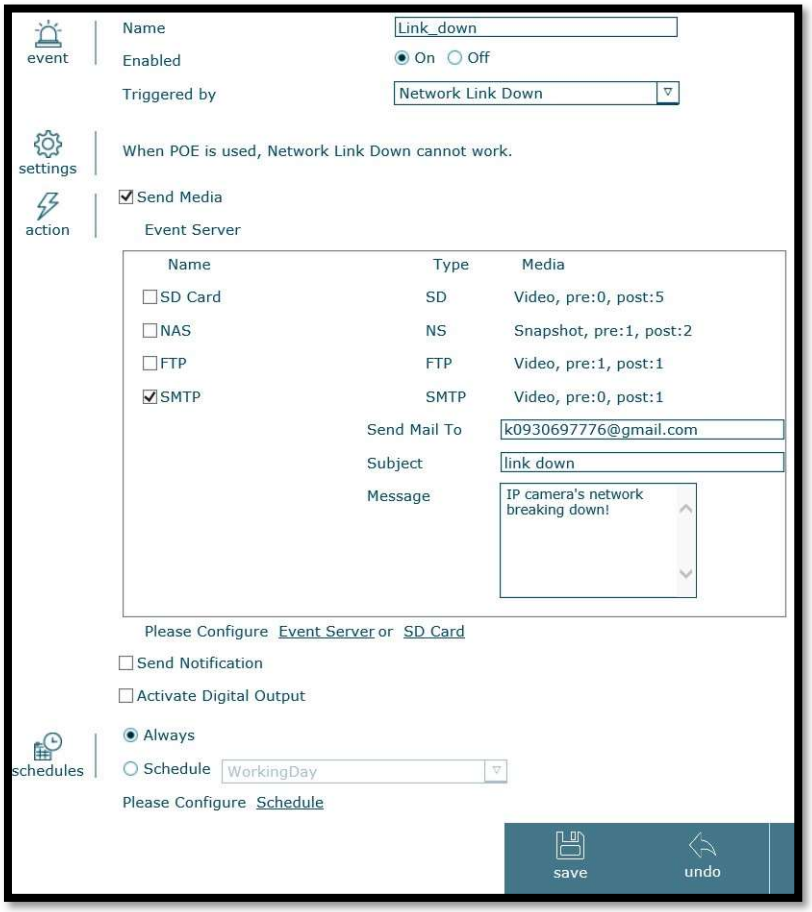
1.9. Network link down recording:

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.

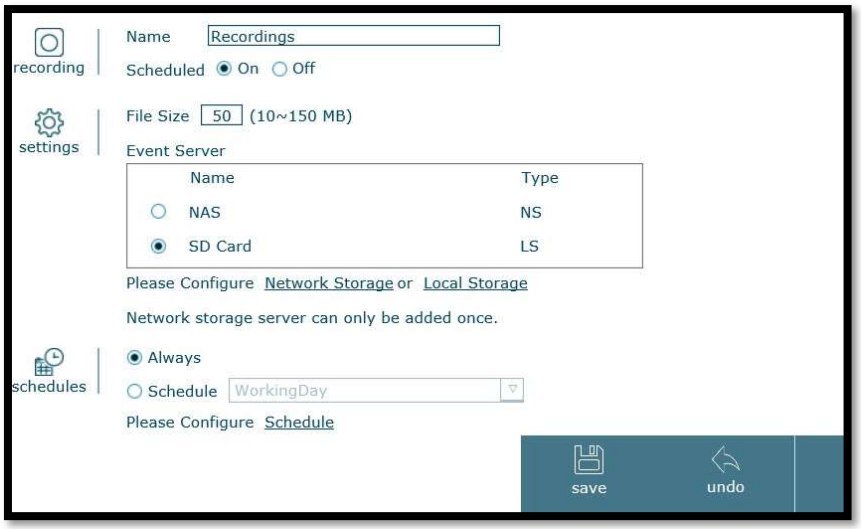
How to create Network link down recording:

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

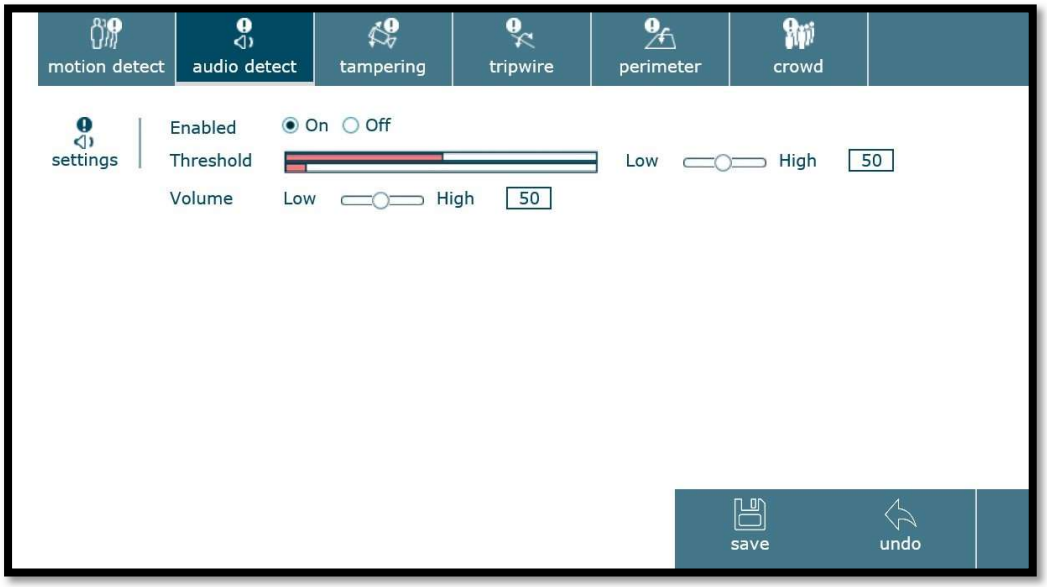
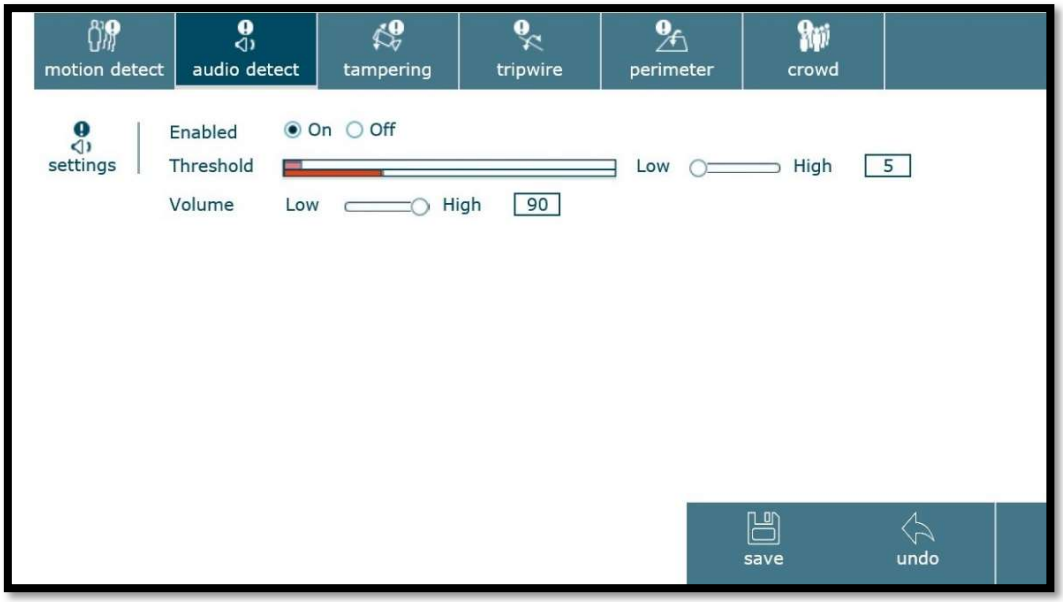


