spark

UltraHD technology

PROFESSIONAL SERIES-MIRA 8000 USER MANUAL

Confidentiality Notice

Table of Contents

1. DOCUMENT DETAILS 4

1.1 Introduction 4
1.2 Legal Considerations 4
1.3 Liability 4

2. ELECTROMAGNETIC COMPATIBILITY (EMC) 5

2.1 FCC Statement 5
2.2 CE Mark Warning 5

3. REQUIREMENTS 6

3.1 System Requirements 6

4. WEB USER INTERFACE 7

4.1 Accessing the web interface 7
4.2 Setup Page 9
4.3 Image 11
4.4 Video 16
4.5 Audio 22
4.6 Network 23
4.7 Date & Time 26
4.8 Accounts 28

5. WEB USER INTERFACE-ADVANCED 29

5.1 Archive 29
5.2 Recording servers 33
5.3 Recordings 42
5.4 Analytics 62
5.5 Schedules 70
5.6 Digital I/O 71
5.7 Network advanced 73
5.8 Security 79
5.9 Maintenance 85
5.10 System log 88

1. DOCUMENT DETAILS

1.1 Introduction

This user manual is designed for SPARK MIRA 8000 Network Camera. It is written with the intention to introduce the camera's web interface and help users with the installations. Please read and follow the instructions on the guide carefully before installing MIRA 8000.

1.2 Legal Considerations

Both Audio and Video surveillance can be prohibited by laws that vary from country to country. Check the laws in your local region before using this product for surveillance purposes.

1.3 Liability

SPARK company limited cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. SPARK company makes no warranty of any kind with regard to the material contained within this document. Including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose. SPARK company shall not be liable nor responsible for incidental or consequential damages in connection with the furnishing, performance or use of this material. This product is only to be used for its intended purpose.

2. ELECTROMAGNETIC COMPATIBILITY (EMC)

2.1 FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. The limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

2.2 CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

3. REQUIREMENTS

3.1 System Requirements

Using one of the browsers as below to access the web interface:

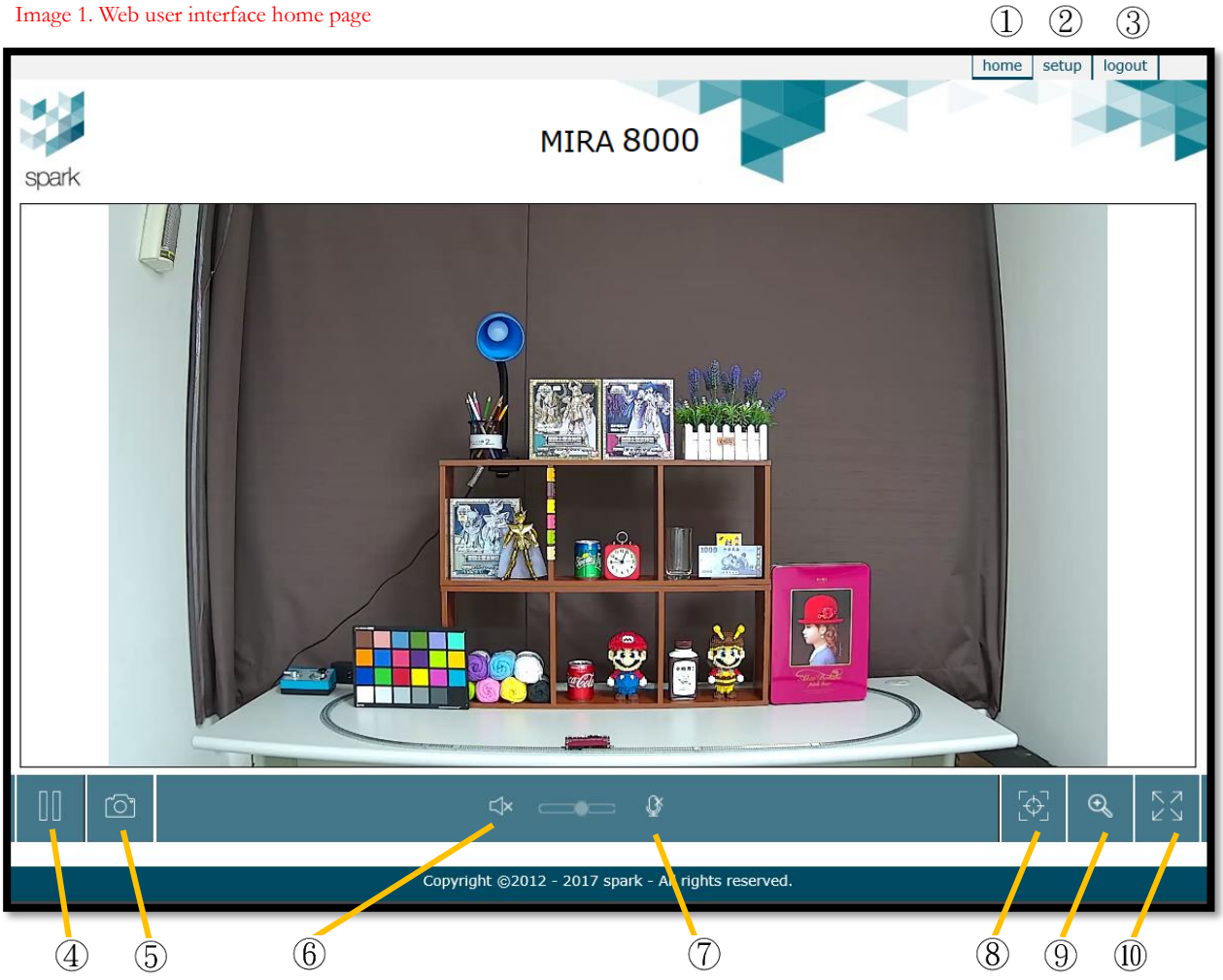
Item	Requirement
Microsoft Internet Explorer	Version 7.0 or later
Google Chrome	Version 8.0 or later
Mozilla Firefox	Version 3.6 or later
Apple Safari	Version 5.0 or later
Android ™	2.2 (Froyo) or later browsers
Apple iOS	Version 5.0 or later browsers

4. WEB USER INTERFACE

4.1 Accessing the web interface

- Open a web browser.
- Fill-in camera IP address.
- Use the default account and password when logging in for the first time.
- Double click the live view screen to enter or exit full screen*.
- Use the mouse scroll to zoom in and out on the live view screen*.

Image 1. Web user interface home page



1	home	**Live View**	Open live view.
2	setup	**Configuration**	Open configuration page.
3	logout	**Logout**	Logout the user account.

4		**Pause/Play**	Pause/Play live view video stream.
5		**Snapshot**	Captures a snapshot of the current live view image, allowing users to save or discard the snapshot.
6		**Sound Mute/ Volume level**	Enable/disable the sound from the camera and configure volume*.
7		**Talk Mute**	Enable/disable the microphone from the camera*.
8		**Re-Focus**	Enable automatic re-focus for clear image.
9		**Zoom in**	Enable users to zoom in on any area of the live view screen. Clicking the zoom in icon will open a small window facilating users to configure the zoom in rate and area. Click on the "T" (tele) and "W" (wide) to adjust the zoom. Click on  to close the window.
10		**Full Screen**	Enables full screen view of the live view screen. Press ESC to exit the full screen video.

Remark *only available for Internet Explorer.

4.2 Setup Page

• There are 8 parts in the setup page:

1. **Information**
2. **Image**
3. **Video**
4. **Audio**
5. **Network**
6. **Date& Time**
7. **Accounts**
8. **Advanced**

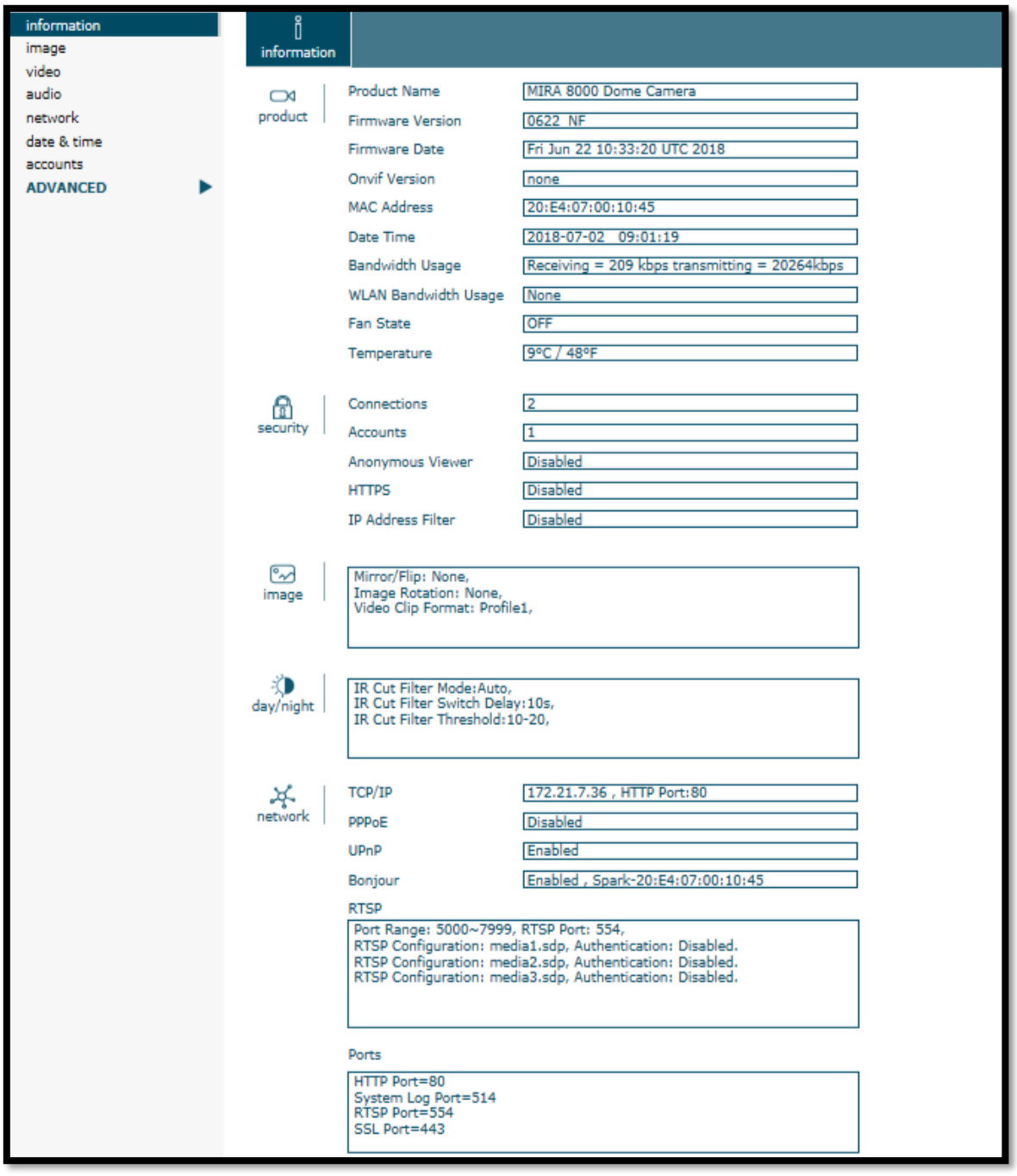
• There are 10 parts in the advanced setup page:

1. **Archive**
2. **Recording servers**
3. **Recordings**
4. **Analytics**
5. **Schedules**
6. **Digital I/O**
7. **Network advanced**
8. **Security**
9. **Maintenance**
10. **System log**

• The information page displays the detail information of IP camera, including:

1. **Product information**
2. **Security information**
3. **Image settings information**
4. **Day/Night mode settings information**
5. **Network settings information**

Image 2. Camera information page



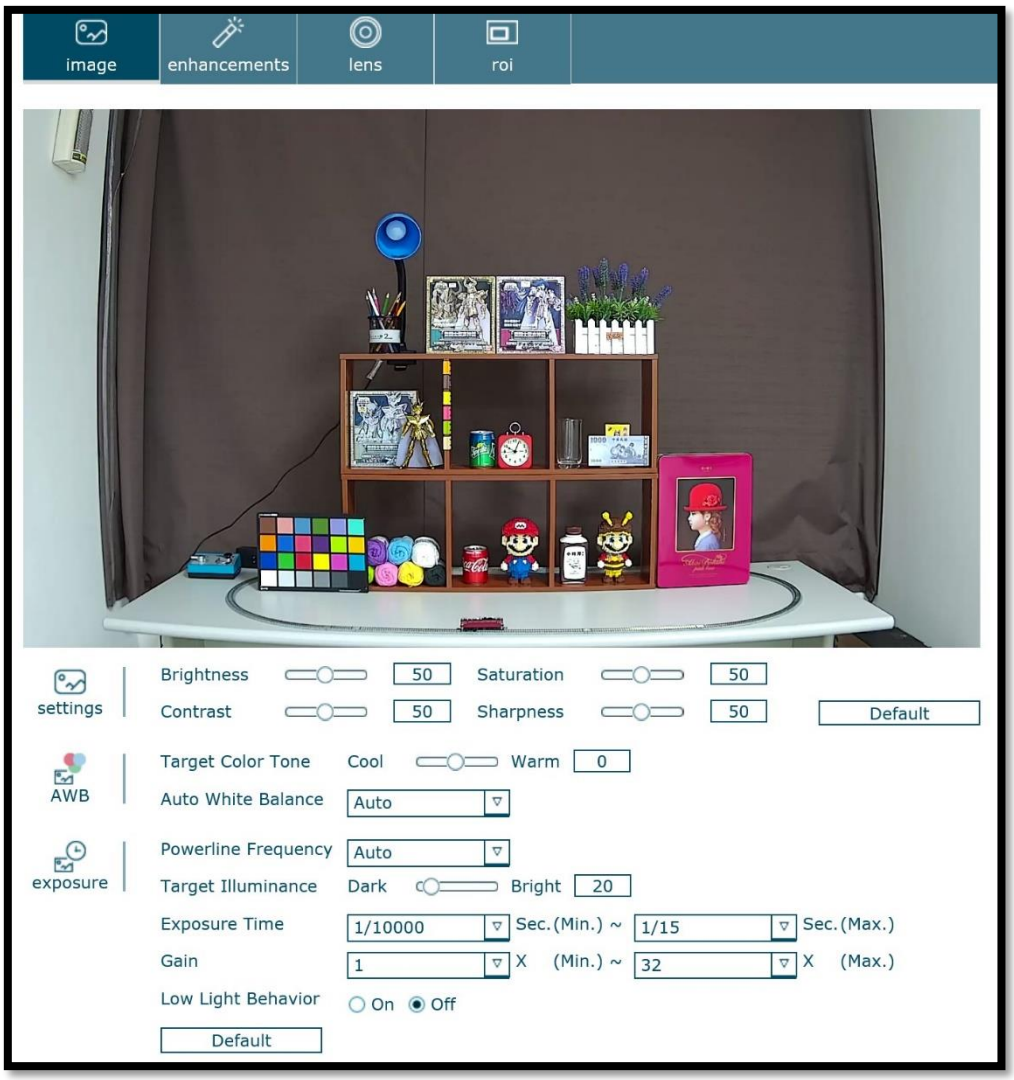
4.3 Image

Note: Remember to click the save button to successfully apply changes.

• Image page includes image, enhancements, lens and ROI.

1. **Image configuration:** image settings, AWB, exposure.

Image 3. Image configuration page



a. Settings:

1	**Brightness**	value from 0~100	Brightness refers to the overall lightness or darkness of the image, the higer the value the brighter the image.
2	**Contrast**	value from 0~100	The relative difference between dark and light, the higher the value the bigger the difference.
3	**Saturation**	value from 0~100	Controls the intensity of color in an image.
4	**Sharpness**	value from 0~100	Controls the level of detail that is achieved in an image.

b. AWB (auto white balance):

1	**Target color tone**	value from -127~127	Move the bar to the value that can best reflect natural colors, higher value produce warmer colors, lower value produce colder colors.
2	**Auto White Balance**	Auto	AWB allows colors in an image to appear the same regardless of the color temperature of the light source. The auto option can automatically identify the light source and compensate for its color. Users can also select other type of light source available on the drop-down list.
		Hold current	
		Fluorescent	
		Incandescent	
		Sunny	
		Cloudy	
		Sun Shade	
		Manual	

c. Exposure

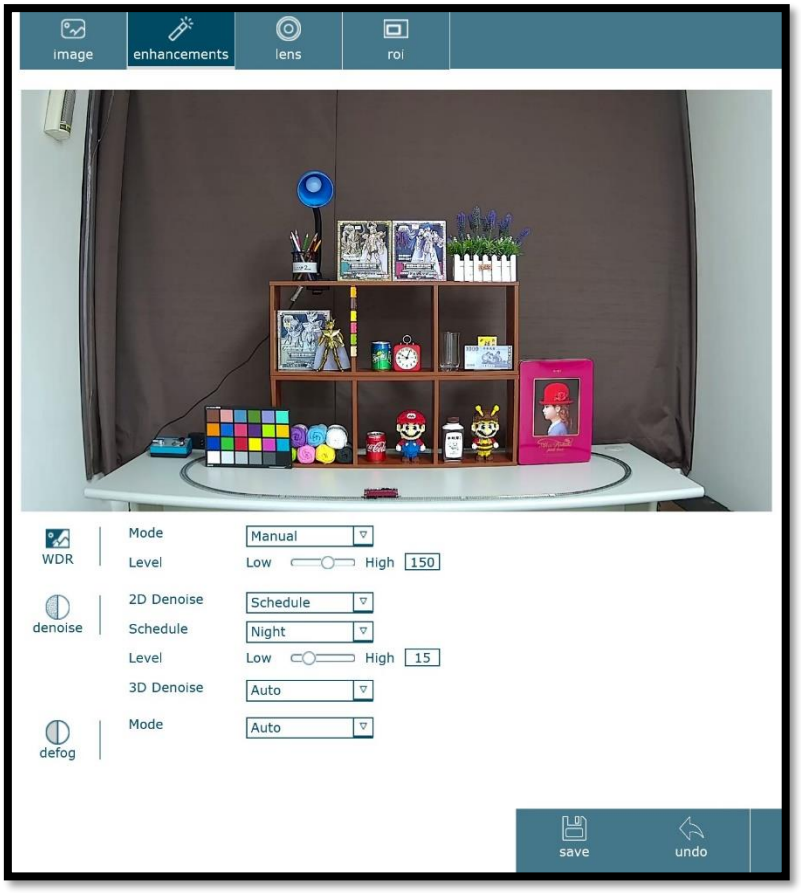
1	**Powerline frequency**	Auto	Select auto if the camera is installed outdoor. On the contrary, please choose the indoor light frequency (e.g. 60Hz for USA, 50Hz for Germany).
		50 Hz	
		60 Hz	
		Hold current	
2	**Target illuminance**	value from 0~100	Target illuminance allow users to adjust the brightness and darkness. This feature is only available under auto exposure time and auto gain.
3	**Exposure time**	value from 1/2~1/30000	Define the minimum and maximum exposure time of the camera's shutter. It is recommend using the smallest exposure time for the min value to ensure crisp images during day time condition. As for the max value, the bigger the value, the longer the camera keeps the shutter open in low light conditions allowing more light to fall onto the image sensor. As a result, the camera can capture images even in very dark environments. However, moving objects will appear blurred as they move while the camera's shutter is open.
4	**Gain**	value from 1~128	The higher the value, the brighter the image, but consequently it will contain more noise.
5	**Low light behavior**	On (setting)	Configure settings for low light conditions.
		Off	

c.1 Low light behavior setting:

1	**Exposure**	Powerline Frequency	Includes auto, 50Hz, 60Hz and hold current.
		Target illuminance	value from 0~100
		Exposure time	value from 1/2~1/30000
		Gain	value from 1~128
2	**Mode**	Mode	Includes schedule and night mode
		Schedule	Includes all the schedules previously saved.

2. **Enhancements:** includes WDR, denoise and defog

Image 4. Enhancements page



a. WDR:

1	**Mode**	Auto	WDR allows the capture of clear video in areas with high lighting contrast. The bigger value means greater range of luminance levels.
		Manual (Value 0~255)	
		Off	

b. Denoise:

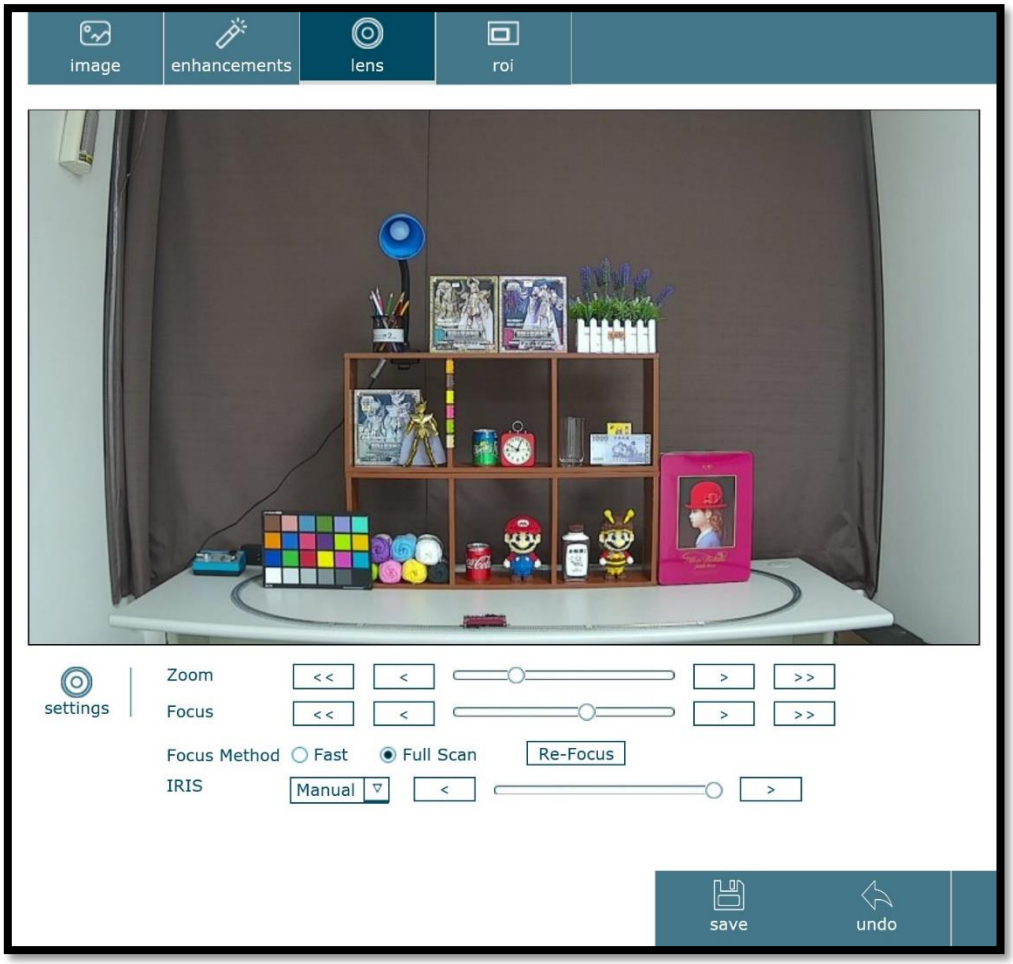
1	**2D Denoise**	Auto	Noise reduction algorithm helps reduce the graining in the video, which occurs under low light conditions. Select the mode that best fit your needs.
		Manual (Value 0~50)	
		Off	
		Schedule (Value 0~50)	
		Night mode (Value 0~50)	
2	**3D Denoise**	Auto	Further improves noise reduction to deliver sharper image.
		Off	

c. Defog:

1	**Defog**	Auto	Enable this feature to allow the camera to automatically increase image contrast and provide better image quality on a foggy day.
		Off	

3. **Lens control:** users can adjust the lens according to the installation needs.

Image 5. Lens control page

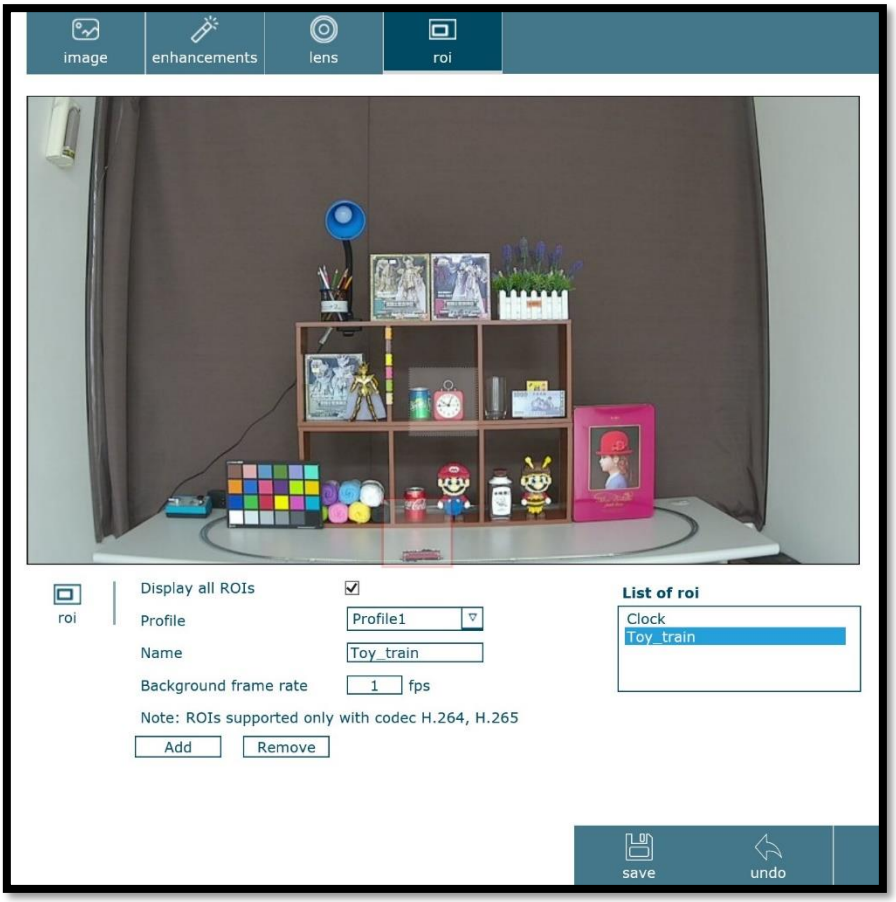


a. Settings:

1	**Zoom**		Use the arrows to zoom in or out. Users can also click on the bar to zoom to specific position.
2	**Focus**		Use the arrows to adjust the focus, or use the mouse to move and resize the focus window
3	**Focus method**	Fast	Focus method allows users to automatically refocus. Use fast focus method to refocus on the current focal length or use full scan to refocus all focal length.
		Full scan	
4	**IRIS**	Auto	Iris controls the depth of field and light level. Select Auto for the iris to automatically maintain the optimum light level to the image sensor so that images can be sharp, clear and correctly exposed with good contrast and resolution. Choose manual to manually set the the iris opening.
		Manual	
		Open	

4. **ROI (Region of Interest):** users can create up to 3 ROI regions according to the installation needs.

