total (T)
<input type="checkbox"/>	1SD	ReadWrite	OK	4G/7G	1Hour/3Hour

Overwrite Auto

Save Format Hard Disk Refresh

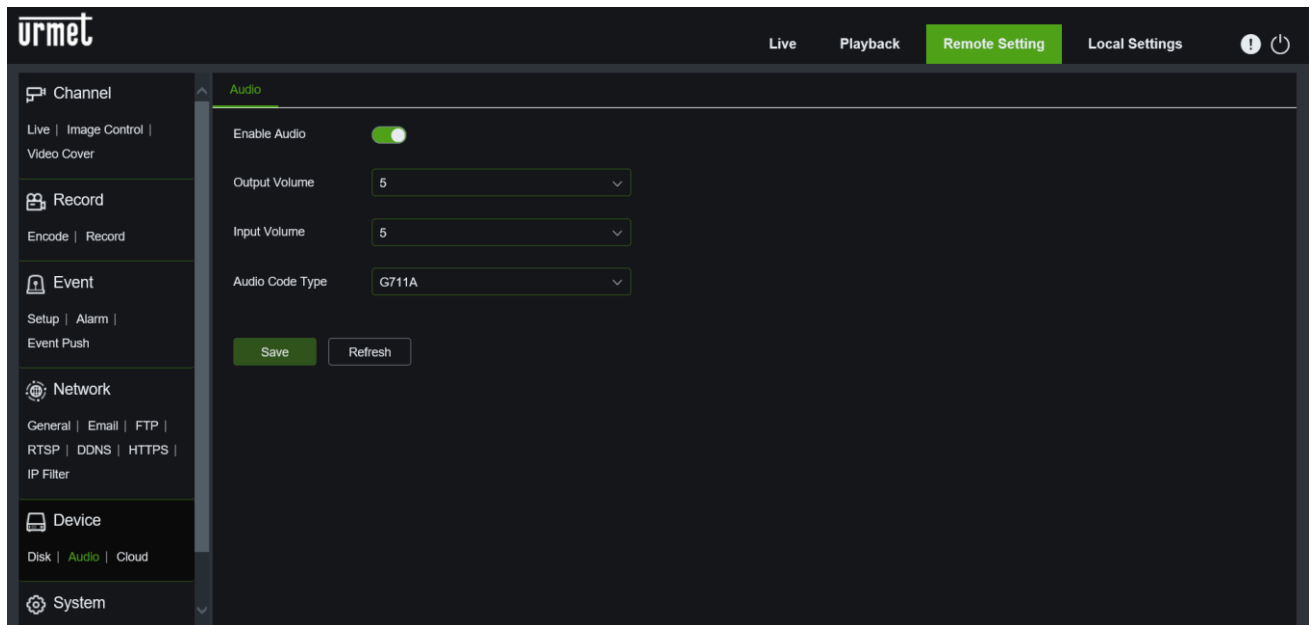
With the device disconnected, insert the SD card in the appropriate slot; when the device is powered, it will automatically detect the total capacity and provide information on the remaining recording time.

- 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.

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

9.5.2 AUDIO

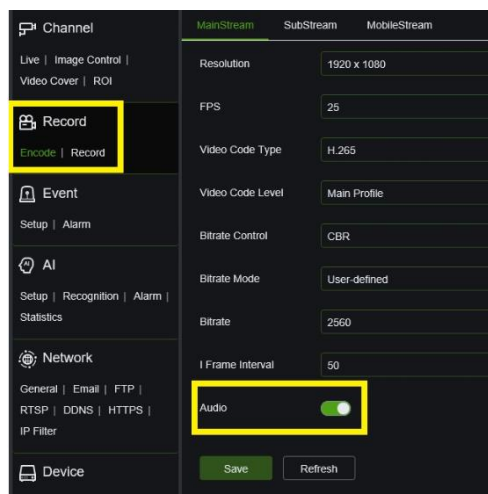
Click on Audio in the Device menu to open the following page:



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.

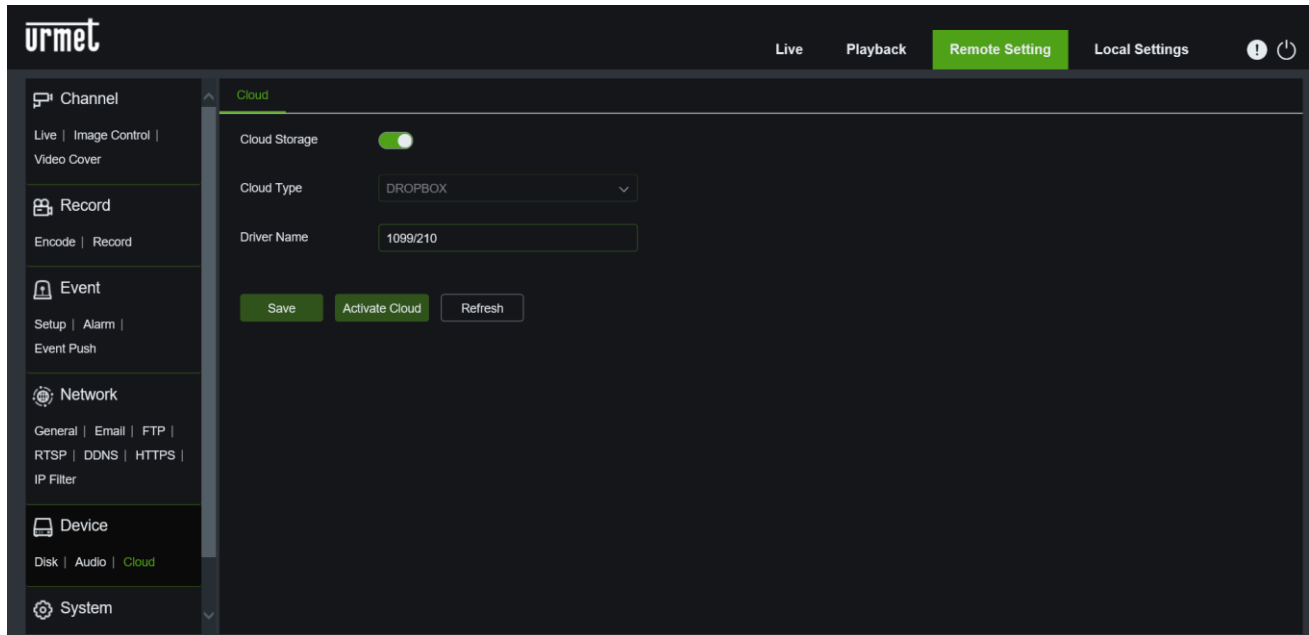
Note: In order to use the audio function, the audio option in **Record/Encode** must be enabled, for each desired type of Stream.



9.5.3 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 camera. 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.
- **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).

