



User Manual

Argo Config

V1.6





Confidentiality Notice

Copyright© 2025 Spark. All rights reserved.

This document is authored by Spark and is Spark intellectual property, including the copyrights in all countries in the world. This document is provided under a license to use only with all other rights, including ownership rights, being retained by Spark. This file may not be distributed, copied, or reproduced in any manner, electronic or otherwise, without the express written consent of Spark.



Table of contents

1. INSTALLATION	1
1.1 ARGO CLIENT AND ARGO CONFIG.....	1
1.2 ARGO RECORDER.....	1
1.3 SYSTEM REQUIREMENT.....	2
2. START	3
2.1 LOG IN.....	3
2.2 ARGO CONFIG INTERFACE	6
3. DEVICES	7
3.1 STATISTICS.....	7
3.2 VIDEO DEVICES	8
3.2.1 Add video devices (Automatic scan/ Manual add).....	8
3.2.2 Edit video devices	11
3.2.3 Delete video device	19
3.2.4 Preview video devices.....	19
3.2.5 Video devices configurations	20
3.2.6 Open device web interface.....	23
3.3 INTERCOMS.....	24
3.3.1 Add Intercoms	24
3.3.2 Edit Intercoms	25
3.3.3 Delete Intercoms	25
3.4 I/O MODULE.....	26
3.4.1 Add I/O module (Auto scan/Manual add).....	26
3.4.2 Edit I/O module.....	28
3.4.2.1 Advantech/ ICPDAS/ Pongee	28
3.4.2.2 Soyal	29
3.4.3 Delete I/O modules	32
3.4.4 Browse I/O modules information and status	32
3.5 SPARK AI DEVICE	33
3.5.1 Add Spark AI Device	34
3.5.1.1 All / Human / Vehicle Detection Devices	34
3.5.1.2 LPR Detection Devices	34
3.5.1.3 MLPR Detection Devices	34
3.5.1.4 Fire & Smoke Devices	35
3.5.1.5 Generic AI Device	37
3.5.1.6 Face Detection	38
3.5.1.7 HTTP POST Device	39
3.5.2 Add Camera to Spark AI Devices	41
3.5.2.1 All/ Vehicle/ Human Detection	41
3.5.2.2 LPR/MLPR Detection	42
3.5.2.3 Fire and Smoke Detection	43
3.5.2.4 Generic AI	43
3.5.2.5 Face Detection	44
3.5.3 Edit Spark AI Devices.....	45
3.5.3.1 All/Human/Vehicle – Parameter Settings	47
3.5.3.2 Taiwan License Plate Device - Parameter Settings	50
3.5.3.3 Multi-country License Plate Device - Parameter Settings-	52
3.5.3.4 Fire and Smoke Detection - Parameter Settings Description	54
3.5.3.5 General AI Device - Parameter Settings Description	60



3.5.3.6 Face Detection - Parameter Settings Description	61
3.5.4 Delete Spark AI Device Stream Analysis	62
3.5.5 Delete Spark AI Device	62
3.5.6 INFO	63
3.6 OTHER SETTINGS.....	64
3.6.1 Database settings	64
3.6.2 License plate recognition upload settings	65
3.6.3 AI Analytics	66
3.6.4 External Network Settings	66
3.6.5 Web server settings.....	68
3.7 STORAGE.....	69
3.7.1 Add storage	69
3.7.2 Edit storage.....	70
3.7.3 Delete storage	70
3.8 INFORMATION.....	71
3.8.1 Information	71
3.8.2 Installed services	71
3.9 SERVER.....	72
3.9.1 Primary server and secondary servers.....	72
3.9.2 Add server.....	73
3.9.3 Delete server	76
3.10 VIEW MODE.....	77
4. USER MANAGEMENT.....	78
4.1 PASSWORD SETTINGS	78
4.2 GROUPS.....	79
4.2.1 Create groups.....	79
4.2.2 Set schedules for each group	79
4.2.3 Set permissions for each group:.....	80
4.2.4 Delete group	83
4.3 USER.....	84
4.3.1 Add user	84
4.3.2 Delete User.....	85
4.4 CLIENT CONNECTION INFORMATION	85
5. HEALTH DOCTOR.....	86
5.1 SYSTEM HEALTH CHECK CONFIGURATION	86
5.2 ADD RESPONSE ACTION.....	87
5.2.1 Send email	88
5.2.2 Line Notify	90
5.3 EDIT RESPONSE ACTION	91
5.4 DELETE RESPONSE ACTION	91
5.5 EXECUTE RESPONSE ACTION	92
6. EVENT AND MANAGEMENT	93
6.1 ADD/EDIT/COPY/DELETE EVENT	94
6.2 EVENT BEHAVIOR.....	96
6.3 TRIGGER CONDITIONS	97
6.3.1 Add trigger condition	97
6.3.2 Advanced Setting for Trigger Conditions.....	100
6.3.3 Edit trigger condition.....	100
6.3.4 Delete trigger condition	101
6.4 RESPONSE ACTION.....	102



6.4.1	Response action schedule	102
6.4.2	Add response action.....	103
6.4.3	Edit response action.....	110
6.4.4	Delete response action	110
6.4.5	Execute response action	110
6.5	SET THE EVENT AS ALARM	111
6.5.1	Edit alarm setting	112
7.	ACCESS CONTROL.....	115
7.1	ADD/EDIT/DELETE LIST	115
7.2	ACCESS ID.....	116
7.2.1	Add access ID	116
7.2.2	Edit access ID	117
7.2.3	Deactivate/Clear access ID	118
7.2.4	Export/Import access ID.....	119
8.	VIDEO ANALYTICS DATA COLLECTION.....	122
8.1	SENS CAM SETTINGS.....	122
8.1.1	Login settings	122
8.1.2	Image setting	123
8.1.3	Analytics settings	124
8.2	VIDEO ANALYTICS DATA COLLECTION SETTINGS	126
8.2.1	Add video analytics parameters.....	126
8.2.2	Set video analytics parameters.....	126
8.2.3	Delete video analytics parameter	127
9.	BACKUP AND RESTORE	128
9.1	BACKUP.....	128
9.2	RESTORE	128
9.3	SCHEDULED BACKUP	129
10.	LICENSE	130
10.1	INFORMATION	130
10.2	MANAGE LICENSE	130
10.3	CHANNEL LICENSE KEY	131
10.4	INTEGRATED DEVICES.....	131
11.	LOG	132
11.1	DATA TRACE	132
11.2	SYSTEM LOG	134
11.3	DETAILED LOG.....	136
12.	ARGO CLIENT	137
13.	OPTIONS	138
13.1	LANGUAGE	138
13.2	INTERFACE	138
13.3	RENDERING.....	139
13.4	USER INTERACTION MODE	141
13.5	WATERMARK	142
13.6	SYSTEM.....	143



14.	USER	144
14.1	CHANGE PASSWORD.....	144
14.2	LOGOUT/CLOSE.....	144
15.	ABOUT	145
16.	OTHER.....	146
16.1	APPLYING FOR LINE MESSAGE TOKEN	146
16.2	APPLYING FOR GMAIL TWO-STEP VERIFICATION FOR APP PASSWORD.....	150
16.3	APPLYING FOR NGROK ACCOUNT TUTORIAL	152



1. INSTALLATION

Argo software is divided into three modules: Argo Client, Argo Config and Argo Recorder. The following content will provide a basic introduction to these three applications:

1.1 Argo Client and Argo Config

Argo Client installation file contains two modules: Argo Client and Argo Config.

- Argo Client: for monitoring real-time images, e-maps, playback, export images, etc.
- Argo Config: for managing users and connected devices, set events, etc.

1.2 Argo Recorder

Use setup_Spark_Argo_Recorder.exe installation file to install Argo Recorder. Argo Recorder will start automatically when the Windows system starts. Note that Argo Config and Argo Client applications can only be used once Argo Recorder is active. Argo Recorder acts as the recording server.

To avoid hardware overload, it is recommended to use different servers. Install Argo Recorder on one server for recording purposes and install Argo Client and Argo Config on another server to act as the main server for real-time viewing and configuration.

Below are reference values to facilitate users the calculation of their specific server requirement. The specific server requirements may vary according to different scenarios.

- CPU: Allocate 90 CPU marks per camera. You can search for suitable CPU specifications on the following website (https://www.cpubenchmark.net/high_end_cpus.html)
e.g.: If you need 50 cameras, the required CPU score would be 90 multiplied by 50, resulting in a total of 4500. After calculating the total score, you can visit the above website to find an appropriate CPU. Additionally, we recommend adding a buffer of 1800 points to ensure the system operates perfectly.
- RAM: 160GB or more
- Operating system: Windows 10(64-bit)
- HDD: Requirement varies depending on camera quantity, recording time and resolution.



- 1 camera recording 20MP for 24hrs requires 211GB.
- 1 camera recording 5MP for 24hrs requires 63GB.
- 1 camera recording 2MP for 24hrs requires 42GB.

1.3 System Requirement

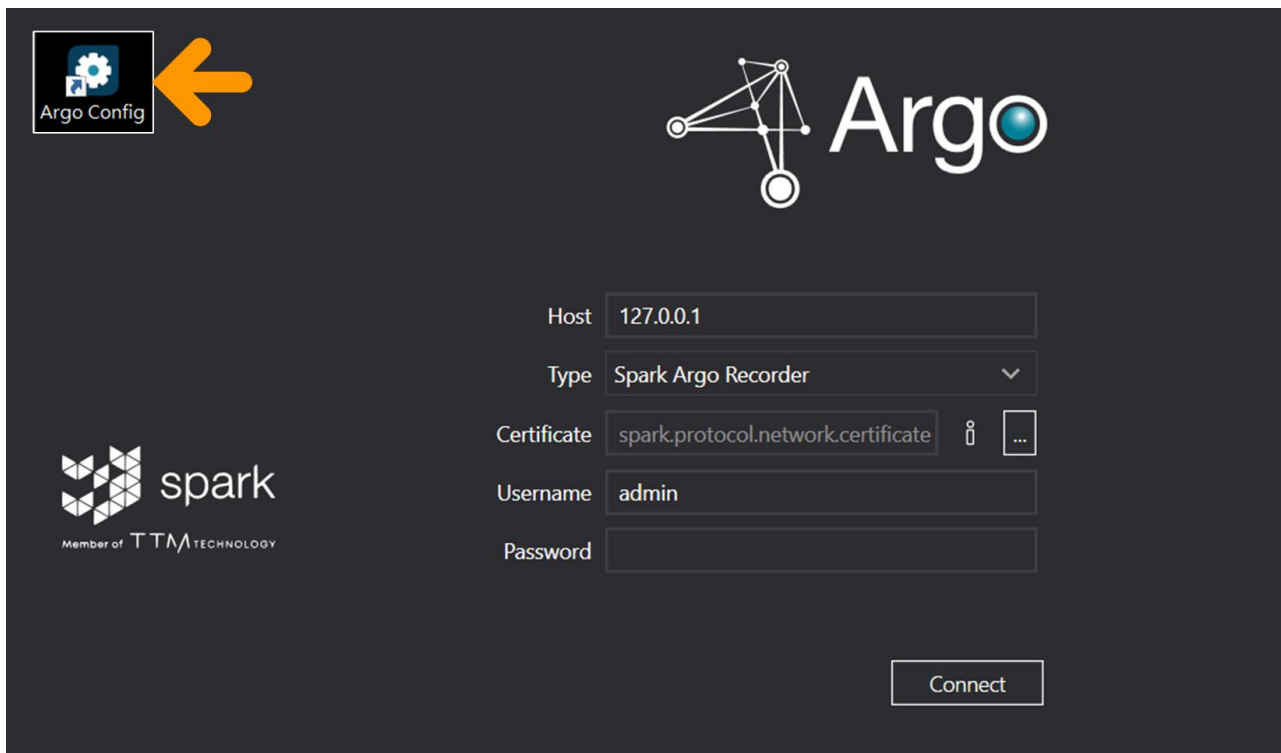
- Spark Client + Config minimum system requirements
CPU: Intel Core i5 @ 2.7GHz RAM 4GB
Disk space: 500 MB free disk space
Graphics Card: 1GHz, 1GB RAM
Screen Resolution: 1920x1080 Network Card Gigabit Ethernet
Operating System: Windows 11 (64-bit)
- Spark Player minimum system requirements
CPU: Intel Core i5 @ 2.7GHz RAM 4GB
Graphics Card: 1GHz, 1GB RAM Screen Resolution: 1024x768
Operating System: Windows 11(32-bit or 64-bit)
- Spark Recorder minimum system requirements
CPU: Intel Core i5 @ 2.7GHz RAM 8GB
Network Card: Gigabit Ethernet
Operating System: Windows 11(64-bit)



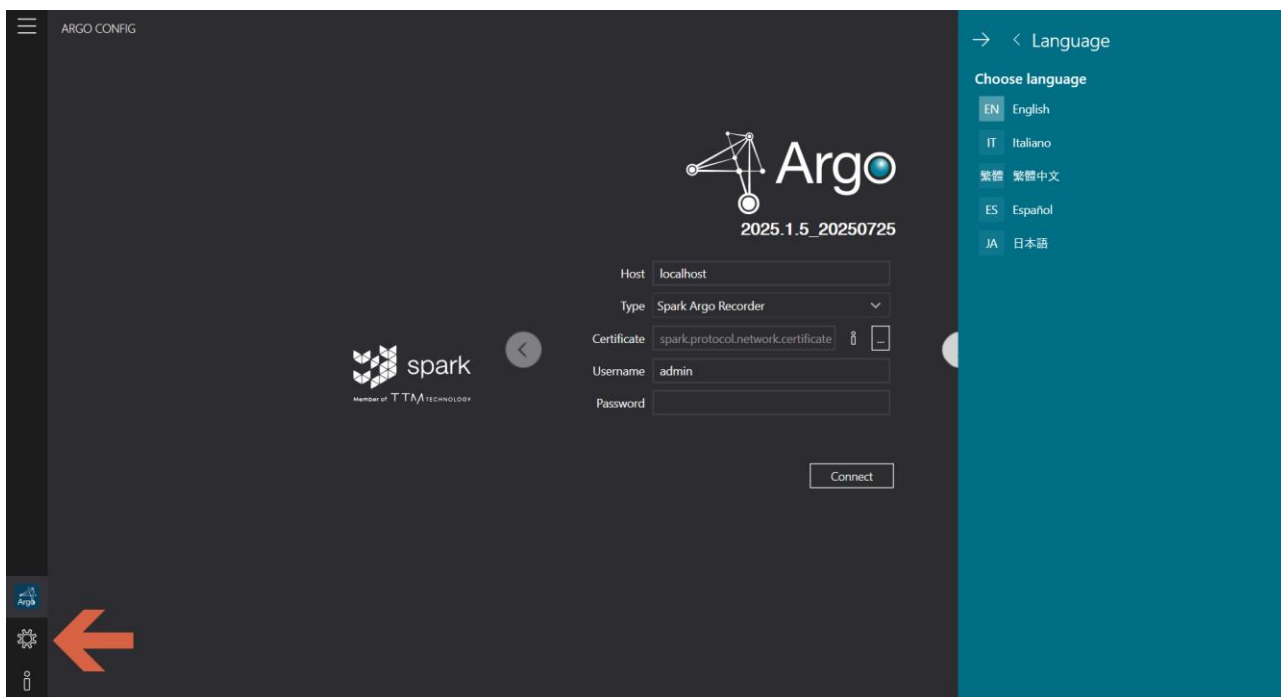
2. START

2.1 Log in

Step1: Double click Argo config to open login window



Step2: Select language



- Click [**Options**] at the bottom left and then click [**Language**].
- After selecting the language, click [**Save**] to save the settings.