Image 6. ROI setting page



a. Roi:

1	**Display all ROIs**	Display/no display	Display all ROIs to see all the regions previously set.
2	**Profile**	Profile 1	Select profile. For profile settings please refer to section 4.4.1
		Profile 2	
		Profile 3	
3	**Name**	Toy_train	Insert ROI name, only allow characters 0-9, a-z, A-Z, “.”, “_”
4	**Background frame rate**	Value 1~30	Users may lower the background frame rate in order to relocate the bitrate resources and increase the video quality on the regions of interest.

How to setup ROI:

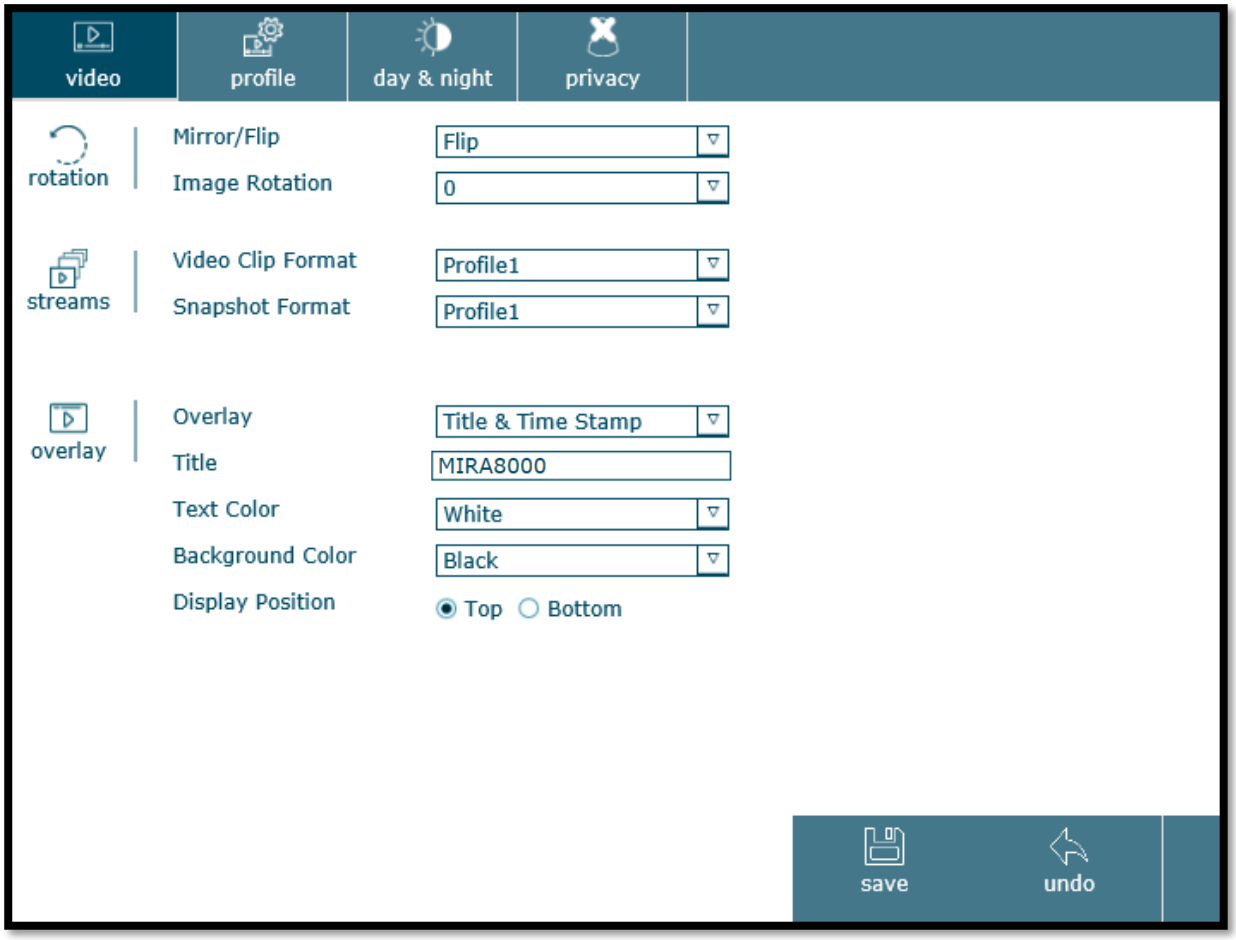
a. Step 1: Choose the profile for ROI
b. Step 2: Key in the ROI name
c. Step 3: Key in the background frame rate (1~30)
d. Step 4: Click add button
e. Step 5: Click the save button

4.4 Video

Note: Remember to click the save button to successfully apply changes.

• Video page includes video configuration, profile, day/night and privacy.

Image 7. Video settings page



a. Rotation:

1	**Mirror/Flip**	None Mirror Flip Mirror + Flip	Allows users to mirror and/or flip the image. Mirror for rotated left and right, flip for rotated up and down.
2	**Image Rotation**	0 ° 90 ° 270 °	Allows users to rotate the image by 0°, 90° or 270° .

b. Streams:

1	**Video Clip Format**	Profile1 Profile2 Profile3	Select profile for video clip format. For profile settings please refer to section 4.4.1
2	**Snapshot Format**	Profile1 Profile2 Profile3	Select profile for snapshot format. For profile settings please refer to section 4.4.1

c. Overlay:

1	**Overlay**	None Time Stamp Title Title & Time Stamp	Overlays are superimposed over the video stream. They are used to provide extra information during recordings, such as a timestamp, or during product installation and configuration.
2	**Title**	MIRA8000	Insert Title name, only allow characters 0-9, a-z, A-Z, ".", "_"
3	**Text Color**	White Black	Users can select the text color that best fit their needs.
4	**Background Color**	White Black Transparent	Users can select the background color that best fit their needs.
5	**Display Position**	Top Bottom	Users can select the display position of overlay that best fit their needs.

1. **Profile page:** Up to 4 configurable profiles, 2 main stream and 2 sub-streams.
   Add/Edit page includes profile name and description and other video and audio configurations such as encoding, profile, resolution, fps and quality.

Image 8. Profile page

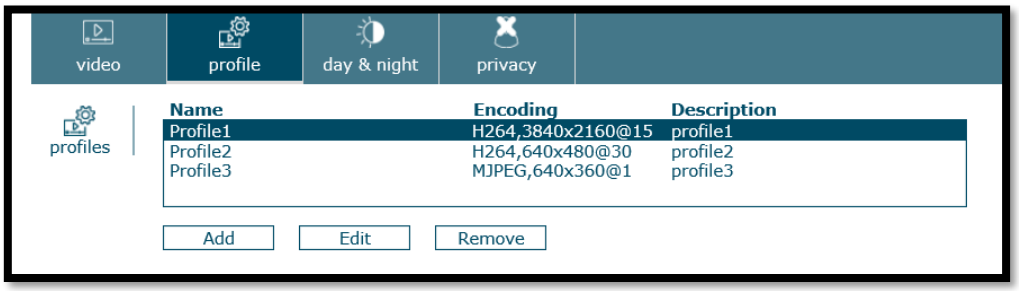
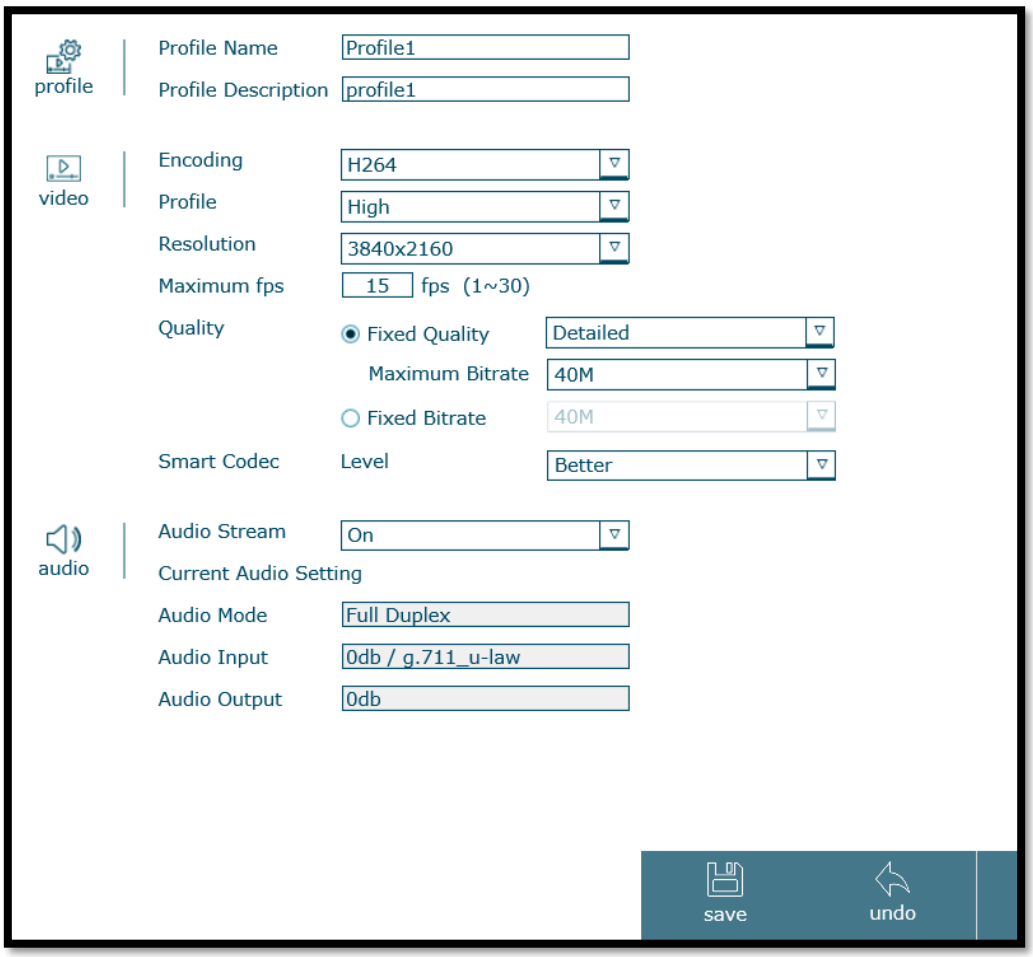


Image 9. Add/Edit profile page



a. Profile:

1	**Profile Name**	Profile1	Insert profile name, only allow characters 0-9, a-z, A-Z, ".", "_"
2	**Profile Description**	Profile1	Insert profile description, only allow characters 0-9, a-z, A-Z, ".", "_"

b. Video:

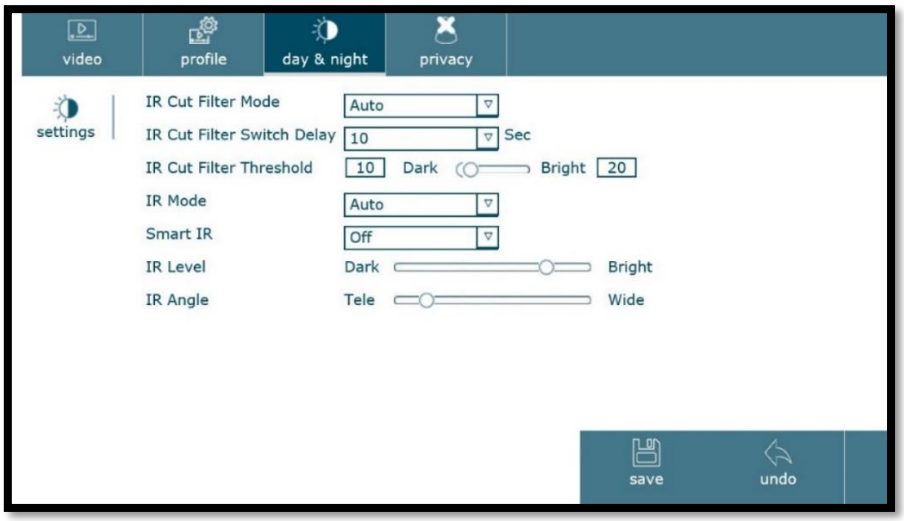
1	**Encoding**	H.264 H.265 MJPEG	The camera can encode video in different formats. Make sure that your video recorder supports the selected format.
2	**Profile**	Baseline Main High	Under H.264 there are three types of compression, users can choose as needed.
3	**Resolution**	Value from 3840x2160~640x360	Resolution will affect the image quality. Available resolution will depend on the profile.
4	**Maximum fps**	Value 1~60	Define the maximum number of frames per second for the profile. Maximum limit will depend on the encoding format.
5	**Quality**	Fixed Quality: Fixed Bitrate: Value from 32k~40M	Choose between Fixed Quality (VBR) and Fixed Bitrate (CBR). Fixed quality options includes: medium, standard, good, detailed and excellent. Fixed bitrate will ensure that the video bitrate does not surpass the specified maximum.
6	**Smart Codec**	Off Better Best	Smart codec further reduces bandwidth and storage requirement without compromising quality.

c. Audio:

1	**Audio Stream**	On Off	Choose to enable or disable the audio.
2	**Current Audio Setting**	Current Audio Setting	Display current audio setting, includes audio mode, audio input and audio output.

2. **Day/Night mode settings:** IR cut filter provides 4 different type of modes: auto, night mode, day mode and schedule.

Image 10. Day/night settings page



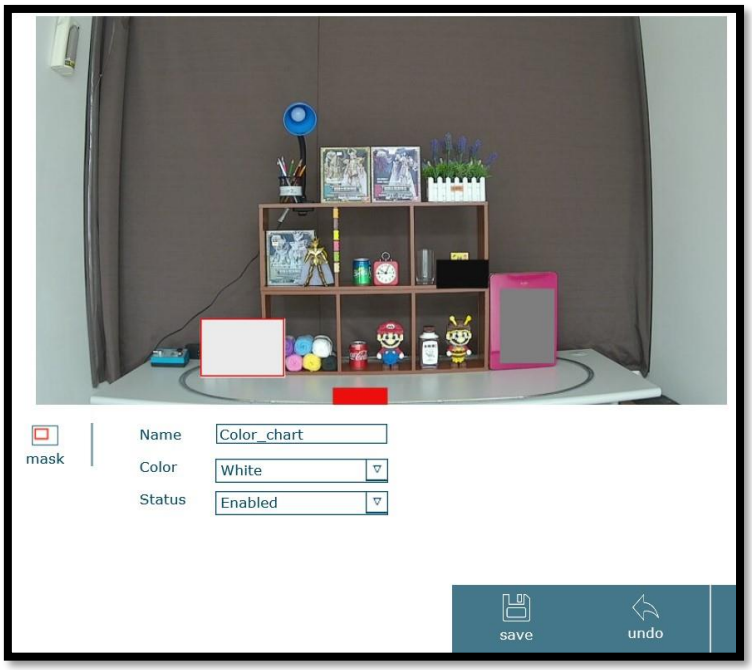
a. Settings

1	**IR Cut Filter Mode**	Auto	By selecting Auto the camera will automatically remove the IR cut filter based on the predefined threshold. On Night mode, the live view image will be black and white as the camera will always remove the IR cut filter regardless of the actual light levels. Opposite to night mode, the Day mode will never remove the IR cut filter from the image sensor allowing visible light to pass through the image, providing colored videos. Schedule mode allows users to program the time for the camera to engage in night mode.
		Night Mode	
		Day Mode	
		Schedule	
2	**IR Cut Filter Switch Delay**	Value 1~10 Sec	Define the duration to enable the IR cut filter to switch mode.
3	**IR Cut Filter Threshold**	Value 0~100	Define the threshold to enable the IR cut filter to switch mode.
4	**IR Mode**	Auto	Auto mode allows the IR to automatically turn on when the IR cut filter is removed. Active mode keeps the IR on regardless of the IR cut filter mode. This mode is not recommended unless the camera is installed in a dark environment that requires IR at all times. Inactive mode will disable the IR even if IR cut filter is removed. Select Schedule mode if you wish to program a specific time for the IR to turn on/off.
		Active	
		Inactive	
		Schedule	
5	**Smart IR**	On	This technology allows the IR to automatically adjust its intensity to the scene content, avoiding overexposure from happening.
		Off	
6	**IR Level/ Angle**	Dark Bright	Turn off smart IR to activate IR manual mode. The higher the IR level the brighter the image. The wider the IR angle the wider the illuminator area.
		Tele Wide	

3. **Privacy mask page:** allows users to set-up up to 5 privacy masks.

Image 11. Privacy mask page

Image 12. Add/Edit privacy mask page



a. Mask:

1	**Name**	Color_chart	Insert mask name, only allow characters 0-9, a-z, A-Z, "-", "_"
2	**Color**	Black Gray White Red	Users can select the mask color that best fit their needs.
3	**Status**	Disabled Enabled	Enable/ disable privacy mask.

How to setup privacy mask:

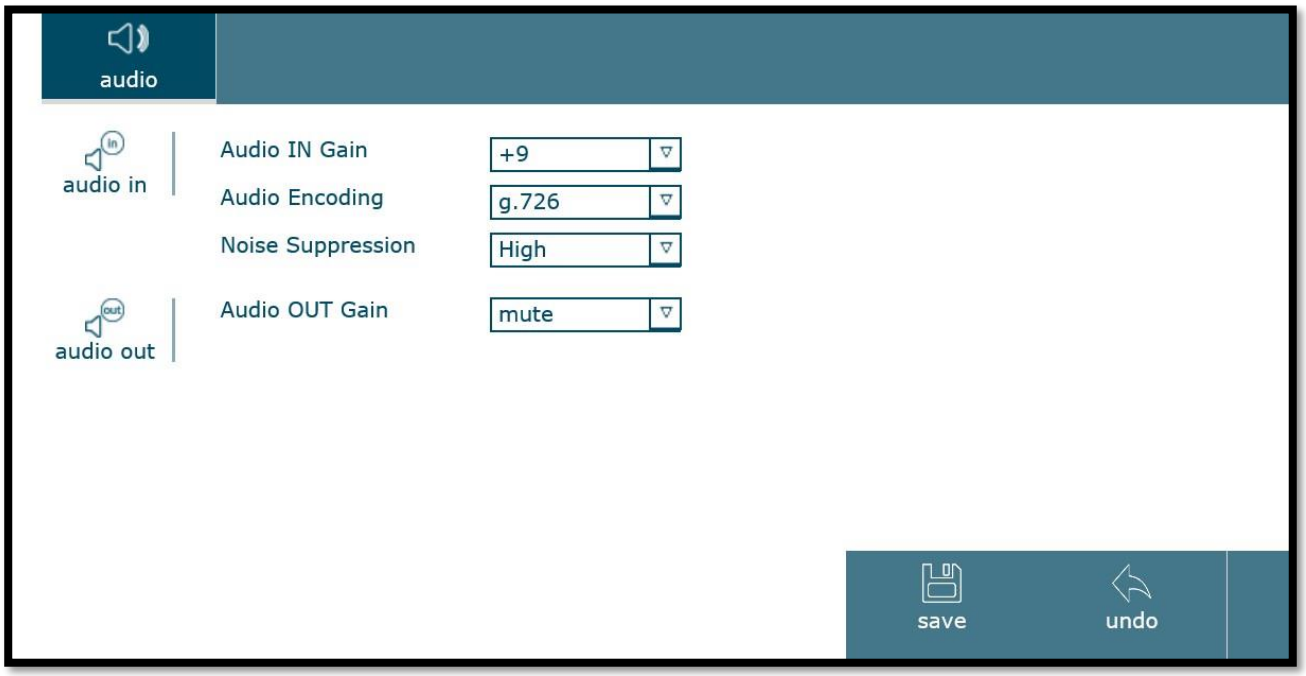
a. Step 1: Click add button
b. Step 2: Set up privacy mask area and key in the mask name
c. Step 3: Choose mask color: black, white, gray and red
d. Step 4: Select the status of the mask
e. Step 5: Click the save button

4.5 Audio

Note: Remember to click the save button to successfully apply changes.

• Audio page includes audio in and audio out settings.

Image 13. Audio page



a. Audio in:

1	**Audio In Gain**	From -12~12 and mute	Select the microphone input gain value from the drop-down menu.
2	**Audio Encoding**	g.711_u-law	Select the encoding from the drop-down menu.
		g.711_a-law	
		AMR	
		g.726	
3	**Noise Suppression**	High	Enable this feature to reduce background noise receive from audio in.
		Low	
		Off	

b. Audio out

1	**Audio Out Gain**	From -12~12 and mute	Select the speaker output gain value from the drop-down menu.

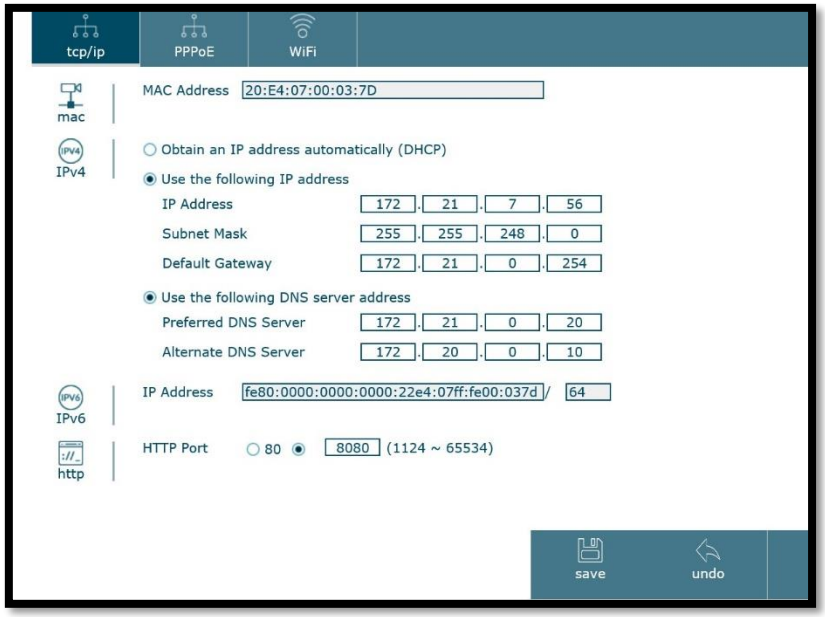
4.6 Network

Note: Remember to click the save button to successfully apply changes.

• Network page includes TCP/IP, PPPoE and WiFi:

1. TCP/IP settings:

Image 14. Network page



a. MAC:

1	**MAC Address**	20:E4:07:00:03:7D	Display the MAC address information.

b. IPv4:

1	**Obtain an IP address automatically(DHCP)**		Select this option to obtain an available dynamic IP address assigned by the DHCP server each time the camera is connected to the LAN.
2	**Use the following IP address**		Select this option to manually assign a static IP address to the Network Camera.
3	**Obtain DNS server address automatically**		Automatically use the DNS server settings provided by the DHCP server.
4	**Use the following DNS server address**		Select this option to assign a DNS server address. When DHCP is disabled, you also need to provide the camera with valid DNS settings.

c. IPv6:

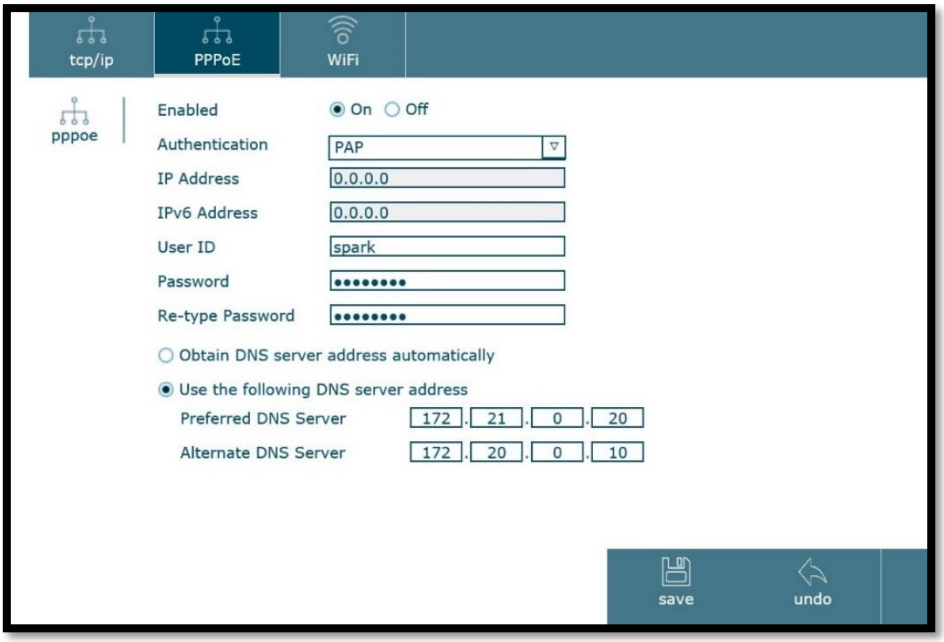
1	**IP Address**		The IPv6 IP address of camera is automatically assigned by converting the MAC address of the IP camera. Users are unable to modify it.

d. HTTP:

1	**HTTP Port**	Default:80 Value 1124~65534	The default value is 80. If you changed the HTTP port to a different value (e.g. 1024), please make sure to restart the camera (Settings > Advanced> Maintenance) and then connect to the camera using the following URL http://camera_ip:portnumber.