Image 47. Audio detect page



a. Settings:

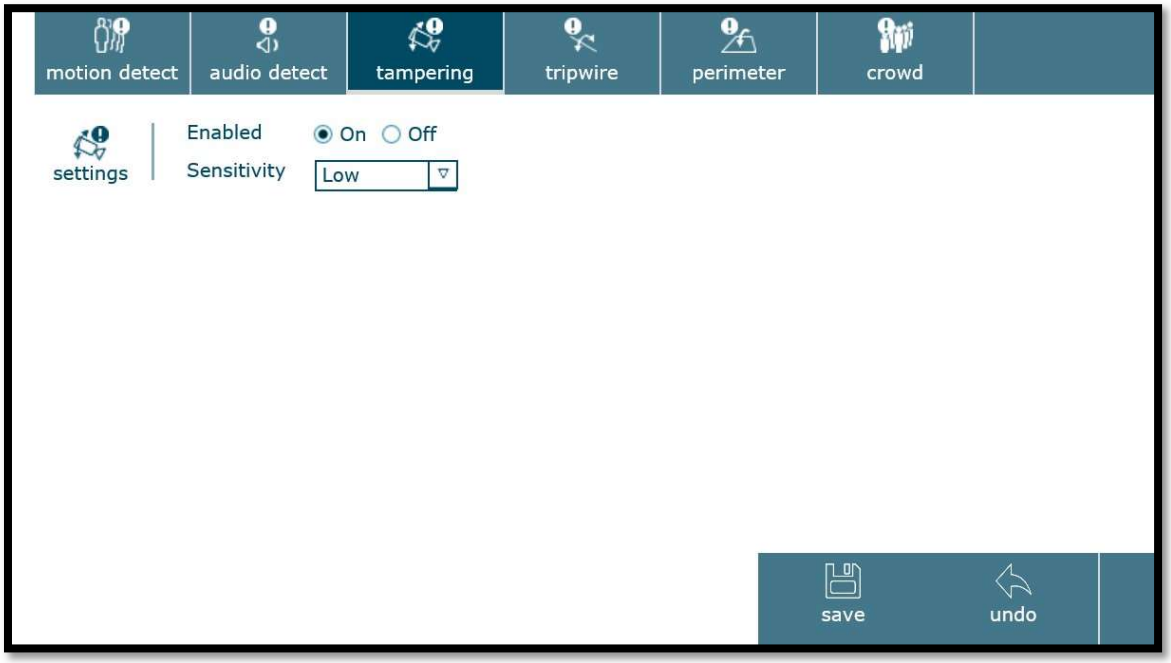
1	**Enabled**	On Off	Users can enabled/ disabled this function.
2	**Threshold**	Value 0~100	Make sure to define sensitivity and threshold according to the environment in order to avoid false alarms. There are no standard values as every site's conditions are different. Generally speaking, increasing 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:

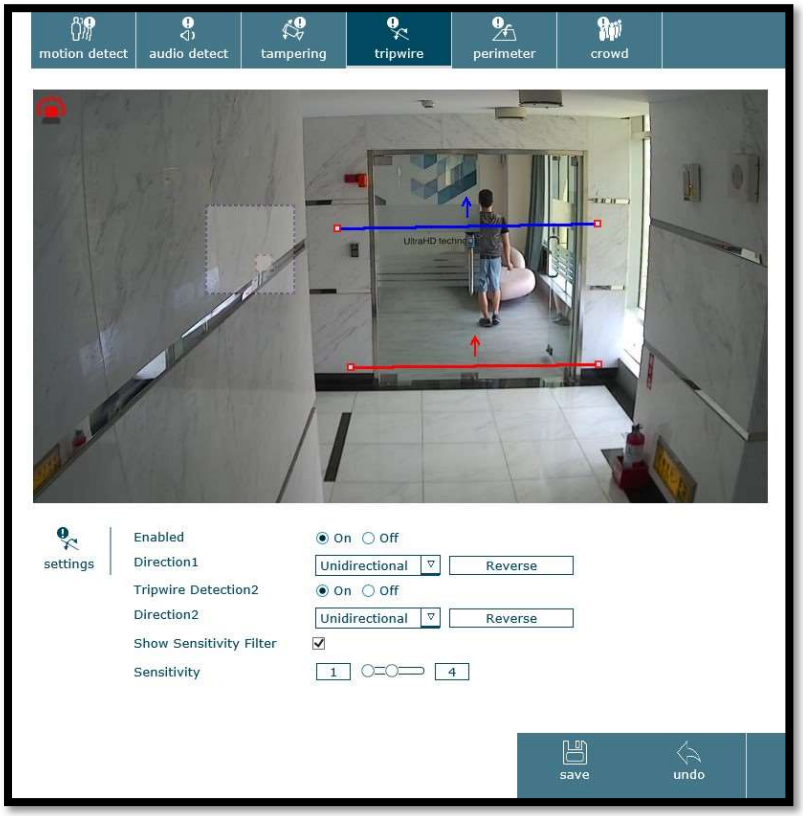
1	**Enabled**	On	Users can enabled/ disabled this function.
		Off	
2	**Sensitivity**	Low	Set the sensitivity level for the tampering detection.
		Middle	
		High	