Step3: Log in Argo config

Host: 127.0.0.1

Type: Spark Argo Recorder

Certificate: spark.protocol.network.certificate

Username: admin

Password:

Connect

- Server: Insert Spark Recorder server' s IP address or insert default IP **127.0.0.1**
- Type: Spark Argo Recorder (default)
- Certificate: Click [...] to automatically navigate to the default authentication folder and select the file.
- Username: **admin** (default)
- Password: **admin** (default)
- Click [**Connect**]

Step4: On first login, you will be asked if you want to import the certificate. Click Yes to save the certificate in the system.

The specified certificate is not stored in the system configuration directory.
Would you like to import the certificate into the system configuration? (Recommended option)

Yes No



Step5: After logging in, the system will ask to change the password. The new password must contain at least one special character, one upper case letter, one lower case letter and a minimum length of 8 characters.

i Change User Password

Username

Old password

New password

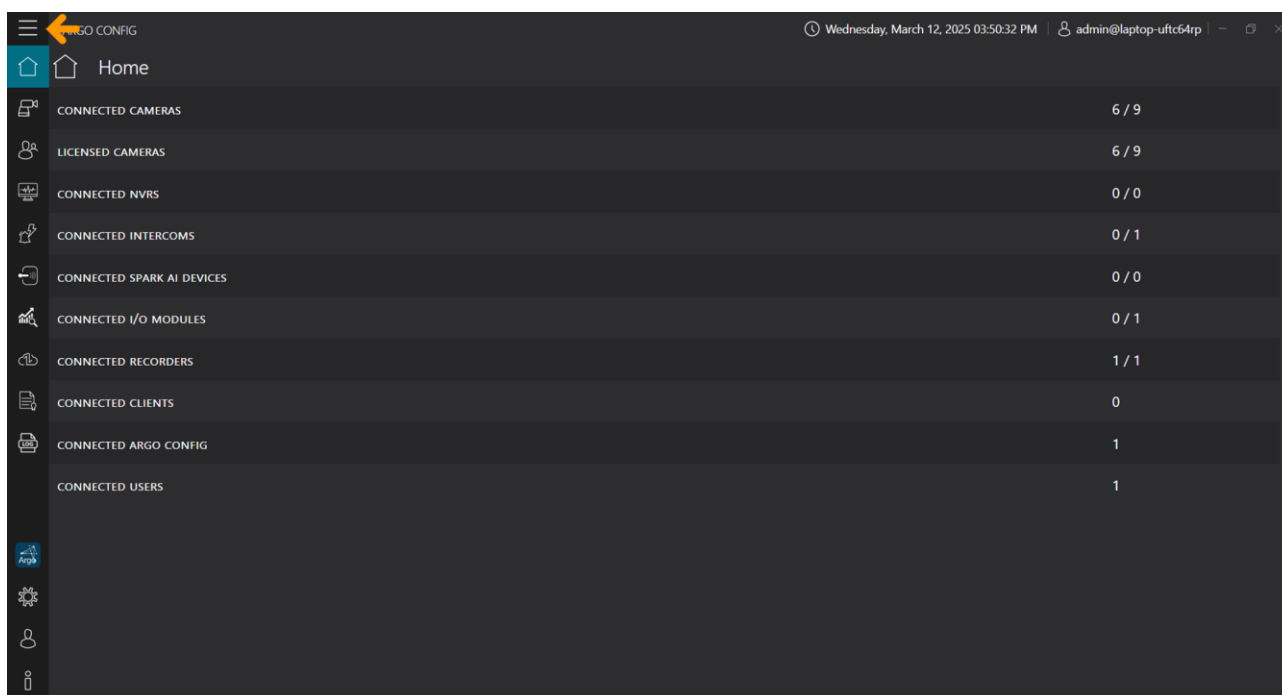
Confirm password

Note: After completing the initial password change, please note the following:

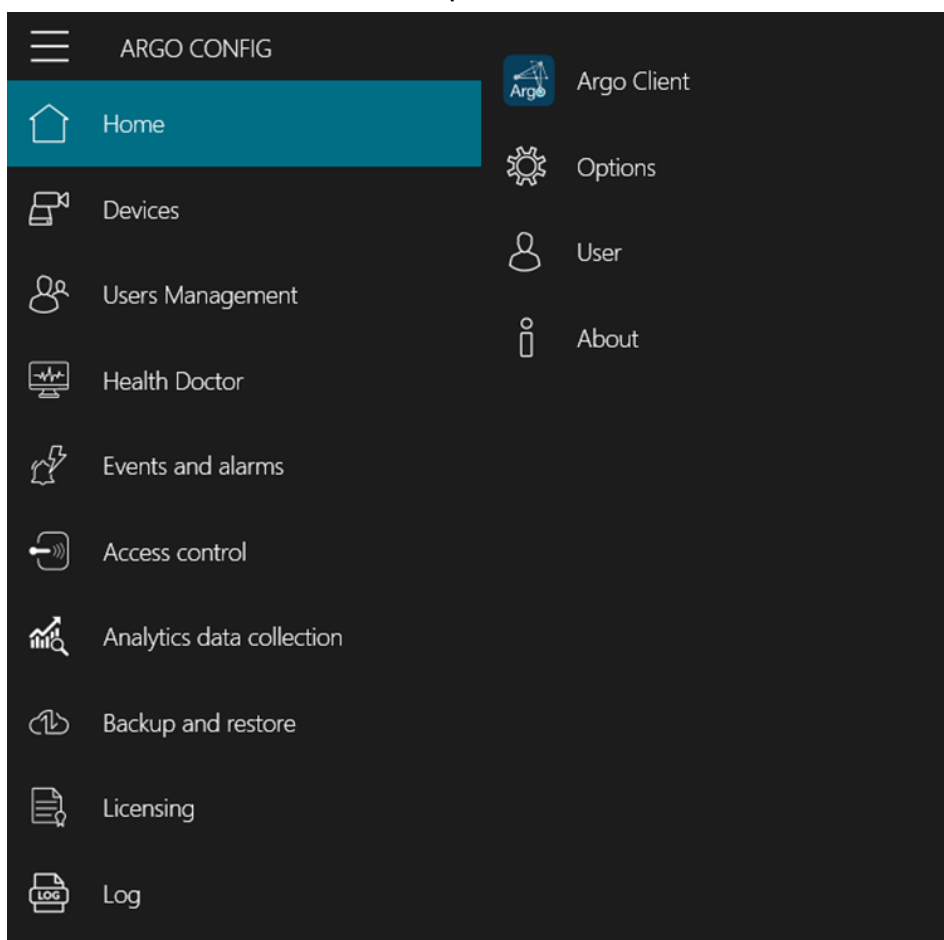
- When using single login interface, users only need to insert the changed password to log in.
- When using quick login interface, users must change the default password to the changed password to log in.



2.2 Argo config interface



- Click the [☰] icon at the top left to browse the icon text



- Menu: Devices/ User management /Health Doctor/Events and alarms/Access Control/ Analytics data collection/Licensing/Log/Argo client/Options/User/About



3. DEVICES

3.1 Statistics

ARGO CONFIG Friday, June 07, 2024 10:35:59 AM admin@spark

Devices Recorder on SPARK

Recorder on SPARK spark - 127.0.0.1

STATISTICS

CPU (11TH GEN INTEL(R) CORE(TM) I7-1165G7 @ 2.80GHZ - 1)
LOGICAL PROCESSORS 8
CPU USAGE 13%

MEMORY
9.75 GB/15.66 GB

STORAGE
TOTAL STORAGE CAPACITY 1.14 TB
USED SPACE FOR RECORDING 128.00 GB
FREE SPACE 439.19 GB

DEVICES
CONNECTED CAMERAS 2

VIDEO DEVICES I/O MODULES OTHER SETTINGS STORAGE INFO

Select all

VIDEO DEVICES

SELECT	ADDRESS	MODEL NAME	STATUS	DEVICE NAME	RECORDING ENABLED
<input type="checkbox"/>	192.168.2.232	BM2	Ready	Camera 1	No
<input type="checkbox"/>	192.168.2.235	SR-C-A2-DF1-F3-IR	Ready	Camera 4	No

2 Video devices
0 Recording devices

Add Delete Scan Add Done Edit

- Click on **[Statistics]**
- Browse device status on Statistics: CPU/memory/Storage/Device



3.2 Video Devices

3.2.1 Add video devices (Automatic scan/ Manual add)

A. Automatic scan

The screenshot shows the ARGO CONFIG interface for a recorder on LAPTOP-UFTC64RP. The 'VIDEO DEVICES' tab is selected, and a modal window is open for adding devices. The modal window displays a table of available devices with the following columns: Selection, Address, Model name, Product code, MAC Address, Vendor, Status, and Added to recorders. The table contains 16 rows of device information. The 'Scan' button at the bottom right of the modal is highlighted with a yellow arrow.

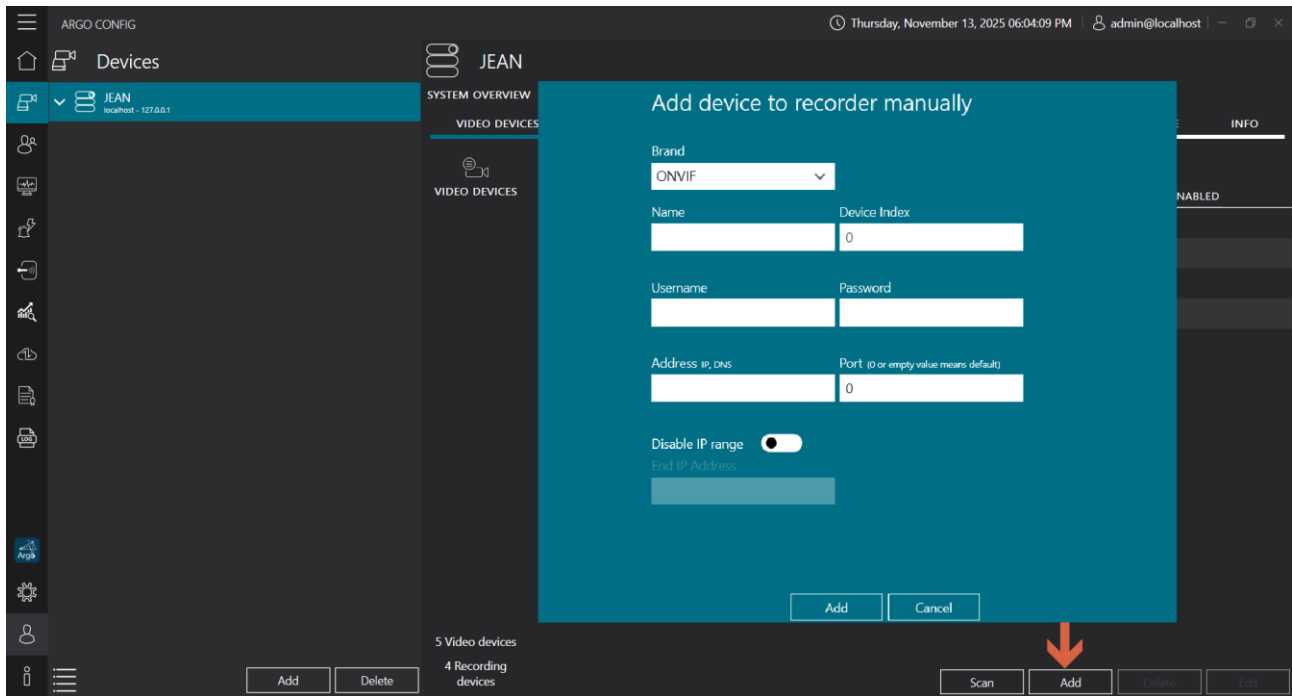
Selection	Address	Model name	Product code	MAC Address	Vendor	Status	Added to recorders
<input type="checkbox"/>	172.21.7.81	Mixa 7MP-12mm (Dome)	SR-C-S2-MIXA-V12-IR	20E4D70002EC	Spark	Available	
<input type="checkbox"/>	172.21.7.81	Mixa 7MP-12mm (Dome)	SR-C-S2-MIXA-V12-IR	20E4D70002EC	CHNRF	Available	
<input type="checkbox"/>	172.21.7.82	Omnikey Advanced Series	SR-C-A5-8M2-V13-IR-2	20E4D70018AF	Spark	Available	
<input type="checkbox"/>	172.21.7.82	Omnikey Advanced Series	SR-C-A5-8M2-V13-IR	20E4D70018AF	CHNRF	Available	
<input type="checkbox"/>	172.21.7.84	Nitida 20000	SR-C-100-NITIDA-M	20E4D7335566	Spark	Available	
<input type="checkbox"/>	172.21.7.84	Nitida 20000	SR-C-100-NITIDA-M	20E4D7335566	CHNRF	Available	
<input type="checkbox"/>	172.21.7.85	Bullet 7MP-10mm	SR-C-E5-R2-V10-IR	20E4D7003366	Spark	Available	
<input type="checkbox"/>	172.21.7.85	Bullet 7MP-10mm	SR-C-E5-R2-V10-IR	20E4D7003366	CHNRF	Available	
<input type="checkbox"/>	172.21.7.89	00	0295F746C827	MET	Available		
<input type="checkbox"/>	172.21.7.56	Bullet 7MP-10mm	SR-C-E2-B1-V12-IR	20E4D70002FF	Spark	Available	
<input type="checkbox"/>	172.21.7.56	Bullet 7MP-10mm	SR-C-E2-B1-V12-IR	20E4D70002FF	CHNRF	Available	
<input checked="" type="checkbox"/>	172.21.7.89	Omnikey Advanced Series	SR-C-A2-PM2-V12S-IR	20E4D7004797	Spark	Added	Recorder on LAPTOP-UFTC64RP

- Click **[Scan]** at the bottom right.
- Select devices and then click **[Add]**
- Username: Insert device username.
- Password: Insert device password.

Remarks: For different devices with the same username and password, you can select add simultaneously. For devices with different usernames and passwords, you will need to insert separately.



B. Add Manually



- Click **[Add]** at the bottom right.
- Brand: Select device brand name (below list for reference)
- IP address: Insert device IP address
- Port: Insert device port number (default is 0)
- Enable IP range: insert desired IP range
- Username: Insert device username.
- Password: Insert device password.