2. PPPoE page: allows users to configure PPPoE.

Image 15. PPPoE page



a. PPPoE:

1	**Enabled**	On	Users can enabled/ disabled this function.
		Off	
	Authentication	PAP	Select the authentication type.
		CHAP	
	IP Address	0.0.0.0	Displays the current IP address obtained from the Internet Service Provider (ISP). It will display 0.0.0.0 if the camera is not connected to the Internet via PPPoE.
	IPv6 Address	0.0.0.0	
	User ID	Spark	Enter the user ID for your DSL service. The user ID is provided by your ISP. Enter the password for the DSL account. Re-type the password in the field below.
	Password	••••••••	
	Re-type Password	••••••••	
	Obtain DNS server address automatically		Typically your ISP will send DNS Server information to the camera when it connects. However, please select "Use the following DNS server address" if your ISP requires entering specific DNS servers manually.
	Use the following DNS server address		

How to setup PPPoE:

a. Step 1: Enable the PPPoE function
b. Step 2: Choose authentication format
c. Step 3: Type in User ID and password
d. Step 4: Choose DNS server address
e. Step 5: Click the save button

3. WiFi page: allows users to configure WiFi.

Image 16. WiFi page

a. WiFi:

1	**Enabled**	On Off	Users can enabled/ disabled this function.
2	**MAC Address**	00:40:25:00:00:00	Display MAC address.
3	**IP Address**	0.0.0.0	Display IP address
4	**ESSID**	SparkAP	The Extended Service Set Identification (ESSID) is one of two types of Service Set Identification (SSID).
5	**Authentication**	Open WPA-PSK WPA2-PSK	WPA and WPA2 are the primary security algorithms for setting up a wireless network. They are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer network. TKIP and AES are encryption methods for the security protocols to further prevent attacks and intrusions. By choosing "open," no authentication will be required.
6	**Encryption**	TKIP AES	
7	**Passphrase**	••••••••	Insert the password.
8	**Re-type**	••••••••	

How to setup WiFi:

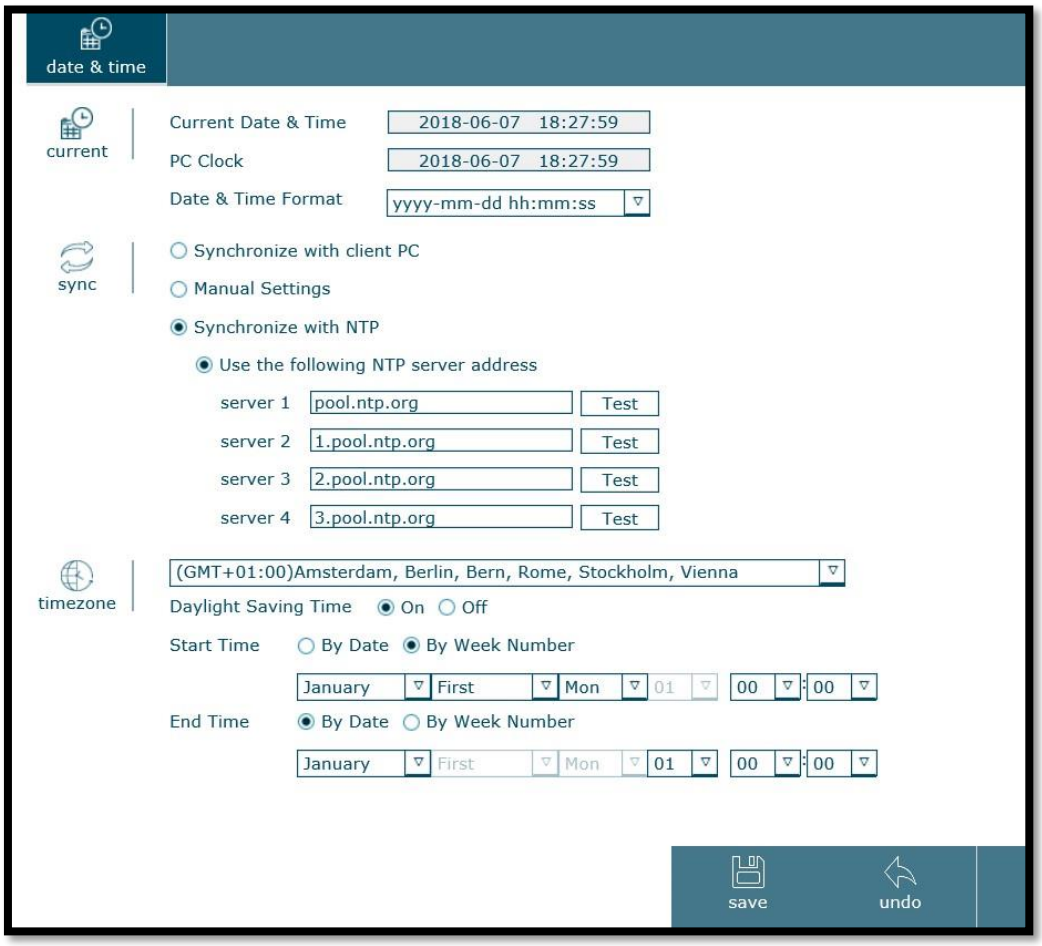
a. Step 1: Enable the WiFi function
b. Step 2: Key in ESSID
c. Step 3: Choose authentication format
d. Step 4: Choose the Encryption
e. Step 5: Type in password
f. Step 6: Click the save button

4.7 Date & Time

Note: Remember to click the save button to successfully apply changes.

• Date & Time allows users to see and configure current date and time.

Image 17. Date & time page



a. Current:

1	**Current Date & Time**	2018-06-07 18:27:59	Display IP camera current date & time
2	**PC Clock**	2018-06-07 18:27:59	Display PC current date & time
3	**Date & Time Format**	yyyy-mm-dd hh:mm:ss	Select the date & time format. The format in which the date and time is displayed on the live video.
		mm-dd-yyyy hh:mm:ss	
		dd-mm-yyyy hh:mm:ss	

b. Sync:

1	**Synchronize with client PC**	Synchronize with client PC	Select if you want to adjust the camera time to your PC. Note that this option synchronizes the time only once. An occasional re-synchronization will be necessary.

2	**Manual Settings**	Manual Settings	Select to manually enter the date and time.
3	**Synchronize with NTP**	Server1	Select to allow the camera to obtain the time from an NTP server. You can use the default value or you can enter a different NTP server manually. Make sure that your camera is connected to the Internet and that no firewall is blocking the outgoing NTP request.
		Server2	
		Server3	
		Server4	

c. Timezone:

1	**Timezone**		Select the correct time zone for your location.
2	**Daylight Saving Time**	On	Define the Daylight Saving Time range by activating this option. The camera will adjust the time depending on the predefined start and end time.
		Off	

4.8 Accounts

Note: Remember to click the save button to successfully apply changes.

• Admin can create up to 10 accounts with different privilege, to create an account, click the add button. To edit or remove an account, select the username on the account list and then click Edit or Remove as needed. Administrators account cannot be deleted.

1. Add accounts:

Image 18. Accounts page Image

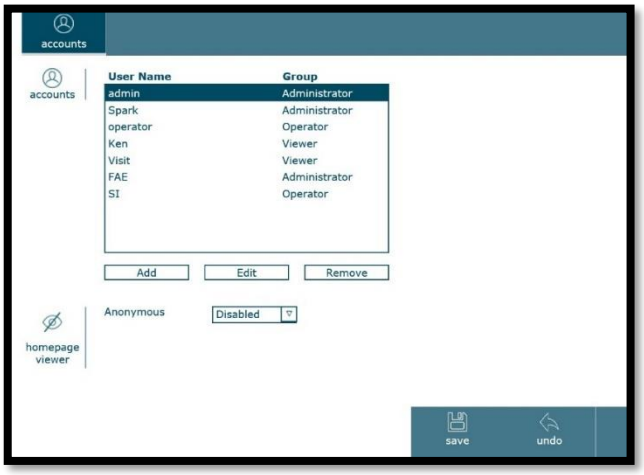
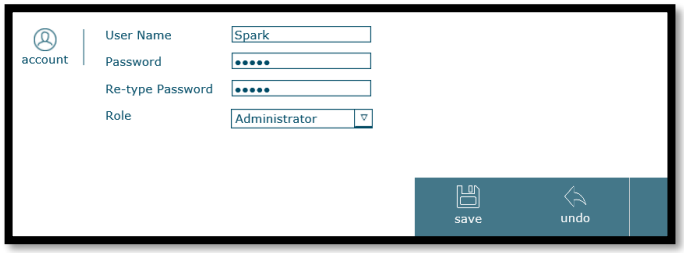


Image 19. Add/edit accounts page



a. Accounts:

1	**User Name**	Spark	Insert user name, only allow characters 0-9, a-z, A-Z, "-", "_"
2	**Password**	•••••	Password less than 4 characters in length
3	**Re-type password**		
4	**Role**	Viewer	There are three user levels: viewer, operator and administrator. The viewers only have access to the live view page of the camera. The operators have access to the live view page, as well as basic image settings (e.g.: brightness, contrast). Only the administrator has full access to the all camera settings.
		Operator	
		Administrator	
5	**Homepage viewer**	Anonymous	Enabling Anonymous Viewer will allow any user to access the live view page without signing in.

How to add account:

a. Step 1: Click add button
b. Step 2: Key in user name, password and choose the user role
c. Step 3: Choose to enable/disable anonymous viewer
d. Step 4: Click the save button

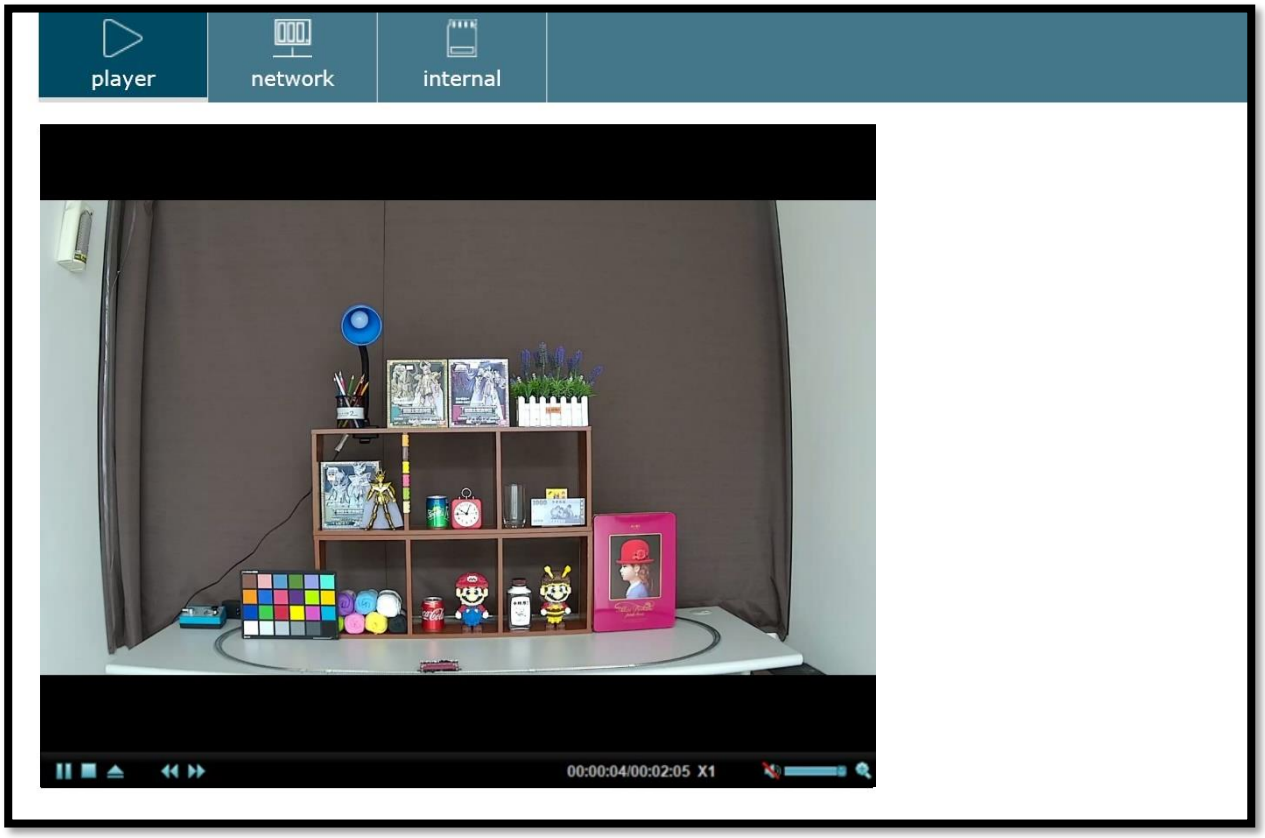
5. WEB USER INTERFACE-ADVANCED

5.1 Archive

• Archive functions include embedded player, network storage and internal storage.

1. Player:

Image 20. Player page



1		**Upload**	Upload the video file from local PC (Format *.mkv).
2		**Pause/Play**	Pause/Play video file.
3		**Stop**	Stop playing video file.
4		**Fast-forward/ Rewind playback**	Fast-forward or rewind playback. Fast-forward speed includes x2 and x4, rewind speed x1/2 and x1/4.
5		**Time stamp and speed**	Display current playing time and playing speed.
6		**Sound Mute/ Volume level**	Enable/disable the sound from the video and configure volume*.
7		**Zoom in**	Enable users to zoom in on any area of the video. Clicking the zoom in icon will open a small window facilating users to configure the zoom in rate and area. Click on the "T" (tele) and "W" (wide) to adjust the zoom. Click on  to close the window.

2. Network playback:

Please check that the network storage is connected.

- Videos successfully saved in the network storage are shown in order of old to new.

Image 21. Network page_1

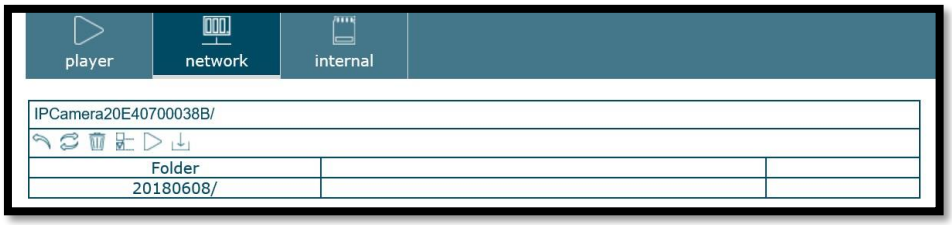


Image 22. Network page_2

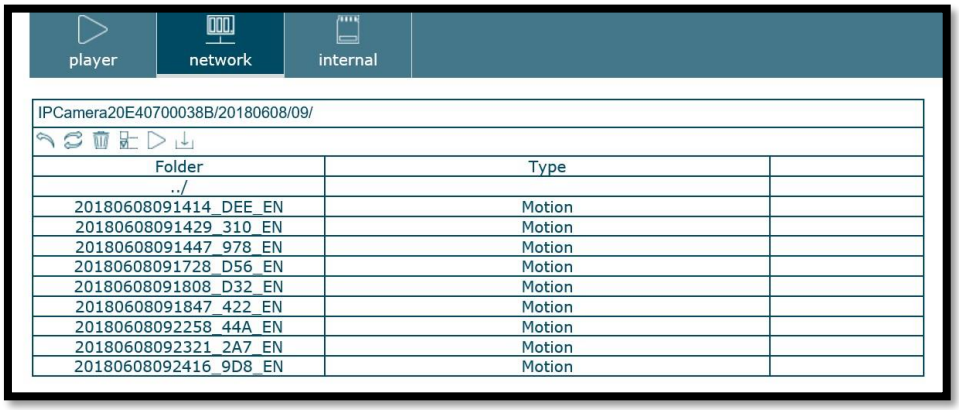
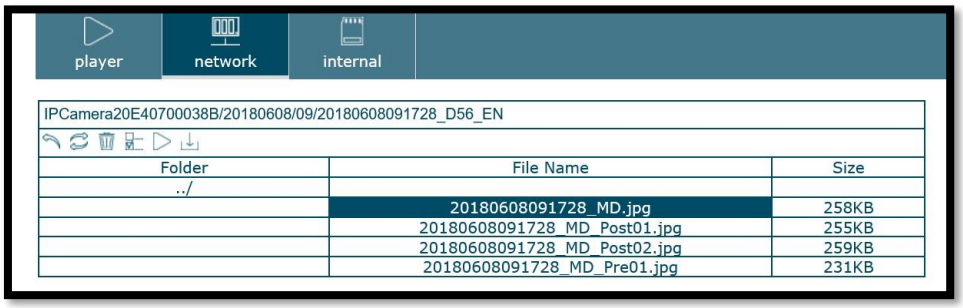


Image 23. Network page_3



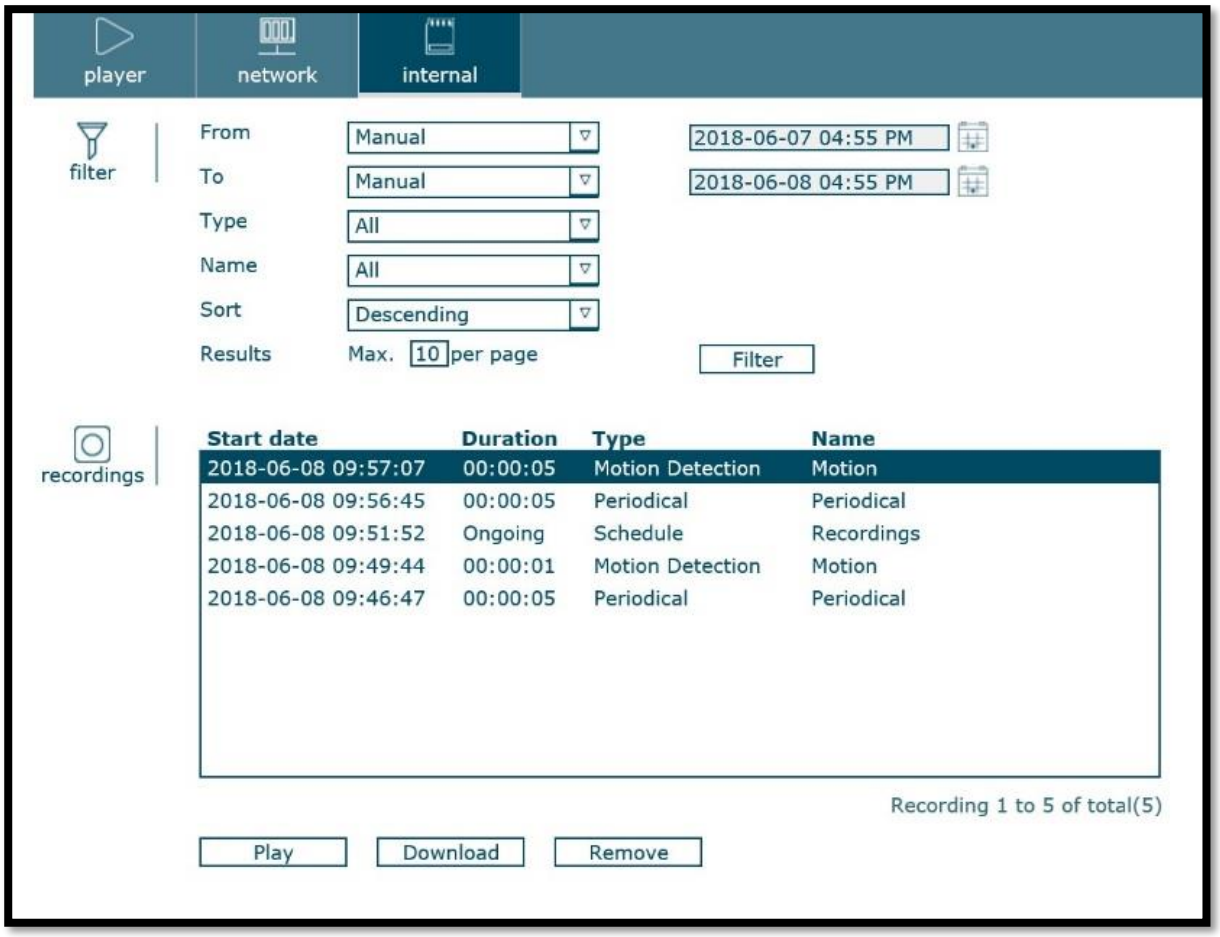
1		**Return**	Go back to the upper level folder.
2		**Refresh**	Refresh the view.
3		**Delete**	Delete the selected file.
4		**Select all**	Select all items in the folder.
5		**Play**	Playback the selected video
6		**Download**	Download selected item to your computer.

3. Internal playback:

Please check that the SD card is inserted.

Users may select search filter according to the search requirements, and may also choose to play, download or remove file.

Image 24. Internal page



a. Filter:

1	**From**	First Recording	Users can manualy set the start time search criteria or select first recording.
		Manual	
2	**To**	Now	Users can manualy set the end time search criteria or select now.
		Manual	
3	**Type**	All	Users can select the event type search criteria.
		Motion Detection	
		Audio Detection	
		Tampering Detection	
		Tripwire Detection	
		Perimeter Detection	

		Crowd	
		Digital Input	
		Periodical	
		Network Link Down	
		Schedule	
4	**Name**	All	Users can search by file name.
5	**Sort**	Descending	Users can arrange the search by alphabetical order.
		Ascending	
6	**Results**	Value 1~20	Users can choose the numbers of results on the page.

b. Recordings:

1	**Start Date**	2018-06-08 09:46:47	Display the recording file date and time.
2	**Duration**	00:00:05	Display the length of the video.
3	**Type**	Periodical	Display the event type of the video.
4	**Name**	Periodical	Display the name of the video.

5.2 Recording servers

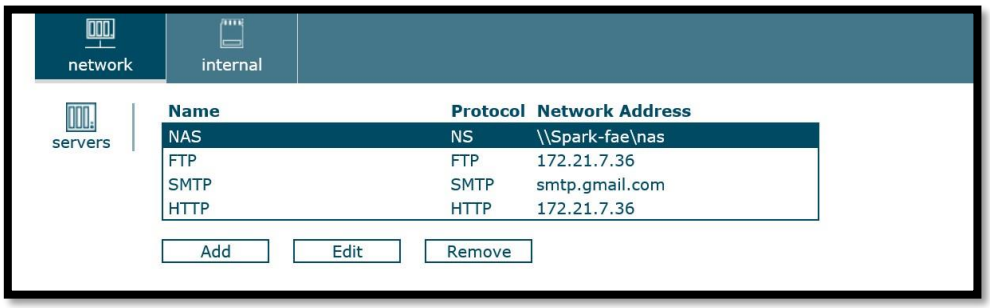
Note: Remember to click the save button to successfully apply changes.

• Recording server page includes network storage and internal storage settings.

• Click the add button to create a new server. A window will prompt requesting the server's information. First fill in the name of the server and then select the server type.

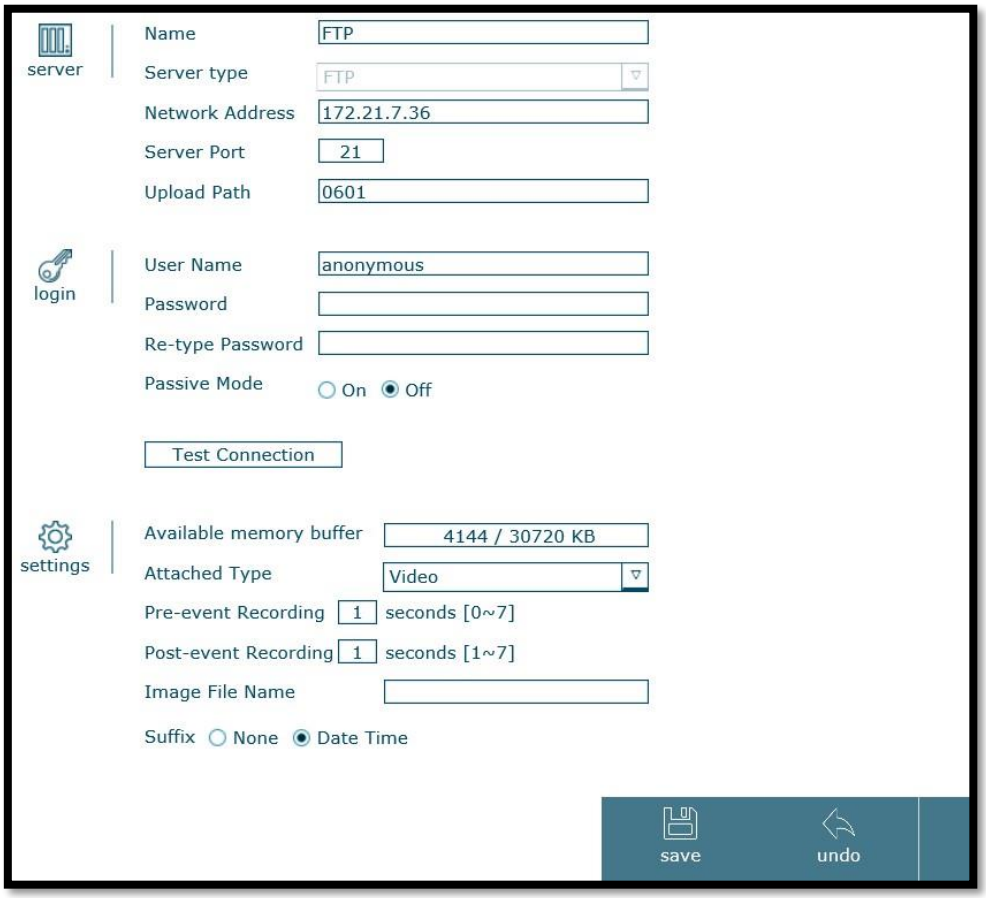
1. **Network server:** users can add, edit and remove network storage. Network server type includes FTP, SMTP, HTTP, HTTPS and Network storage.