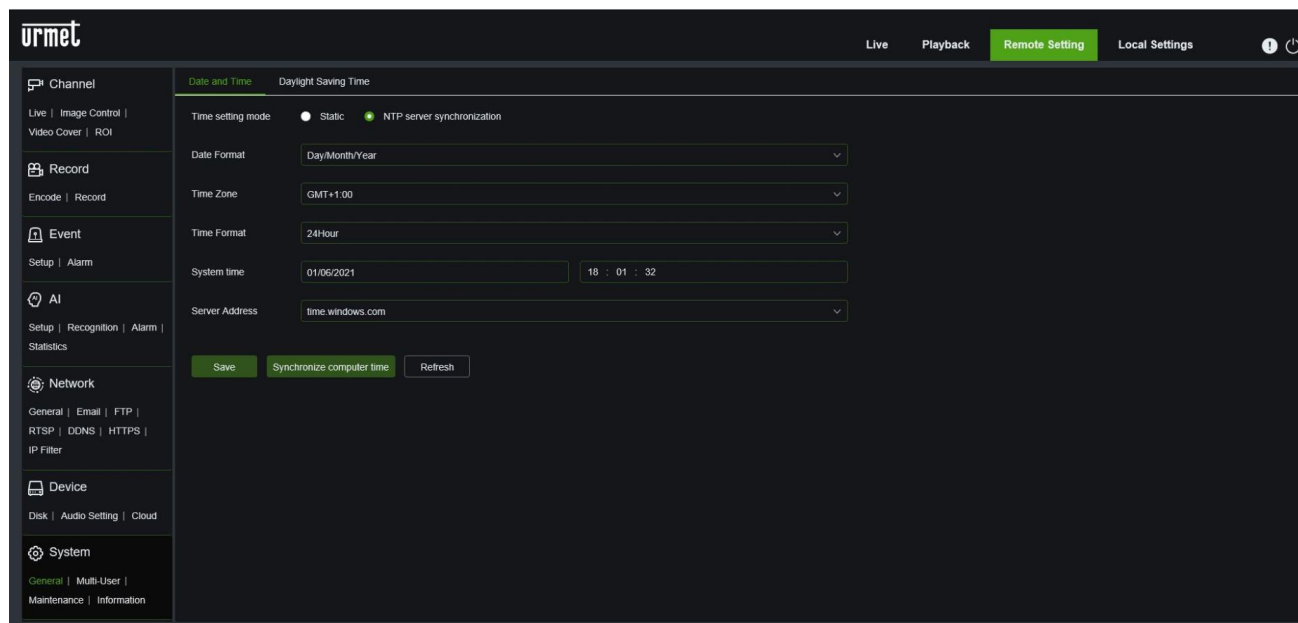
9.6 SYSTEM

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

9.6.1 GENERAL

9.6.1.1 Date and Time

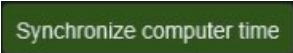
Select General in the System menu to open the following page



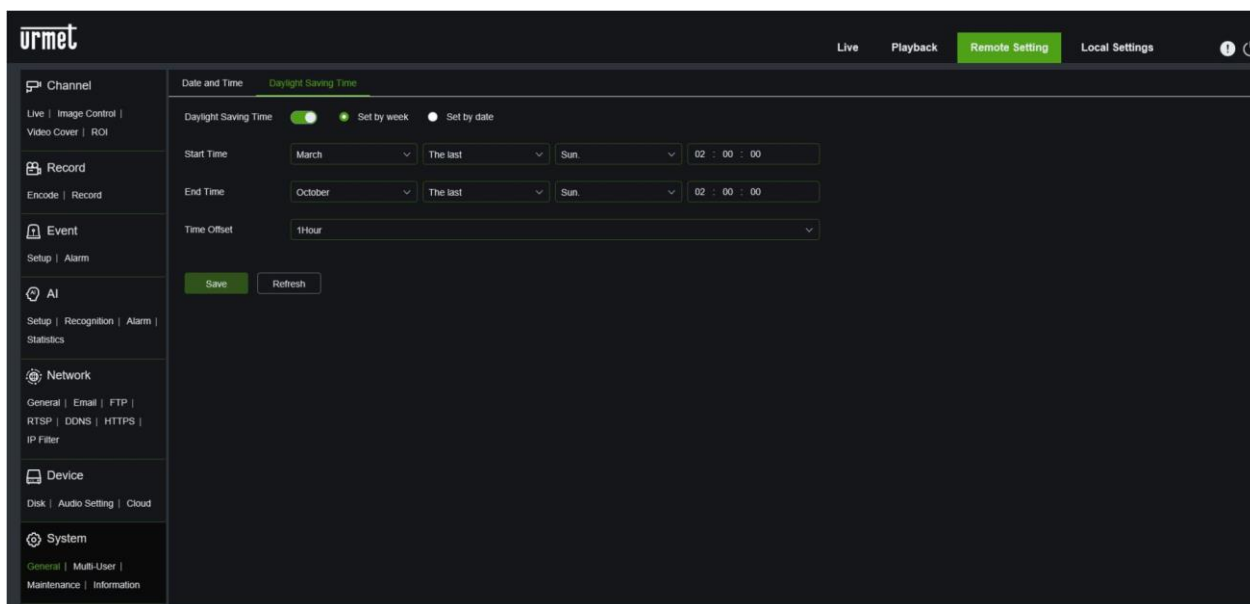
The screenshot shows the 'urmet' system settings interface. The sidebar menu on the left includes options like Channel, Record, Event, AI, Network, Device, and System. The main area is titled 'Date and Time' and contains settings for Time setting mode (Static or NTP server synchronization), Date Format, Time Zone, Time Format, System time, and Server Address. There are buttons for Save, Synchronize computer time, and Refresh.

- **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.

9.6.1.2 Daylight Saving Time



The screenshot shows the 'urmet' system settings interface. The sidebar menu on the left includes options like Channel, Record, Event, AI, Network, Device, and System. The main area is titled 'Daylight Saving Time' and contains settings for Daylight Saving Time (On or Off), Set by week or Set by date, Start Time, End Time, and Time Offset. There are buttons for Save and Refresh.

- **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.

9.6.2 MULTI USER

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

NO.	Username	Level	Status	Password	Policy
1	admin	admin	Enable	ℓ	🔒
2	user1	user1	Disable	ℓ	🔑
3	user2	user2	Disable	ℓ	🔑
4	user3	user3	Disable	ℓ	🔑
5	user4	user4	Disable	ℓ	🔑
6	user5	user5	Disable	ℓ	🔑
7	user6	user6	Disable	ℓ	🔑

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.

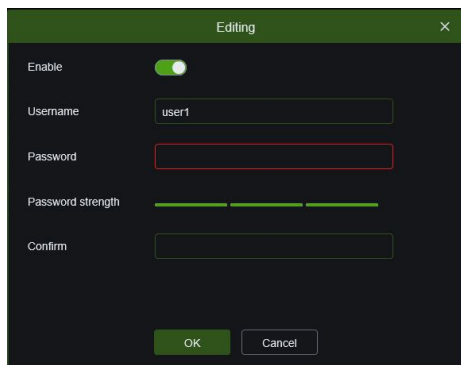
1. Password

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. The password must be a combination of at least two conditions between capital letters, lower case letters, special characters or numbers and cannot be the same as the one used as the user name. Enter the new password a second time to confirm it, then click **Save** to save it.

Length must be 8 ~ 16;
Combination should consist of at least 2 from uppercase letters, lowercase letters, digit, special characters;
Special characters include `~!@#\$%^&*()_-=+\\|{};:~'"<>/?
The password cannot be the same as the username or the username written backwards

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.