Brand	Description
AMTK	AMTK devices
Generic	Supports RTSP URL. If the camera model is displayed as Unknown, you may add it using the Generic API.
ICE	ICE license plate recognition devices
LPR Reader	License plate recognition devices
Milesight	Milesight devices
ONVIF	ONVIF compliant devices
Spark	Spark devices



C. Adding Camera Streams from NVR/DVR

Add device to recorder manually

Brand
Generic

Name Device Index
 Device Index 0

Username Password

Address IP, DNS RTSP Port (0 or empty value means default)
 RTSP Port 0

Disable IP range

End IP Address

RTSP URL

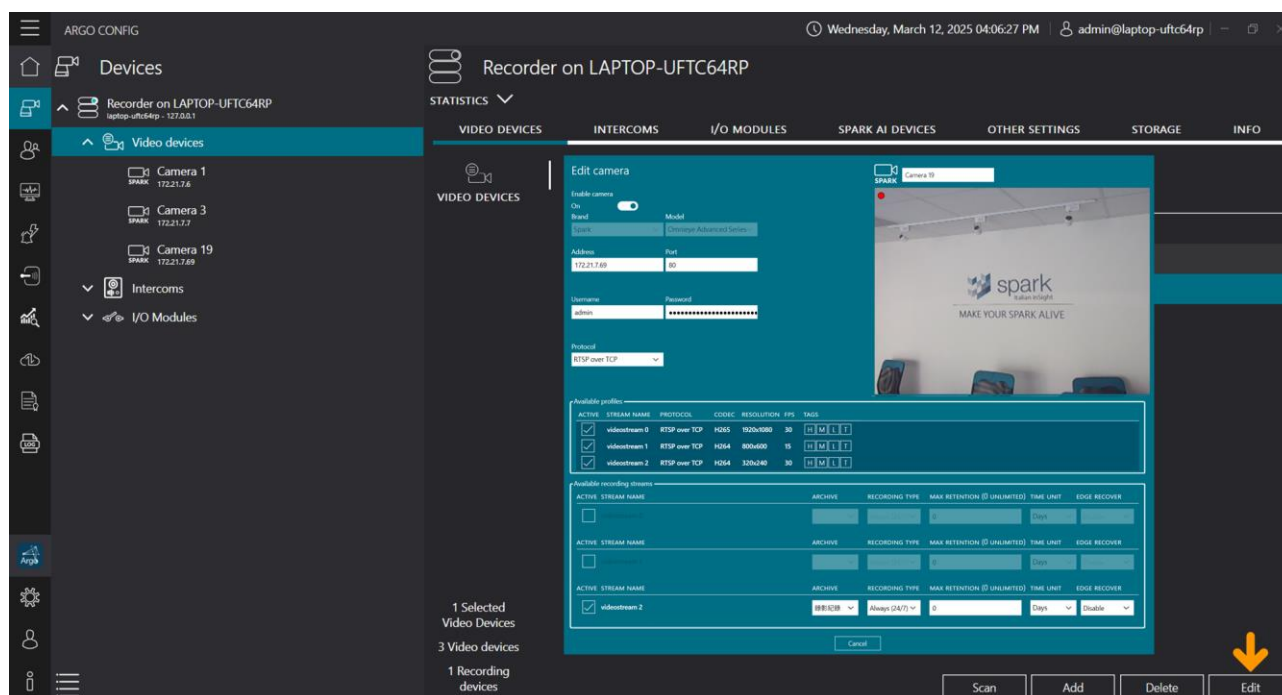
ACTIVE	URL
<input type="checkbox"/>	rtsp://\$USERNAME:\$PASSWORD@\$IPADDRESS:\$RTSPPORT/ media1.amp
<input type="checkbox"/>	rtsp://\$USERNAME:\$PASSWORD@\$IPADDRESS:\$RTSPPORT/ media2.amp
<input type="checkbox"/>	rtsp://\$USERNAME:\$PASSWORD@\$IPADDRESS:\$RTSPPORT/ media3.amp

Add Cancel

- Click **[Add]** at the bottom-right corner.
- Brand: Select Generic.
- Name: Enter the camera name.
- Index: Default is 0. (The app sorts cameras in ascending order based on the index number.)
- IP Address: Enter the device IP address or DNS.
- RTSP Port: Default is 0.
- Username: Enter the device account name.
- Password: Enter the device password.
- Enable/Disable IP Range: The system will add multiple cameras automatically based on the configured IP range.
- RTSP URL: Select the stream to enable and enter the required RTSP path (RTSP paths vary by camera brand).

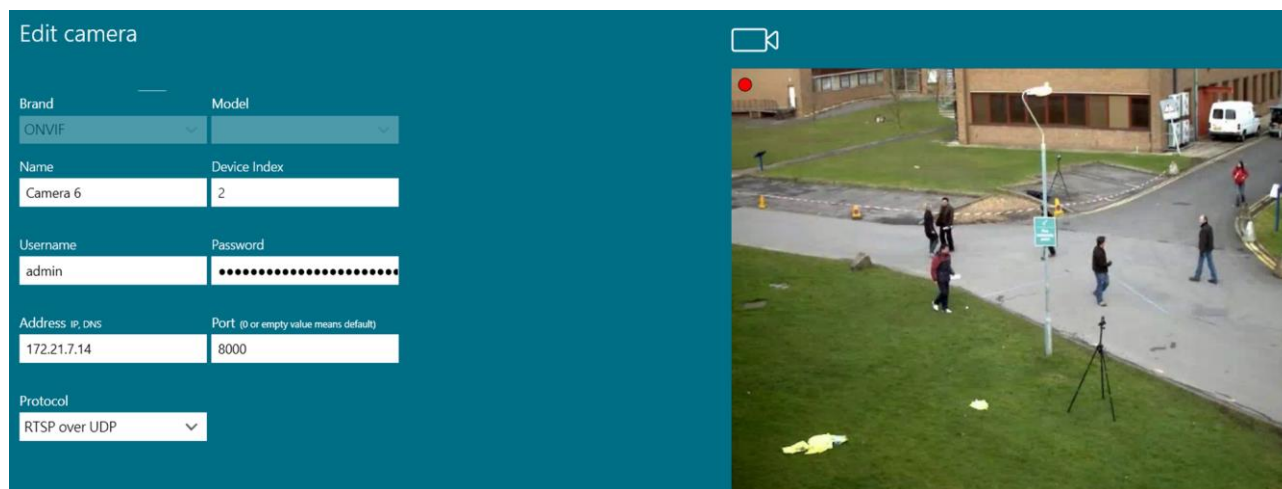


3.2.2 Edit video devices



- Select Check the video device you want to edit and click **[Edit]** at the bottom right.

Step 1. Edit camera



- Brand: selected during camera addition, cannot be modified.
- Model: selected during camera addition, cannot be modified.
- IP address: edit device IP address
- Port: edit device port number (default is 0)
- Username: edit device username.
- Password: edit device password.
- Protocol: select protocol (TCP/UDP/HTTP)



Step 2. Available profiles

ACTIVE	STREAM NAME	PROTOCOL	CODEC	RESOLUTION	FPS	TAGS
<input checked="" type="checkbox"/>	videostream 0	RTSP over TCP	H264	1920x1080	30	[H] [M] [L] [T]
<input checked="" type="checkbox"/>	videostream 1	RTSP over TCP	H264	1280x720	5	[H] [M] [L] [T]
<input checked="" type="checkbox"/>	videostream 2	RTSP over TCP	H264	320x240	30	[H] [M] [L] [T]

- Select the profile(s) to display (default is all enabled).

Step 3. Available recording streams

Recording license enabled

Available recording streams

ACTIVE	STREAM NAME	ARCHIVE	RECORDING TYPE	MAX RETENTION (0 UNLIMITED)	TIME UNIT	EDGE RECOVER
<input checked="" type="checkbox"/>	videostream ProfileToken_1	Archive	Scheduled	0	Days	Disable

Week's day: Everyday [⋮] →

Selected time slot: 12:00 AM : 12:00 AM (+1h) (Interval duration: 24h : 00m)

Recording on event: Continuous (no event-base)

ACTIVE	STREAM NAME	ARCHIVE	RECORDING TYPE	MAX RE
<input type="checkbox"/>	videostream ProfileToken_2		Always (24/7)	0

Edit days

Monday: Off

Tuesday: Off

Wednesday: Off

Thursday: Off

Friday: Off

Saturday: Off

Sunday: Off

Cancel

- Recording functionality can be used only after the recording license is enabled.
- Select the stream for recording
- Archive: select folder for recording on hard drive. You need to add storage space first (refer to Device 1.5 Storage)
- Recording type: select recording schedule
 - Always (24/7): Continuous recording (24 hours a day, 7 days a week).
 - Scheduled: Select the recording time slot.
 - Manual: Manually start and stop recording

Week's day: Everyday [⋮]

Selected time slot: 12:00 AM : 1:00 AM (Interval duration: 01h : 00m)

- Add schedule: Click [+] and drag left or right to adjust the time slot, or input the selected time slot.
- Delete schedule: Select the time slot you want to delete and click [-].
- Edit schedule: Select the time slot and drag left or right to adjust it, or input the selected time slot.

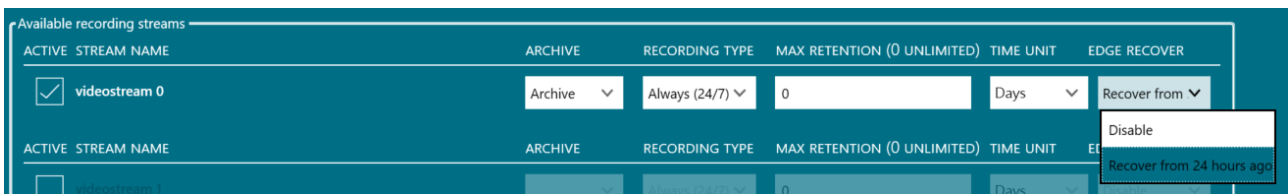


- E. Event triggered recording: select always (non-event triggered) or event.
- always (non-event triggered): records according to schedule.
 - Event X: select event and set range of seconds for recording of pre and post event triggers.
 - Pre event recording: starts recording N seconds before the event is triggered.
 - Post event recording: keeps recording N seconds after the event is triggered.
- Recording range: 0 to 300 seconds

- F. Max. retention: when the recording storage space is full, clearing space will retain recording files from the previous N hours/days.

Note that if the maximum retention is 0, existing recording files will be overwritten based on the actual disk size and recording will continue.

- G. Time unit: select the time unit for maximum retention space.



- H. Edge Recover: select Recover from 24 hours ago/Disable, activate/deactivate edge recover.
- Mechanism: prevents expected interruptions in recording caused by improper use of camera cables or deterioration of network cables causing disconnection, leading to the inability to trace past recording records.
 - Advantages: When the camera disconnects from the server, preventing recording on the server's hard drive, it will instead record onto the camera's SD card. Upon reconnection to the server, Argo's failover mechanism seamlessly integrates the camera's recording into the server's hard drive, ensuring uninterrupted recording.
 - Camera and System Configuration
Divided into three parts: OMNIEYE camera settings, Argo Config system settings, and Argo Client system settings.
For OMNIEYE cameras, please insert the IP address of the camera to configure parameters for edge recover. The default IP address is 192.168.1.219



a. OMNIEYE camera settings

Step 1. Time settings

The screenshot shows the OMNIEYE SECURITY web interface. The top navigation bar includes 'Live View', 'Playback', 'Configuration', and a language dropdown set to 'English'. The left sidebar has a 'System' menu item highlighted. The main content area is titled 'Date & Time' and contains several tabs: 'Date & Time', 'Audio', 'Firmware', 'Initialization', 'OSD', and 'Events'. The 'Date & Time' tab is active, showing 'Basic Setting' and 'Time Zone Setting' sections. In the 'Basic Setting' section, the 'Synchronization Mode' is set to 'Synchronize with PC', which is highlighted with a red box. The 'Time Zone Setting' section shows 'GMT+8' selected in a dropdown menu.

- In advanced settings click **[System]**
 - Select **[Date and Time]**
- Basic settings-Synchronization Mode: Click **[Synchronize with PC]**.
- Time zone settings- Select the correct time zone and click **[Save]**.
- E.g. for Taiwan time, select GMT+8.

Step 2. Event Source - Time Schedule Settings

The screenshot shows the OMNIEYE SECURITY web interface. The top navigation bar includes 'Live View', 'Playback', 'Configuration', and a language dropdown set to 'English'. The left sidebar has an 'Event Source' menu item highlighted. The main content area is titled 'Event Source' and contains several tabs: 'Alarm', 'Audio', 'Defocus', 'Motion', 'Network', 'Schedule', 'Tamper', and 'mSD healthiness'. The 'Schedule' tab is active, showing 'Basic Setting' and 'Handlers' sections. In the 'Basic Setting' section, the 'Enable' checkbox is checked and highlighted with a red box. In the 'Handlers' section, the 'Edge Record' checkbox is checked and highlighted with a red box.

- In advanced settings click **[Event Source]**.
 - Select **[Schedule]**
- In basic settings click [enable]
- Basic settings - Process method - recording click **[Edge record]** then click **[Save]**



Step 3. Event configuration- recording settings

The screenshot shows the 'Event Setting' configuration page. The 'Record Status' dropdown is set to 'Continuous' and is highlighted with a red box. The 'Record Type' is 'Video', 'Clip Size' is '50', and 'Record Codec' is 'H264'.

- In advanced settings click **[Event Setting]**
 - Select **[Record settings]**
- Basic settings- recording status select **[continuous]** and click **[save]**

Step 4. Event configuration - SD card

The screenshot shows the 'SD Card' configuration page. The 'Overwrite' dropdown is set to 'On' and is highlighted with a red box. The 'Format' button is also highlighted with a red box.

- In advanced settings click **[Event Setting]**
- Select **[SD card]**
- Click **[Format]** to format the SD card and check if it is functioning properly and if the capacity is correct.
- It is recommended to enable the overwrite function (default is disabled). Then click **[Save]**.



b. Argo Config system configuration

Step 5. License

CHANNELS LICENSE		SUMMARY OF INSTALLED LICENSES PER CHANNEL						
LICENSE NAME		LICENSE NAME	TYPE	USED	AVAILABLE	TOTAL	EXPIRATION DATE	STATUS
		Omnieye Advanced Series channel license	Trial	2	6	8	9/15/2024	OK
		ONVIF channels license	Trial	2	6	8	9/15/2024	OK
		RFID reader license	Trial	1	0	1	9/5/2024	OK

- Check Argo license status to see if there is a channel available for the OMNIEYE Advanced Series.