Image 25. Network server page



1.1. FTP server:

Image 26. FTP server page



a. Server:

1	**Name**		Insert FTP server name, only allow characters 0-9, a-z, A-Z, “.”, “_”
2	**Server type**	FTP	Select FTP server.
3	**Network address**	172.21.7.36	Insert the FTP network’s address.
4	**Server port**	21	Default is 21. Change only if your FTP server uses a different port.
5	**Upload path**	0601	Provide the upload path.

b. Login:

1	**User name**	anonymous	Provide valid login credentials for the FTP server.
2	**Password**	•••••	
3	**Re-type password**		
4	**Passive mode**	On	Enable if your FTP server utilizes passive FTP, which is the most common method.
		Off	
5	**Test connection**	Test Connection	Click test connection button to check if the FTP server is connected, If the connection is successful, a window will pop-out.

c. Settings:

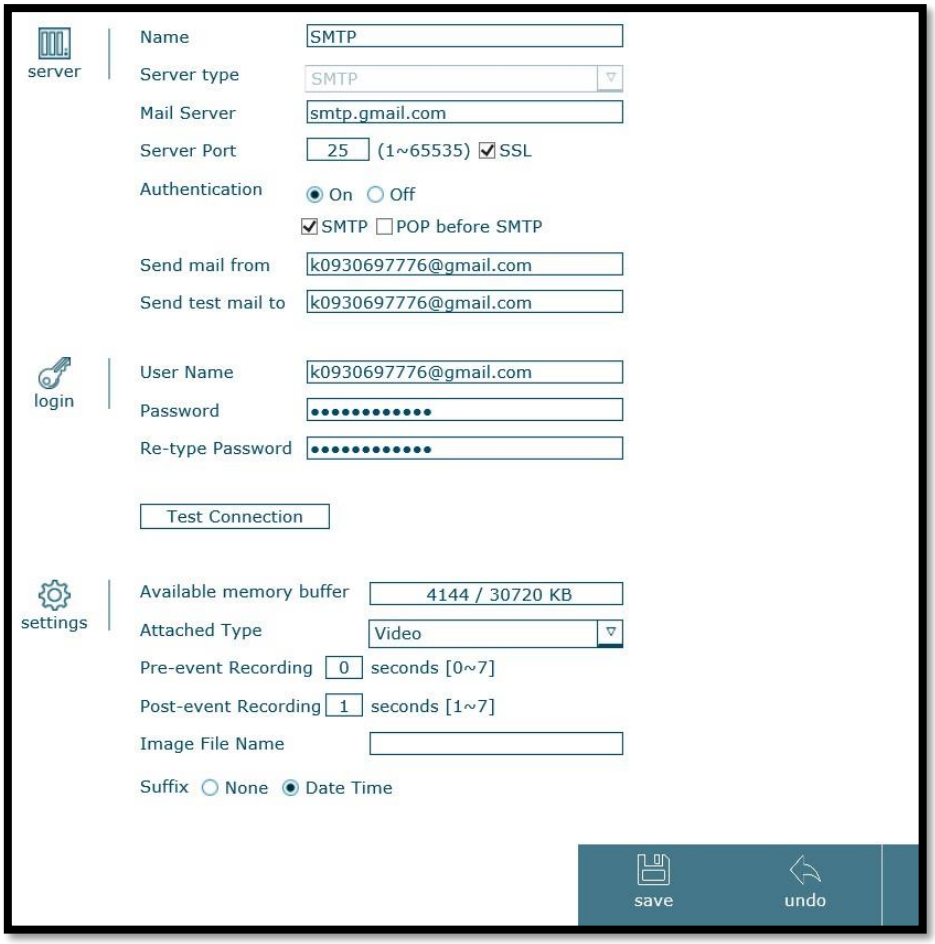
1	**Available memory buffer**	4144 / 30720 KB	The camera will reserve a buffer in its memory for the recording and snapshot. This section displays the remaining available memory.
2	**Attached type**	Video	Select attached format.
		Snapshot	
3	**Pre-event Recording seconds/ Send Image**	0~7 recording seconds/ 0~7 images	Select the start time for recording/ snapshot prior to event.
4	**Post-event Recording seconds/ Send Image**	0~7 recording seconds/ 0~7 images	Select the end time for recording/ snapshot subsequent to event.
5	**Image file name**		Insert Image file name, only allow characters 0-9, a-z, A-Z, “.”, “_”
6	**Suffix**	None	Allows users to add date time to the file name.
		Date Time	

How to create FTP server:

a. Step 1: Key in FTP server information
b. Step 2: Configure login details
c. Step 3: Click “Test Connection” to make sure the server is detected
d. Step 4: Choose the attached type and configure related settings
e. Step 5: Click the save button

1.2. SMTP server:

Image 27. SMTP server page



a. Server:

1	**Name**		Insert SMTP server name, only allow characters 0-9, a-z, A-Z, ".", "_"
2	**Server type**	SMTP	Select SMTP server.
3	**Mail Server**	smtp.gmail.com	Insert mail server's address.
4	**Server port**	25 (1~65535) SSL	Standard value is 25, but your server may be using different values.
5	**Authentication**	On (SMTP/ POP)	Enable if server requires authentication in for sending email.
		Off	
6	**Send mail from**	k0930697776@gmail.com	Insert the address from which the camera will send the emails. It does not necessarily need to be a valid email.
7	**Send test mail to**	k0930697776@gmail.com	Insert a valid email address to test the above settings. If the test succeeds, proceed to provide the information for the media settings. The actual recipient email address is defined when setting up the event in the next section.

b. Login:

1	**User name**		Provide valid login credentials for the SMTP server. For user name and password, please insert the sender's e-mail address and password.
2	**Password**		
3	**Re-type password**		
4	**Test connection**	Test Connection	Click test connection button to check if the SMTP server is connected, If the connection is successful, a window will pop-out.

c. Settings:

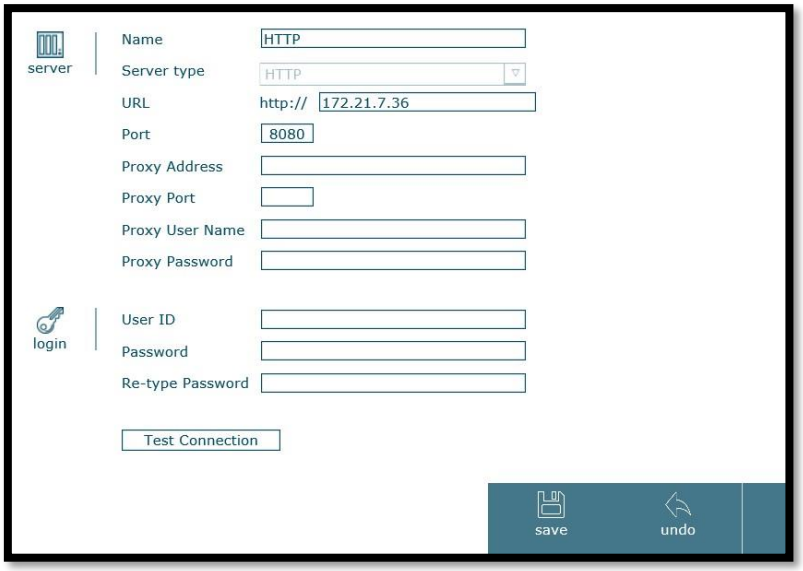
1	**Available memory buffer**	4144 / 30720 KB	The camera will reserve a buffer in its memory for the recording and snapshot. This section displays the remaining available memory.
2	**Attached type**	Video	Select attached format.
		Snpshot	
3	**Pre-event Recording seconds/ Send Image**	0~7 recording seconds/ 0~7 images	Select the start time for recording/ snapshot prior to event.
4	**Post-event Recording seconds/ Send Image**	0~7 recording seconds/ 0~7 images	Select the end time for recording/ snapshot subsequent to event.
5	**Image file name**		Insert Image file name, only allow characters 0-9, a-z, A-Z, ".", "_"
6	**Suffix**	None	Allows users to add date time to the file name.
		Date Time	

How to create SMTP server:

a. Step 1: Key in SMTP server information
b. Step 2: Key in login details
c. Step 3: Click "Test Connection" to make sure the server is detected
d. Step 4: Choose the attached type and configure related settings
e. Step 5: Click the save button

1.3. HTTP server:

Image 28. HTTP server page



a. Server:

1	**Name**		Insert HTTP server name, only allow characters 0-9, a-z, A-Z, ".", "_"
2	**Server type**	HTTP	Select HTTP server.
3	**URL**	http:// 172.21.7.36	Insert HTTP's address.
4	**Port**	8080	Insert HTTP's port.
5	**Proxy Address**		Insert proxy address.
6	**Proxy Port**		Insert proxy port.
7	**Proxy User Name**		If the proxy is not free, please insert user name and password.
8	**Proxy Passoword**		

b. Login:

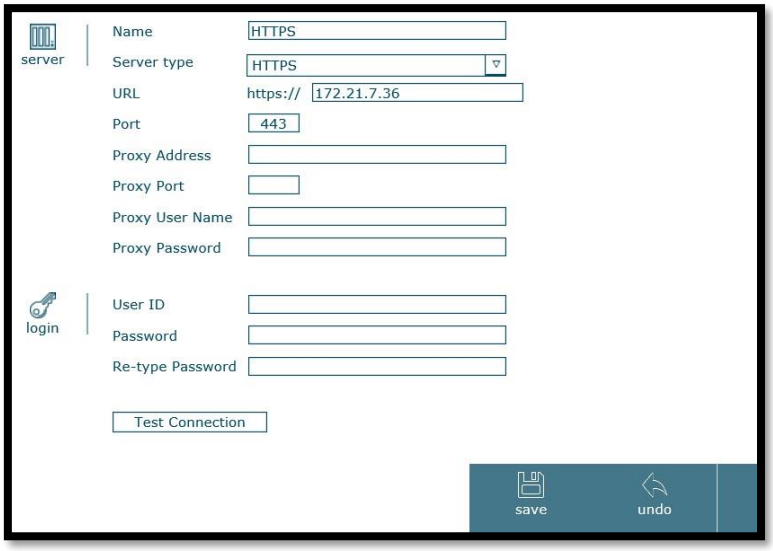
1	**User ID**		Provide valid login credentials for the HTTP server.
2	**Password**		
3	**Re-type password**		
4	**Test connection**	Test Connection	Click test connection button to check if the HTTP server is connected, If the connection is successful, a window will pop-out.

How to create HTTP server:

a. Step 1: Key in HTTP server information
b. Step 2: Key in login details
c. Step 3: Click "Test Connection" to make sure the server is detected
d. Step 4: Click the save button

1.4. HTTPS server:

Image 29. HTTPS server page



a. Server:

1	**Name**		Insert HTTPS server name, only allow characters 0-9, a-z, A-Z, ".", "_"
2	**Server type**	HTTPS	Select HTTPS server.
3	**URL**	http:// 172.21.7.36	Insert HTTP's address.
4	**Port**	443	Insert HTTP's port.
5	**Proxy Address**		Insert proxy address.
6	**Proxy Port**		Insert proxy port.
7	**Proxy User Name**		If the proxy is not free, please insert user name and password.
8	**Proxy Passoword**		

b. Login:

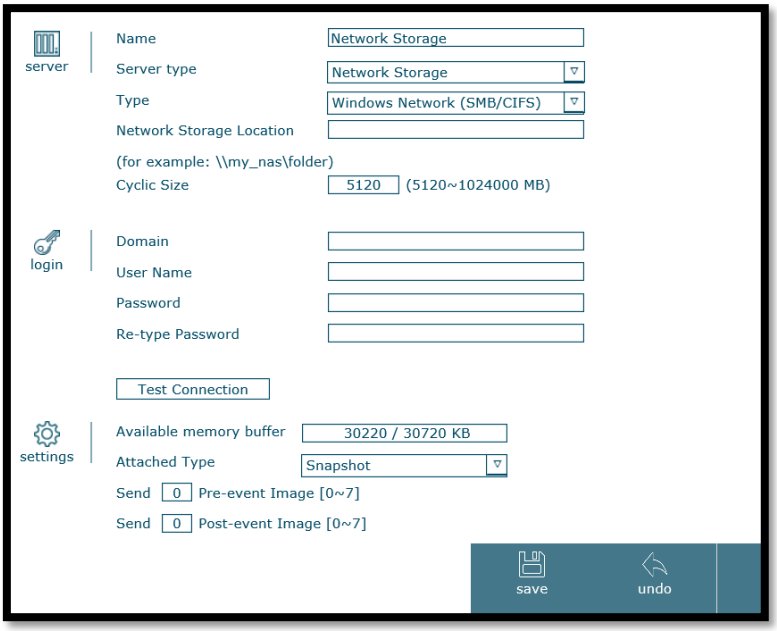
1	**User ID**		Provide valid login credentials for the HTTPS server.
2	**Password**		
3	**Re-type password**		
4	**Test connection**	Test Connection	Click test connection button to check if the HTTPS server is connected, If the connection is successful, a window will pop-out.

How to create HTTPS server:

a. Step 1: Key in HTTPS server information
b. Step 2: Key in login details
c. Step 3: Click "Test Connection" to make sure the server is detected
d. Step 4: Click the save button

1.5. Network Storage:

Image 30. Network storage page



a. Server:

1	**Name**		Insert Network Storage server name, only allow characters 0-9, a-z, A-Z, ".", "_"
2	**Server type**	Network Storage	Select Network Storage server.
3	**Type**	Windows Network(SMB/CIFS) Network File System(NFS)	Select the network storage type (Windows SMB/ CIFS or Linux NFS).
4	**Network Storage Location**		Insert the address of your local storage server.
5	**Cyclic Size**	5120~1024000MB	Insert limit for the file size.

b. Login:

1	**Domain**		Insert network storage domain.
2	**User Name**		Provide valid login credentials for the network storage server.
3	**Password**		
4	**Re-type password**		
5	**Test connection**	Test Connection	Click test connection button to check if the Network Storage server is connected, If the connection is successful, a window will pop-out.

c. Settings:

1	**Available memory buffer**	4144 / 30720 KB	The camera will reserve a buffer in its memory for the recording and snapshot. This section displays the
2	**Attached type**	Video	Select attached format.
		Snpshot	
3	**Pre-event Recording seconds/ Send Image**	0~7 recording seconds/ 0~7 images	Select the start time for recording/ snapshot prior to event.
4	**Post-event Recording seconds/ Send Image**	0~7 recording seconds/ 0~7 images	Select the end time for recording/ snapshot subsequent to event.

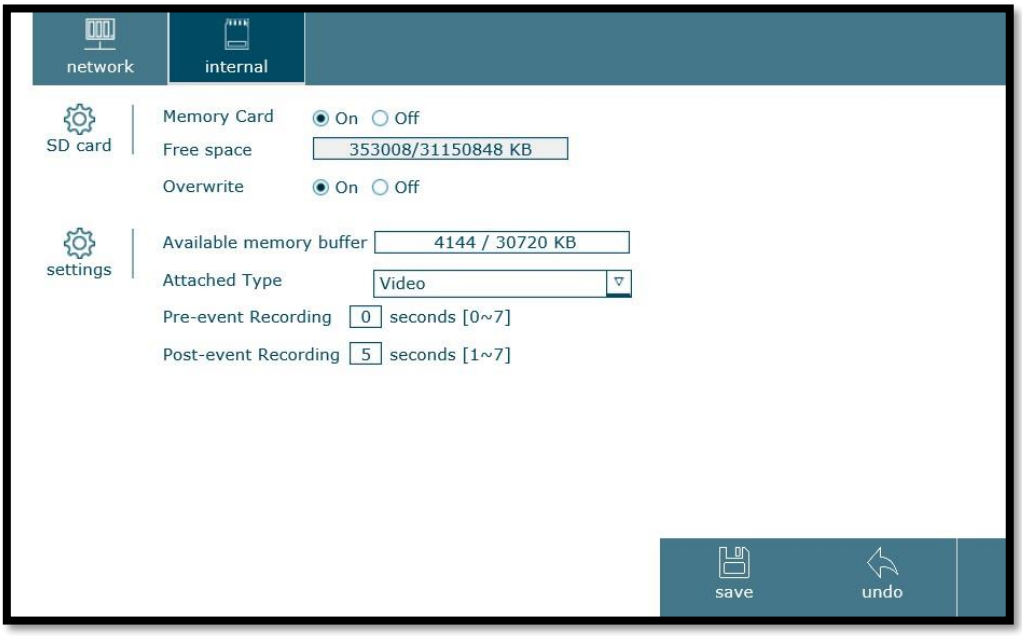
How to create Network storage:

a. Step 1: Key in Network Storage server information
b. Step 2: Key in login details
c. Step 3: Click "Test Connection" to make sure the server is detected
d. Step 4: Click the save button

2. Internal SD card settings:

Please check that the SD card is inserted.

Image 31. SD card page



a. SD card:

1	**Memory Card**	On Off	This feature is only available if the memort card is inserted.
2	**Free space**	353008/31150848 KB	Display the total amount of space on the micro SD card and the available memory.
3	**Overwrite**	On Off	Enabling this feature will allow the camera to overwrite the old recordings with new one.

b. Settings:

1	**Available memory buffer**	4144 / 30720 KB	The camera will reserve a buffer in its memory for the recording and snapshot. This section displays the remaining available memory.
2	**Attached type**	Video Snpshot	Select attached format.
3	**Pre-event Recording seconds/ Send Image**	0~7 recording seconds/ 0~7 images	Select the start time for recording/ snapshot prior to event.
4	**Post-event Recording seconds/ Send Image**	0~7 recording seconds/ 0~7 images	Select the end time for recording/ snapshot subsequent to event.

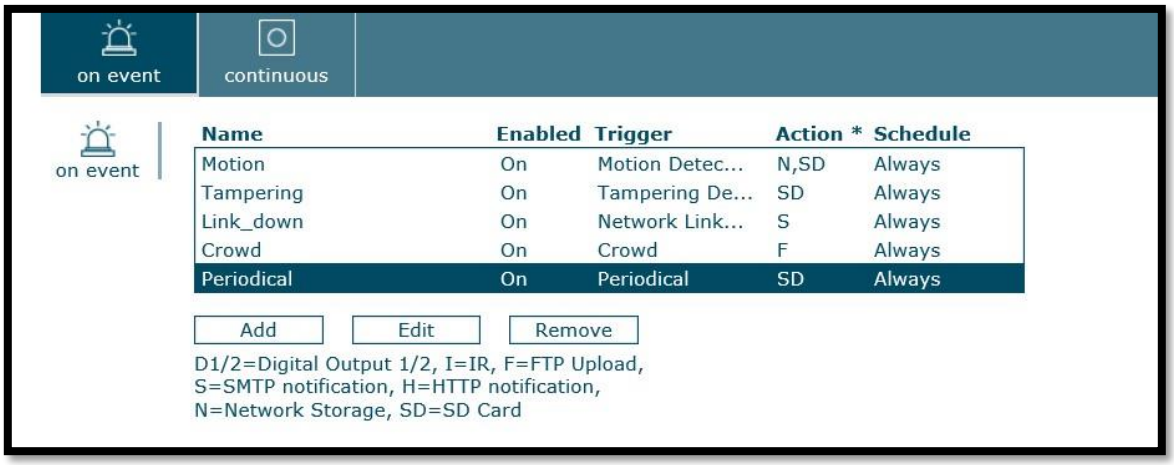
5.3 Recordings

Note: Remember to click the save button to successfully apply changes.

• Recording page includes on event recording and continuous recording settings.

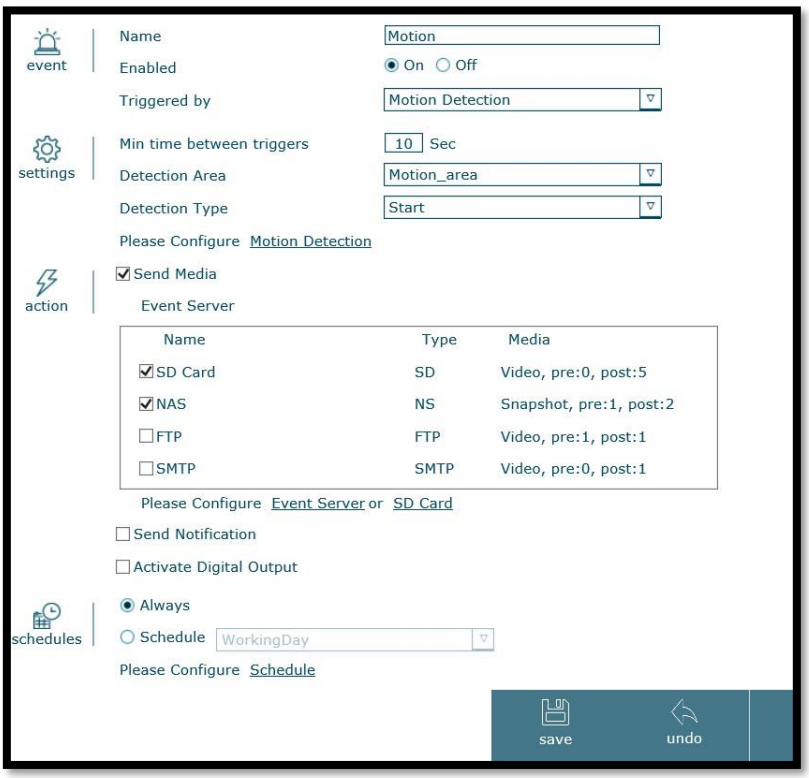
1. **On event** recording allows users to set-up 9 different types of event recording: motion detection, audio detection, tampering detection, tripwire detection, perimeter detection, crowd, digital input, periodical and network link down.

Image 32. Recordings page



1.1. Motion Recording:

Image 33. Motion recording page



a. Event:

1	**Name**		Insert Motion detection event name, only allow characters 0-9, a-z, A-Z, ".", "_"
2	**Enabled**	On Off	Users can enabled/ disabled this function.
3	**Triggered by**	Motion Detection	Select the motion detection as the trigger event type.

b. Settings:

1	**Min time between triggers**	Value 1~999 sec	Minimum interval for an event to trigger the next action.
2	**Detection Area**	Motion_area	Select the motion detection area for the trigger action. If no motion detection area was added on the analytics page, detection area will appear as none.
3	**Detection Type**	Start Stop	Select when to initiate the trigger event.
4	**Please Configure Motion Detection**	Please Configure Motion Detection	Click on Motion Detection to go to motion detection configuration page.

c. Action:

1	**Send Media**	Event Server SD Card	Instructs the camera to send out media. You will need to specify whether you want to use FTP, network storage or SD card. Make sure that the servers are set up before using it.
2	**Send Notification**	HTTP HTTPS	This action type uses the HTTP and HTTPS recording server. You can use this to have the camera trigger a script on a server.
3	**Activate Digital Output**	Digital Output1	Allows you to perform an action with the camera's digital output. You may also specify the duration you want the camera to trigger the event.

d. Schedules:

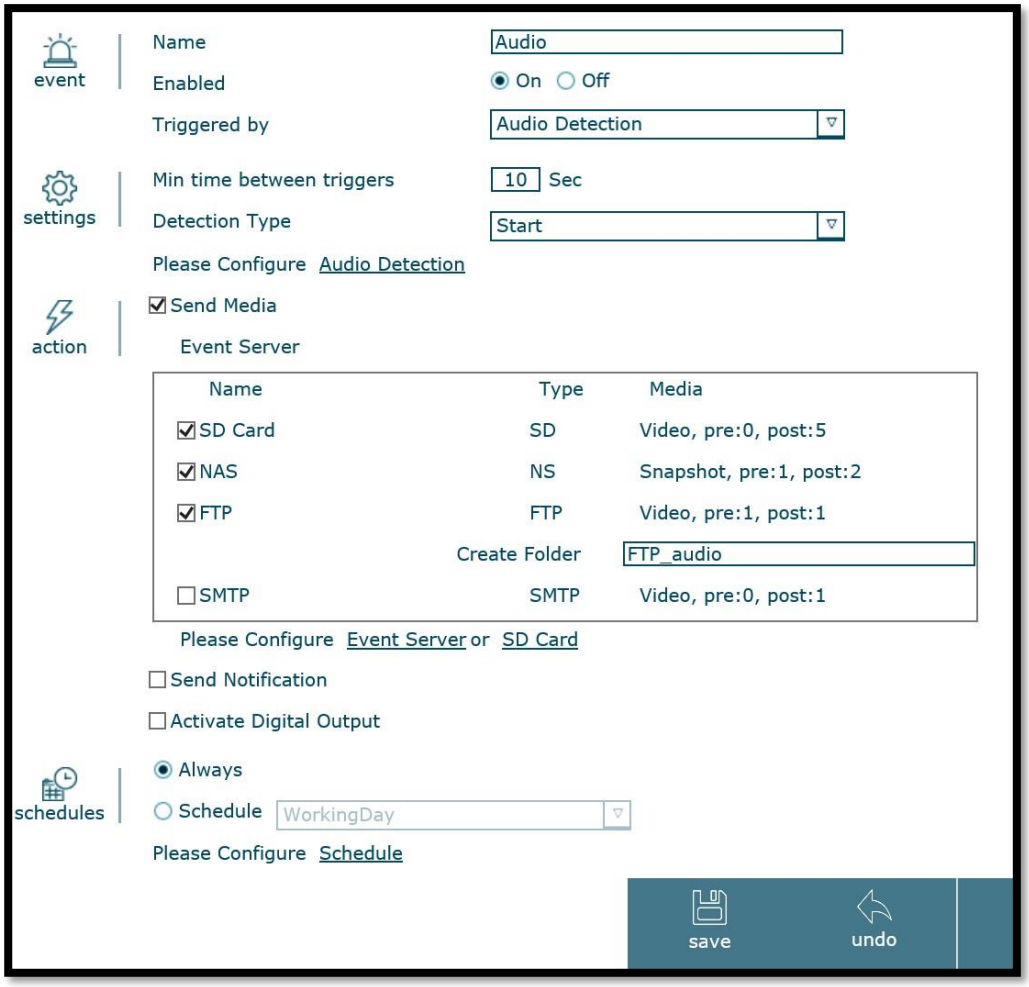
1	**Always**	Always	Select the schedule for the above Event settings to be active. You may choose one of the available or schedule, or configure another schedule on the schedule menu.
2	**Schedule**	Schedule	
3	**Please Configure Schedule**	Please Configure Schedule	Click on Schedule to go to schedule configuration page.