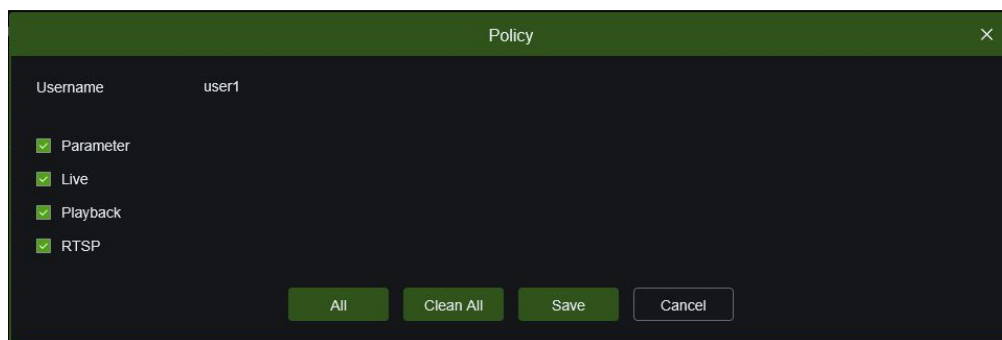
The 'Editing' dialog box has a title bar with 'Editing' and a close button. It contains the following fields: 'Enable' with a toggle switch, 'Username' with a text field containing 'user1', 'Password' with a text field, 'Password strength' with a progress bar, and 'Confirm' with a text field. At the bottom are 'OK' and 'Cancel' buttons.

- 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:



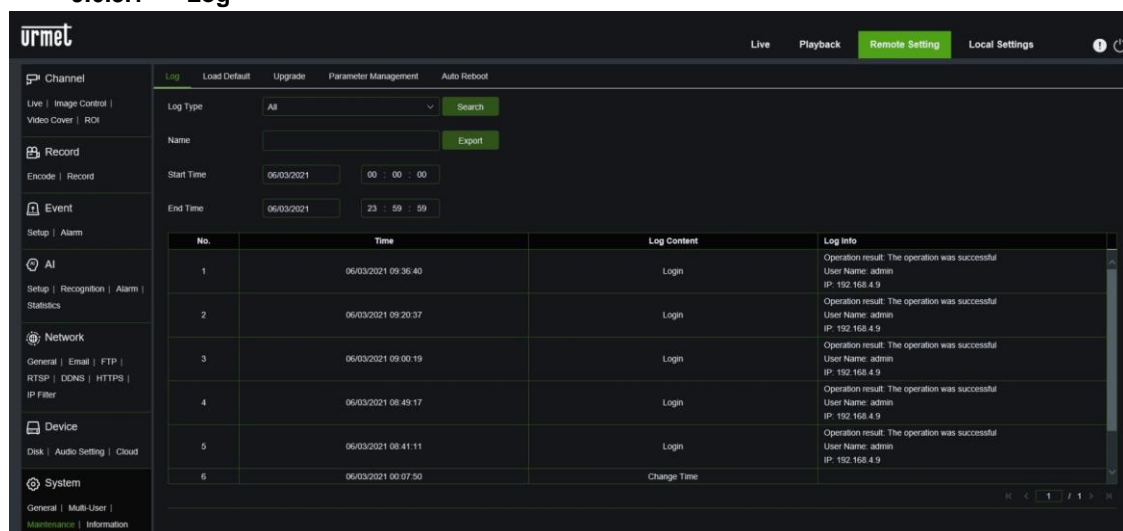
The 'Policy' dialog box has a title bar with 'Policy' and a close button. It contains the following fields: 'Username' with a text field containing 'user1', and four checkboxes: 'Parameter', 'Live', 'Playback', and 'RTSP', all of which are checked. At the bottom are 'All', 'Clean All', 'Save', and 'Cancel' buttons.

- 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.

9.6.3 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.

9.6.3.1 Log



The 'Log' interface has a title bar with 'urmet' and navigation buttons: 'Live', 'Playback', 'Remote Setting' (selected), and 'Local Settings'. It has a sidebar with 'Channel', 'Record', 'Event', 'Setup', 'AI', 'Network', 'Device', and 'System'. The main area has tabs: 'Log' (selected), 'Load Default', 'Upgrade', 'Parameter Management', and 'Auto Reboot'. The 'Log' tab has a 'Log Type' dropdown set to 'All', a 'Search' button, a 'Name' text field, an 'Export' button, and 'Start Time' and 'End Time' date/time pickers. Below is a table with 4 columns: 'No.', 'Time', 'Log Content', and 'Log Info'.

No.	Time	Log Content	Log Info
1	06/03/2021 09:35:40	Login	Operation result: The operation was successful User Name: admin IP: 192.168.4.9
2	06/03/2021 09:20:37	Login	Operation result: The operation was successful User Name: admin IP: 192.168.4.9
3	06/03/2021 09:00:19	Login	Operation result: The operation was successful User Name: admin IP: 192.168.4.9
4	06/03/2021 08:49:17	Login	Operation result: The operation was successful User Name: admin IP: 192.168.4.9
5	06/03/2021 08:41:11	Login	Operation result: The operation was successful User Name: admin IP: 192.168.4.9
6	06/03/2021 00:07:50	Change Time	

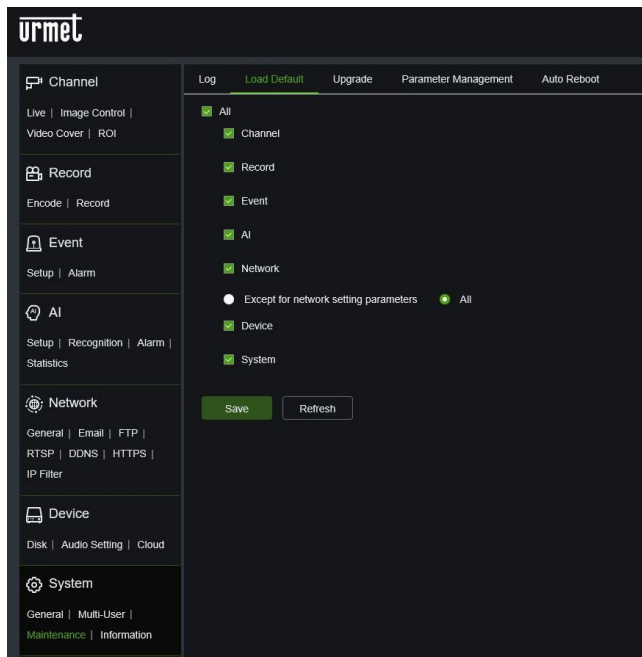
Log Search and Back up:

- 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

9.6.3.2 Load Default:

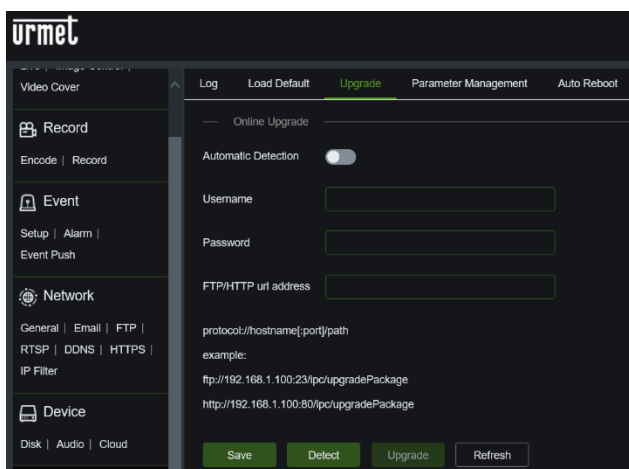
Through this menu you can reset the camera's factory settings. You can choose to reset all settings at once or only specific menu settings. Restoring the default settings will not erase recordings and snapshots saved on a SD card.