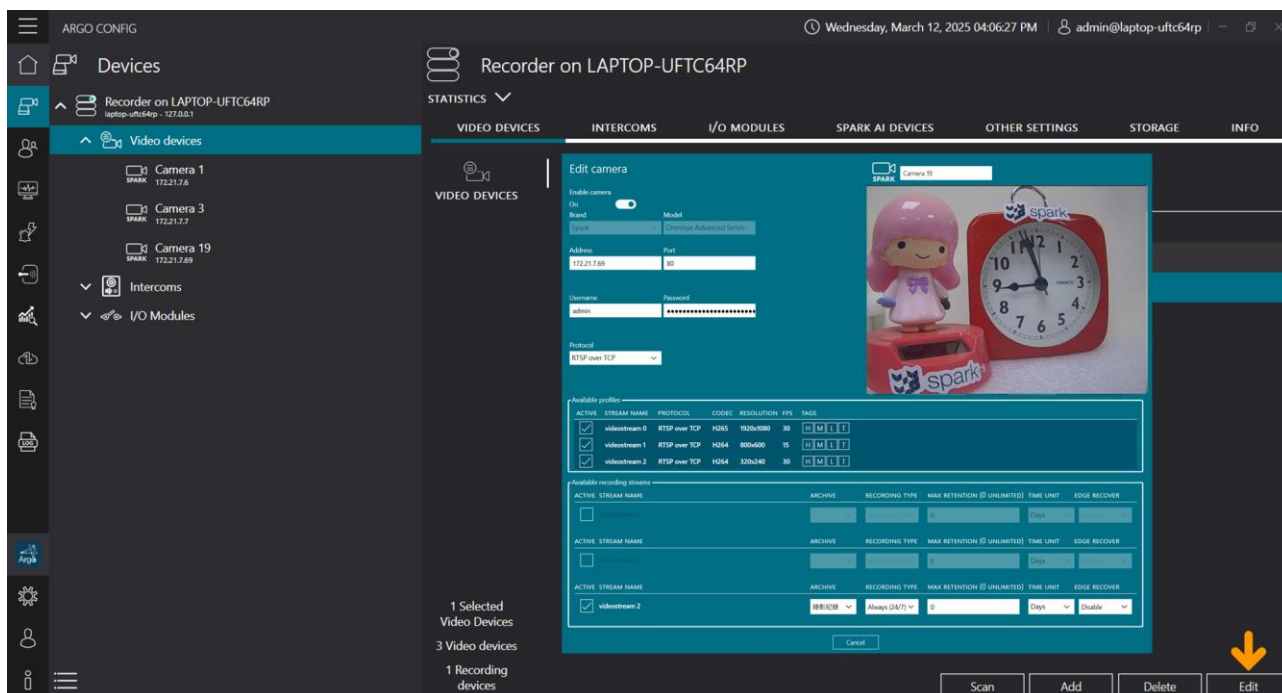
Step 6. Add device - video devices

The screenshot shows the 'Recorder on LAPTOP-UFTC64RP' configuration page. A modal window titled 'Add devices to recorder: Recorder on LAPTOP-UFTC64RP (laptop-uftc64rp)' is open, displaying a list of available video devices. The list includes columns for Selection, Address, Model name, Product code, MAC Address, Vendor, Status, and Added to recorders. A yellow arrow points to the 'Scan' button at the bottom right of the modal.

Selection	Address	Model name	Product code	MAC Address	Vendor	Status	Added to recorders
<input type="checkbox"/>	172.21.7.41	Mira 2MP-12mm (Dome)	SR-C-S2-MIRA-V12-IR	20E4D7000CEC	Spark	Available	
<input type="checkbox"/>	172.21.7.41	Mira 2MP-12mm (Dome)	SR-C-S2-MIRA-V12-IR	20E4D7000CEC	ONVIF	Available	
<input type="checkbox"/>	172.21.7.42	Omnieye Advanced Series	SR-C-A5-IM2-V13-IR-2	20E4D70018AF	Spark	Available	
<input type="checkbox"/>	172.21.7.42	Omnieye Advanced Series	SR-C-A5-IM2-V13-IR-2	20E4D70018AF	ONVIF	Available	
<input type="checkbox"/>	172.21.7.44	Nitida 2000	SR-C-L00-NITEIDA-M	20E4D0335586	Spark	Available	
<input type="checkbox"/>	172.21.7.44	Nitida 2000	SR-C-L00-NITEIDA-M	20E4D0335586	ONVIF	Available	
<input type="checkbox"/>	172.21.7.45	Bullet 2MP-10mm	SR-C-E5-B0-V10-IR	20E4D7003366	Spark	Available	
<input type="checkbox"/>	172.21.7.45	Bullet 2MP-10mm	SR-C-E5-B0-V10-IR	20E4D7003366	ONVIF	Available	
<input type="checkbox"/>	172.21.7.49		00	0295F746C827	MIT	Available	
<input type="checkbox"/>	172.21.7.56	Bullet 2MP-10mm	SR-C-E2-B1-V12-IR	20E4D70002FF	Spark	Available	
<input type="checkbox"/>	172.21.7.56	Bullet 2MP-10mm	SR-C-E2-B1-V12-IR	20E4D70002FF	ONVIF	Available	
<input checked="" type="checkbox"/>	172.21.7.69	Omnieye Advanced Series	SR-C-A2-PM1-V12R-IR	20E4D0304297	Spark	Added	Recorder on LAPTOP-UFTC64RP



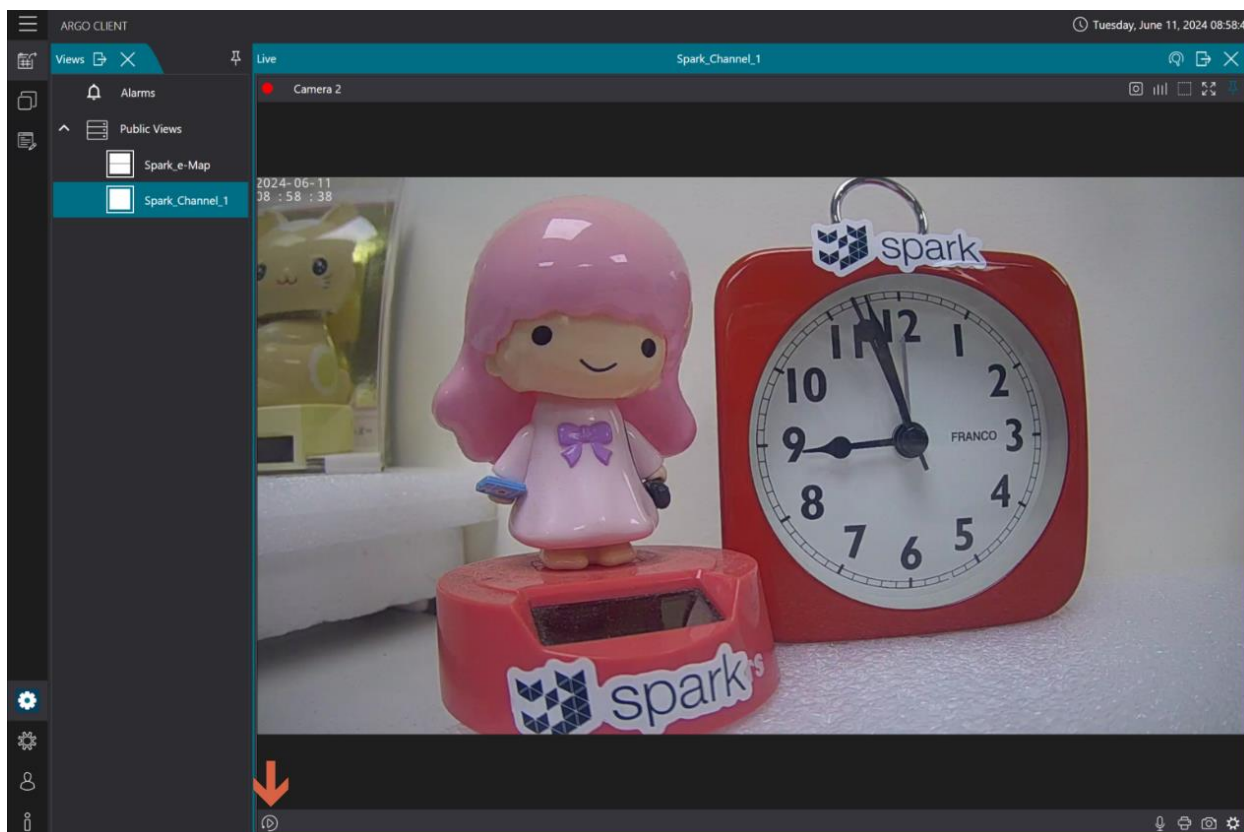
Step 7. Edit device - video devices



- Select device and click **[edit]**
- After selecting available profiles, set the failover setting to **[Recover from 24 hours ago]**

c. Argo Client system configuration

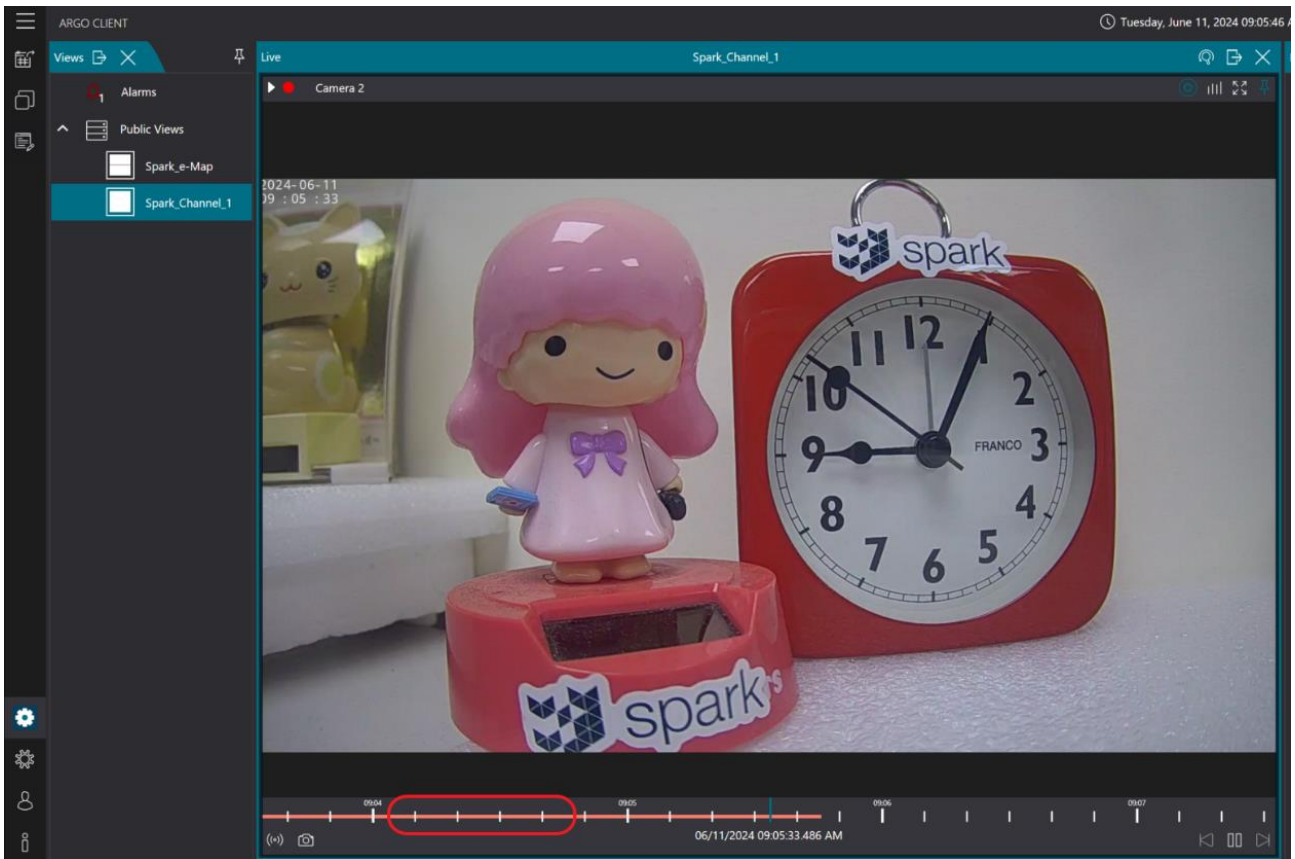
Step 8. monitoring interface





- In Argo Client, select the camera for which you want to view the failover recording, then click [**Instant Playback**].

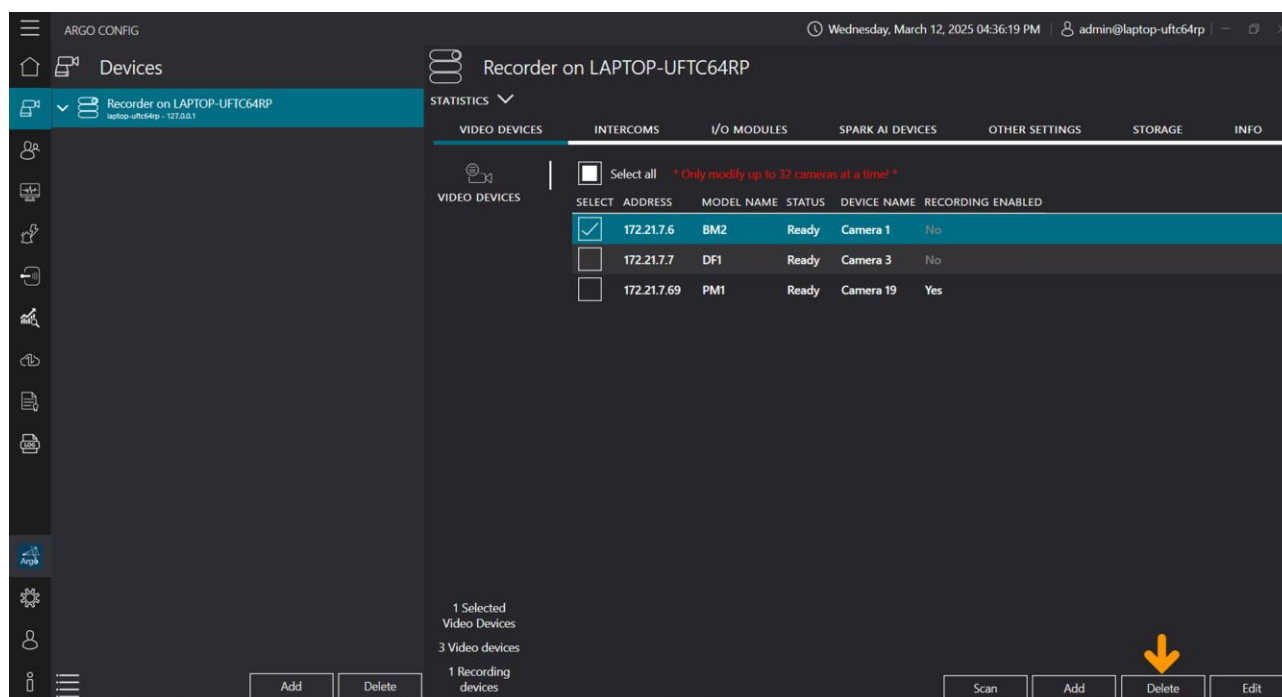
Step 9. Playback



- Select camera disconnection time slot to playback the failover recording.