How to create Motion recording:

a. Step 1: Key in event name and enable motion detection
b. Step 2: Configure motion detection settings. Remember to first add motion detection area on the analytics page or click the link provided "motion detection."
c. Step 3: Select the action type after event triggered. Action options includes send media to event server, send notification to HTTP/HTTPS server and activation of digital output.
d. Step 4: Select motion detection recording schedule
e. Step 5: Click the save button

1.2. Audio Recording:

Image 34. Audio recording page



a. Event:

1	**Name**		Insert Audio recording event name, only allow characters 0-9, a-z, A-Z, ".", "_"
2	**Enabled**	On	Users can enabled/ disabled this function.
		Off	
3	**Triggered by**	Audio Detection	Select the audio detection as the trigger event type.

b. Settings:

1	**Min time between triggers**	Value 1~999 sec	Minimum interval for an event to trigger the next action.
2	**Detection Type**	Start	Select when to initiate the trigger event.
		Stop	
3	**Please Configure Audio Detection**	Please Configure Audio Detection	Click on Audio Detection to go to audio detection configuration page.

c. Action:

1	**Send Media**	Event Server	Instructs the camera to send out media. You will need to specify whether you want to use FTP, network storage or SD card. Make sure that the servers are set up before using it.
		SD Card	
2	**Send Notification**	HTTP	This action type uses the HTTP and HTTPS recording server. You can use this to have the camera trigger a script on a server.
		HTTPS	
3	**Activate Digital Output**	Digital Output1	Allows you to perform an action with the camera's digital output. You may also specify the duration you want the camera to trigger the event.

d. Schedules:

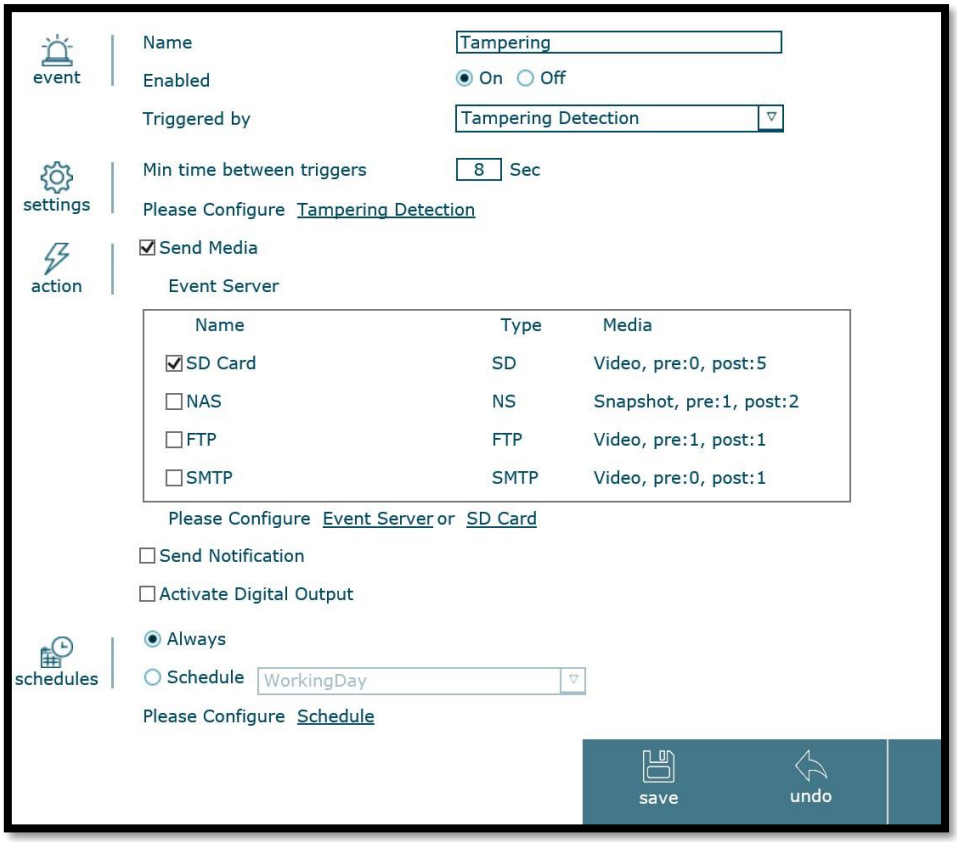
1	**Always**	Always	Select the schedule for the above Event settings to be active. You may choose one of the available or schedule, or configure another schedule on the schedule menu.
2	**Schedule**	Schedule	
3	**Please Configure Schedule**	Please Configure Schedule	Click on Schedule to go to schedule configuration page.

How to create Audio recording:

a. Step 1: Key in event name and enable audio detection
b. Step 2: Configure audio detection settings. Remember to first enable audio detection on the analytics page or click the link provided "audio detection."
c. Step 3: Select the action type after event triggered. Action options includes send media to event server, send notification to HTTP/HTTPS server and activation of digital output.
d. Step 4: Select audio detection recording schedule
e. Step 5: Click the save button

1.3. Tampering Recording:

Image 35. Tampering recording page



a. Event:

1	**Name**		Insert Tampering recording event name, only allow characters 0-9, a-z, A-Z, ".", "_"
2	**Enabled**	On	Users can enabled/ disabled this function.
		Off	
3	**Triggered by**	Tampering Detection	Select the tampering detection as the trigger event type.

b. Settings:

1	**Min time between triggers**	Value 1~999 sec	Minimum interval for an event to trigger the next action.
2	**Please Configure Tampering Detection**	Please Configure Tampering Detection	Click on Tampering Detection to go to tampering detection configuration page.

c. Action:

1	**Send Media**	Event Server	Instructs the camera to send out media. You will need to specify whether you want to use FTP, network storage or SD card. Make sure that the servers are set up before using it.
		SD Card	
2	**Send Notification**	HTTP	

		HTTPS	This action type uses the HTTP and HTTPS recording server. You can use this to have the camera trigger a script on a server.
3	**Activate Digital Output**	Digital Output1	Allows you to perform an action with the camera's digital output. You may also specify the duration you want the camera to trigger the event.

d. Schedules:

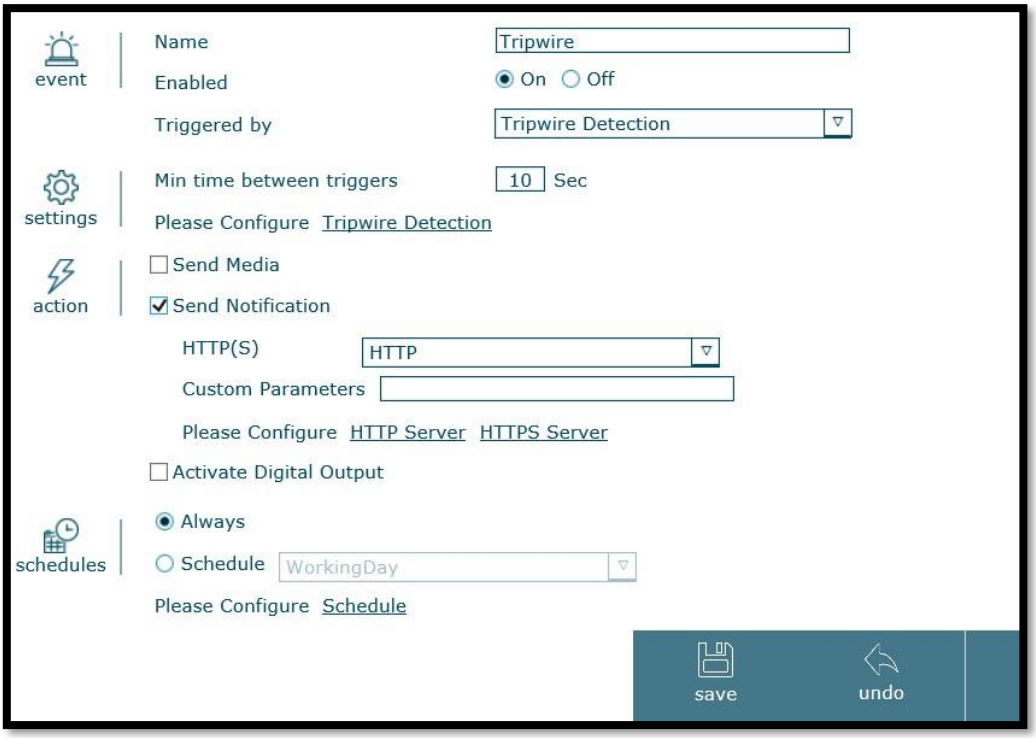
1	**Always**	Always	Select the schedule for the above Event settings to be active. You may choose one of the available or schedule, or configure another schedule on the schedule menu.
2	**Schedule**	Schedule	
3	**Please Configure Schedule**	Please Configure Schedule	Click on Schedule to go to schedule configuration page.

How to create Tampering recording:

a. Step 1: Key in event name and enable tampering detection
b. Step 2: Configure tampering detection settings. Remember to first enable tampering detection on the analytics page or click the link provided "tampering detection."
c. Step 3: Select the action type after event triggered. Action options includes send media to event server, send notification to HTTP/HTTPS server and activation of digital output.
d. Step 4: Select tampering detection recording schedule
e. Step 5: Click the save button

1.4. Tripwire Recording:

Image 36. Tripwire recording page



a. Event:

1	**Name**		Insert Tripwire recording event name, only allow characters 0-9, a-z, A-Z, ".", "_"
2	**Enabled**	On	Users can enabled/ disabled this function.
		Off	
3	**Triggered by**	Tripwire Detection	Select the tripwirre detection as the trigger event type.

b. Settings:

1	**Min time between triggers**	Value 1~999 sec	Minimum interval for an event to trigger the next action.
2	**Please Configure Tripwire Detection**	Please Configure Tripwire Detection	Click on Tripwire Detection to go to tripwire detection configuration page.

c. Action:

1	**Send Media**	Event Server	Instructs the camera to send out media. You will need to specify whether you want to use FTP, network storage or SD card. Make sure that the servers are set up before using it.
		SD Card	
2	**Send Notification**	HTTP	This action type uses the HTTP and HTTPS recording server. You can use this to have the camera trigger a script on a server.
		HTTPS	

3	**Activate Digital Output**	Digital Output1	Allows you to perform an action with the camera's digital output. You may also specify the duration you want the camera to trigger the event.

d. Schedules:

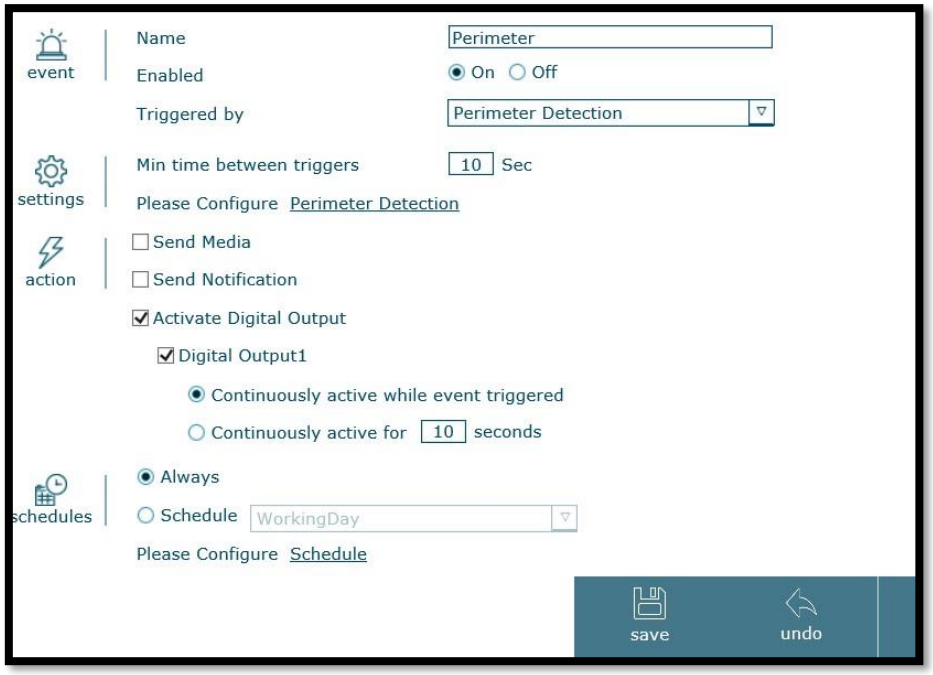
1	**Always**	Always	Select the schedule for the above Event settings to be active. You may choose one of the available or schedule, or configure another schedule on the schedule menu.
2	**Schedule**	Schedule	
3	**Please Configure Schedule**	Please Configure Schedule	Click on Schedule to go to schedule configuration page.

How to create Tripwire recording:

a. Step 1: Key in event name and enable tripwire detection
b. Step 2: Configure tripwire detection settings. Remember to first add tripwire detection on the analytics page or click the link provided "tripwire detection."
c. Step 3: Select the action type after event triggered. Action options includes send media to event server, send notification to HTTP/HTTPS server and activation of digital output.
d. Step 4: Select tripwire detection recording schedule
e. Step 5: Click the save button

1.5. Perimeter Recording:

Image 37. Perimeter recording page



a. Event:

1	**Name**		Insert Perimeter recording event name, only allow characters 0-9, a-z, A-Z, ".", "_"
2	**Enabled**	On	Users can enabled/ disabled this function.
		Off	
3	**Triggered by**	Perimeter Detection	Select the perimeter detection as the trigger event type.

b. Settings:

1	**Min time between triggers**	Value 1~999 sec	Minimum interval for an event to trigger the next action.
2	**Please Configure Perimeter Detection**	Please Configure Perimeter Detection	Click on Perimeter Detection to go to perimeter detection configuration page.

c. Action:

1	**Send Media**	Event Server	Instructs the camera to send out media. You will need to specify whether you want to use FTP, network storage or SD card. Make sure that the servers are set up before using it.
		SD Card	
2	**Send Notification**	HTTP	This action type uses the HTTP and HTTPS recording server. You can use this to have the camera trigger a script on a server.
		HTTPS	

3	**Activate Digital Output**	Digital Output1	Allows you to perform an action with the camera's digital output. You may also specify the duration you want the camera to trigger the event.

d. Schedules:

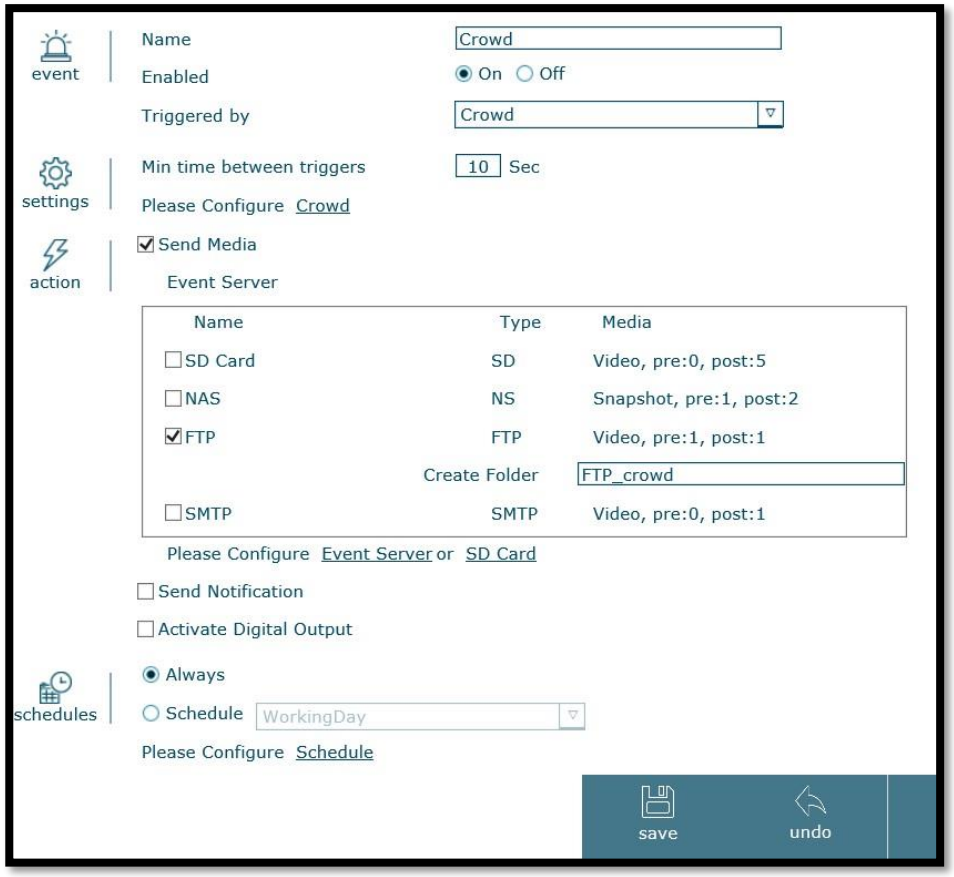
1	**Always**	Always	Select the schedule for the above Event settings to be active. You may choose one of the available or schedule, or configure another schedule on the schedule menu.
2	**Schedule**	Schedule	
3	**Please Configure Schedule**	Please Configure Schedule	Click on Schedule to go to schedule configuration page.

How to create Perimeter recording:

a. Step 1: Key in event name and enable perimeter detection
b. Step 2: Configure perimeter detection settings. Remember to first add perimeter detection area on the analytics page or click the link provided "perimeter detection."
c. Step 3: Select the action type after event triggered. Action options includes send media to event server, send notification to HTTP/HTTPS server and activation of digital output.
d. Step 4: Select perimeter detection recording schedule
e. Step 5: Click the save button

1.6. Crowd Recording:

Image 38. Crowd recording page



a. Event:

1	**Name**		Insert Crowd recording event name, only allow characters 0-9, a-z, A-Z, ".", "_"
2	**Enabled**	On	Users can enabled/ disabled this function.
		Off	
3	**Triggered by**	Crowd Detection	Select the perimeter detection as the trigger event type.

b. Settings:

1	**Min time between triggers**	Value 1~999 sec	Minimum interval for an event to trigger the next action.
2	**Please Configure Crowd Detection**	Please Configure Crowd	Click on Crowd Detection to go to crowd detection configuration page.

c. Action:

1	**Send Media**	Event Server	Instructs the camera to send out media. You will need to specify whether you want to use FTP, network storage or SD card. Make sure that the servers are set up before using it.
		SD Card	

2	**Send Notification**	HTTP HTTPS	This action type uses the HTTP and HTTPS recording server. You can use this to have the camera trigger a script on a server.
3	**Activate Digital Output**	Digital Output1	Allows you to perform an action with the camera's digital output. You may also specify the duration you want the camera to trigger the event.

d. Schedules:

1	**Always**	Always	Select the schedule for the above Event settings to be active. You may choose one of the available or schedule, or configure another schedule on the schedule menu.
2	**Schedule**	Schedule	
3	**Please Configure Schedule**	Please Configure Schedule	Click on Schedule to go to schedule configuration page.

How to create Crowd recording:

Step 1: Key in event name and enable crowd detection.

Step 2: Configure crowd detection settings. Remember to first enable crowd detection on the analytics page or click the link provided "crowd."

Step 3: Select the action type after event triggered. Action options includes send media to event server, send notification to HTTP/HTTPS server and activation of digital output.

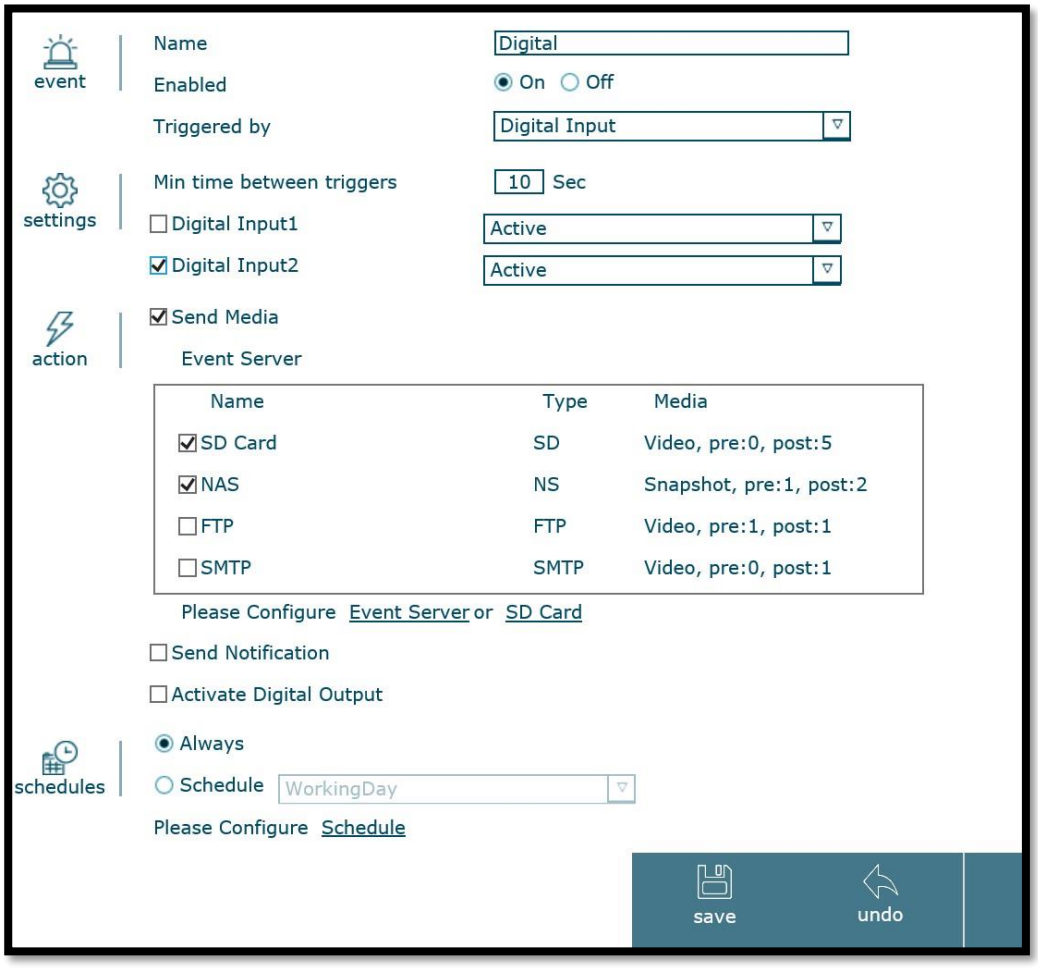
Step 4: Select crowd detection recording schedule.

Step 5: Click the save button.

1.7. Digital input Recording:

Note: Please check digital input is connected.