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

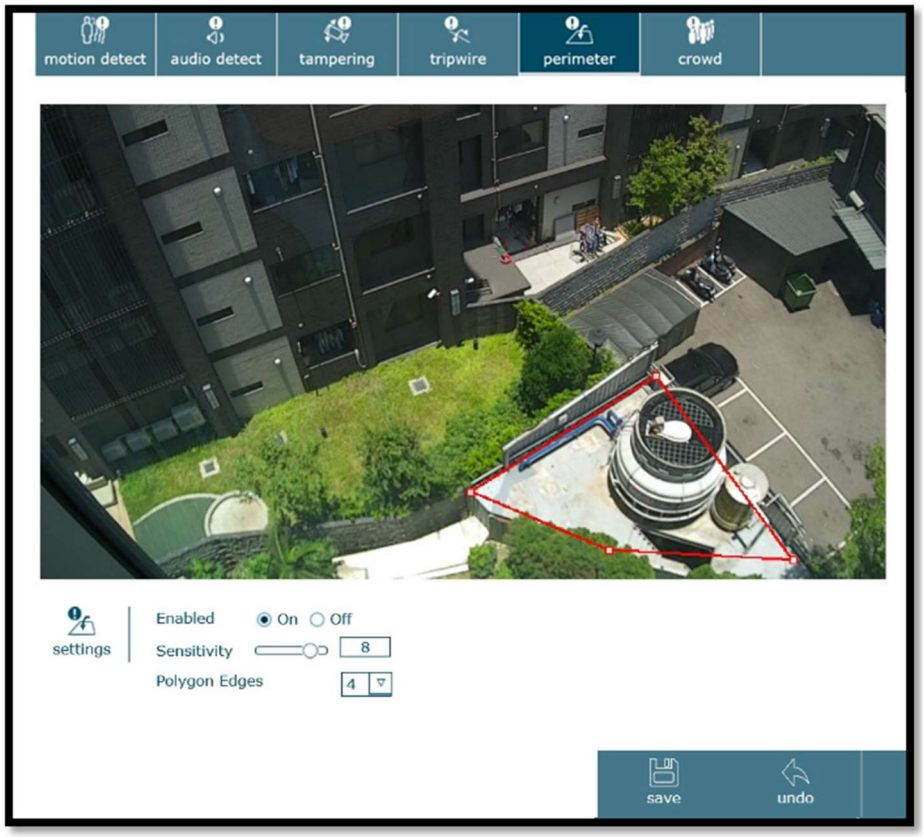
1	**Enabled**	On Off	Users can enabled/ disabled this function.
2	**Direction 1**	Bidirectional Unidirectional	Set the direction for triggering. To change the unidirectional orientation, reverse.
3	**TripwireDetection 2**	On Off	Select on to enable the second tripwire detection.
4	**Direction 2**	Bidirectional 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:

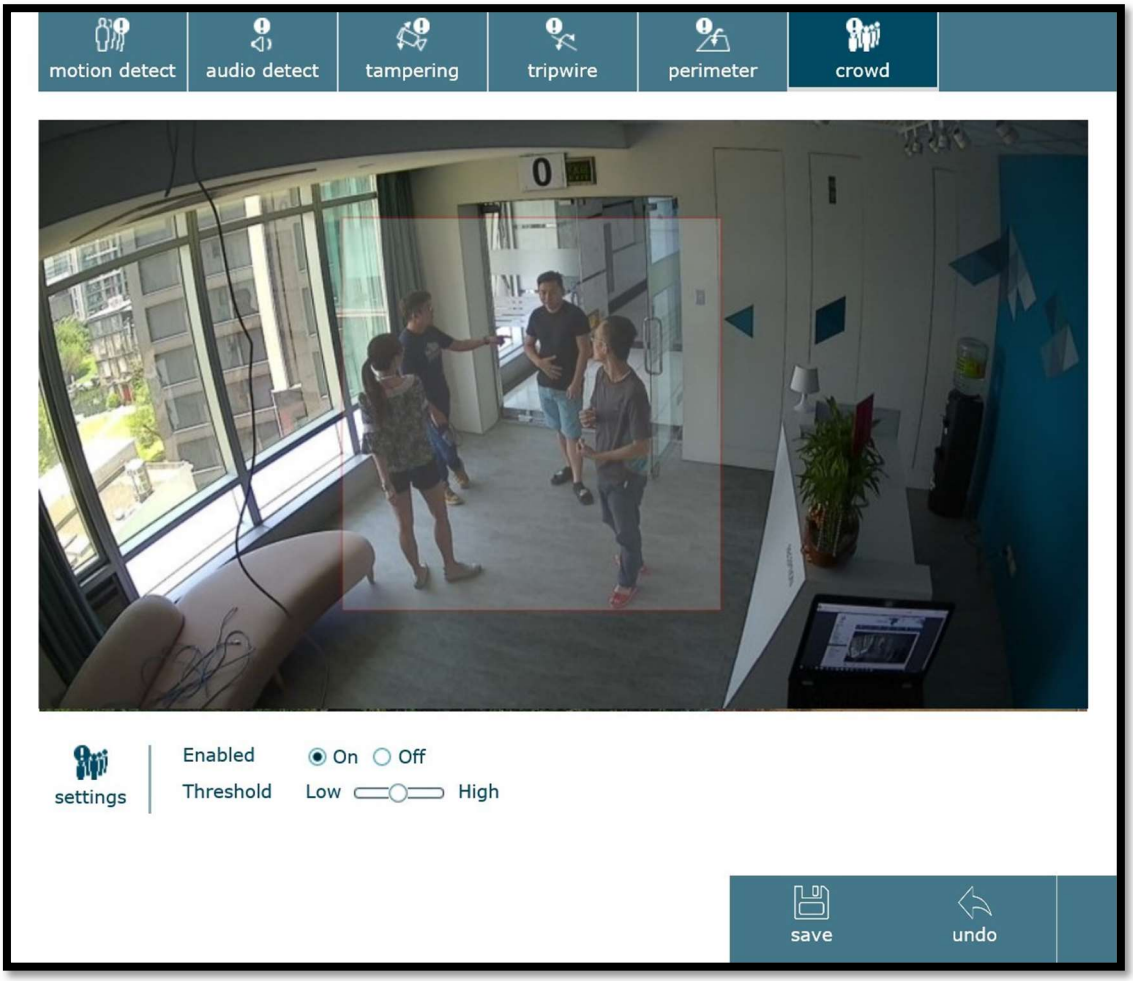
1	**Enabled**	On	Users can enabled/ disabled this function.
		Off	
2	**Sensitivity**	Value 1~10	Set the sensitivity level for perimeter detection.
3	**Polygon Edges**	4	Set the number of sides for perimeter detection area.
		5	
		6	
		7	
		8	