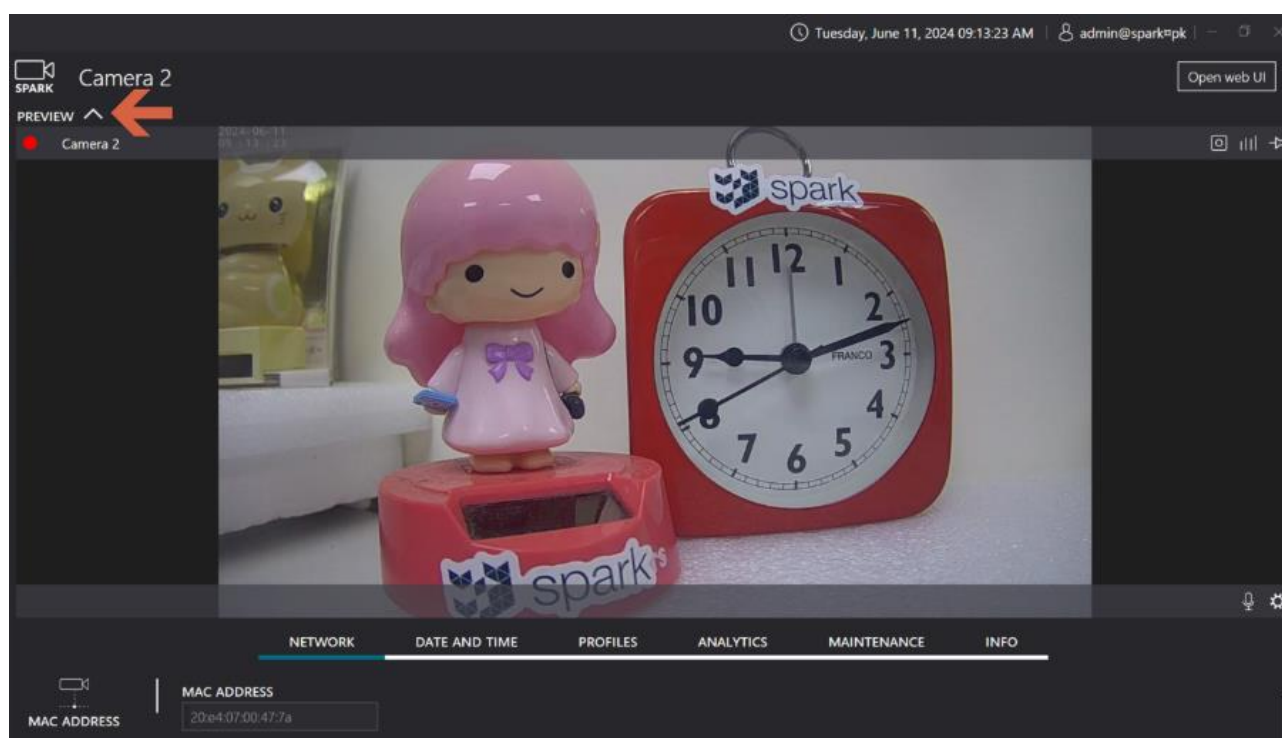


3.2.3 Delete video device



A. Select the devices you want to delete and then click **[delete]** at the bottom right.

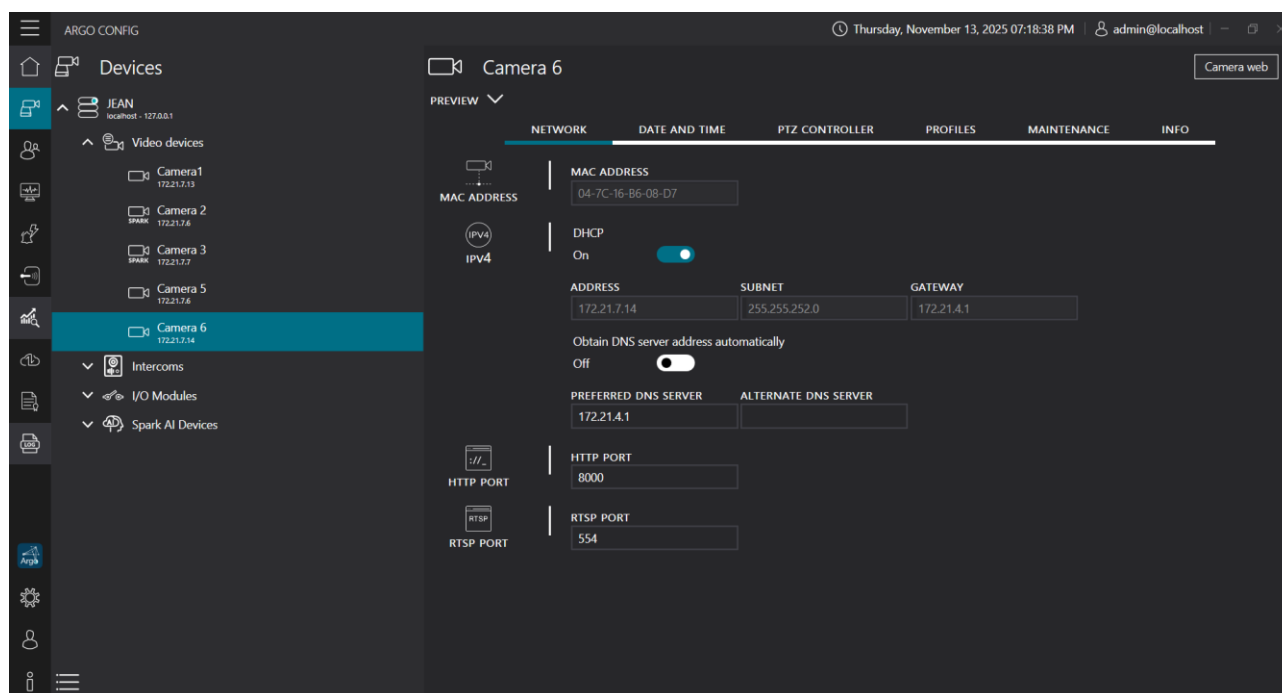
3.2.4 Preview video devices



B. Click **[Preview]**

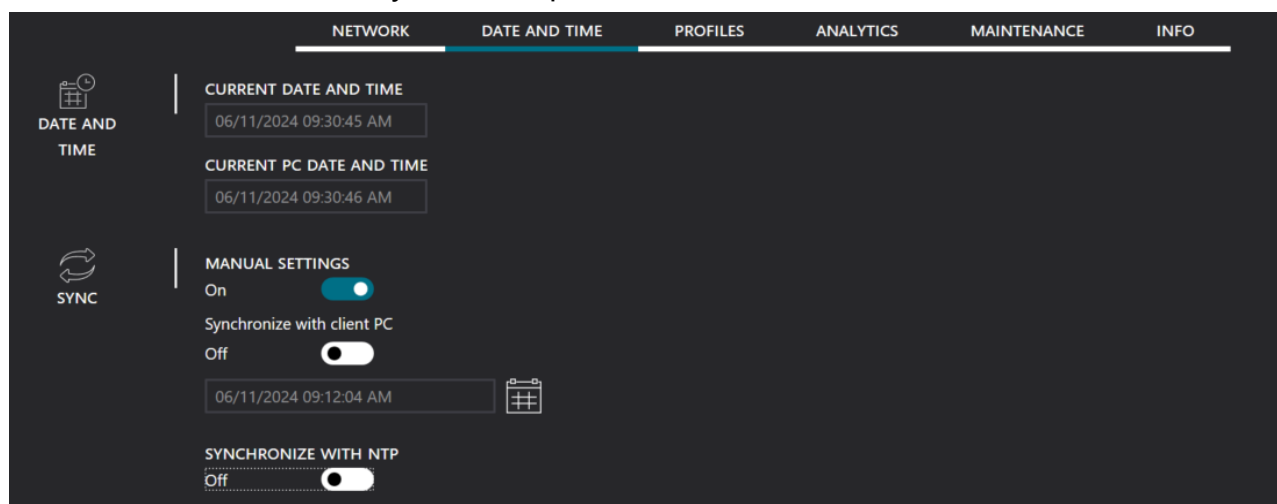


3.2.5 Video devices configurations



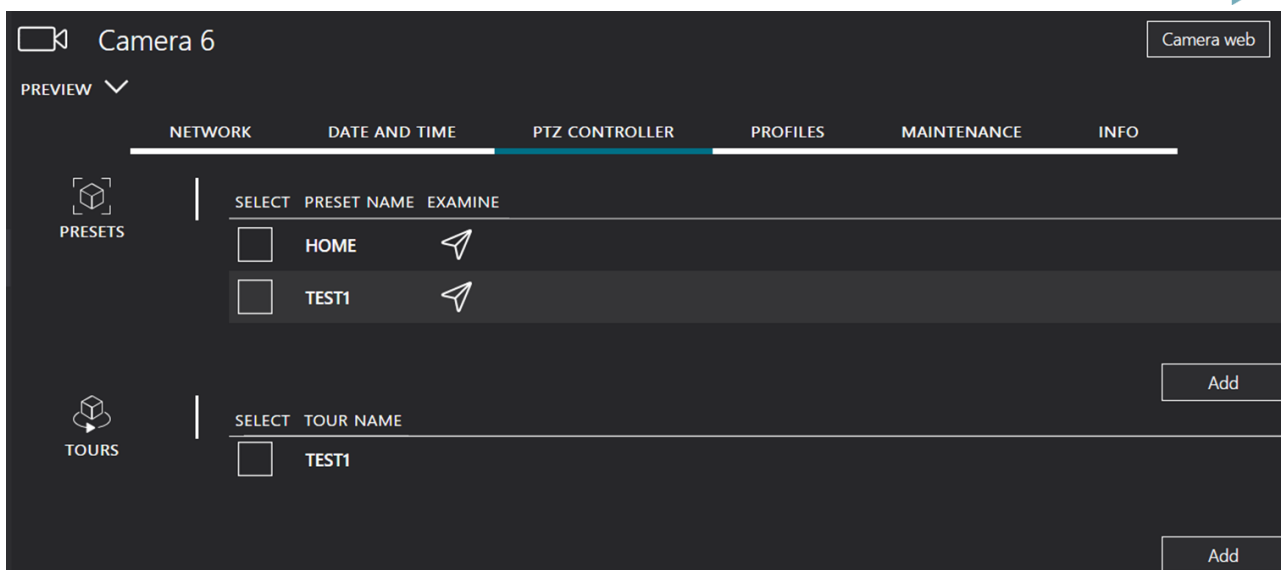
A. Network: edit device network settings

- MAC address: unable to edit.
- IPV4: When DHCP is Disable, you can edit the IP address, subnet mask, and gateway.
- When automatic acquisition of DNS server addresses is enabled, you can edit the preferred DNS server and alternate DNS server.
- HTTP PORT: modify the HTTP port address if needed.
- RTSP PORT: modify the RTSP port address if needed.



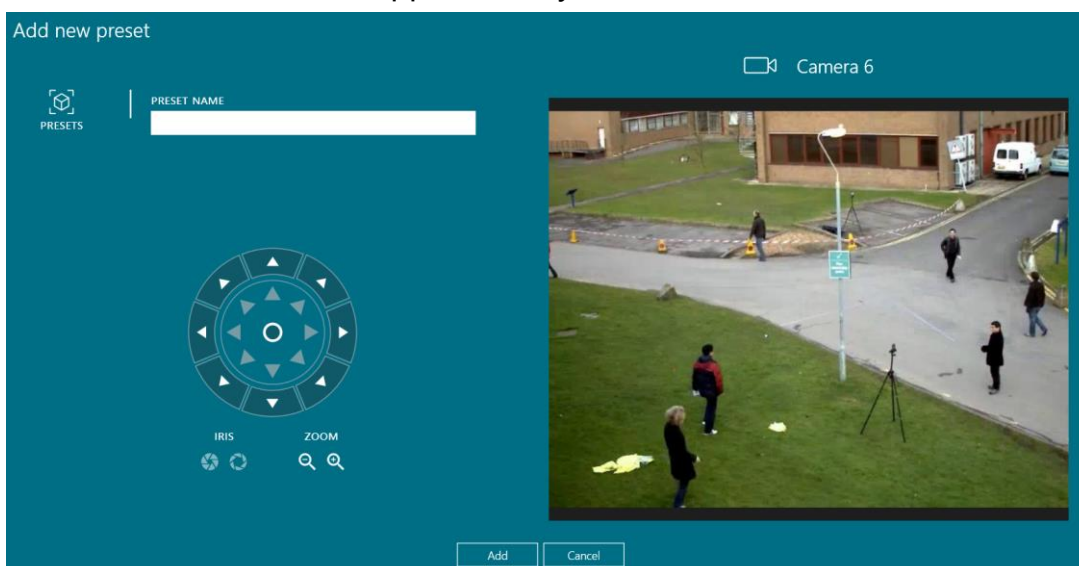
B. Date and time: Edit device date and time settings.

- Date and Time: Browse current date and time, and computer date and time.
- SYNC : Enable manual settings to turn on/off synchronization with the Client and NTP synchronization.

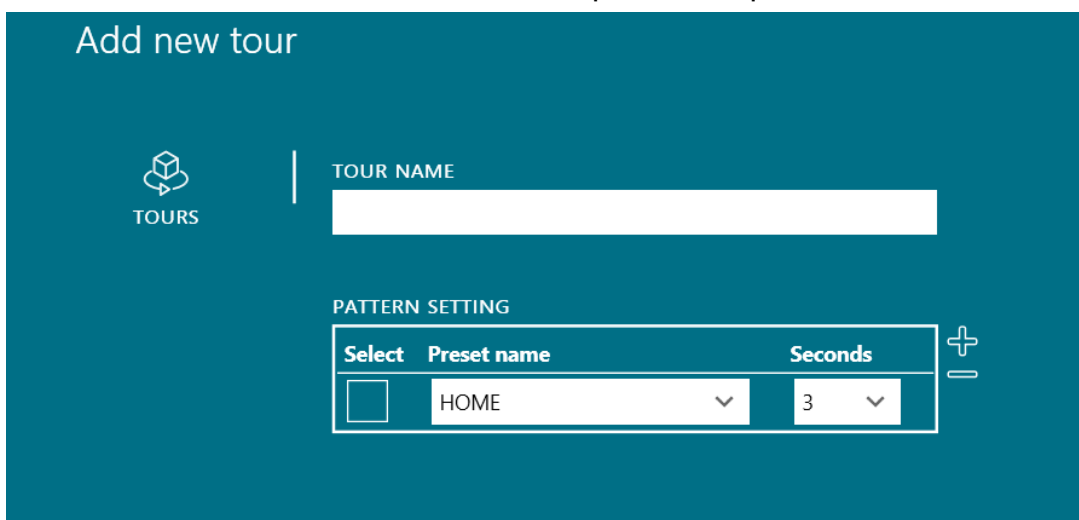


C. PTZ controller: Edit Preset and Tour.

Note: This feature is supported only for ONVIF PTZ cameras.



- Add Preset: Create and save a new preset PTZ position.