Image 39. Digital recording page



a. Event:

1	**Name**		Insert Digital input recording event name, only allow characters 0-9, a-z, A-Z, ".", "_"
2	**Enabled**	On Off	Users can enabled/ disabled this function.
3	**Triggered by**	Digital Input	Select the digital input as the trigger event type.

b. Settings:

1	**Min time between triggers**	Value 1~999 sec	Minimum interval for an event to trigger the next action.
2	**Digital Input 1**	Active	Define the status of the digital input for the camera to trigger recording. Select active to trigger recording when digital input status has changed from its normal state. Select inactive to trigger recording when digital input status is in its normal state. Select chamge to trigger recording every time the state of the digital input changes.
		Inactive	
		Change	
3	**Digital Input 2**	Active	
		Inactive	
		Change	

c. Action:

1	**Send Media**	Event Server	Instructs the camera to send out media. You will need to specify whether you want to use FTP, network storage or SD card. Make sure that the servers are set up before using it.
		SD Card	
2	**Send Notification**	HTTP	This action type uses the HTTP and HTTPS recording server. You can use this to have the camera trigger a script on a server.
		HTTPS	
3	**Activate Digital Output**	Digital Output1	Allows you to perform an action with the camera's digital output. You may also specify the duration you want the camera to trigger the event.

d. Schedules:

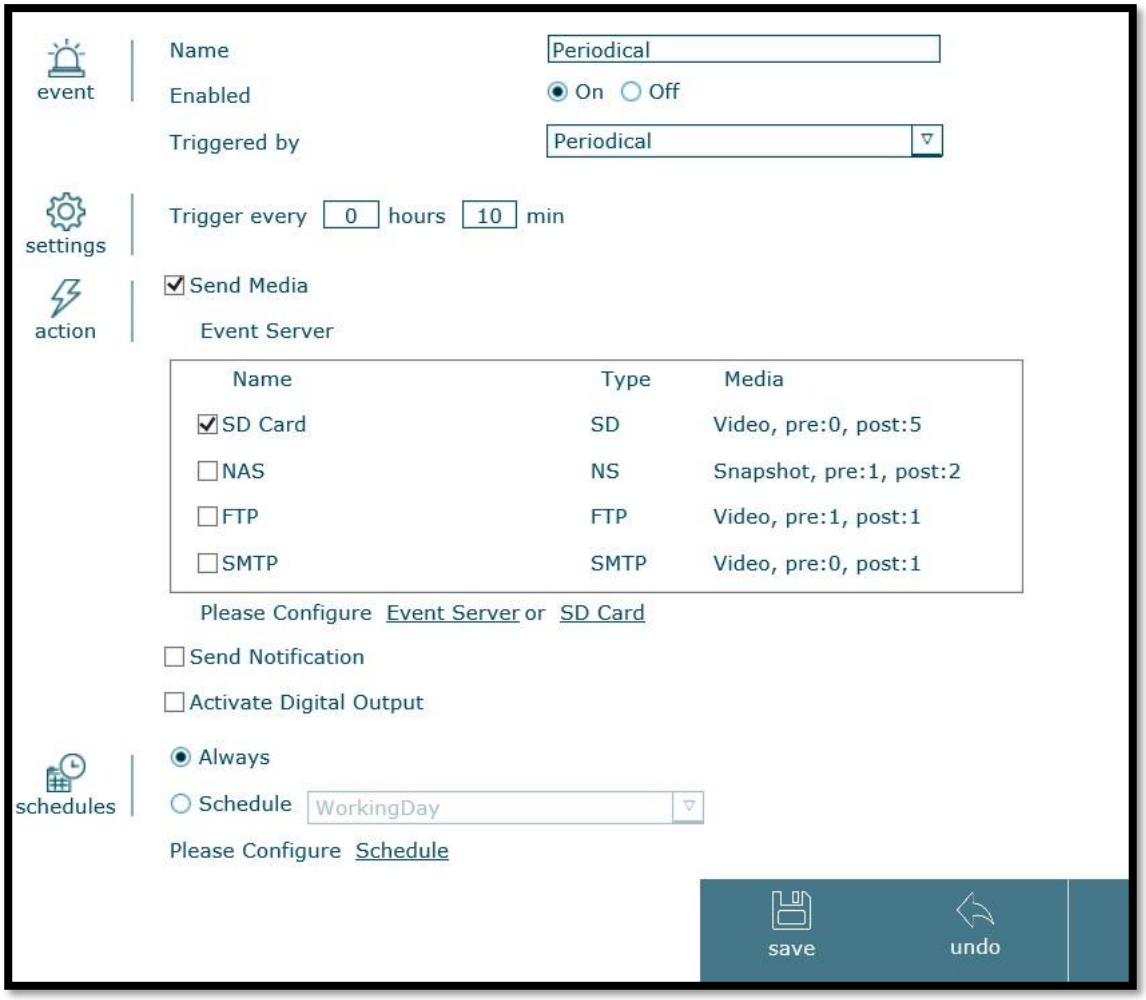
1	**Always**	Always	Select the schedule for the above Event settings to be active. You may choose one of the available or schedule, or configure another schedule on the schedule menu.
2	**Schedule**	Schedule	
3	**Please Configure Schedule**	Please Configure Schedule	Click on Schedule to go to schedule configuration page.

How to create Digital input recording:

Step 1: Key in event name and enable digital input
Step 2: Configure digital input settings.
Step 3: Select the action type after event triggered. Action options includes send media to event server, send notification to HTTP/HTTPS server and activation of digital output.
Step 4: Select digital input recording schedule
Step 5: Click the save button

1.8. Periodical recording:

Image 40. Periodical recording page



a. Event:

1	**Name**		Insert Periodical recording event name, only allow characters 0-9, a-z, A-Z, ".", "_"
2	**Enabled**	On	Users can enabled/ disabled this function.
		Off	
3	**Triggered by**	Periodical	Select the periodical as the trigger event type.

b. Settings:

1	**Trigger every hours/ min**	0 hours 10 min	Users can customize the the time gap between trigger.

c. Action:

1	**Send Media**	Event Server	Instructs the camera to send out media. You will need to specify whether you want to use FTP, network storage or SD card. Make sure that the servers are set up before using it.
		SD Card	
2	**Send Notification**	HTTP	This action type uses the HTTP and HTTPS recording server. You can use this to have the camera trigger a script on a server.
		HTTPS	
3	**Activate Digital Output**	Digital Output1	Allows you to perform an action with the camera's digital output. You may also specify the duration you want the camera to trigger the event.

d. Schedules:

1	**Always**	Always	Select the schedule for the above Event settings to be active. You may choose one of the available or schedule, or configure another schedule on the schedule menu.
2	**Schedule**	Schedule	
3	**Please Configure Schedule**	Please Configure Schedule	Click on Schedule to go to schedule configuration page.

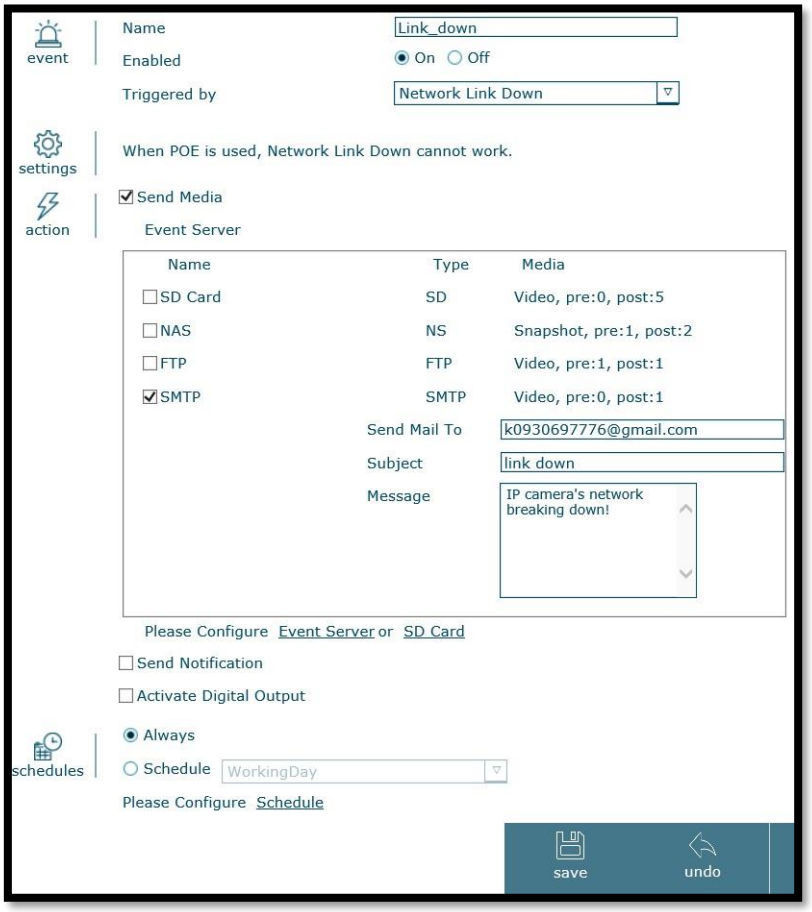
How to create Periodical recording:

a. Step 1: Key in event name and enable periodical recording
b. Step 2: Configure periodical recording settings.
c. Step 3: Select the action type. Action options includes send media to event server, send notification to HTTP/HTTPS server and activation of digital output.
d. Step 4: Select periodical recording schedule.
e. Step 5: Click the save button.

1.9. Network link down recording:

Note: This feature is not available if camera is using PoE as power supply.

Image 41. Network link down recording page



a. Event:

1	**Name**		Insert Network link down recording event name, only allow characters 0-9, a-z, A-Z, ".", "_"
2	**Enabled**	On	Users can enabled/ disabled this function.
		Off	
3	**Triggered by**	Network Link Down	Select the network link down as the trigger event type.

b. Action:

1	**Send Media**	Event Server	Instructs the camera to send out media. You will need to specify whether you want to use FTP, network storage or SD card. Make sure that the servers are set up before using it.
		SD Card	
2	**Send Notification**	HTTP	This action type uses the HTTP and HTTPS recording server. You can use this to have the camera trigger a script on a server.
		HTTPS	

3	**Activate Digital Output**	Digital Output1	Allows you to perform an action with the camera's digital output. You may also specify the duration you want the camera to trigger the event.

c. Schedules:

1	**Always**	Always	Select the schedule for the above Event settings to be active. You may choose one of the available or schedule, or configure another schedule on the schedule menu.
2	**Schedule**	Schedule	
3	**Please Configure Schedule**	Please Configure Schedule	Click on Schedule to go to schedule configuration page.

How to create Network link down recording:

Step 1: Key in event name and enable network link down detection

Step 2: Configure network link down detection settings.

Step 3: Select the action type after event triggered. Action options includes send media to event server, send notification to HTTP/HTTPS server and activation of digital output.

Step 4: Select network link down detection recording schedule

Step 5: Click the save button

2. Continuous:

Image 42. Continuous recording page

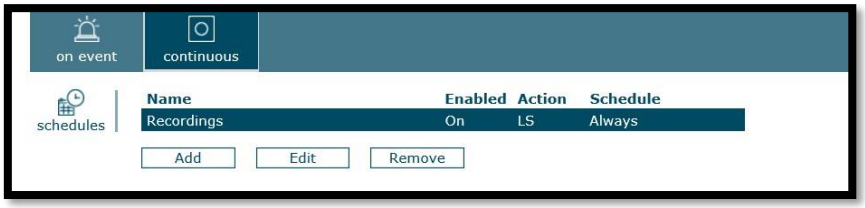
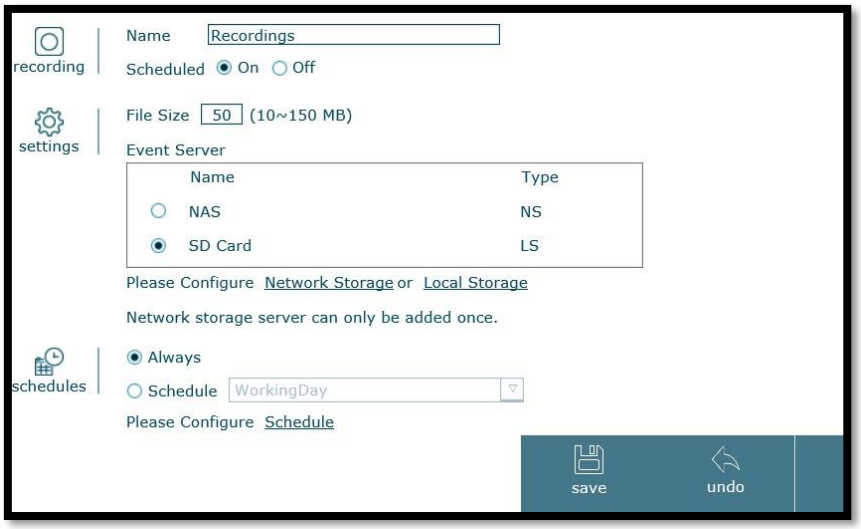


Image 43. Add/ edit Continuous recording page



a. Recording

1	**Name**	Recordings	Insert Continuous recording name, only allow characters 0-9, a-z, A-Z, ".", "_"
2	**Enabled**	On	Users can enabled/ disabled this function.
		Off	

b. Settings

1	**File Size**	Value 10~150 MB	Insert limit for the file size.
2	**Event Server**	Network Storage	Select the server for the recording.
		Local Storage	
3	**Please Configure Network Storage/ Local Storage**	Please Configure Network Storage or Local Storage	Click on Network Storage/ Local Storage to go to its configuration page.

c. Schedule

1	**Always**	Always	Select the schedule for the above Event settings to be active. You may choose one of the available or schedule, or configure another schedule on the schedule menu.
2	**Schedule**	Schedule	
3	**Please Configure Schedule**	Please Configure Schedule	Click on Schedule to go to schedule configuration page.

How to create Continuous recording:

a. Step 1: Key in event name and enable continuous recording
b. Step 2: Configure the maximum file size per recording
c. Step 3: Select location to save the recording files
d. Step 4: Select continuous recording schedule
e. Step 5: Click the save button

5.4 Analytics

Note: Remember to click the save button to successfully apply changes.

• Analytics includes 6 different types of detection: motion detection, audio detection, tampering detection, tripwire detection, perimeter detection and crowd.

1. **Motion detect:** allows users to create up to 3 motion detection areas.

*Colors line inside detection area:

- Threshold
- Motion below threshold detected (no event triggered)
- Motion above threshold detected (event triggered)

Image 44. Analytics page (no event triggered)

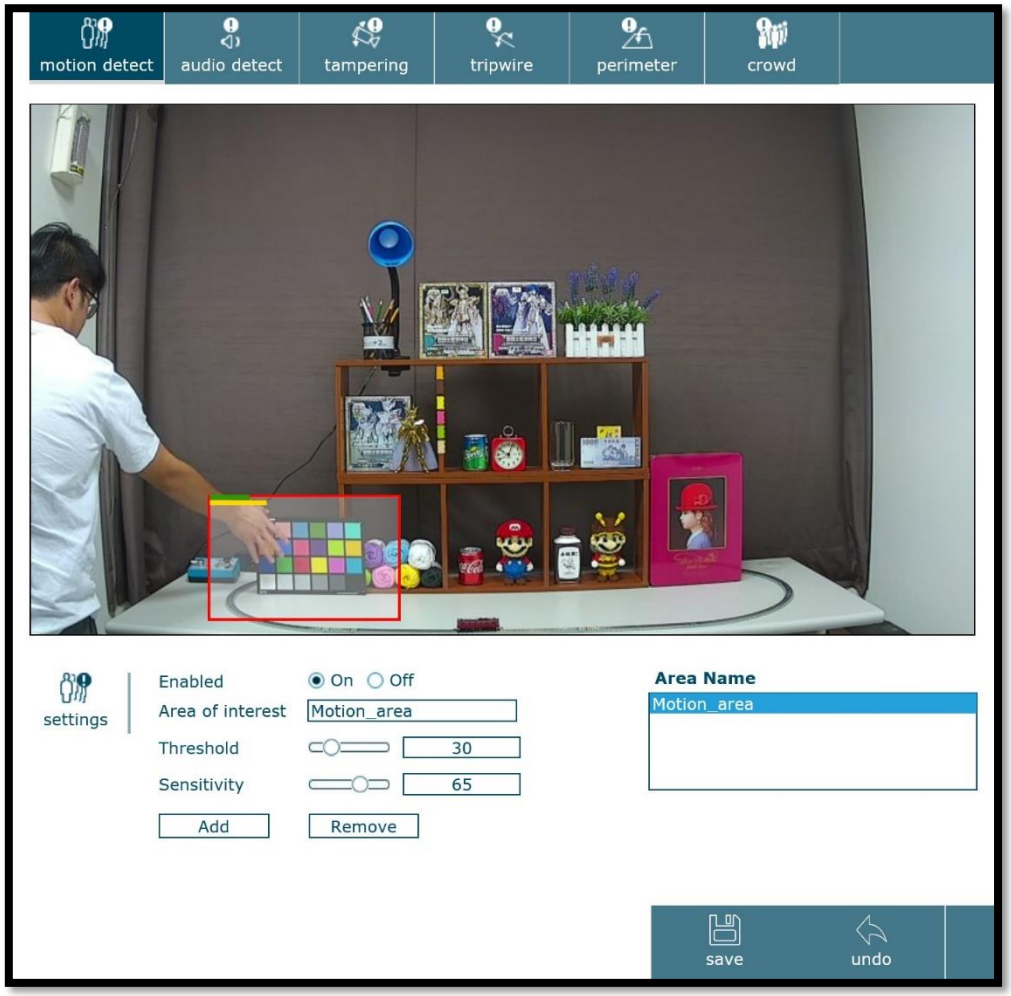
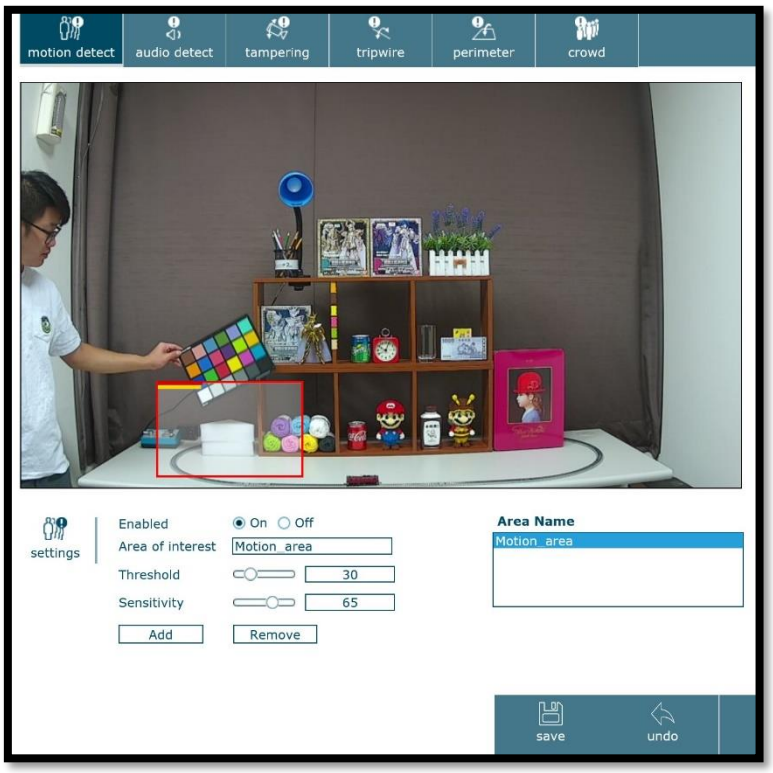


Image 45. Analytics page (event triggered)



a. Settings:

1	**Enabled**	On Off	Users can enabled/ disabled this function.
2	**Area of interest**	Motion_area	Insert Area Name, only allow characters 0-9, a-z, A-Z, ".", "_"
3	**Threshold**	Value 0~100	Make sure to define sensitivity and threshold according to the environment in order to avoid false alarms. There are no standard values as every site's conditions are different. Generally speaking, increasing sensitivity and lowering threshold will allow the camera to detect most of the motion detection, hence the increase of false alarms. Doing the opposite can reduce false alarms but might increase the risk of missing a key event.
4	**Sensitity**	Value 0~100	

How to create Motion detection:

a. Step 1: Enable motion detection.
b. Step 2: Key in detection area name.
c. Step 3: Configure threshold and sensitivity.
d. Step 4: Click the add button.
e. Step 5: Configure the size of the detection area as needed.
f. Step 6: Click the save button.

2. Audio detect:

*Threshold line:

Light red audio below threshold detected (no event triggered)

Dark red audio above threshold detected (event triggered)

Image 46. Audio detect page

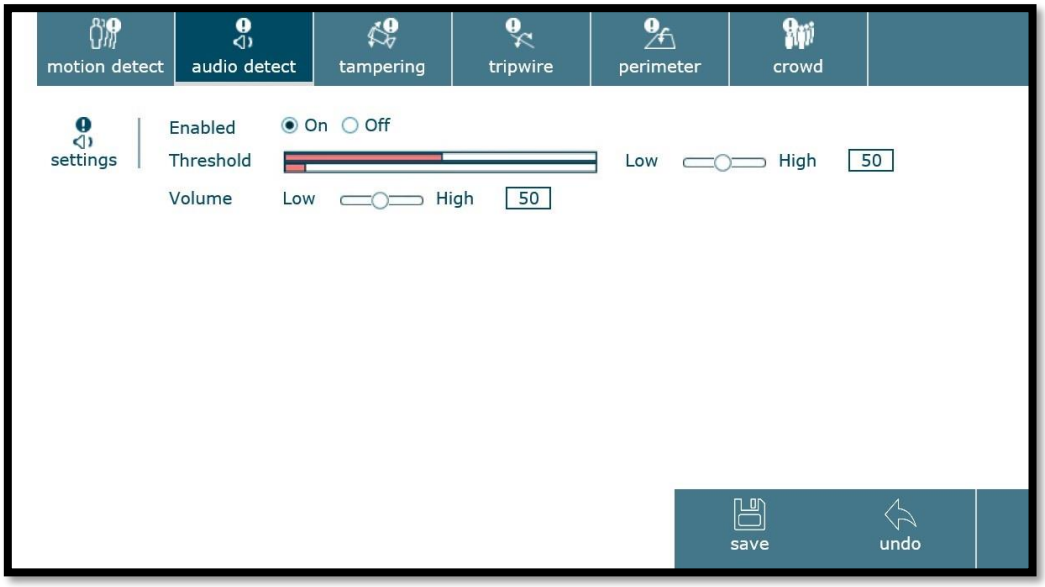
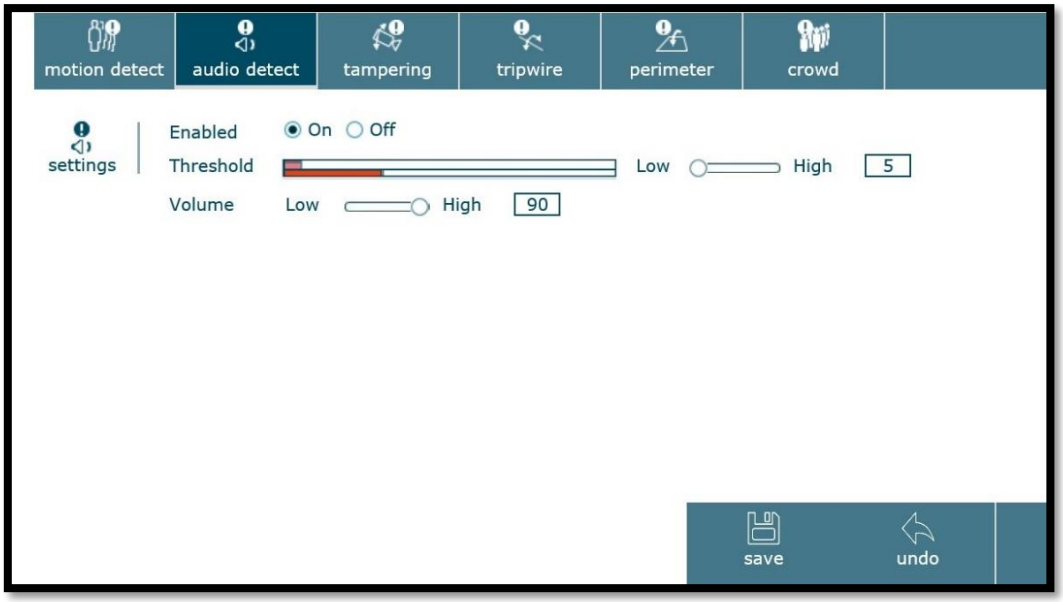


Image 47. Audio detect page



a. Settings:

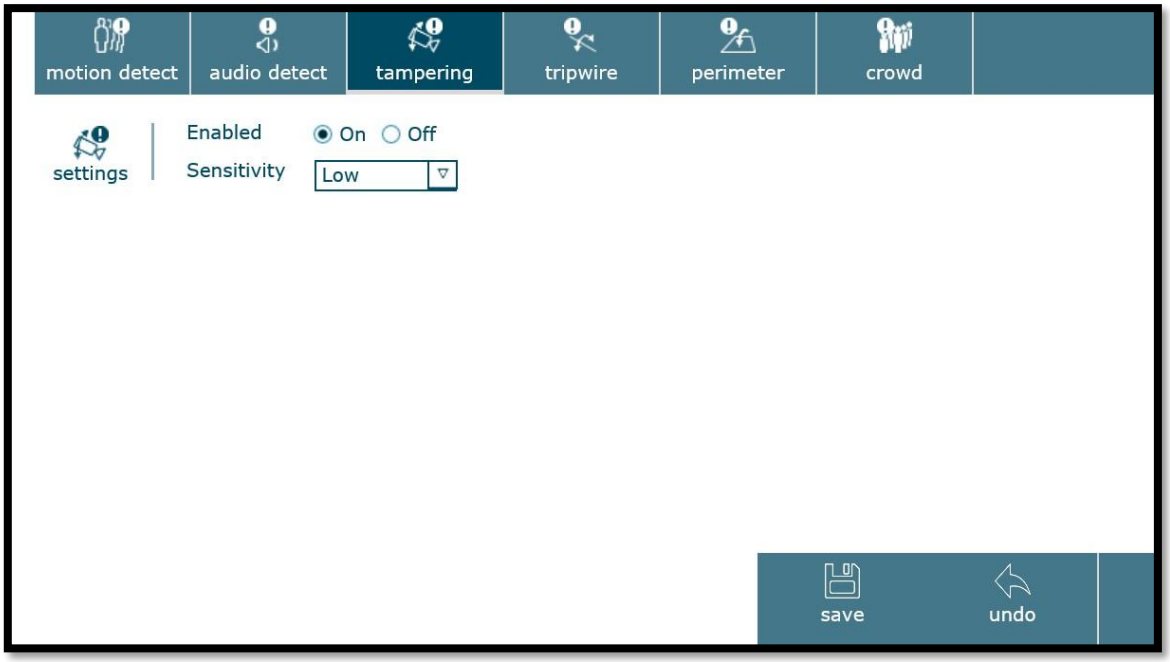
1	**Enabled**	On Off	Users can enabled/ disabled this function.
2	**Threshold**	Value 0~100	Make sure to define sensitivity and threshold according to the environment in order to avoid false alarms. There are no standard values as every site's conditions are different. Generally speaking, increasing sensitivity and lowering threshold will allow the camera to detect most of the motion detection, hence the increase of false alarms. Doing the opposite can reduce false alarms but might increase the risk of missing a key event.
3	**Volume**	Value 0~100	Set the volume sensitivity for the audio detection.