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

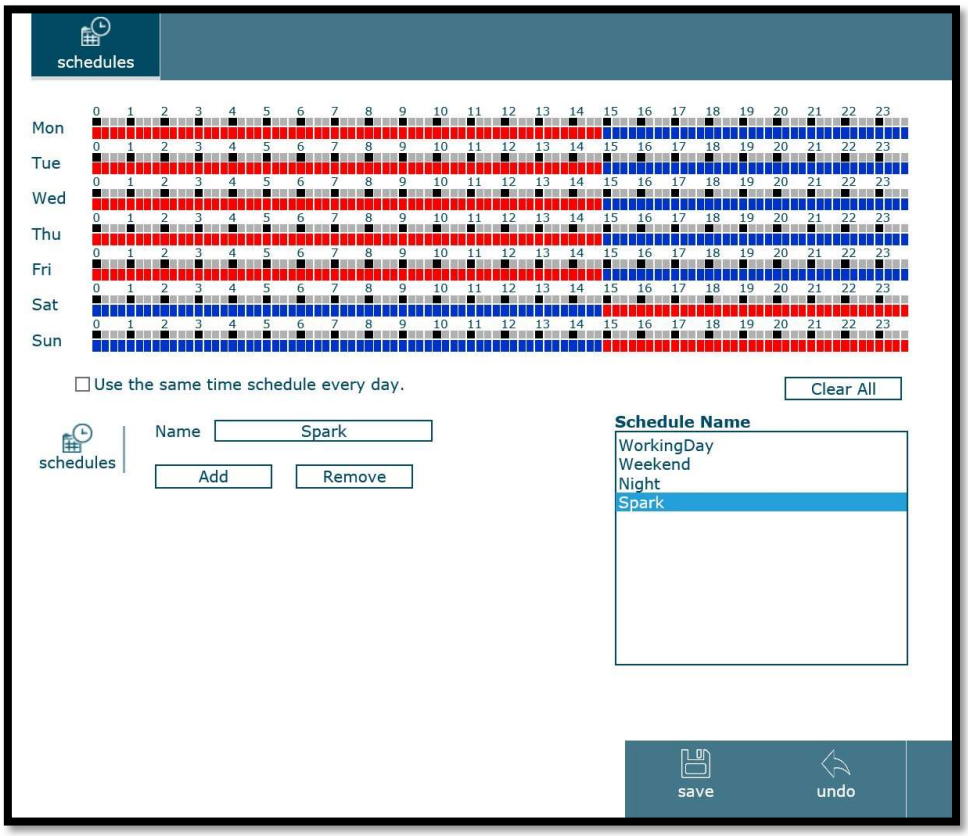
Note: Remember to click the save button to successfully apply changes.

• 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.

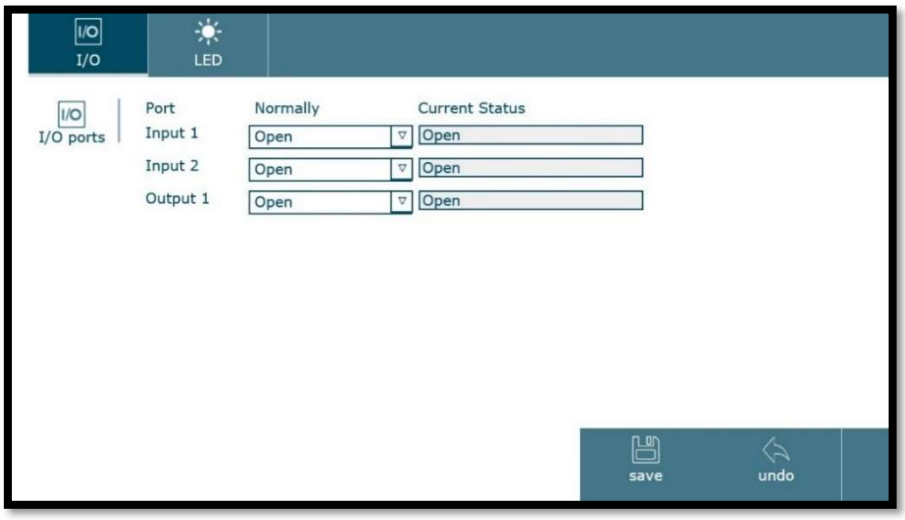
d. Step 4: Click the save button.

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

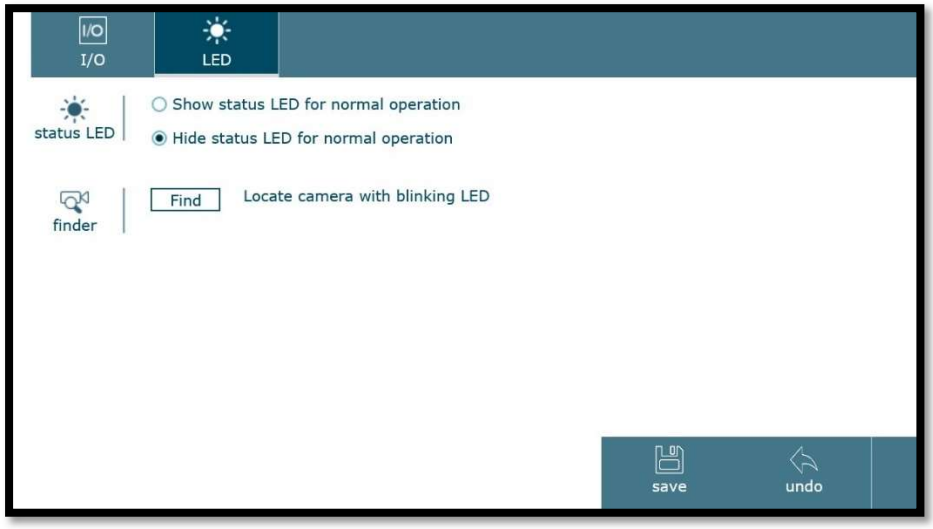


a. I/O ports:

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:

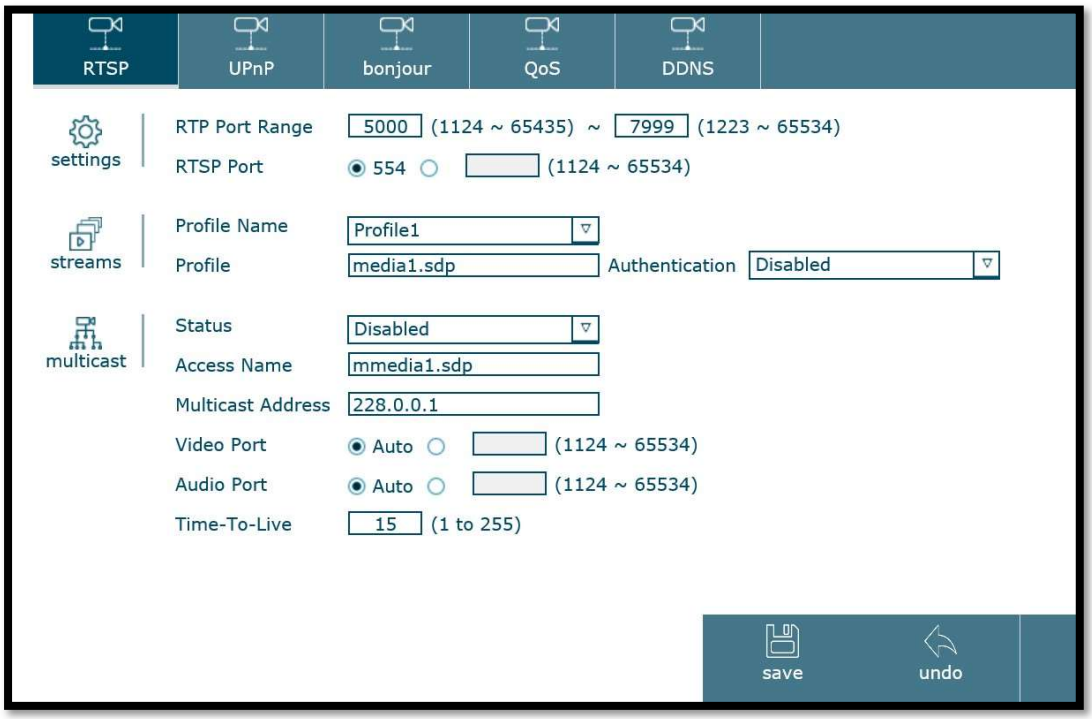
1	**Locate camera with blinking LED**	Find	This feature enables users to easily locate the camera. When users click the Find button, the LED on the IR board will blink for 30 seconds.

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:

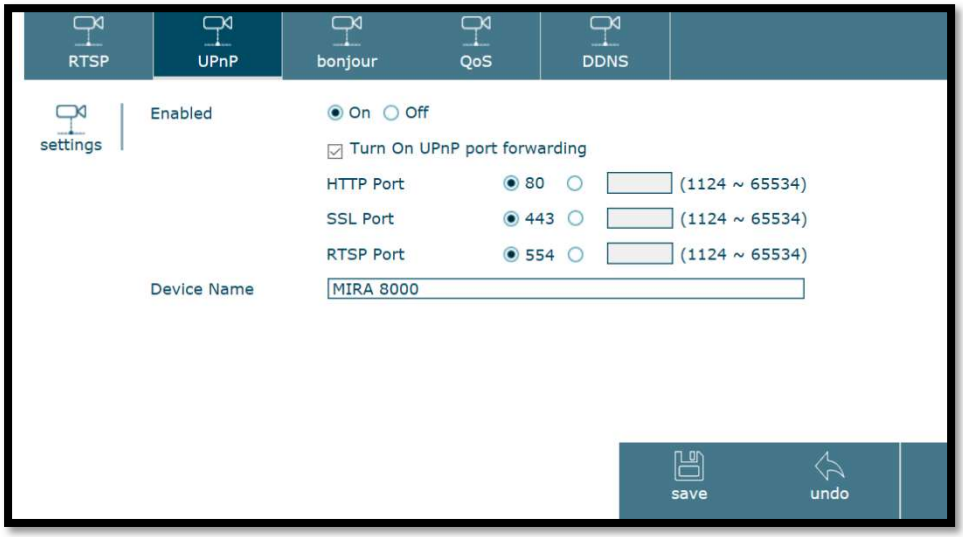
1	**Status**	Disabled Enabled	Multicasting provides efficient usage of bandwidth when there is large numbers of clients viewing simultaneously.
2	**Access Name**	mmedia1.sdp	Default access name: rtsp://camera_address/mmedia1.sdp
3	**Multicast Address**	228.0.0.1	Default address is 228.0.0.1
4	**Video 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:

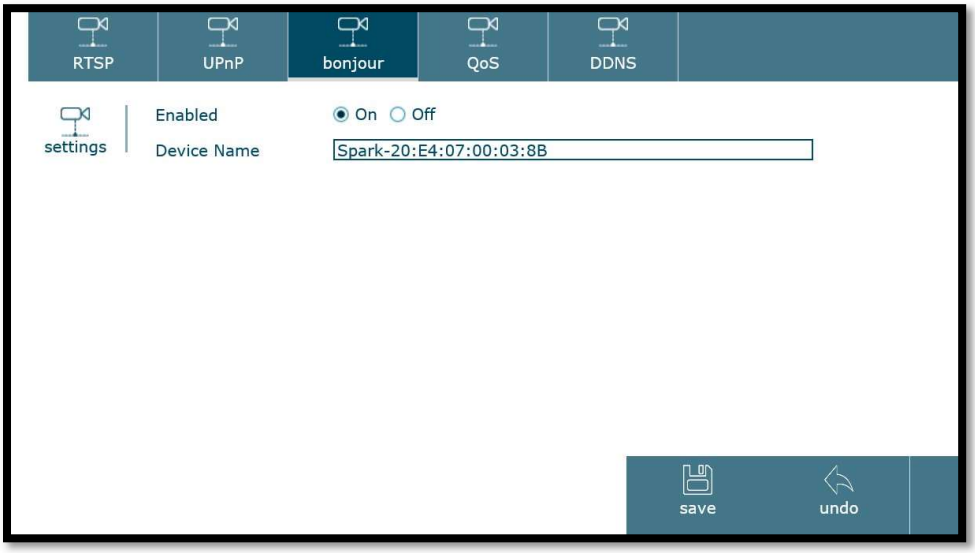
1	**Enabled**	On Off	UPnP allows the camera to announce their presence to other devices that support UPnP in the local network. Users can enabled/ disabled this function.
2	**Turn on UpnP port forwarding**	HTTP Port Value 1124~65534 SSL Port Value 1124~65534 RTSP Port Value 1124~65534	By default, the 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:

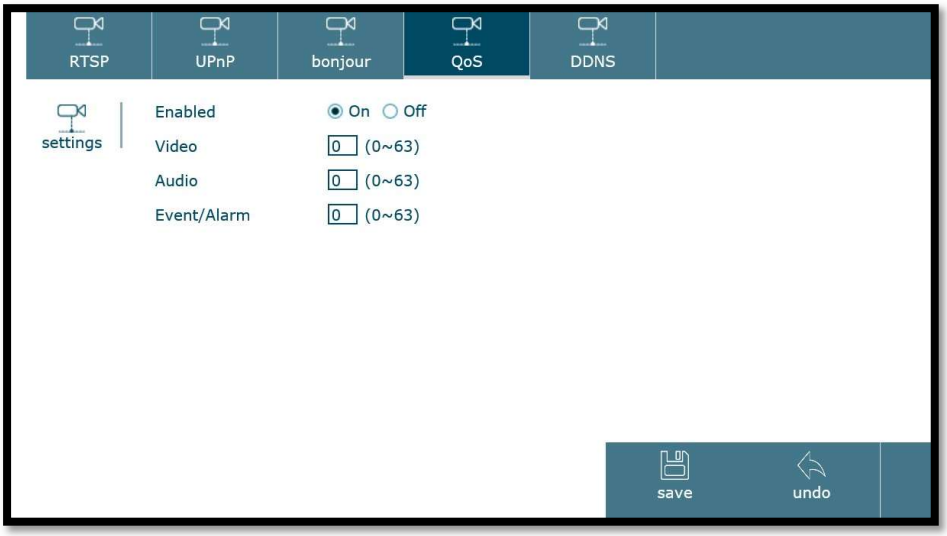
1	**Enabled**	On	Bonjour is a service that helps to find the camera on the network. This feature will be enabled by default. Users can enabled/ disabled this function.
		Off	
2	**Device Name**	Spark-20:E4:07:00:03:8B	Default device name is spark plus MAC address, but users can customize the device name.

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:

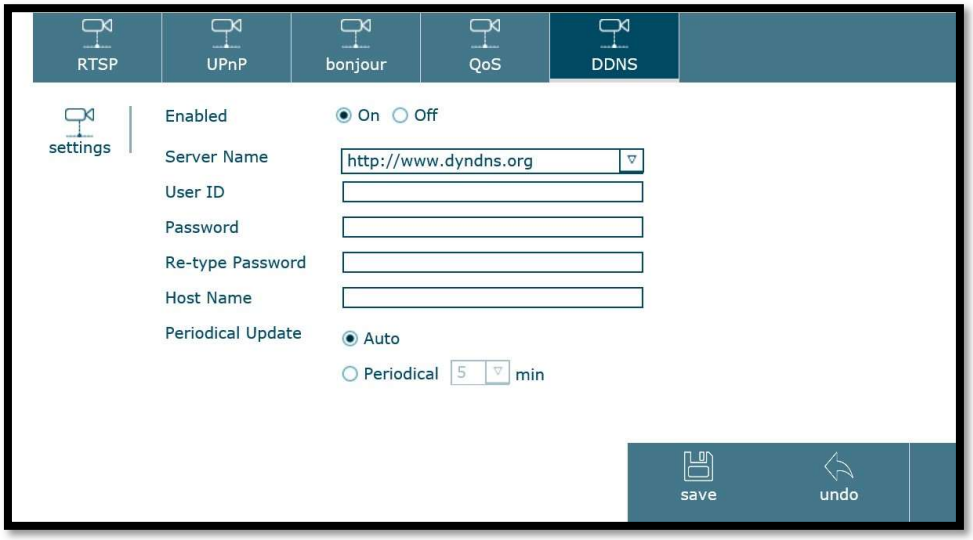
1	**Enabled**	On	QoS (Quality of Service) enables server to prioritize network traffic, providing a greater network reliability by controlling the amount of bandwidth an application may use.
		Off	
2	**Video**	Value 0~63	Insert the priority value for video packet. The higher the value the higher the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

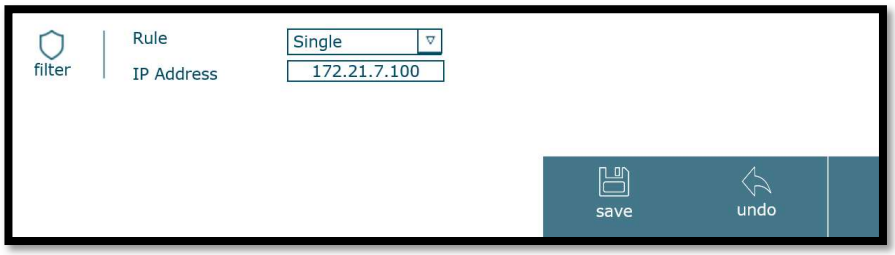


Image 62. Add/Edit IP filter page_2

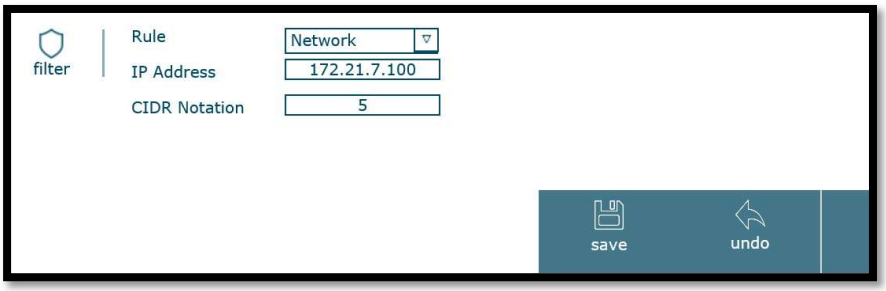
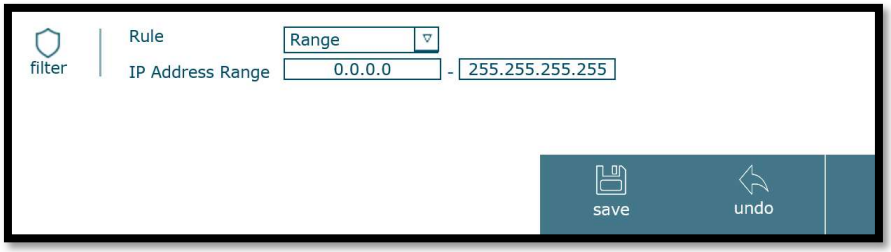


Image 63. Add/Edit IP filter page_3



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:

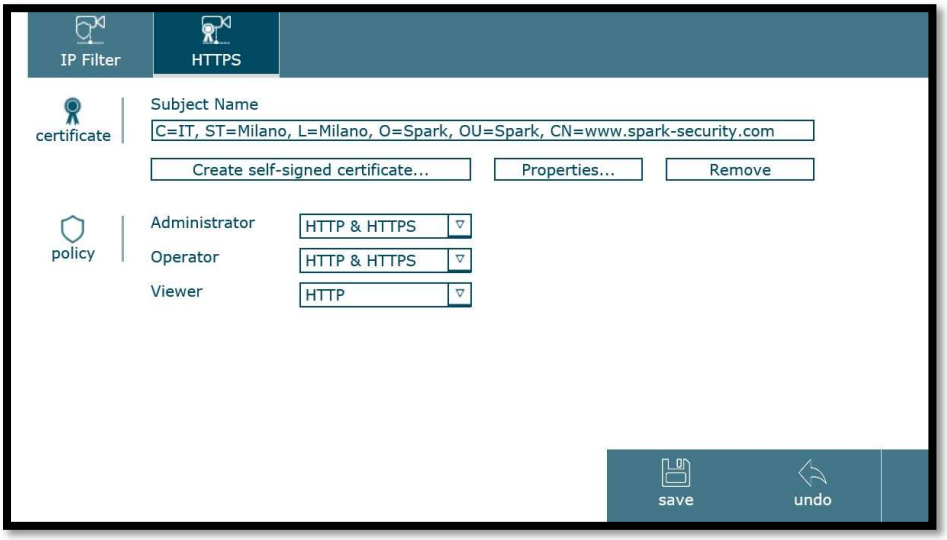
1	**Rule**	Single	Insert the IP address to allow or deny access.
		Network	Insert IP address and CIDR notation. The system will automatically allow or deny within IP range.
		Range	Insert the IP range to allow or deny access.

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:

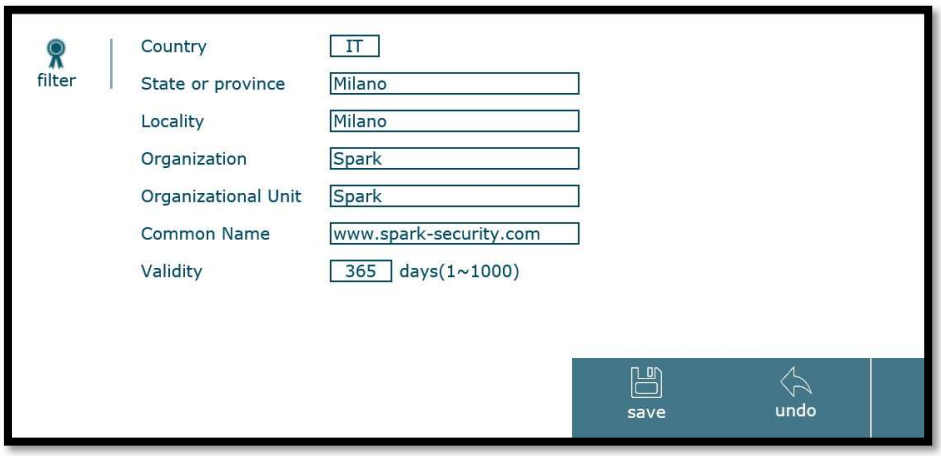
Image 64. HTTPS page



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.

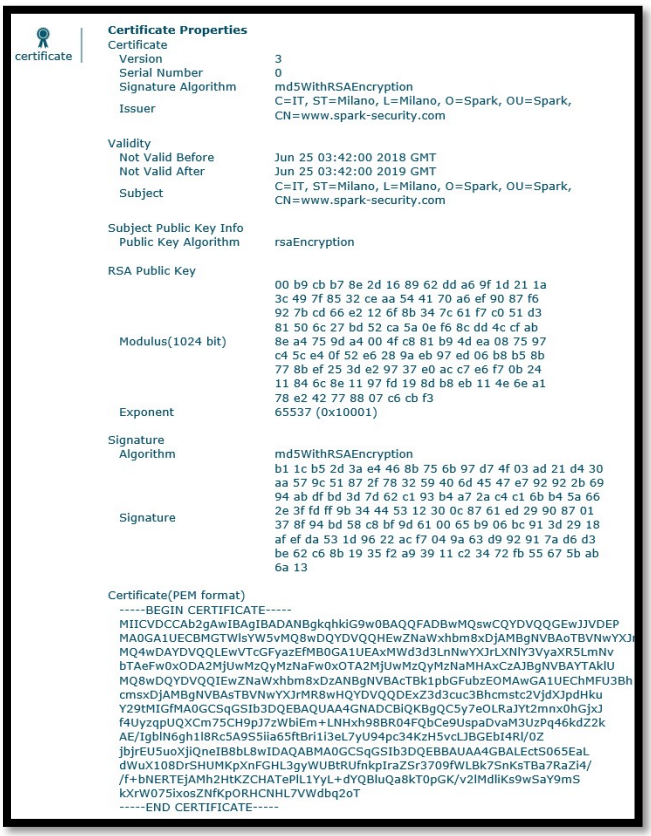
Image 65. Create self-signed certificate page



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

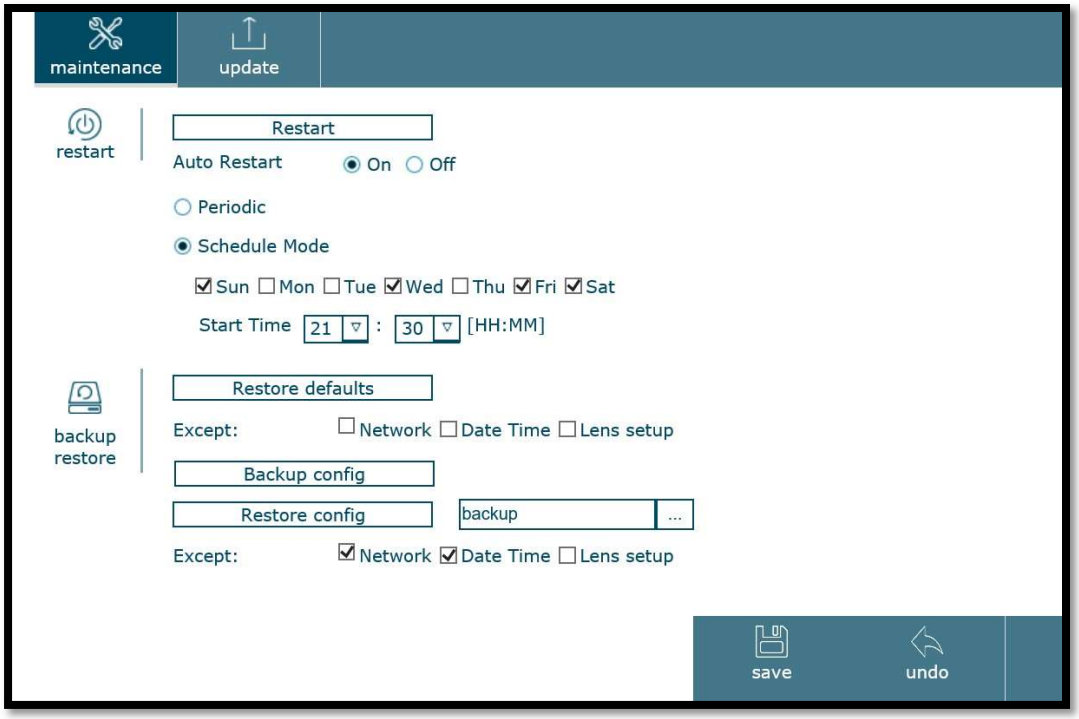
5.9 Maintenance

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:

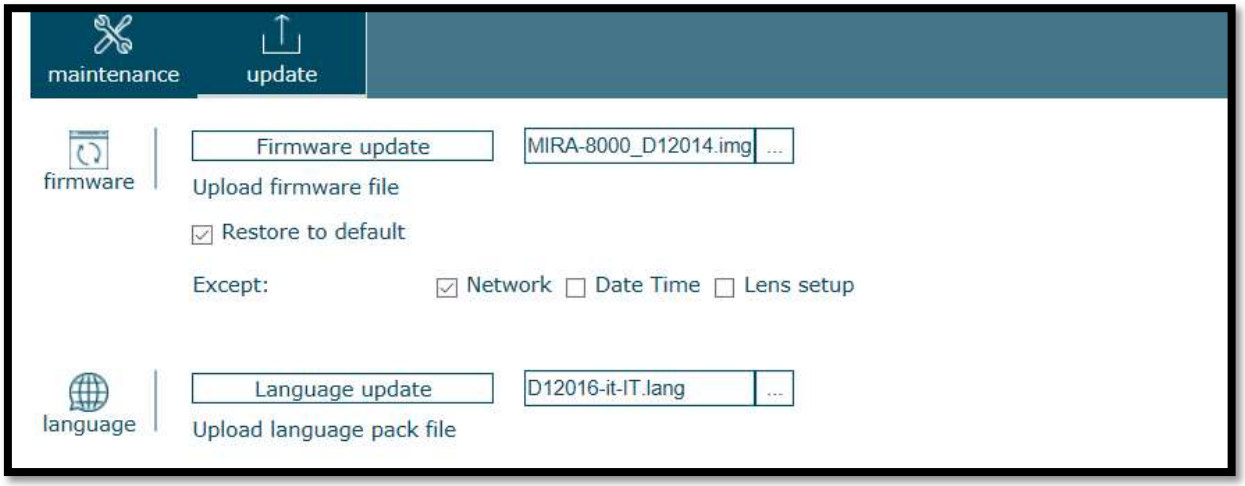
1	**Periodic**	Value 1~7 days	Set specific interval days for automatic restart.
2	**Schedule Mode**	Schedule Mode	Set specific dates and time for automatic restart.

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:

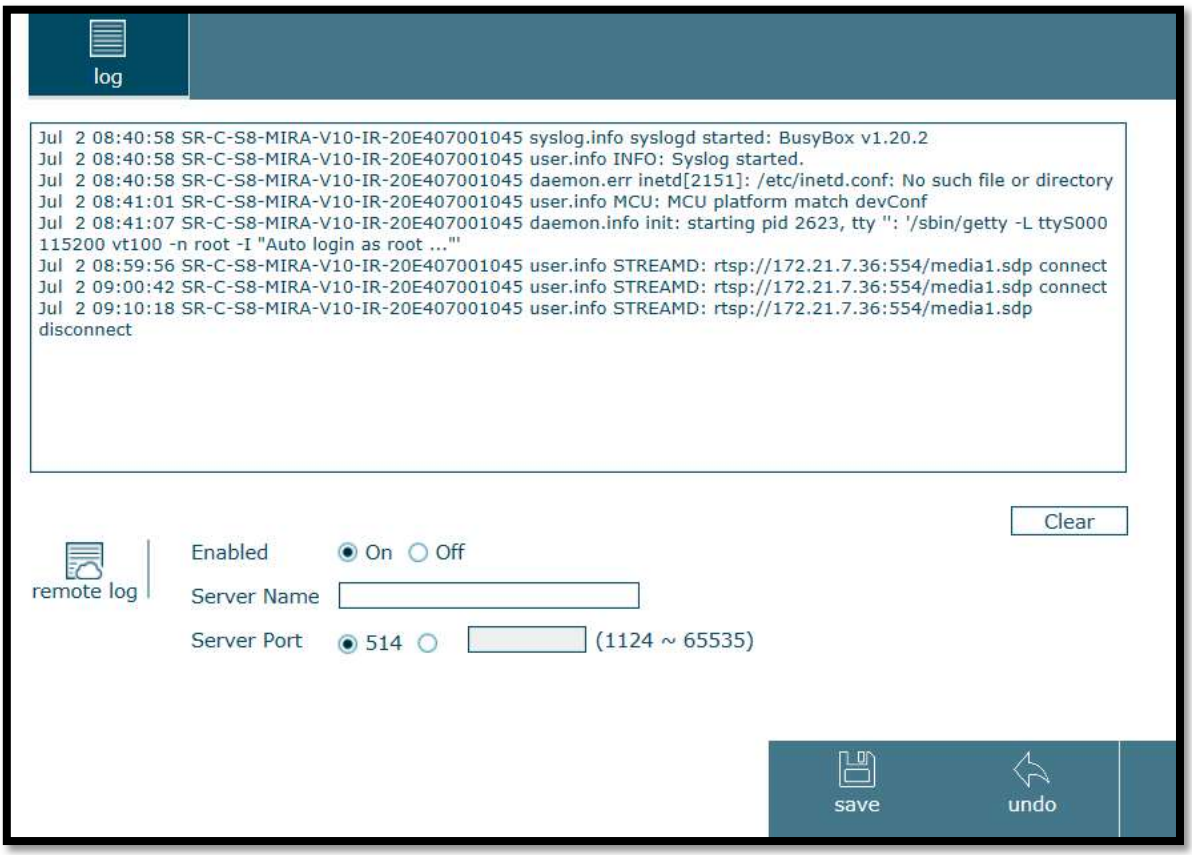
1	**Language update**	Language update	Language update allows users to change the language of the camera's web interface.

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.