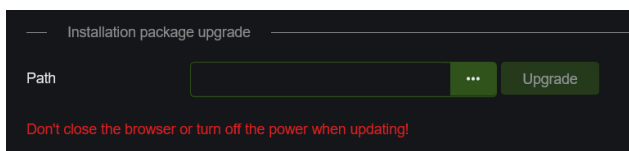
Select all the items to reset or select **All** to select all items. Click **Save** to load the default settings for the selected items.

9.6.3.3 Upgrade:

This feature allows you to update the NVR firmware. At the moment, only the manual update functionality is active.



Online Upgrade Automatic Detection: allows the camera to automatically search for and perform an upgrade (FOR FUTURE USES).

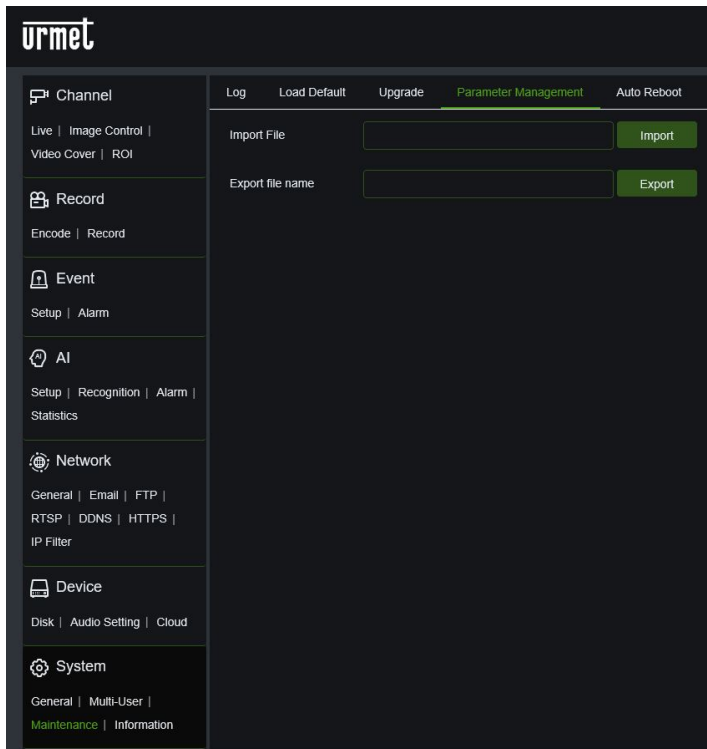


Click the **Select File** button **...** to select the firmware file (.sw file), and then click OK.

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.**

9.6.3.4 Parameter Management

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

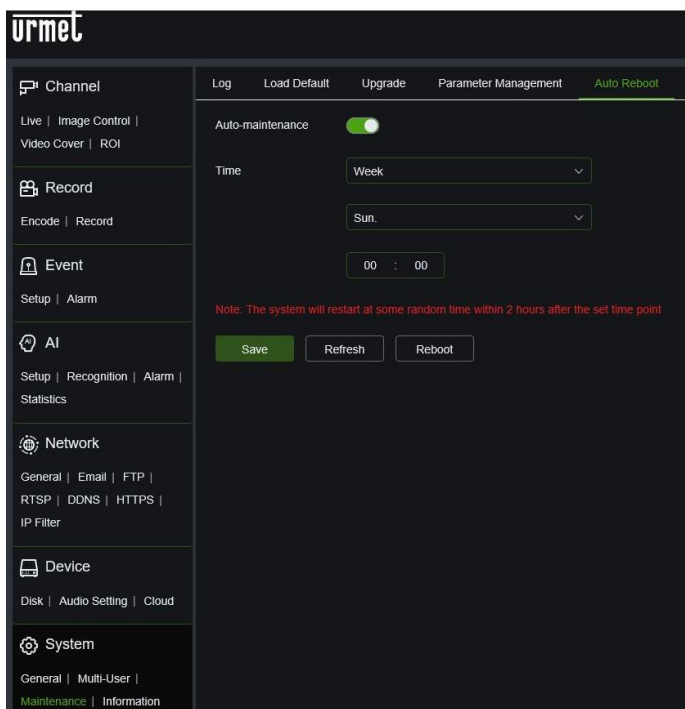


- Click in the **Import file** window to open the dialogue where you can select the backup file to import, and confirm by clicking on the **Import** button.
- Type the name of the backup file you want to export in the **export file name** window, then click on the **Export** button to complete the operation.

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

9.6.3.5 Auto Reboot

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

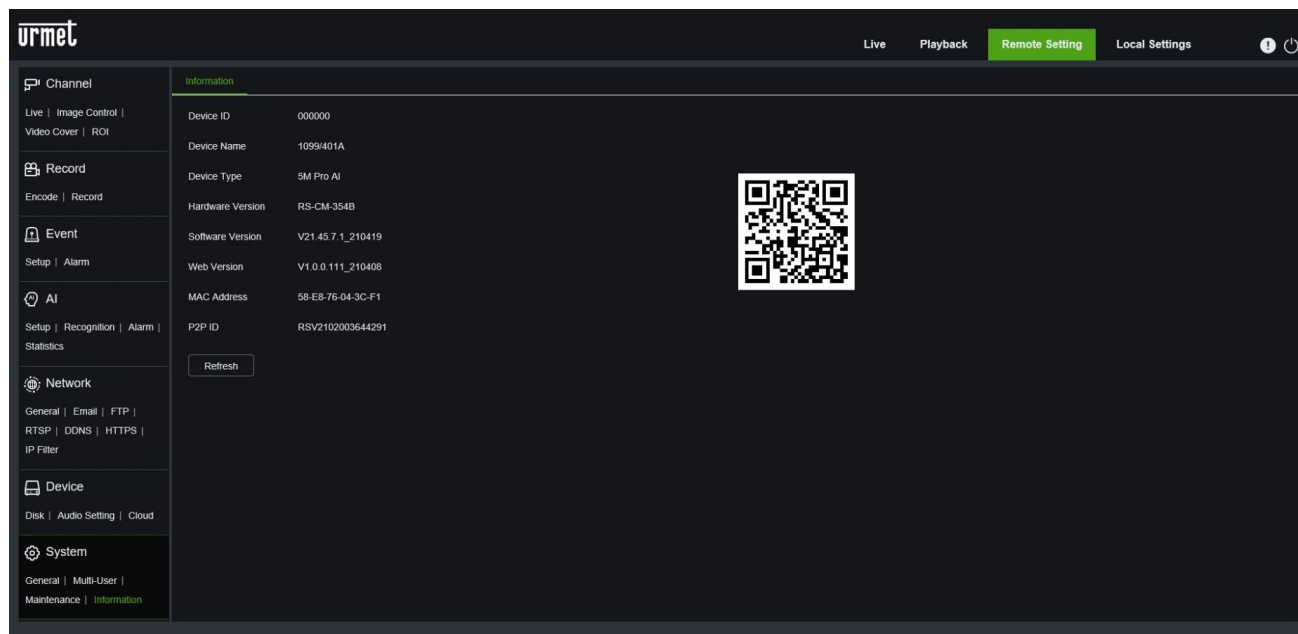


- **Auto Reboot:** click to enable feature
- **Time:** You can set the day, week, or month the camera is restarted.