How to create Audio detection:

a. Step 1: Enable audio detection.
b. Step 2: Configure threshold.
c. Step 3: Configure the min. detection volume.
d. Step 4: Click the save button.

3. **Tampering:** allows camera to triggered event when tampering is detected

Image 48. Tampering page



a. Settings:

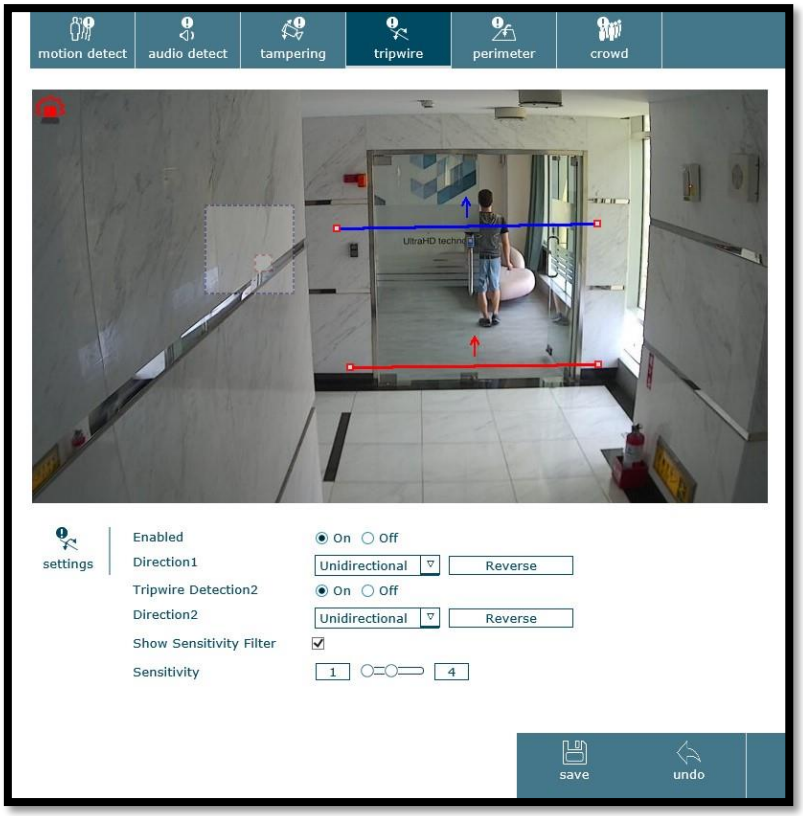
1	**Enabled**	On	Users can enabled/ disabled this function.
		Off	
2	**Sensitivity**	Low	Set the sensitivity level for the tampering detection.
		Middle	
		High	

How to create Tampering detection:

a. Step 1: Enable tampering detection.
b. Step 2: Select level of sensitivity.
c. Step 3: Click the save button.

4. Tripwire:

Image 49. Tripwire page



a. Settings

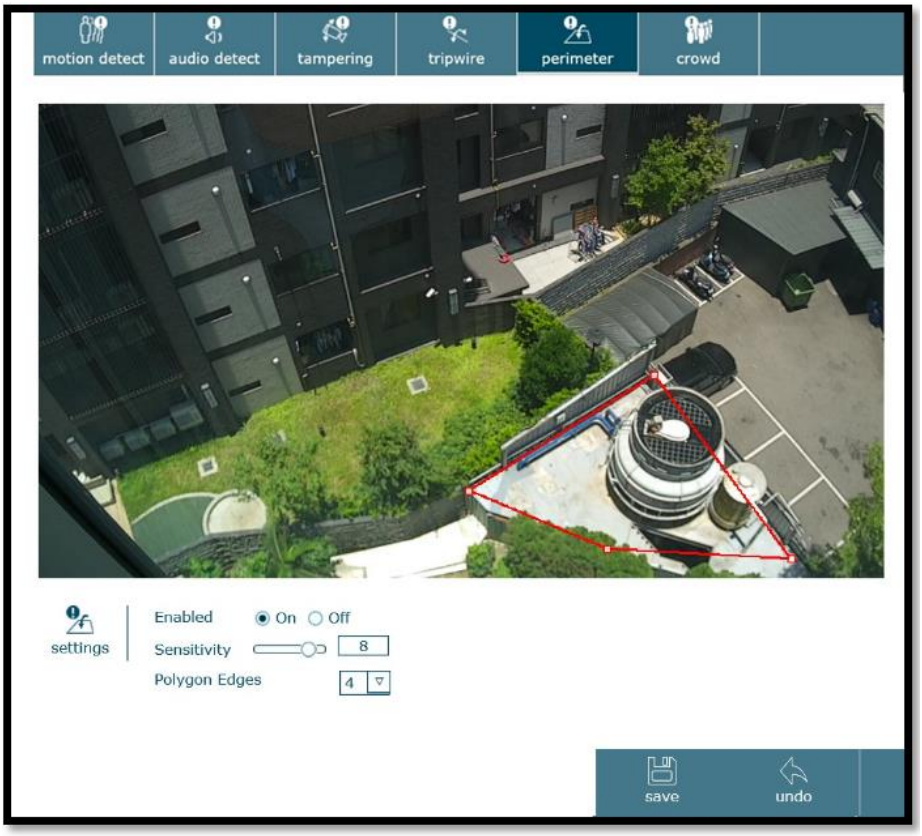
1	**Enabled**	On Off	Users can enabled/ disabled this function.
2	**Direction 1**	Bidirectional Unidirectional	Set the direction for triggering. To change the unidirectional orientation, reverse.
3	**TripwireDetection 2**	On Off	Select on to enable the second tripwire detection.
4	**Direction 2**	Bidirectional Unidirectional	Set the direction for triggering. To change the unidirectional orientation, reverse.
5	**Show Sensitivity Filter**	☑	Check on the box to display the sensitivity filter.
6	**Sensitivity**	4 — 5	Set the minimum size (red square) and maximum size (blue square).

How to create Tripwire detection:

a. Step 1: Enable tripwire detection
b. Step 2: Configure the direction of up to two tripwires
c. Step 3: Configure sensitivity
d. Step 4: Click the save button

5. Perimeter:

Image 50. Perimeter page



a. Settings:

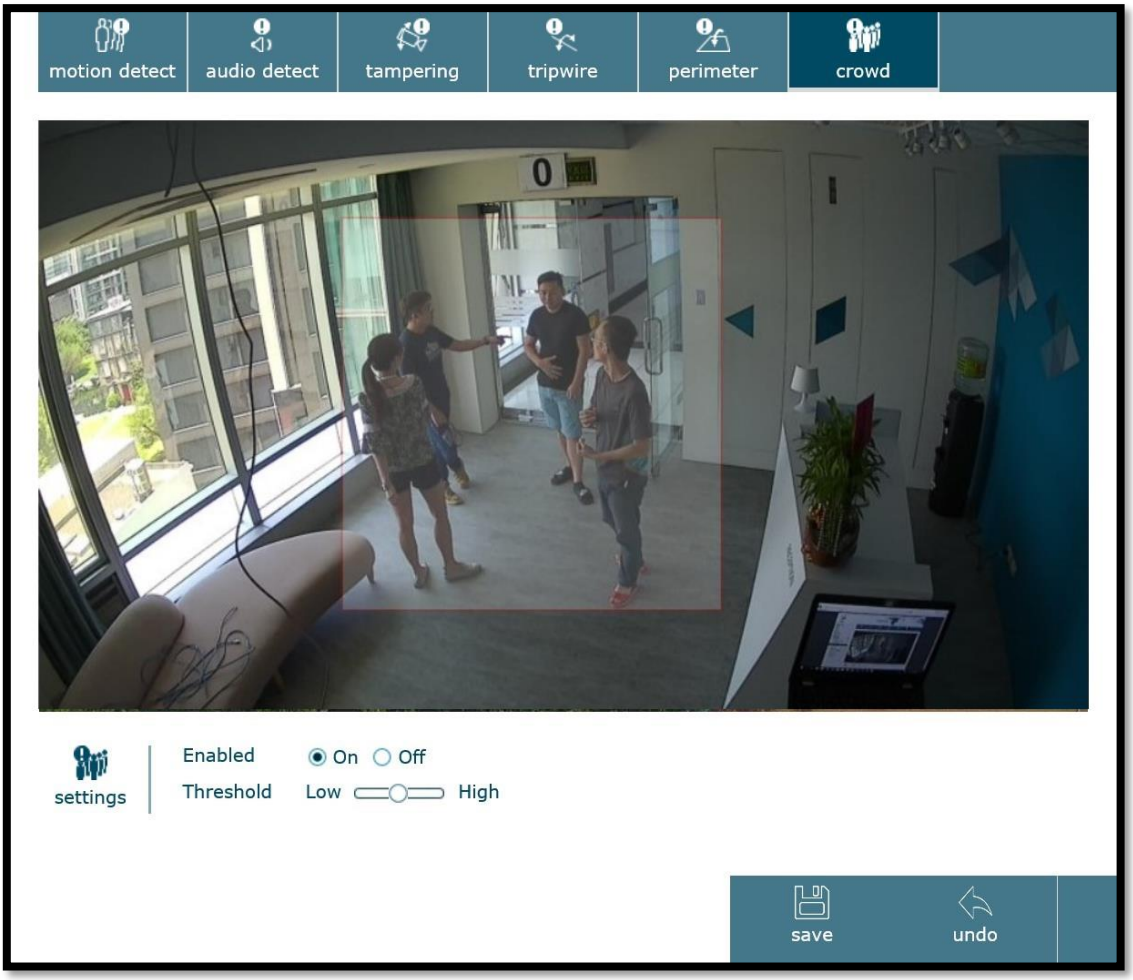
1	**Enabled**	On	Users can enabled/ disabled this function.
		Off	
2	**Sensitivity**	Value 1~10	Set the sensitivity level for perimeter detection.
3	**Polygon Edges**	4	Set the number of sides for perimeter detection area.
		5	
		6	
		7	
		8	

How to create Perimeter detection:

a. Step 1: Enable perimeter detection.
b. Step 2: Configure sensitivity (value 1~10).
c. Step 3: Select the number of polygon edges for the detection area.
d. Step 4: Click the save button.

6. Crowd:

Image 51. Crowd page



a. Settings:

1	**Enabled**	On Off	Users can enabled/ disabled this function.
2	**Threshold**	Low High	Set the threshold for the crowd detection.

How to create Crowd detection:

a. Step 1: Enable crowd detection.
b. Step 2: Set the detection area.
c. Step 3: Configure threshold.
d. Step 4: Click the save button.

5.5 Schedules

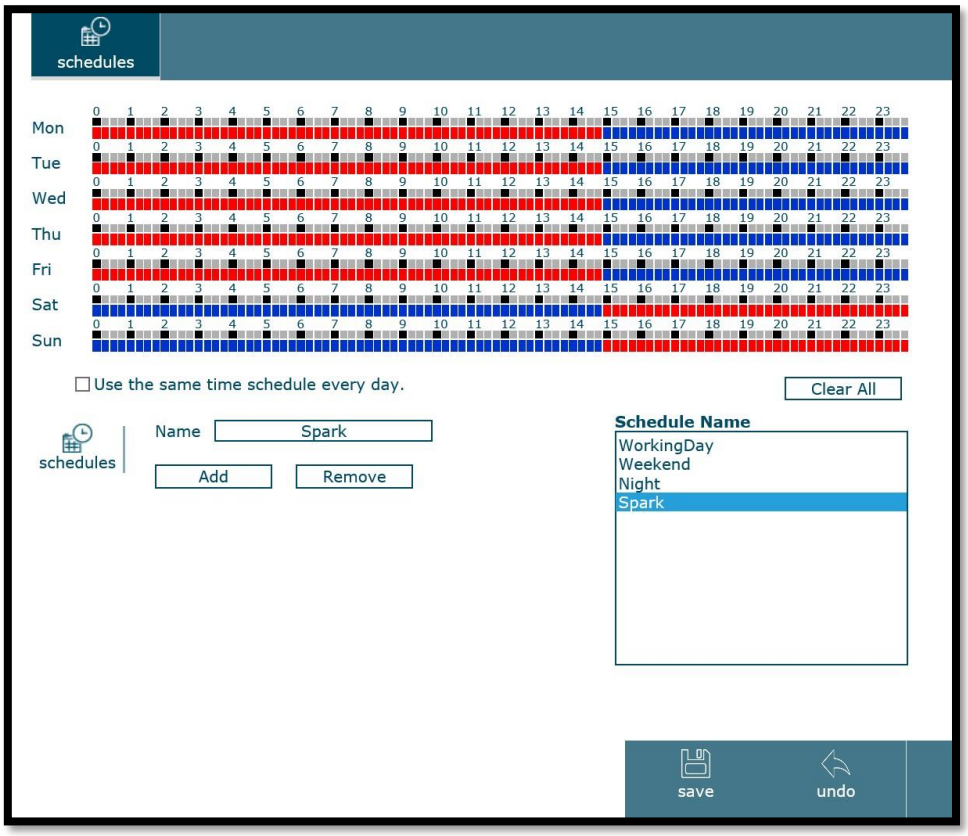
Note: Remember to click the save button to successfully apply changes.

• Schedules allows users to create up to 10 different schedules. Each small square is equivalent to 15 minutes. Each day has a total of 96 square (24hours).

Red square: not scheduled time

Blue square: scheduled time

Image 52. Schedules page



a. Schedule:

1	**Name**	Weekend	Insert Schedule name, only allow characters 0-9, a-z, A-Z, "-", "_"

How to create Schedule:

a. Step 1: Click and drag on the red square to select the recording schedule time. Users may also select the schedule on a certain day and copy to other days by checking the box of use the same time schedule every day.

b. Step 2: Key in schedule name and click the add button.

c. Step 3: To remove the schedule, select the schedule and then click the remove button.

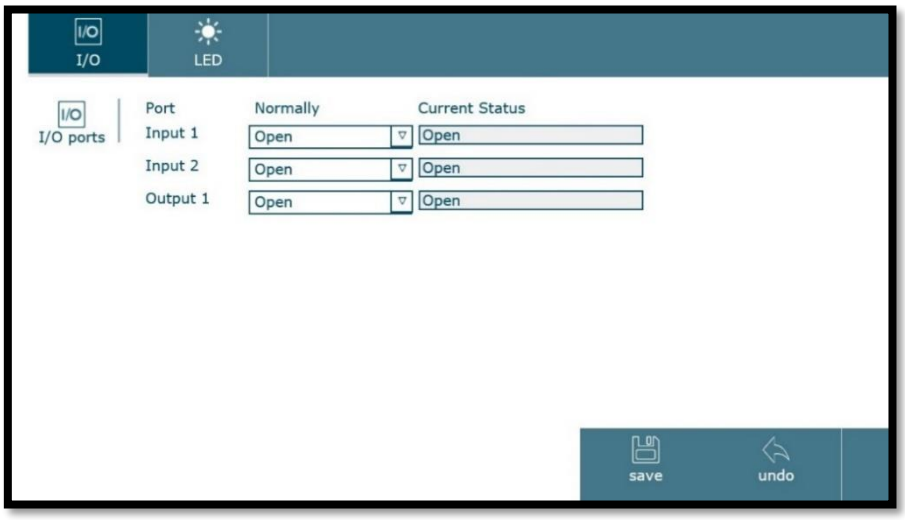
d. Step 4: Click the save button.

5.6 Digital I/O

Note: (1) Please check if digital input/output is connected. (2) Remember to click the save button to successfully apply changes.

1. **I/O:** Shows digital input/output current status and allows users to configure input and output normal status.

Image 53. Digital I/O page

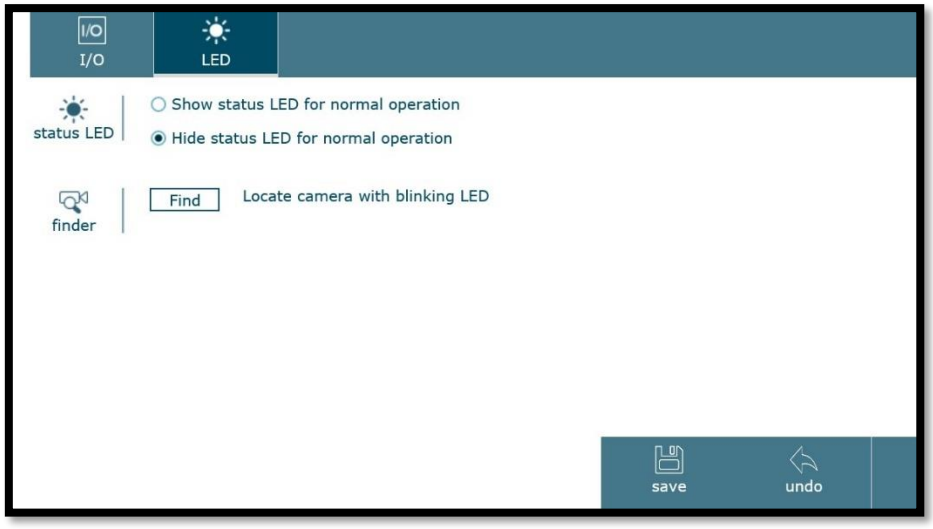


a. I/O ports:

1	**Input 1**	Open	Configure your camera's digital I/O on this page. This section shows the digital I/O current status and allows you to define its normal state (non-alert state).
		Close	
2	**Input 2**	Open	
		Close	
3	**Output 1**	Open	
		Close	

2. LED:

Image 54. LED page



a. Status LED:

1	**Show status LED for normal operation**	Show status LED for normal operation	Allow users to select the status of the LED on the IR board during normal operation.
2	**Hide status LED for normal operation**	Hide status LED for normal operation	

b. Finder:

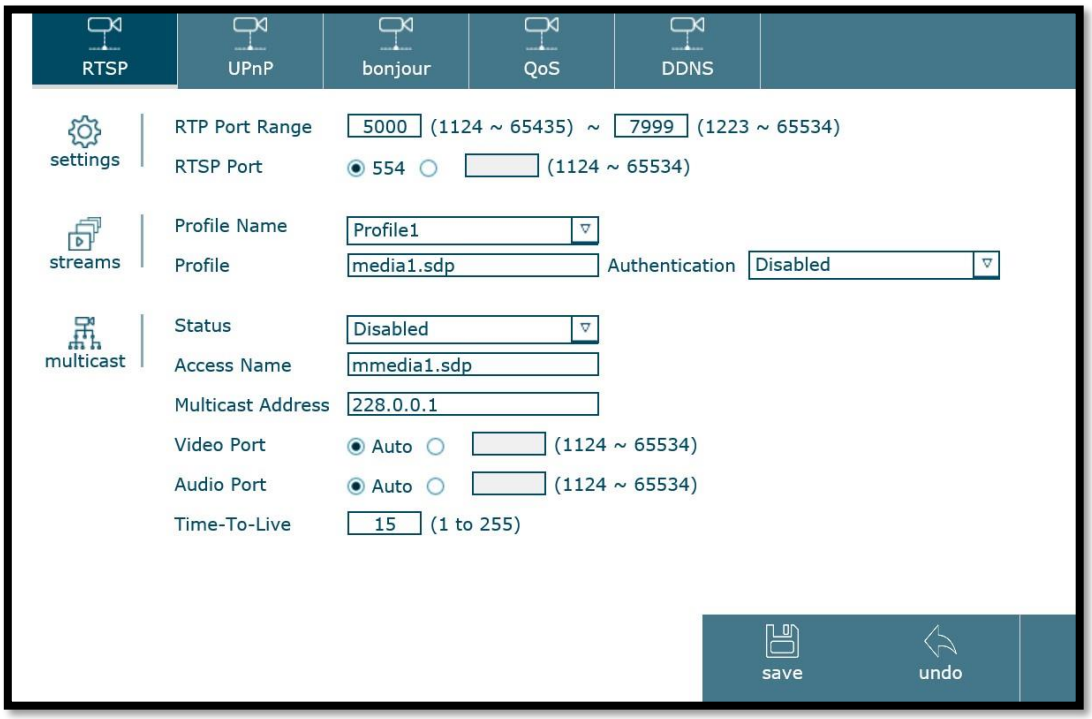
1	**Locate camera with blinking LED**	Find	This feature enables users to easily locate the camera. When users click the Find button, the LED on the IR board will blink for 30 seconds.

5.7 Network advanced

Note: Remember to click the save button to successfully apply changes.

1. RTSP:

Image 55. RTSP page



a. Settings:

1	**RTP Port Range**	Value 1124~65534	Default value is 5000 ~ 7999 and can be changed from 1124 to 65534.
2	**RTSP Port**	554	Default value is 554 and can be changed from 1124 to 65534.
		1124~65534	

b. Streams:

1	**Profile Name**	Profile 1 Profile 2 Profile 3	Select the profile for the RTSP streams.
2	**Profile**	mmedia1.sdp	This option allows you to set up the URL for each profile and define whether or not you want to enable authentication. The default video URL will be related to the profile number, e.g., profile1 = media1.sdp. Based on the default URLs, access to the RTSP streams would be: rtsp://camera_address/media1.sdp If authentication is enabled, the URLs will change as follows: rtsp://username:password@camera_address/media1.sdp

c. Multicast:

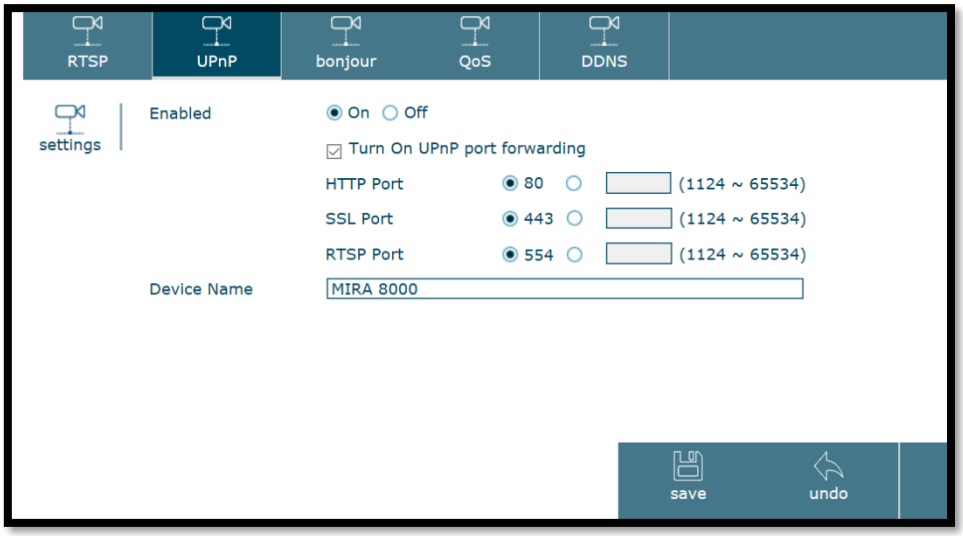
1	**Status**	Disabled Enabled	Multicasting provides efficient usage of bandwidth when there is large numbers of clients viewing simultaneously.
2	**Access Name**	mmedia1.sdp	Default access name: rtsp://camera_address/mmedia1.sdp
3	**Multicast Address**	228.0.0.1	Default address is 228.0.0.1
4	**Video Port**	Auto 1124~65534	Users can select the video port or select the auto mode for multicast.
5	**Audio Port**	Auto 1124~65534	Users can select the audio port or select the auto mode for multicast.
6	**Time-To-Live**	Value 1~255	Time-to-live (TTL) value is the hop limit that tells a network router whether or not the packet has been in the network too long and should be discarded.

How to create RTSP:

a. Step 1: Configure RTP port range.
b. Step 2: Configure RTSP port (default value is 554).
c. Step 3: Select profile name.
d. Step 4: Configure RTSP profile name and authentication.
e. Step 5: Configure RTSP multicast settings.
f. Step 6: Click the save button.

2. UPnP:

Image 56. UPnP page



a. Settings:

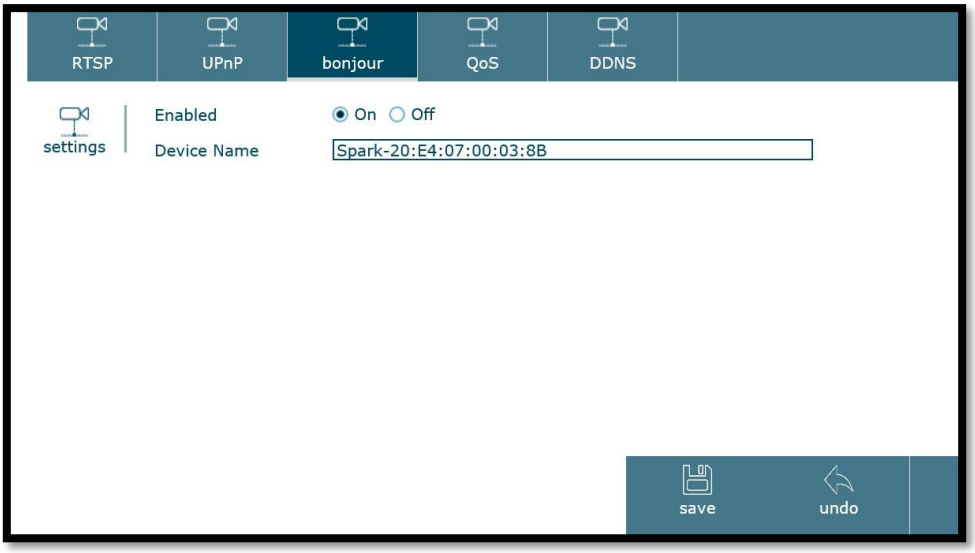
1	**Enabled**	On Off	UPnP allows the camera to announce their presence to other devices that support UPnP in the local network. Users can enabled/ disabled this function.
2	**Turn on UpnP port forwarding**	HTTP Port Value 1124~65534 SSL Port Value 1124~65534 RTSP Port Value 1124~65534	By default, the UPnP will be enabled and the port-forwarding will be disabled. When enabling the port-forwarding, you will need to define the port numbers for the three protocols. Normally there is no need to change the port numbers, unless one of them is already used by another device or application. Please make sure that your router supports the protocol.
3	**Device Name**	MIRA8000	Default device name is product name, but users can customize the device name.