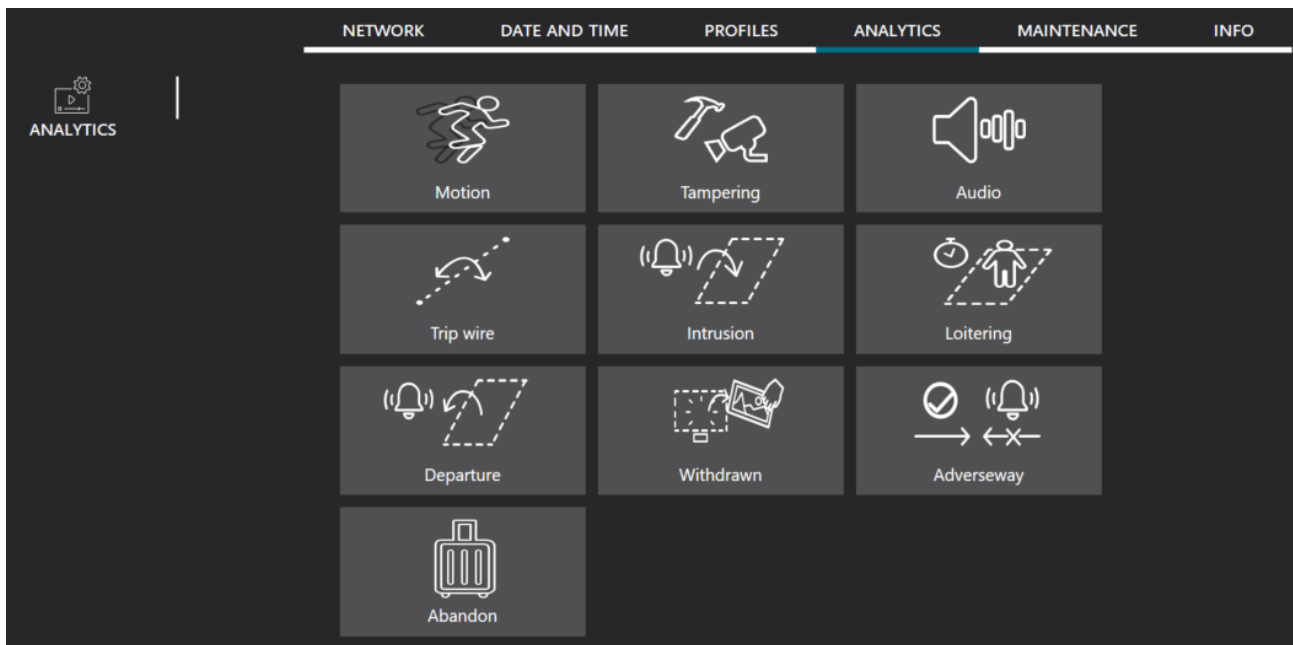


- Add Tour.: Configure a patrol route based on the preset positions already created.

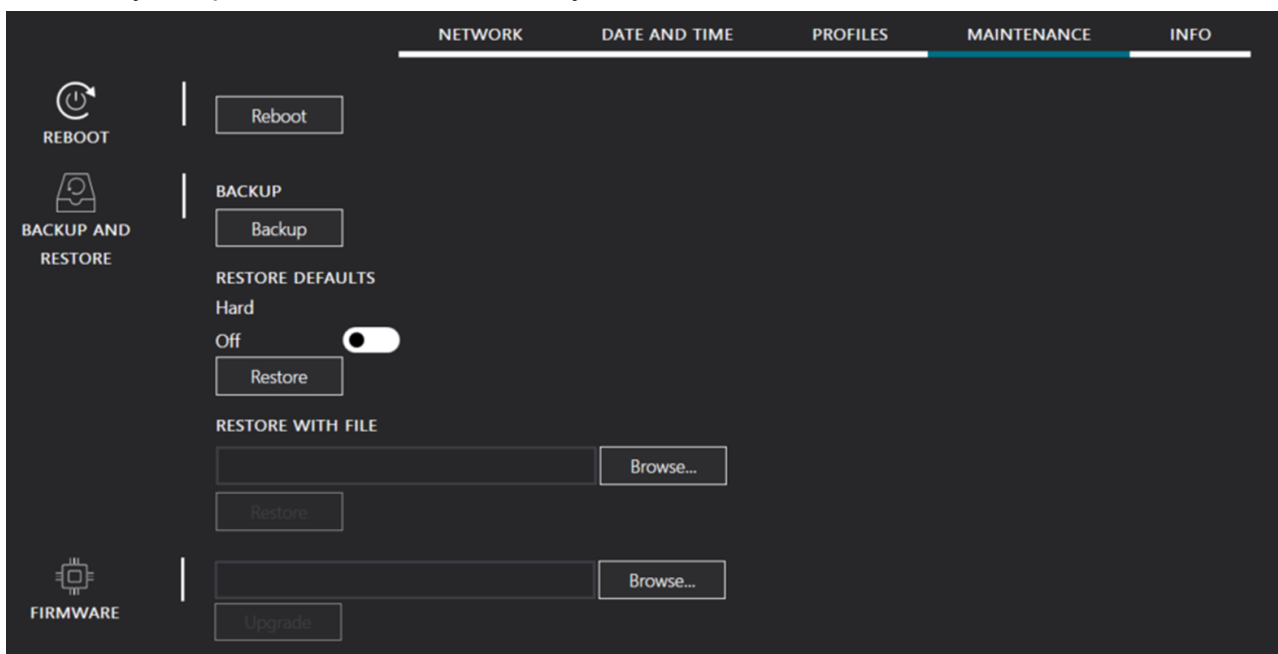


	NETWORK	DATE AND TIME	PROFILES	ANALYTICS	MAINTENANCE	INFO	
PROFILES	<input type="checkbox"/>	videostream 0	RTSP over TCP	H264	1920x1080	30	Yes
	<input type="checkbox"/>	videostream 1	RTSP over TCP	H264	1280x720	5	Yes
	<input type="checkbox"/>	videostream 2	RTSP over TCP	H264	320x240	30	Yes

D. Profiles: select the stream you want to edit for advanced settings.



E. Analytics: preview device video analytics status.

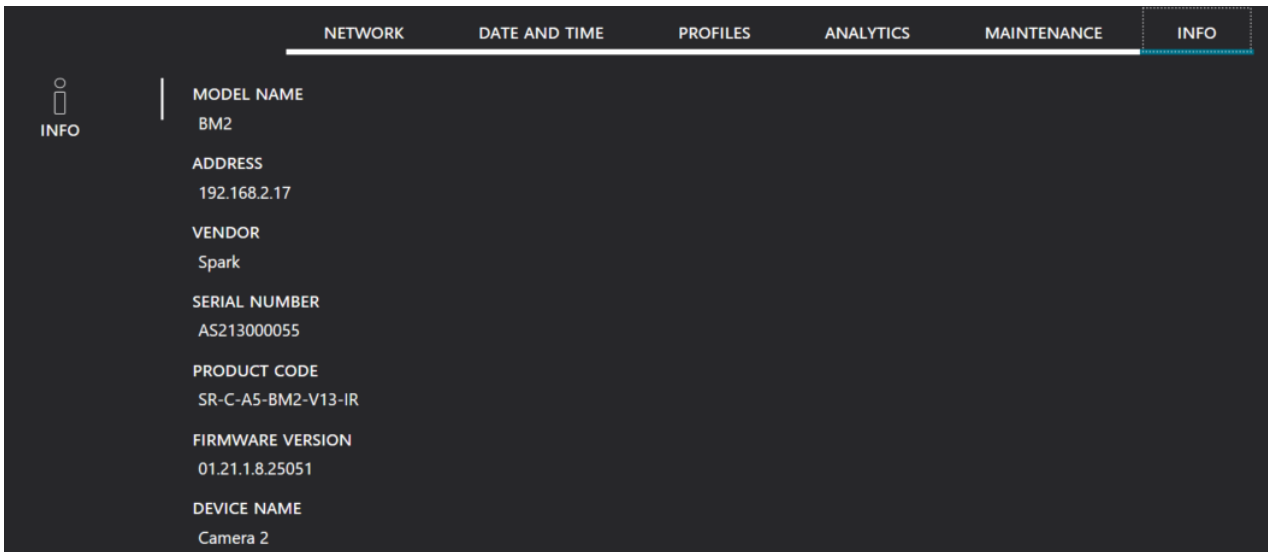


F. Maintenance: edit device maintenance settings.

- Reboot: Restart device.
- Backup: Backup device settings.
- Restore: Restore device settings.

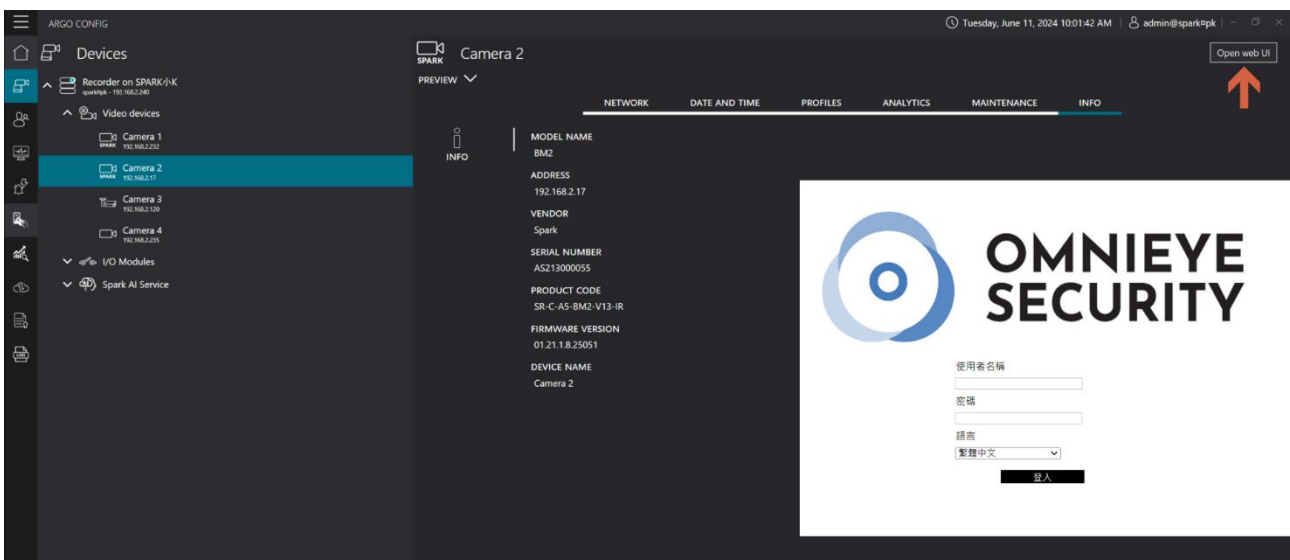


- Firmware: Update firmware version of the camera.



G. Info: browse device information

3.2.6 Open device web interface



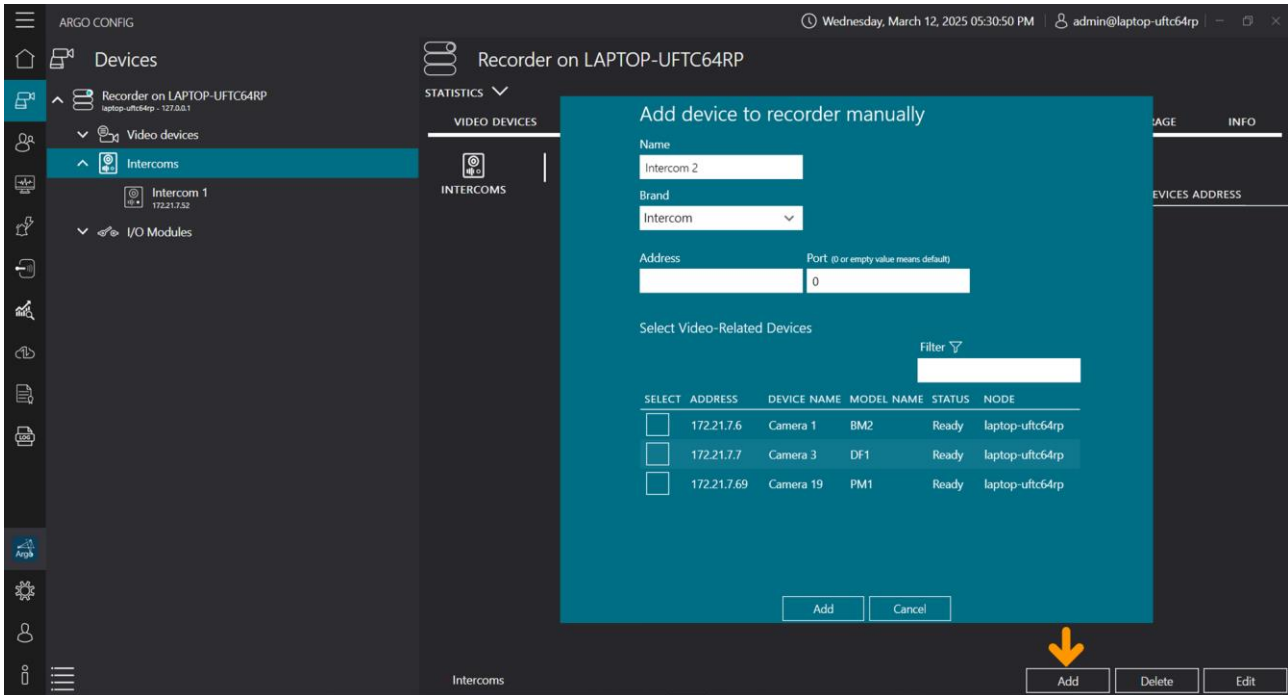
- Click on [**Open Web UI**]
- Username: insert username
- Password: insert password
- Language: select language



3.3 Intercoms

Support for SIP Intercom Devices, Primarily for Voice Communication with Real-Time Two-Way Conversation. Some Devices Support Video Intercom, Allowing Synchronized Video Display

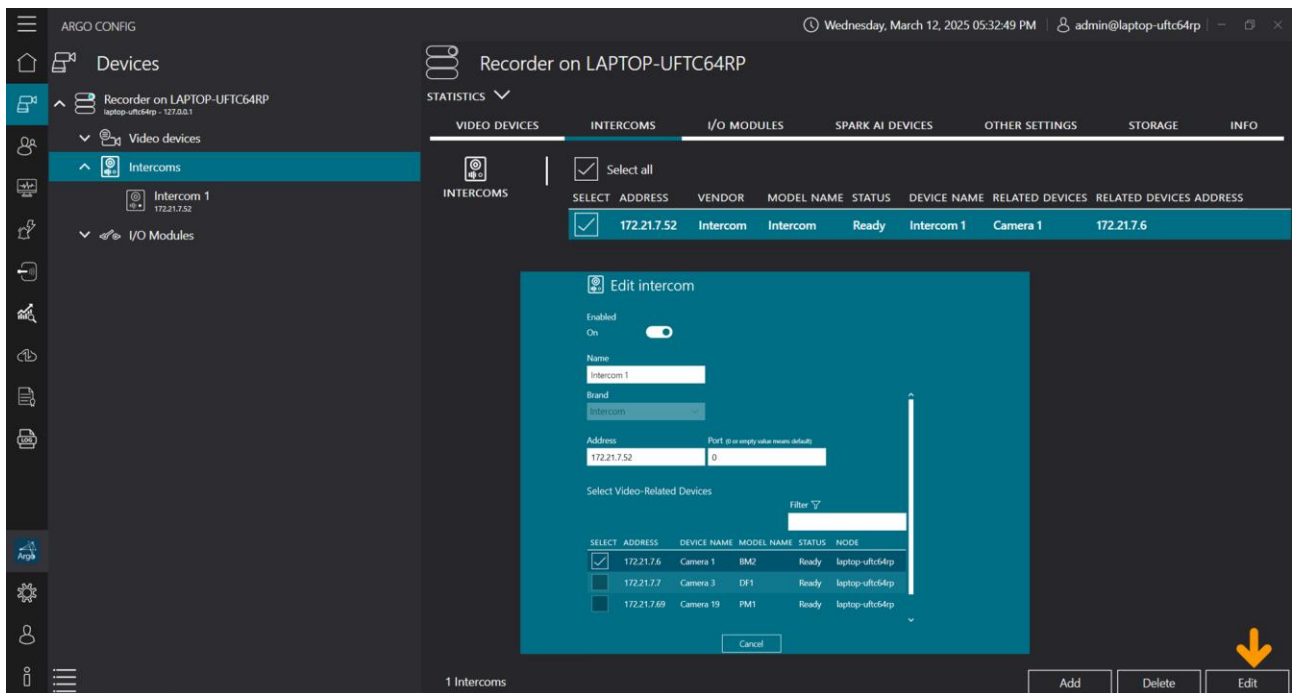
3.3.1 Add Intercoms



- Click on **[Add]**
- Enter the intercom device name.
- Enter the intercom device IP address(port 0 represents the default value of 5060).
- Select the video feed to display during the intercom call.