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

9.6.4 INFORMATION

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



The screenshot displays the urmet web interface. The top navigation bar includes 'Live', 'Playback', 'Remote Setting' (highlighted in green), and 'Local Settings'. A sidebar on the left contains menu items: Channel, Record, Event, AI, Network, Device, and System. The 'System' menu is expanded, showing 'General', 'Multi-User', 'Maintenance', and 'Information' (highlighted in green). The main content area is titled 'Information' and displays the following details:

Device ID	000000
Device Name	1099401A
Device Type	5M Pro AI
Hardware Version	RS-CM-354B
Software Version	V21.45.7.1_210419
Web Version	V1.0.0.111_210408
MAC Address	58-E8-76-04-3C-F1
P2P ID	RSV2102003644291

A QR code is displayed next to the P2P ID. Below the P2P ID is a 'Refresh' button.

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 TECHNICAL SPECIFICATIONS FOR THE BULLET 5M ECO 2 IP CAMERAS

Items		Description		
		Starlight Bullet IP Camera		
		1099/500A	1099/501A	1099/502A
Camera	Image Sensor	1/2.7" Progressive CMOS		
	Sensor Type	SC5235		
	Video Format	Optional format P/N		
	Minimum Luminance	Color 0.05lux @ F1.2(AGC ON) ; B/W 0 lux @ IR ON		
	Lens Mount/Lens Type	Fixed Lens 2.8 mm	2.7 - 13.5 mm	5 - 50 mm
	Viewing angle	Horizontal:99°, Vertical:72°, Diagonal:131°	Horizontal: 101 ~ 31°, Vertical: 71 ~ 23°, Diagonal: 138 ~ 38°	Horizontal: 45.32 ~ 7°, Vertical: 33.48 ~ 5.2°, Diagonal: 57.94 ~ 9°
	Shutter Speed	1/5 ~ 1/20000s		
	Shutter Slowdown	Supported		
	G/N change mode	IR cut filter with auto switch (Day/Night/Auto/Schedule)		
	Wide Dynamic Range	DWDR		
	Digital noise reduction	3D DNR		
	IR illuminator range	2pcs (ARRAY) / Up to 30m	4pcs (ARRAY) / Up to 45m	8pcs (ARRAY) / Up to 80m
Standard Compression	Standard Video Compression	H.265+ / H.264+ / H.265 / H.264/ MJPG (solo SubStream)		
	Video Compression Rate	8Kbps ~ 8Mbps		
Picture	Max. Resolution	5MP 2592(H)×1944(V)		
	Frame Rate	Mainstream (1-20fps) 5MP(2592×1944), Mainstream (1-25fps) 4MP(2592x1520) 3MP(2304x1296),1080P(1920x1080) 960P(1280x960), Substream (1-25fps) 720P(1280x720),VGA(640x480), Mobile Stream (1-25fps) VGA(640x480), QVGA (320x240)		
	Image settings	Rotation, Saturation, Brightness, Contrast, Sharpness, settings can be adjusted via Client Software or Web Browser		
Users	N°. Max. Stream/PC Acces	Max 7 (admin+user)		
Software Functions	E-mail Alarm	YES		
	FTP	Image upload to FTP Server/ Cloud Dropbox		
	RTSP	YES		
	P2P	YES		
	NTP, DST, Sinc. con ora PC	YES		

Items		Description		
		Starlight Bullet IP Camera		
		1099/500A	1099/501A	1099/502A
	ROI	NO		
	Web/Client/ Mobile	Multi-Browser Support: IE 10,11, Edge, Chrome, Firefox, Safari Urmet UVS Pro Client Support: Windows 7 O.S. or higher / MAC O.S. 10.8.0 or higher iUVS Pro Software Mobile Support: (iOS, Android)		
SMART capability	Smart analysis	NO		
Network	Protocols	TCP/IP, HTTP, DHCP, DNS, DDNS, RTP/RTSP, SMTP, NTP, UPnP, SNMP, HTTPS, FTP		
Interface	Communication interface	1 RJ45 10M / 100M Ethernet Interface		
	System compatibility	ONVIF(Profile S/G/T)		
	Security	IP filtering function; password strength; username and password authentication		
	Alarm trigger	NO	1 input alarm, 1 output alarm	
	Audio	Built-in microphone	1 audio input(RCA), 1 audio output(RCA)	
	Protection rating	IP66		
	Protective connector	Waterproof RJ45 connector		
	Reset button	YES		
	SD Card	Supports up to 256GB (not included in supply)		
	Analogue Video Output	NO		
	PoE	YES		
General Specifications	Operating conditions	-30~+60°C/ meno del ≤ 95% RH		
	Power supply	12 VDC ± 10%, PoE (802.3af)		
	Power consumption	2.1 W(D) / 5.3W(N)	2.3W(D) / 6.3W(N)	2.3W(D) / 9.5W(N)
	Dimensions (LxHxD or ØxH in mm)	Ø70x150	89x86,5X239,5	90x95X300
	Weight (g)	390	810	1465

※**IMPORTANT NOTES**

- Product specifications may be subject to change without prior notice.

11 TECHNICAL SPECIFICATIONS FOR THE DOME 5M ECO 2 IP CAMERAS

Items		Descrizione		
		Starlight Dome IP Camera		Starlight Vandal Dome IP Camera
		1099/550A	1099/551A	1099/552A
Camera	Image Sensor	1/2.7" Progressive CMOS		
	Sensor Type	SC5235		
	Video Format	Optional format P/N		
	Minimum Luminance	Color 0.05lux @ F1.2(AGC ON) ; B/W 0 lux @ IR ON		
	Lens Mount/Lens Type	Fixed Lens 2.8 mm	2.7 - 13.5 mm	
	Viewing angle	Horizontal:99°, Vertical:72°, Diagonal:131°	Horizontal: 101 ~ 31°, Vertical: 71 ~ 23°, Diagonal: 138 ~ 38°	
	Shutter Speed	1/5 ~ 1/20000s		
	Shutter Slowdown	Supported		
	G/N change mode	IR cut filter with auto switch (Day/Night/Auto/Schedule)		
	Wide Dynamic Range	DWDR		
	Digital noise reduction	3D DNR		
	IR illuminator range	2pcs (ARRAY) / Up to 30m	4pcs (ARRAY) / Up to 45m	2pcs (ARRAY) / Up to 30m
Standard Compression	Standard Video Compression	H.265+ / H.264+ / H.265 / H.264/ MJPG (only SubStream)		
	Video Compression Rate	8Kbps ~ 8Mbps		
Picture	Max. Resolution	5MP 2592(H)×1944(V)		
	Frame Rate	Mainstream (1-20fps) 5MP(2592×1944), Mainstream (1-25fps) 4MP(2592×1520) 3MP(2304×1296),1080P(1920×1080) 960P(1280×960), Substeam (1-25fps) 720P(1280×720),VGA(640×480), Mobile Stream (1-25fps) VGA(640×480), QVGA (320×240)		
	Image settings	Rotation, Saturation, Brightness, Contrast, Sharpness, settings can be adjusted via Client Software or Web Browser		
Users	N°. Max. Stream/PC Acces	Max 7 (admin+user)		
Software Functions	E-mail Alarm	YES		
	FTP	Image upload to FTP Server/ Cloud Dropbox		
	RTSP	YES		
	P2P	YES		