How to create UPnP:

a. Step 1: Enable UPnP
b. Step 2: Choose whether to turn on or off UPnP port forwarding
c. Step 3: Key in UPnP device name
d. Step 4: Click the save button

3. Bonjour:

Image 57. Bonjour page



a. Settings:

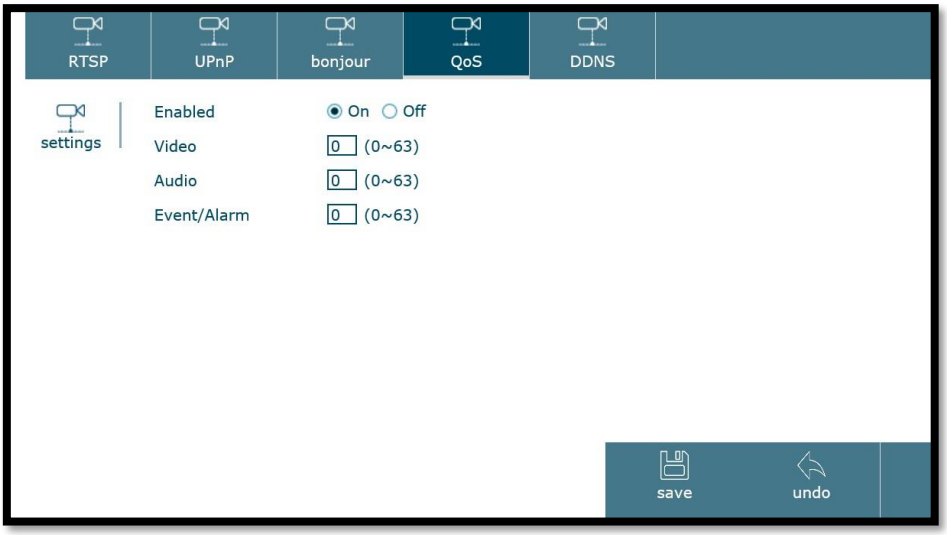
1	**Enabled**	On	Bonjour is a service that helps to find the camera on the network. This feature will be enabled by default. Users can enabled/ disabled this function.
		Off	
2	**Device Name**	Spark-20:E4:07:00:03:8B	Default device name is spark plus MAC address, but users can customize the device name.

How to create Bonjour:

a. Step 1: Enable bonjour
b. Step 2: Key in bonjour device name
c. Step 3: Click the save button

4. QoS:

Image 58. QoS page



a. Settings:

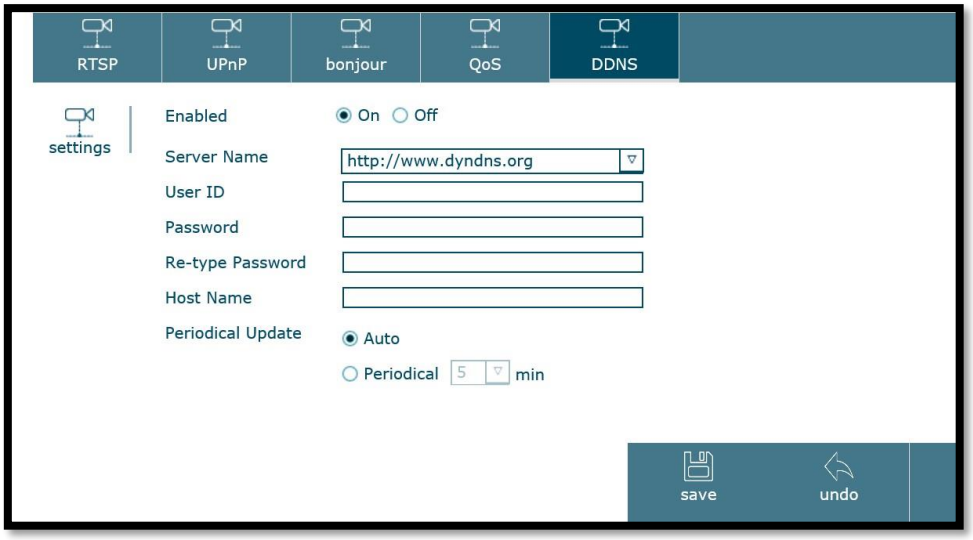
1	**Enabled**	On	QoS (Quality of Service) enables server to prioritize network traffic, providing a greater network reliability by controlling the amount of bandwidth an application may use.
		Off	
2	**Video**	Value 0~63	Insert the priority value for video packet. The higher the value the higher the priority.
3	**Audio**	Value 0~63	Insert the priority value for audio packet. The higher the value the higher the priority.
4	**Event/ Alarm**	Value 0~63	Insert the priority value for event/ alarm packet. The higher the value the higher the priority.

How to create QoS:

a. Step 1: Enable QoS
b. Step 2: Configure priority value for video, audio and event/alarm
c. Step 3: Click the save button

5. DDNS:

Image 59. DDNS page



a. Settings:

1	**Enabled**	On	Dynamic DNS allows you to create a domain name for your network, facilitating the access to the camera from a remote site. Users can enabled/ disabled this function.
		Off	
2	**Server Name**	http://www.dyndns.org	Select the DDNS provider of your choice.
		http://www.dhs.org	
		http://www.tzo.com	
		http://www.no-ip.com	
3	**User ID**		Insert the user ID and password to log into your account settings. Do not enter your DSL user account information.
4	**Password**		
5	**Re-type Password**		
6	**Host Name**		Insert the full host name that you have created in your server account.
7	**Periodical Update**	Auto	Specify the time for the camera to update its IP information with the DDNS provider or select auto and the camera will automatically update the changes.
		Periodical	

How to create DDNS:

a. Step 1: Enable DDNS
b. Step 2: Select DDNS server name
c. Step 3: Key in user ID, password and host name
d. Step 4: Choose periodical update mode
e. Step 6: Click the save button

5.8 Security

1. IP filter:

Image 60. Security page

Image 61. Add/Edit IP filter page_1

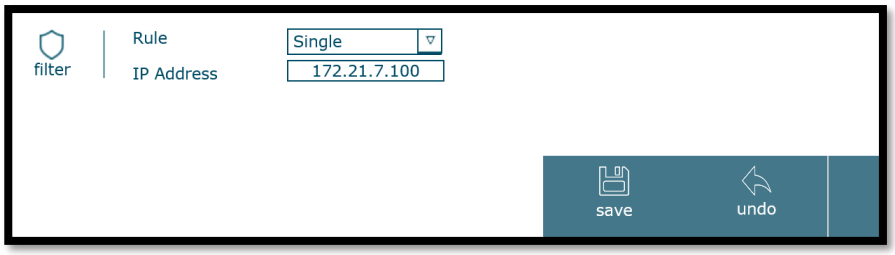


Image 62. Add/Edit IP filter page_2

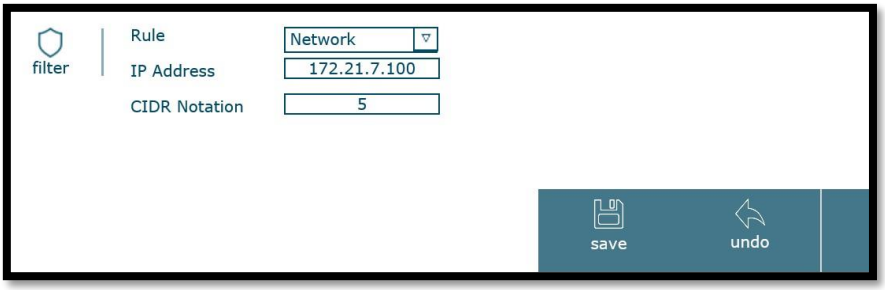
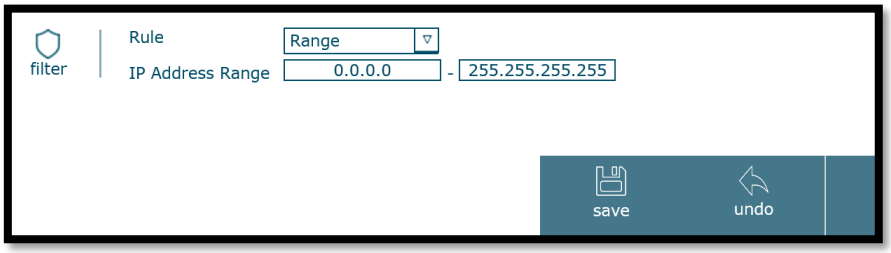


Image 63. Add/Edit IP filter page_3



a. Settings:

1	**Enabled**	On	Users can enabled/ disabled this function.
		Off	
2	**Filter Type**	Allow	Users can create lists of IP address to be allowed or denied to access the camera.
		Deny	

b. Filter:

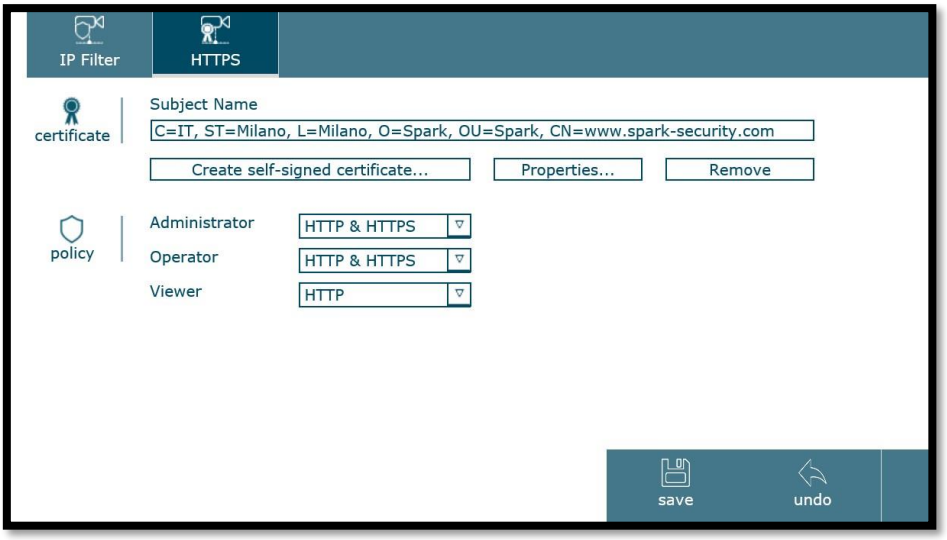
1	**Rule**	Single	Insert the IP address to allow or deny access.
		Network	Insert IP address and CIDR notation. The system will automatically allow or deny within IP range.
		Range	Insert the IP range to allow or deny access.

How to create IP Filter:

a. Step 1: Enable IP filter
b. Step 2: Choose filter type
c. Step 3: Click the add button
d. Step 4: Select rule and fill in the necessary information
e. Step 5: Click the save button on the add/edit IP filter page
f. Step 6: Click the save button on the IP filter page

2. HTTPS:

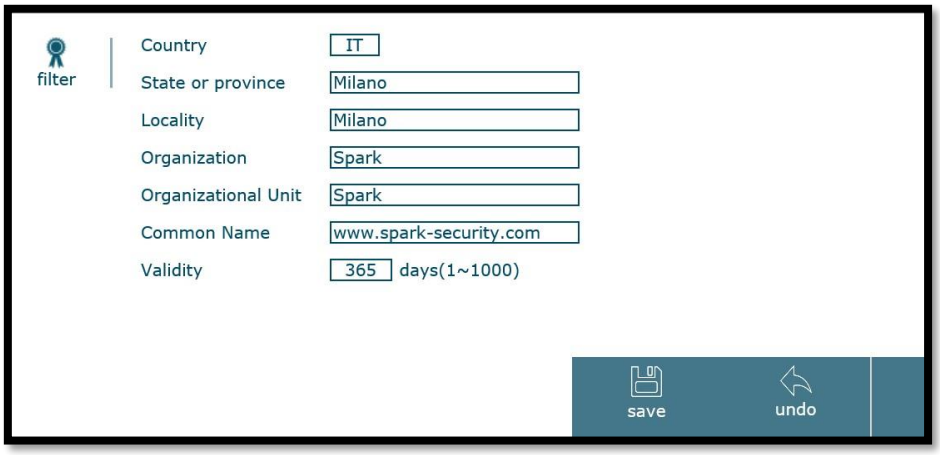
Image 64. HTTPS page



a. Certificate:

1	**Create self-signed certificate**	Create self-signed certificate...	Create a self-signed certificate for HTTPS to recognize.
2	**Properties**	Properties...	Display the properties of the installed certificate.
3	**Remove**	Remove	Remove the properties of the installed certificate.

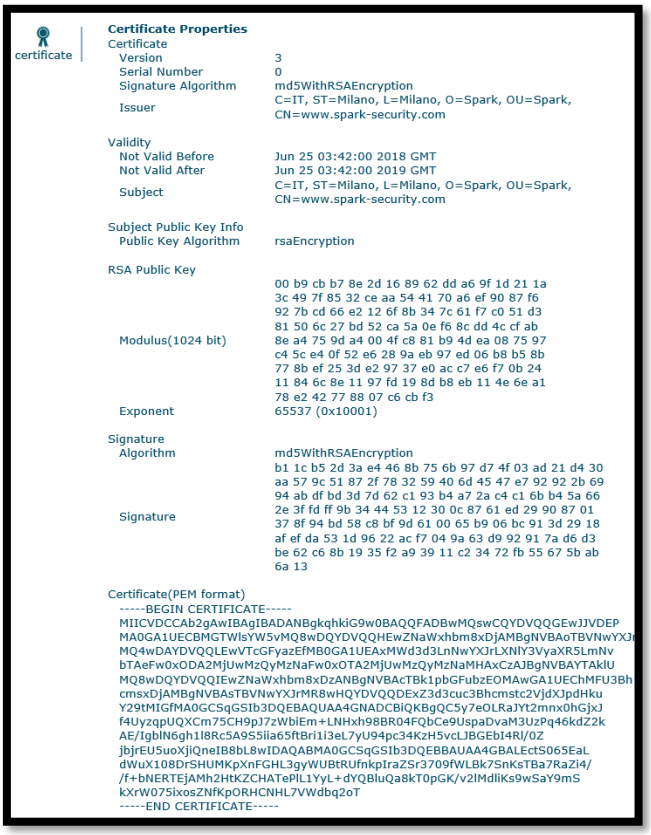
Image 65. Create self-signed certificate page



a.1. Create self-signed certificate:

1	**Filter**	Country	Insert 2 letter code country name.
		State or province	Insert state or province full name.
		Locailty	Insert city or district name.
		Organization	Insert company name.
		Organizational Unit	Insert organizational unit. If your company dose not have organizational unit please insert company name.
		Common Name	Insert server IP address or company website.
		Validity (value 1~1000)	Insert the validity days for the certificate.

Image 66. Properties page



a.2. Properties:

Display certificate properties information.

b. Policy:

1	**Administrator**	HTTP	Set HTTPS connection policy for different level of users. To use the HTTPS encryption, please set up "Create self-signed certificate" for the first time you use the HTTPS function, and then set up the connection policy for different users.
		HTTPS	
		HTTP & HTTPS	
2	**Operator**	HTTP	
		HTTPS	
		HTTP & HTTPS	
3	**Viewer**	HTTP	
		HTTPS	
		HTTP & HTTPS	

How to create HTTPS Filter:

a. Step 1: Click the Create self-signed certificate button
b. Step 2: Fill in the information on the popped-out window. The information filled will appeared on the properties page.
c. Step 3: Configure users policy rule
d. Step 4: Click the save button

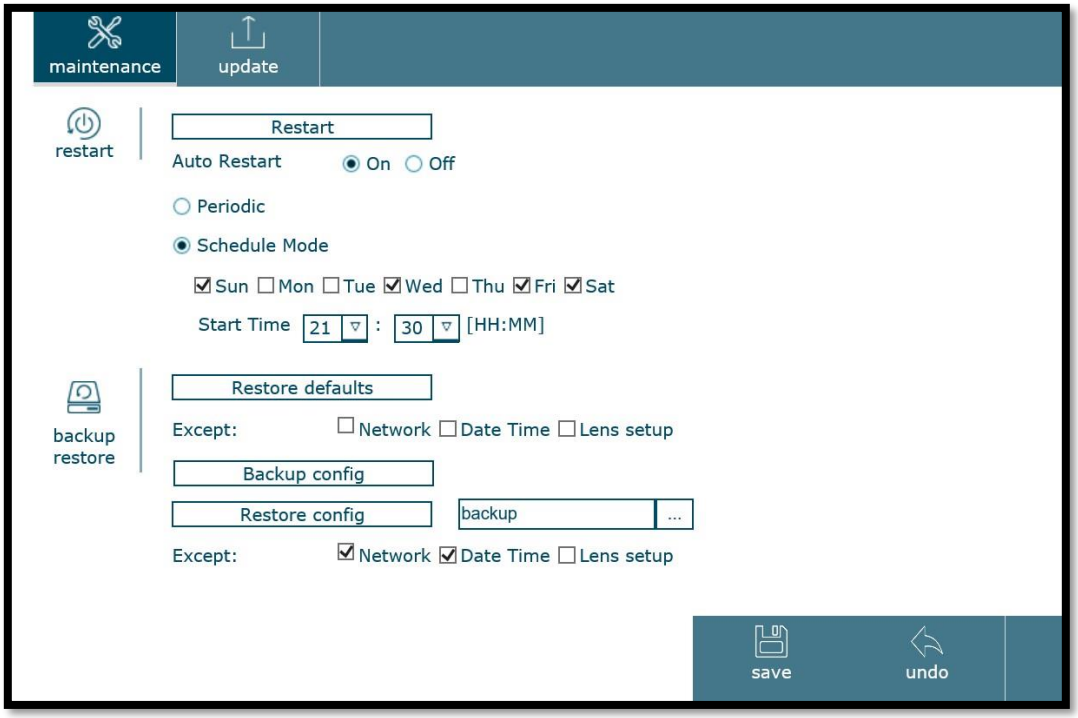
5.9 Maintenance

Note: Remember to click the save button to successfully apply changes.

• Maintenance page includes maintenance and update functions.

1. **Maintenance:** Users can configure restart and backup/restore time.

Image 67. Maintenance page



a. Restart:

1	**Restart**	Restart	This feature allows you remotely restart the camera, even set a schedule for the camera to automatically restart.
2	**Auto Restart**	On	
		Off	

a.1. Auto Restart:

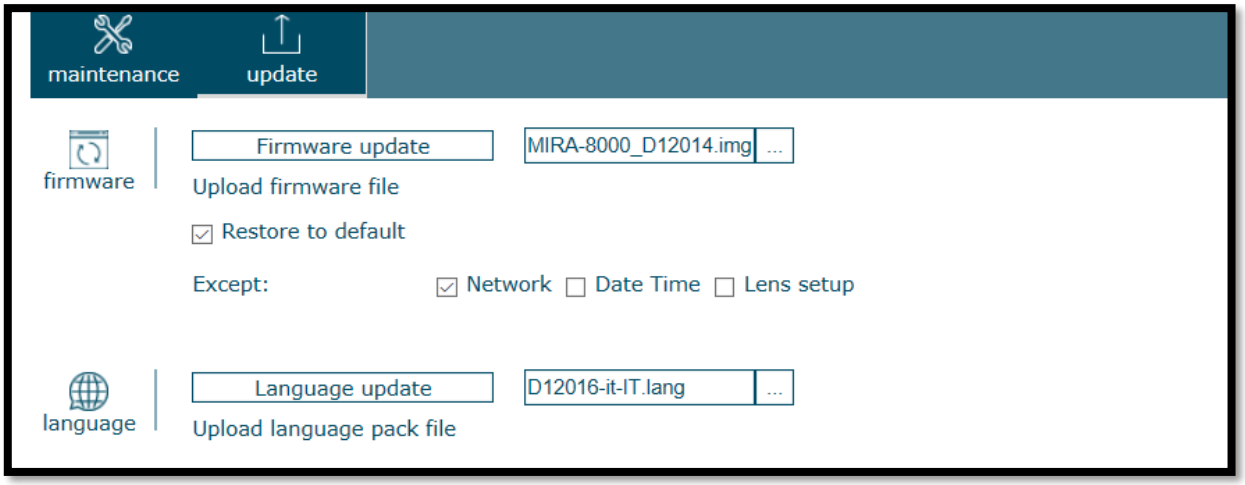
1	**Periodic**	Value 1~7 days	Set specific interval days for automatic restart.
2	**Schedule Mode**	Schedule Mode	Set specific dates and time for automatic restart.

b. Backup/ Restore

1	**Restore defaults**	Restore defaults	When restoring default values, users may choose to hold current values for network, date, time and lens set up.
2	**Backup config**	Backup config	Click to save the camera's current configuration on your computer. This feature can significantly save configuration time by allowing users to load the current configuration on another camera of the same model and firmware version. Make sure to change the IP address configuration to avoid IP conflict.
3	**Restore config**	Restore config	Click to load the backup configuration file. The camera will reboot to finalize the process and the new settings will become effective. Users may also choose to hold current values for network, date, time and lens set up.

2. **Update:** includes firmware and language update

Image 68. Update page



a. Firmware:

1	**Firmware update**	Firmware update	Having the camera's firmware updated will allow you to enjoy the camera at its best, as new firmware often enhance the functionality of the camera and solves known-issues. Before updating the firmware version, please follow below instructions: (1) Check that the firmware corresponds to your camera model. (2) Check that the firmware is not on a compressed file. The firmware should be .bin format. (3) Avoid wireless connections as they tend to be unstable.
2	**Reset to defaults**	☑ Restore to default	Users may also choose to hold current values for network, date, time and lens set up.

b. Language:

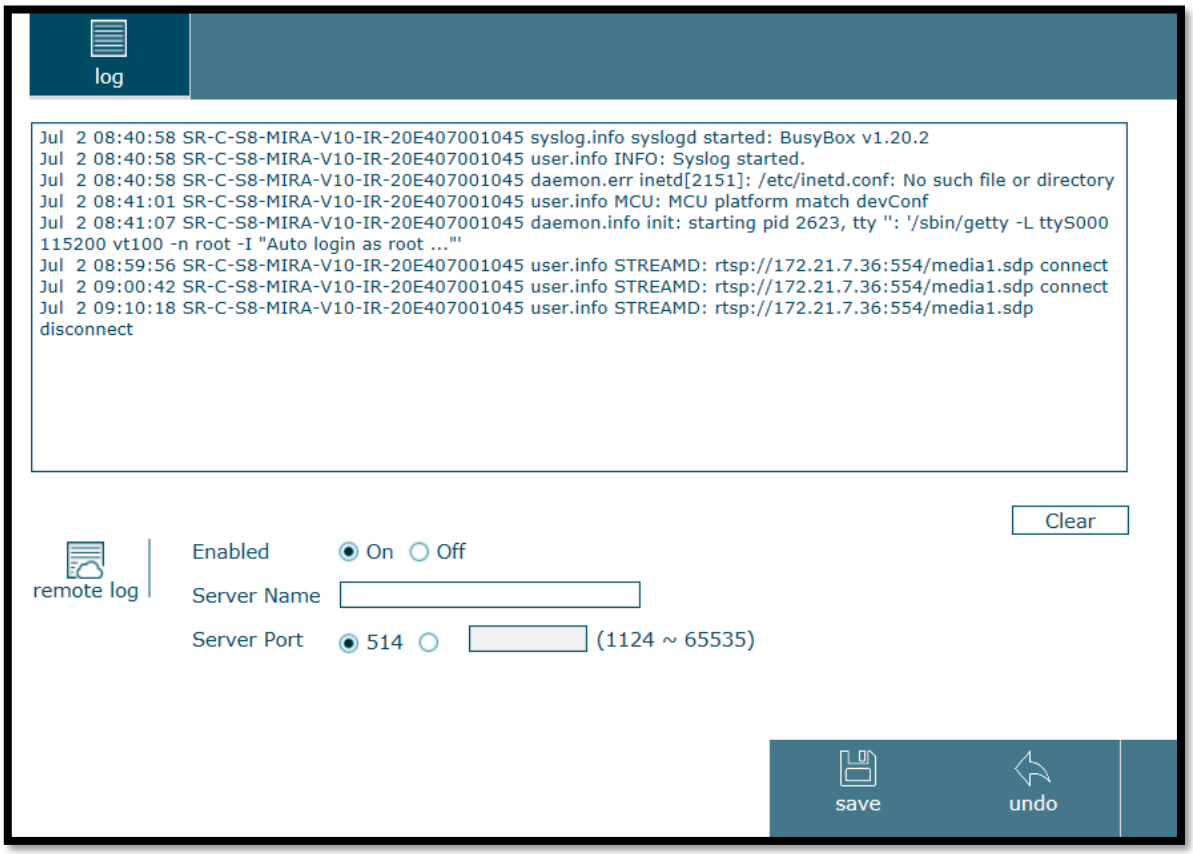
1	**Language update**	Language update	Language update allows users to change the language of the camera's web interface.

5.10 System log

- System log displays the system information, allowing users to clear log and/or enabled remote log:

1. Log:

Image 69. System log page



a. Remote log:

1	**Enabled**	On	The system records all the actions in its internal memory and displays it on the Current Log, but due to limited memory the logs will be overwritten. Enable remote log if you wish to keep all the logs.
		Off	
2	**Server Name**		Insert the network address of the system log server. Enter the address without any leading characters, such as http://
3	**Server Port**	Value 1124~65535	Default is 514. Change the value if your system log server is set up differently.