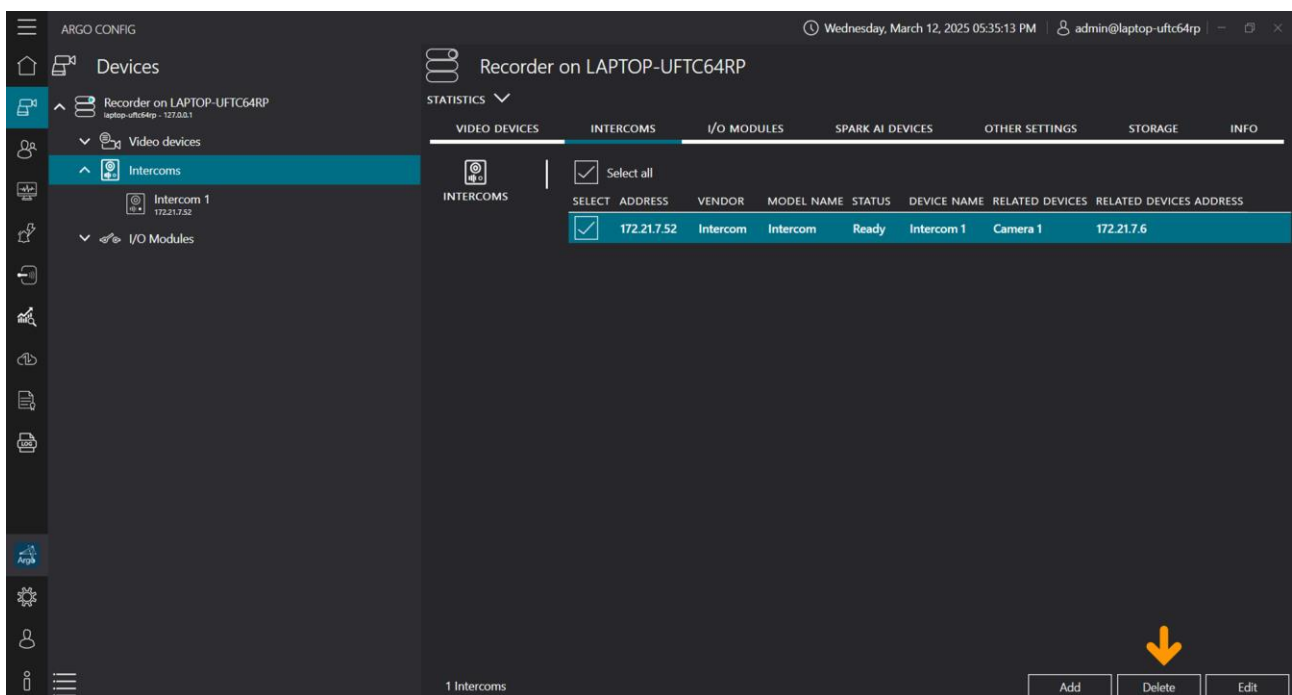


3.3.2 Edit Intercoms



- Select the intercom device to edit and click **[Edit]** at the bottom right.
- Enable intercom device: Turn on/off the use of I/O devices.
- Name: Edit the device name.
- IP Address: Editing may cause the device to become unavailable.
- Port: Edit the device port number (default is 0).

3.3.3 Delete Intercoms



- Select the I/O module to delete and click **[Delete]**.



3.4 I/O Module

3.4.1 Add I/O module (Auto scan/Manual add)

A. Auto scan

The screenshot shows the ARGO CONFIG interface for a recorder on LAPTOP-UFTC64RP. The 'I/O MODULES' section is active, showing a table of detected devices. A modal window titled 'Add I/O modules to recorder: Recorder on LAPTOP-UFTC64RP (laptop-uftc64rp)' is open, displaying a table of detected devices. A red arrow points to the 'Scan' button at the bottom of the modal.

Select	Address	Vendor	Model Name	Status	Device Name
<input type="checkbox"/>	172.21.7.21	Advantech	6060	Ready	I/O Module 1
<input type="checkbox"/>	172.21.7.72	Advantech	6060	Ready	I/O Module 2
<input type="checkbox"/>	172.21.7.184	ICPDAS	tET-PD2POR2	Ready	I/O Module 3

Select	Address	Product code	MAC Address	Vendor	Status	Add to recorder
<input type="checkbox"/>	172.21.7.21	6060	748F-0E-48-0E-8D	Advantech	Added	Recorder on LAPTOP-UFTC64RP
<input type="checkbox"/>	172.21.7.72	6060	748F-0E-48-0E-8D	Advantech	Added	Recorder on LAPTOP-UFTC64RP
<input type="checkbox"/>	172.21.7.184	tET-PD2POR2	000B-7D-6A-7C-7C	ICPDAS	Added	Recorder on LAPTOP-UFTC64RP
<input type="checkbox"/>	172.21.7.184	01-70-50-00-00	000B-7D-6A-7C-7C	ICPDAS	Added	Recorder on LAPTOP-UFTC64RP
<input type="checkbox"/>	172.21.7.184	01-70-50-00-00	000B-7D-6A-7C-7C	ICPDAS	Added	Recorder on LAPTOP-UFTC64RP
<input type="checkbox"/>	172.21.7.184	tET-PD2POR2	000B-7D-6A-7C-7C	ICPDAS	Added	Recorder on LAPTOP-UFTC64RP

- Click on [Scan]
- Select I/O modules to add

B. Manual add I/O modules

The screenshot shows the ARGO CONFIG interface for a recorder on LAPTOP-UFTC64RP. The 'I/O MODULES' section is active, showing a table of detected devices. A modal window titled 'Add device to recorder manually' is open, with fields for Name, Brand, and Address. A red arrow points to the 'Add' button at the bottom of the modal.

Select	Address	Vendor	Model Name	Status	Device Name
<input type="checkbox"/>	172.21.7.21	Advantech	6060	Ready	I/O Module 1
<input type="checkbox"/>	172.21.7.72				
<input type="checkbox"/>	172.21.7.184				

Name: I/O Module 4
Brand: Advantech
Address: 0

- Click on [Add]



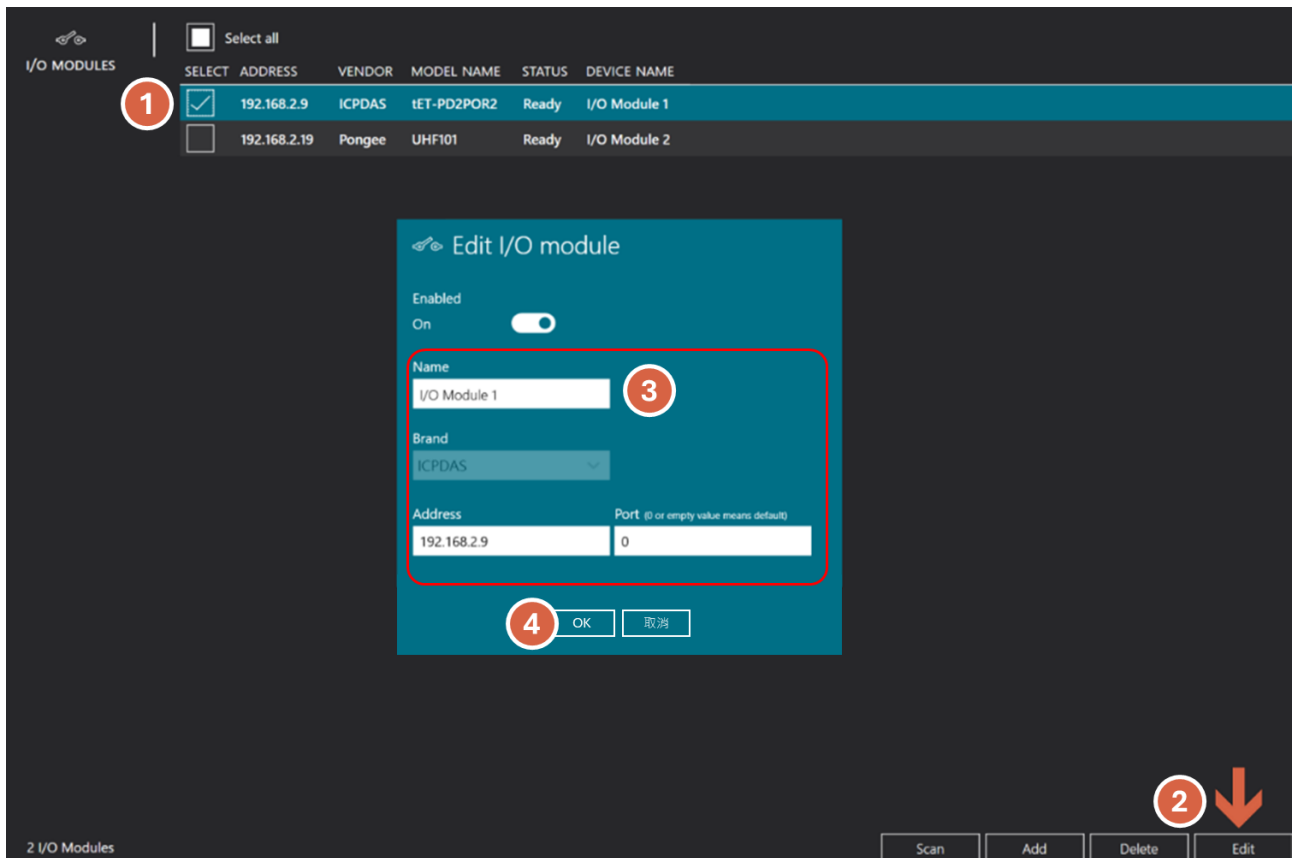
- Name: insert I/O module name
- Enter the device port number (default is 0, for Pongee devices enter 4001).
- Brand: select I/O module brand

Brand	Description
Advantech	Advantech' s I/O module for connecting DIDO devices
Pongee	Pongee' s I/O modules: RFID reader
ICPDAS	ICPDASs I/O module for connecting DIDO devices
Soyal	Soyal I/O Module for connect DIDO devices and read RFID.



3.4.2 Edit I/O module

3.4.2.1 Advantech/ ICPDAS/ Pongee



- Select the I/O module you want to edit and click **[Edit]**
- Enable I/O device: enable/disable I/O device
- Name: edit device name
- IP address: editing IP address might render the device unusable
- Port: Edit device port number (default is 0, for Pongee devices enter 4001).

Brand	Port
Advantech	0
ICPDAS	0
Pongee	4001

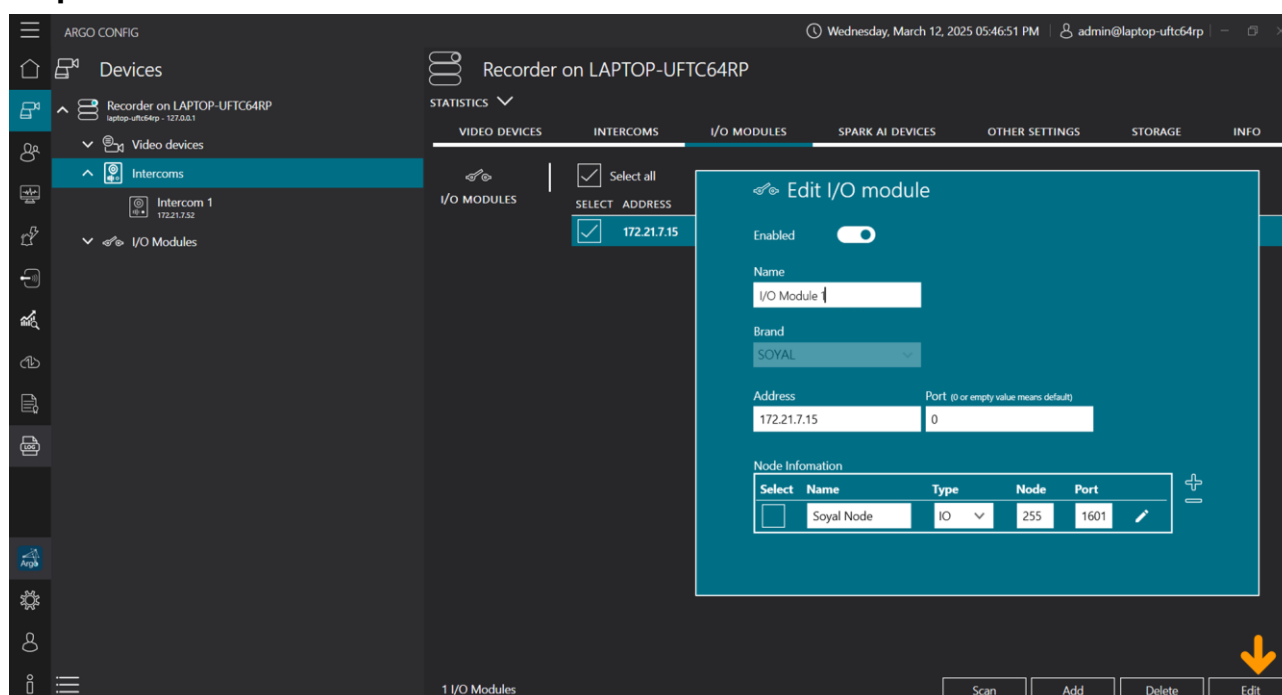


3.4.2.2 Soyal

This section explains how to use the expanded version of the access control panel or access card reader. For direct device connection without going through the controller, please refer to section 3.4.2.1.

Category	Model	Description
Access Control Panel	AR-716-E	TCP/IP network-based multi-door controller, capable of managing multiple access control devices.
	AR-727-CM	Supports TCP/IP, suitable for medium to large access control systems, with real-time monitoring and logging features.
	AR-829E	Multi-door access control panel, expandable for additional devices.
Access Card Reader	AR-721-H	Supports RFID cards and password input, suitable for access control and attendance management.
	AR-837-E	Supports multiple card formats (Mifare, NFC, etc.), suitable for advanced access control integration.
	AR-331-E	Equipped with TCP/IP network communication, ideal for remote management.
Expansion Modules	AR-401-IO-0016R	Input/output expansion module, can be used to integrate access control and alarm systems.
	AR-403-IO-0016R	More I/O expansion options, suitable for complex access control management.