Items		Descrizione		
		Starlight Dome IP Camera		Starlight Vandal Dome IP Camera
		1099/550A	1099/551A	1099/552A
	NTP, DST, Synchronisation with PC time	YES		
	ROI	NO		
	Web/Client/ Mobile	Multi-Browser Support: IE 10,11, Edge, Chrome, Firefox, Safari Urmet UVS Pro Client Support: Windows 7 O.S. or higher / MAC O.S. 10.8.0 or higher iUVS Pro Software Mobile Support: (iOS, Android)		
SMART capability	Smart analysis	NO		
Network	Protocols	TCP/IP, HTTP, DHCP, DNS, DDNS, RTP/RTSP, SMTP, NTP, UPnP, SNMP, HTTPS, FTP		
Interface	Communication interface	1 RJ45 10M / 100M Ethernet Interface		
	System compatibility	ONVIF(Profile S/G/T)		
	Security	IP filtering function; password strength; username and password authentication		
	Alarm trigger	NO	1 input alarm, 1 output alarm	
	Audio	Built-in microphone	1 audio input(RCA), 1 audio output(RCA)	
	Protection rating	IP66		
	Protective connector	Waterproof RJ45 connector		
	Reset button	YES		
	SD Card	Supports up to 256GB (not included in supply)		
	Analogue Video Output	NO		
	PoE	YES		
General Specifications	Operating conditions	-30~+60°C/ less than ≤ 95% RH		
	Power supply	12 VDC ± 10%, PoE (802.3af)		
	Power consumption	2.1 W(D) / 5.3W(N)	2.3W(D) / 6.5W(N)	2.2W(D) / 4.3W(N)
	Dimensions (LxHxD or ØxH in mm)	Ø100x95	Ø136X140	Ø147x115
	Weight (g)	420	850	960

※**IMPORTANT NOTES**

- Product specifications may be subject to change without prior notice.

12 TECHNICAL SPECIFICATIONS FOR THE BULLET DETERRENCE ECO 2 IP CAMERAS

General Specifications	1099/208A
Power consumption (W)	2.1W(D) / 5.3W(N)
Power supply	12Vdc / PoE
Dimensions (LxHxD or ØxH in mm)	Ø 70mm x 151mm
Weight(g)	435g
Type of case	Bullet
Product color	White (frontal black)
Operating conditions	-30°C ~ +60°C
Protection rating	IP 66
Video format	PAL/NTSC
Main characteristics	
Image sensor	1/2.7" SC5235 Progressive CMOS
Lens Mount/Lens Type	Lens 2.8mm, F No. 1.6±5%
Viewing angle	Horizontal:99°, Vertical:72°, Diagonal:131°
Shutter Speed	1/5 ~ 1/20.000s
Minimum Luminance	COLOR 0.05Lux@F1.2 (AGC ON), B/W 0 Lux with IR ON
IR Filter	IR cut filter with auto switch (Day/Night/Auto/Schedule)
Max resolution (H x V)	5M (2592x1944)
Video Compression Rate	8Kbps - 8Mbps
Software/firmware features	
Standard Video Compression	H.265+, H.264+, H.265, H.264, MJPEG
Frame rate	Mainstream (H264, H265, H264+, H265+) 5M(2592x1944)@20fps 4M(2592x1520)@25fps 3M(2304x1296)@25fps 2M(1920x1080)@25fps 1280x960@25fps 1280x720@25fps Substream (H264, H265, H264+, H265+, MJPEG) 1280x720@20fps VGA(640x480)@20fps QVGA(320x240)@20fps Mobilestream (H264, H265, H264+, H265+) QVGA(320x240)@20fps
Protocols	TCP/IP, HTTP, DHCP, DNS, DDNS, RTP/RTSP, SMTP, NTP, UPnP, SNMP, HTTPS, FTP
Web/Client/ Mobile	Supporto Multi-Browser: IE 10,11, Edge, Chrome, Firefox, Safari Urmet UVS Pro Client Support: Windows 7 O.S. o superiore / MAC O.S. 10.8.0 o superiore iUVS Pro Software Mobile Support: (iOS, Android) ONVIF (Profile S/G/T)
Security	IP filtering function; password strength; username and password authentication
Functions	
Image settings	Rotation, Saturation, Brightness, Contrast, Sharpness, settings can be adjusted via Client Software or Web Browser
Audio In	Built-in microphone
Audio Out	Built-in Speaker (for Voice and Siren)
Motion	YES
PIR	YES
White light	YES
Smart analysis	NO

Digital noise reduction	3D DNR
Backlight Compensation	BLC / D-WDR
No.: Max. Stream/PC access	Max 7 (admin+user)
E-mail Alarm	YES
FTP/Cloud	Image upload to FTP Server/ Cloud Dropbox
P2P	YES
NTP, DST, Sync. with PC time	YES
Hardware features	
IR illuminator range	2 Array IR LED / ~ 30m
White illuminator range	4 PCS Up to 10m
PIR angle / Distance	Up 115°, Up 7 m
Micro-SD card slot (card not included)	YES, Max 256GB
Communication interface	1 RJ45 10M / 100M Ethernet interface
Reset button	YES

※**IMPORTANT NOTES**

- Product specifications may be subject to change without prior notice.

13 TECHNICAL SPECIFICATIONS FOR CUBE CAMERA IP WIFI 2M

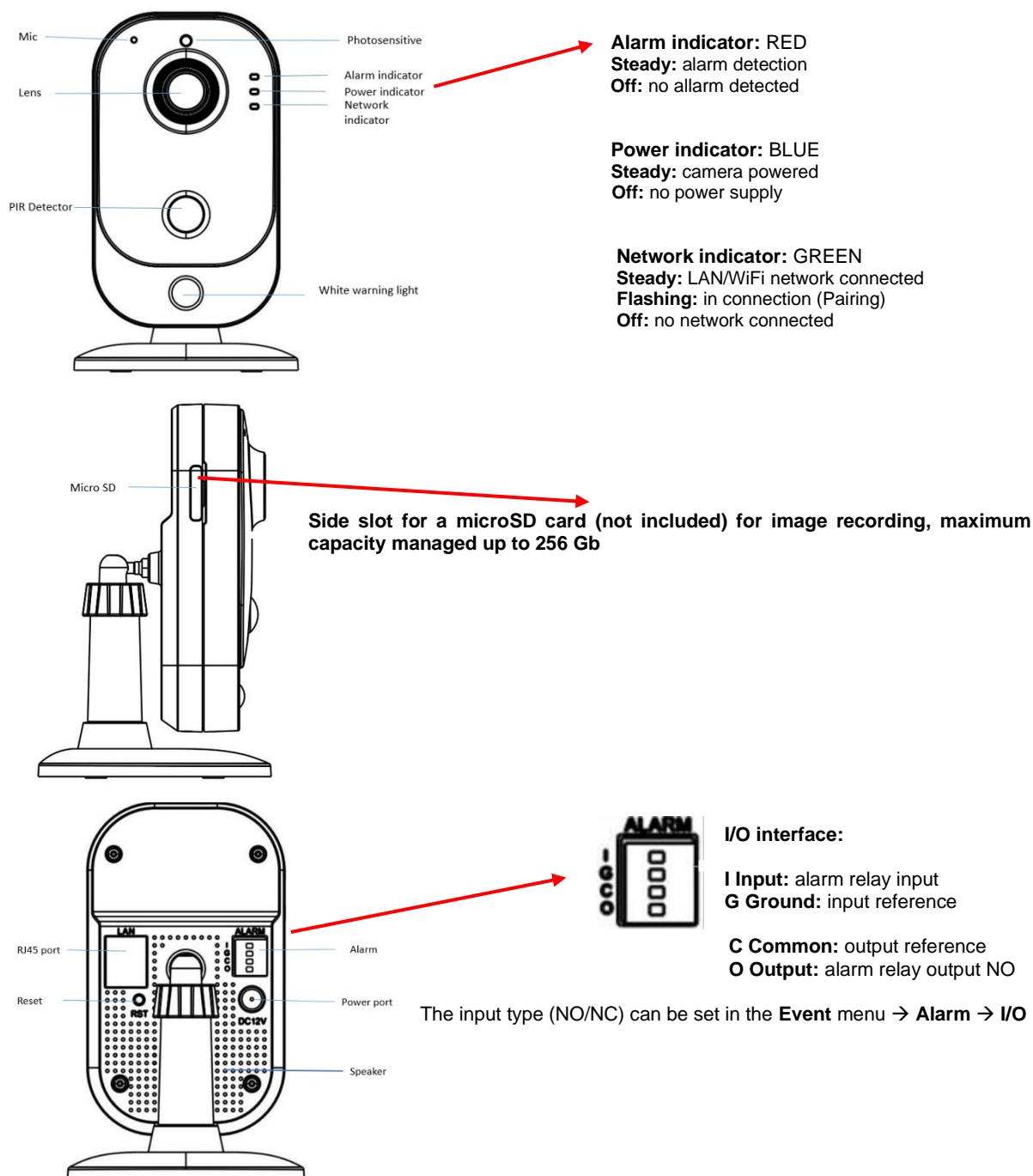
General Specifications		1099/210
Power consumption (W)		$\leq 4.5W$
Power supply		12Vdc / PoE
Dimensions (LxHxD mm)		63x120x33
Weight(g)		195g
Type of case		Plastic
Product color		White (frontal black)
Operating conditions		-10°C ~ +45°C
Protection rating		Indoor
Video format		PAL/NTSC
Main characteristics		
Image sensor		1/2. 2.8" 2Megapixel Progressive CMOS
Lens Mount/Lens Type		Fixed Lens 2.8mm, F No. 2 \pm 10%
Viewing angle		Horizontal:92.7°, Vertical:48.5°, Diagonal: 115.2°
Close Focus Distance		0.2m
Minimum Luminance		Color 0.006lux @ F1.6 (AGC ON) ; B/W 0 lux @ IR ON
IR Filter		IR cut filter with auto switch Day/Night/Auto)
Max resolution (H x V)		2M (1920x1080)
Video Compression Rate		8Kbps - 8Mbps
Software/firmware features		
Standard Video Compression		H.265, H.264
Frame rate		Mainstream (H264, H265) 2M(1920x1080)@25fps 1280x960@25fps 1280x720@25fps Substream (H264, H265) 1280x720@20fps VGA (640x480) @20fps QVGA (320x240) @20fps Mobilestream (H264, H265) QVGA (320x240) @ 20fps
Protocols		TCP/IP, HTTP, DHCP, DNS, DDNS, RTP/RTSP, SMTP, NTP, UPnP, HTTPS.
Web/Client/ Mobile		Supporto Multi-Browser: IE 10,11, Edge, Chrome, Firefox, Safari Urmet UVS Pro Client Support: Windows 7 O.S. o superiore / MAC O.S. 10.8.0 o superiore iUVS Pro Software Mobile Support: (iOS, Android) ONVIF (Profile S/G/T)
Security		IP filtering function; password strength; username and password authentication
Functions		
Image settings		Rotation, Saturation, Brightness, Contrast, Sharpness, settings can be adjusted via Client Software or Web Browser
Audio In		Built-in microphone
Audio Out		Built-in Speaker (for Voice and Siren)
Motion		YES
PIR		YES
White light		YES
Smart analysis		NO
Digital noise reduction		3D DNR
Backlight Compensation		BLC / D-WDR
No.: Max. Stream/PC access		Max 7 (admin+user)
E-mail Alarm		YES

FTP/Cloud	Image upload to Cloud Dropbox
P2P	YES
NTP, DST, Sync. with PC time	YES
Hardware features	
N. LED IR / illuminator distance (m)	12 Array IR LED / up to 10m
N. White LED / White illuminator range (m)	1 / up to 10m
PIR angle / Distance	Up to 115°, Up to 7 m
Micro-SD card slot (card not included)	YES, Max 256GB
Communication interface	1 RJ45 10M / 100M Ethernet interface 1 Wi-Fi 2.4 GHz, max. range 10m
I/O Interface	YES, 1 input (programmable NC/NO) and 1 relay NO output (30Vdc/2A)
Reset button	YES

※**IMPORTANT NOTES**

- Product specifications may be subject to change without prior notice.

14 LED, I/O INTERFACE AND MICRO SD CARD SLOT DESCRIPTION FOR 1099/210



15 MAXIMUM RECORDING TIME WITH SD CARD

15.1 REF. 1099/500A – 1099/501A – 1099/502A – 1099/550A – 1099/551A – 1099/552A – 1099/208A

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

- “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**

16 APPENDIX

16.1 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.

LINKSYS[®] by Cisco

Firmware Version: v1.0.05

Wireless-N Home Router WRT120N

Applications & Gaming

Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Single Port Forwarding Port Range Forwarding Port Range Triggering DMZ QoS

Port Range Forwarding

Application Name

Start ~ End Port	Protocol	To IP Address	Enabled
9988 to 9988	Both	192.168.1.168	<input checked="" type="checkbox"/>
8000 to 8000	Both	192.168.1.168	<input type="checkbox"/>
	Both	192.168.1.	<input type="checkbox"/>
	Both	192.168.1.	<input type="checkbox"/>
	Both	192.168.1.	<input type="checkbox"/>
	Both	192.168.1.	<input type="checkbox"/>
	Both	192.168.1.	<input type="checkbox"/>
	Both	192.168.1.	<input type="checkbox"/>
	Both	192.168.1.	<input type="checkbox"/>
	Both	192.168.1.	<input type="checkbox"/>
	Both	192.168.1.	<input type="checkbox"/>
	Both	192.168.1.	<input type="checkbox"/>


Help...

Save Settings Cancel Changes

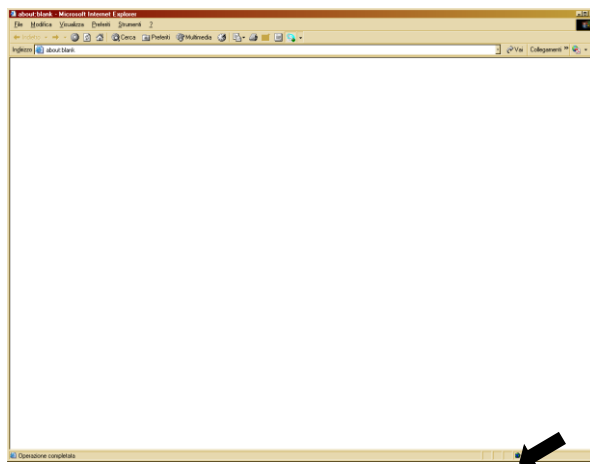
CISCO


16.2 INSTALLING ACTIVEX

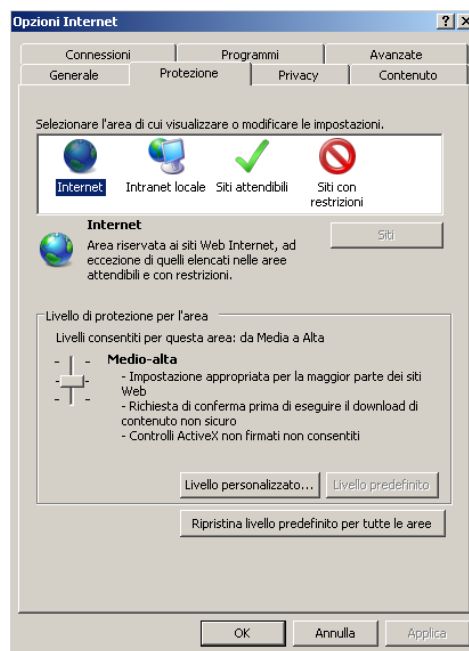
If you need to install an ActiveX component, you may do so as follows.
Before connecting the PC, activate the IE protection settings, as shown below:

Double click on the  icon to open Internet Explorer.

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

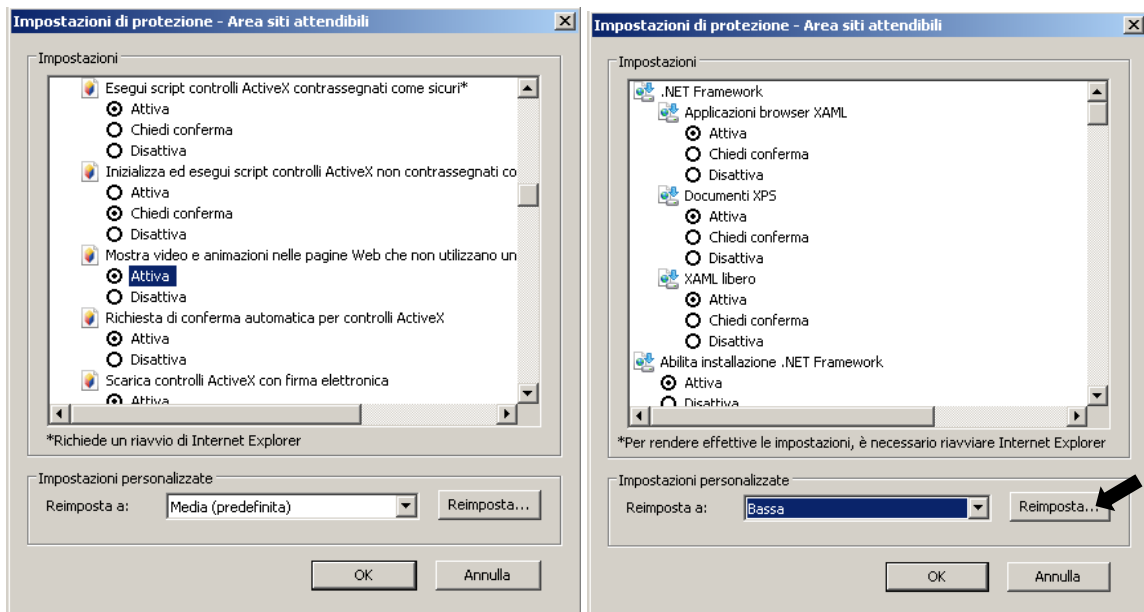
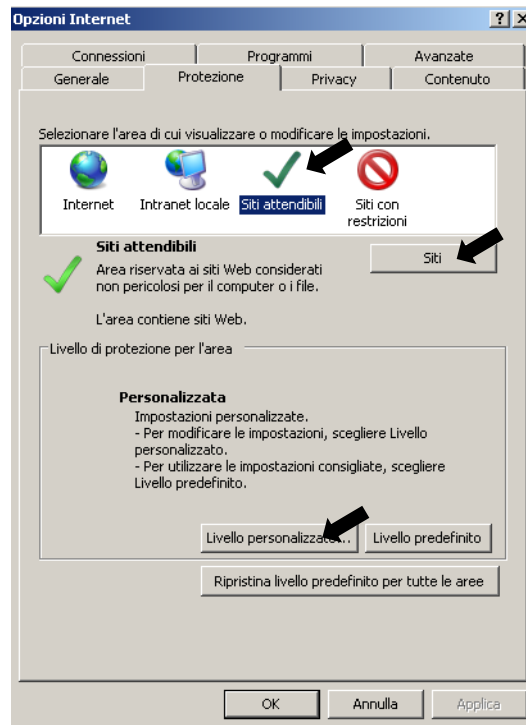


- Double click on the  icon to open Internet Explorer.
- The “Internet Options” window will appear.



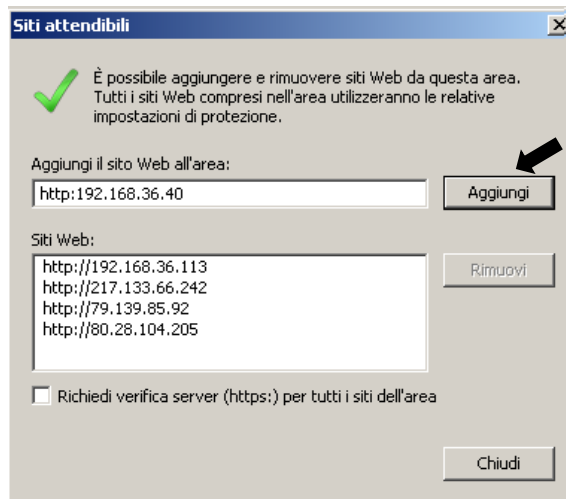
- Select the **“Trusted Sites”** area.
- Click **“Custom Level”** and check that:
 - “Initialise and script ActiveX controls not marked as safe” is set to “Enable” or “Prompt”.
 - “Download signed ActiveX controls” is set to “Enable” or “Prompt”.

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.

16.3 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 Edge in Internet Explorer mode.**

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 Edge in IE mode?**

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.

DS1099-130B

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



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