Step1: Select the I/O module to edit.





- Select the I/O module to edit and click [Edit] at the bottom right.
- IP Address: IP address for the expansion modules (AR-401-IO-0016R/AR-403-IO-0016R).
- Port: Edit the device port number (default is 0).

Step2: Select the I/O module to edit.

Edit I/O module

Enabled

Name
I/O Module 1

Brand
SOYAL

Address: 172.21.7.15 Port (0 or empty value means default): 0

Node Information

Select	Name	Type	Node	Port
<input type="checkbox"/>	Soyal Node	RFID	255	1601

- Enable I/O Device: Toggle to enable or disable the I/O device.
- Name: Edit the device name.
- Address: Modifying this may cause the device to become unavailable.
- Port: Edit the device port number (default: 0).
- Node Information: Click [+] to add node information.
 - **Name:** Edit the device name.
 - **Type:** Select **RFID**.
 - **Node:** Select the parameter node configured for the device (parameters must be verified via the device or machine' s web interface).
 - **Port:** Select the port connected to the expansion board (the port number must first be configured on the expansion board' s web interface and entered accordingly).



Step3: Adding IO Devices and Configuring DI/DO

Edit I/O module

Enabled

Name
I/O Module 1

Brand
SOYAL

Address: 172.21.7.15 Port (0 or empty value means default): 0

Select	Name	Type	Node	Port
<input type="checkbox"/>	Soyal Node	RFID	255	1601
<input type="checkbox"/>	Soyal Node	IO	256	1621

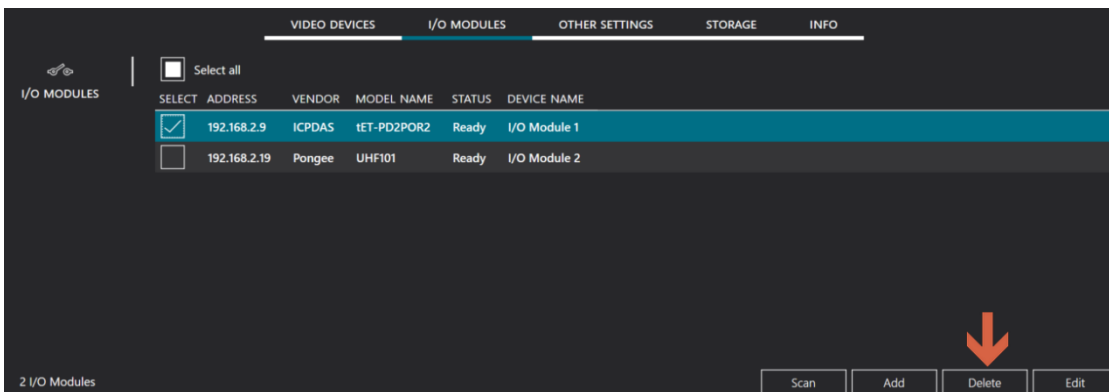
Select	Name	Type	ID
<input type="checkbox"/>	Soyal IO	DI	0
<input type="checkbox"/>	Soyal IO	DO	1

Cancel

- **Enable I/O Device:** Toggle to enable or disable the I/O device.
- **Name:** Edit the device name.
- **Address:** Modifying this may cause the device to become unavailable.
- **Port:** Edit the device port number (default: 0).
- **Node Information:** Click [+] to add node information.
 - **Name:** Edit the device name.
 - **Type:** Select **IO**.
- **I/O Map Information:** Click [+] to add node information.
 - **Name:** Select the parameter node configured for the device (parameters must be verified via the device or machine' s web interface).
 - **Type:** Select **DI** (Digital Input) or **DO** (Digital Output).
 - **ID:** Select the parameter node configured for the device (parameters must be verified via the device or machine' s web interface).

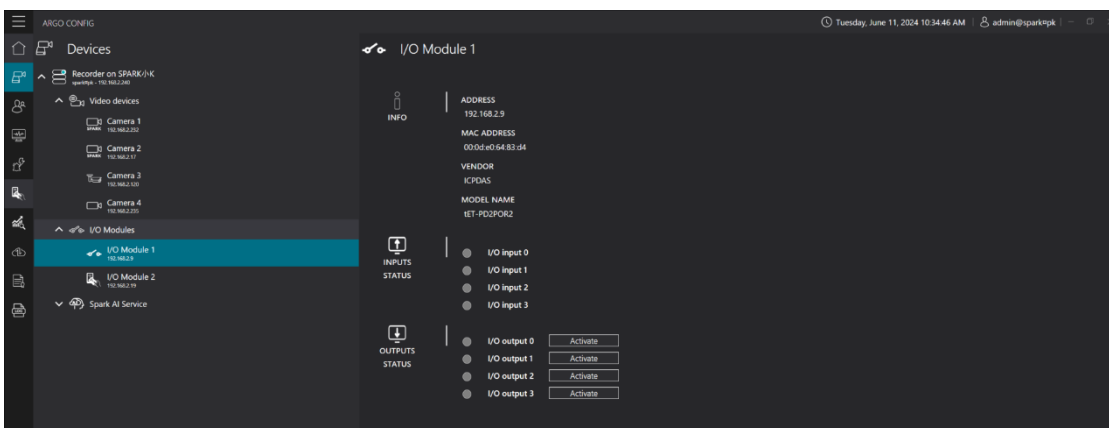


3.4.3 Delete I/O modules



- Select the I/O module you want to delete and click **[Delete]**

3.4.4 Browse I/O modules information and status



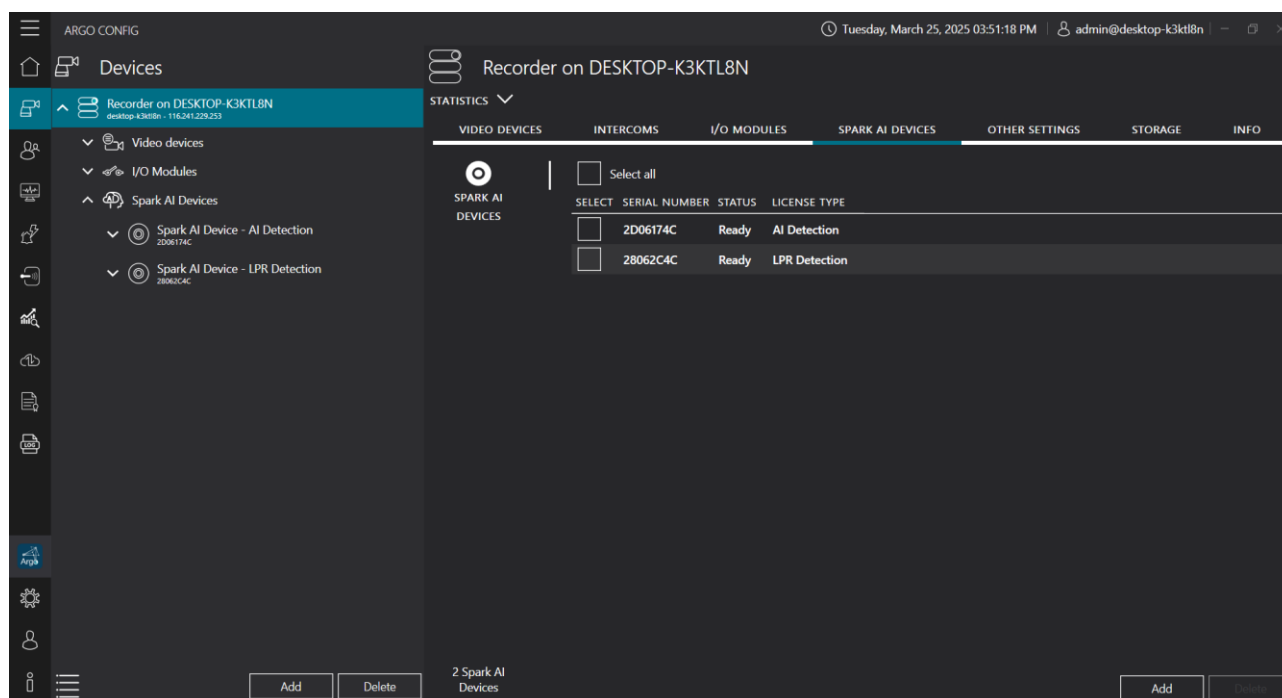
- Information: View I/O module information.
- Input Status: View input status through indicator lights.
- Output Status: View output activation status through indicator lights.



3.5 Spark AI Device

Spark AI performs intelligent software analysis based on different object detection types, allowing users to configure various detection modes. The system provides details on the serial number, status, and license type of each Spark AI device, supporting detection for human shapes, vehicles, intelligent analytics, license plate recognition, and fire/smoke detection.

Spark AI Device	Description	Detection Types
AI Detection	Analyzes human shapes and vehicle types	Area, Line Crossing
Human Detection	Detecting human shapes	Area, Line Crossing
Vehicle detection	Detecting bicycles, cars, motorcycles, buses, trucks	Area, Line Crossing
Fire and Smoke detection	Detects flames and smoke	Fire & Smoke
LPR Detection	Recognizes Taiwanese license plates	License Plate
MLPR Detection	Recognizes license plates from multiple countries	License Plate, Vehicle Type, Vehicle Color





3.5.1 Add Spark AI Device

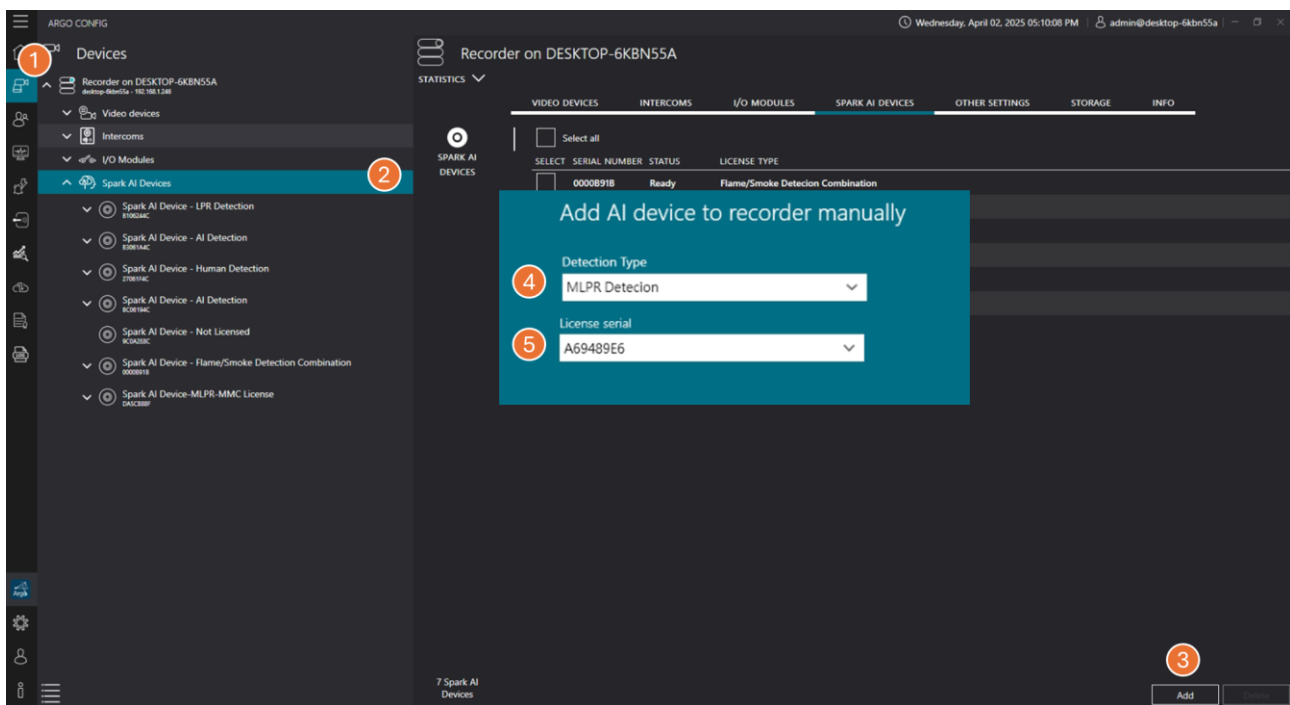
3.5.1.1 All / Human / Vehicle Detection Devices

- Ensure the license certificate has been successfully uploaded.
- Insert the Spark AI Dongle into the computer: Once connected, the system will automatically add the Spark AI device and display the recognition categories based on the license type.

3.5.1.2 LPR Detection Devices

- Ensure the license certificate has been successfully uploaded.
- Insert the Spark AI Dongle into the computer: Once connected, the system will automatically add the Spark AI device and display the recognition categories based on the license type.

3.5.1.3 MLPR Detection Devices

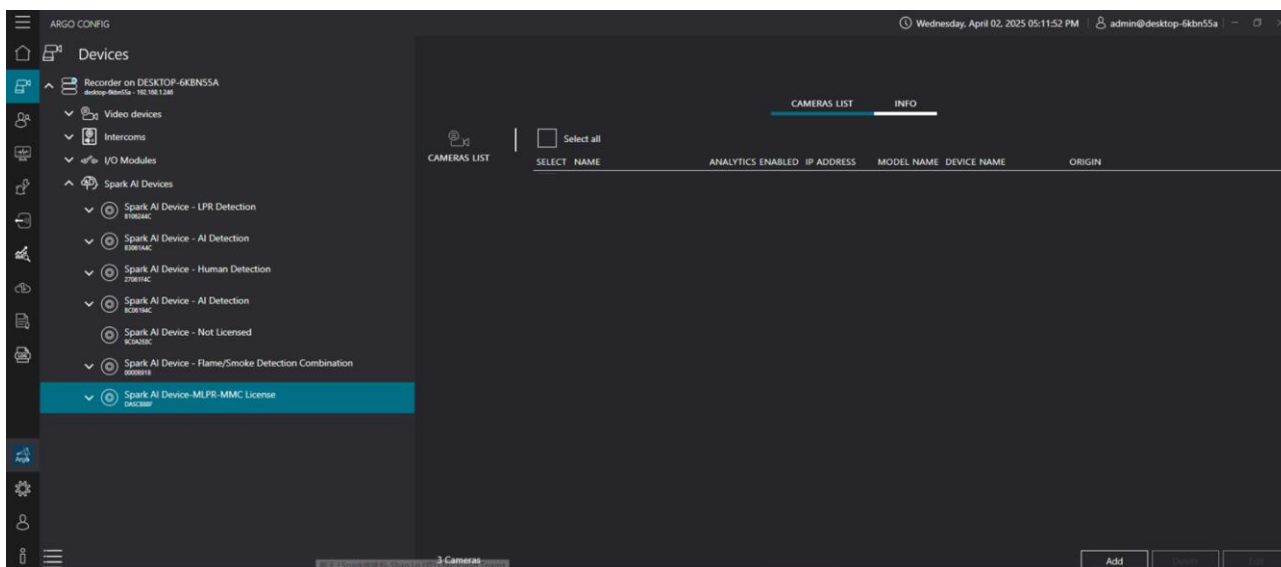


Step1: Add License

- Select Device.
- Click on SPARK AI Device.
- Click **[Add]**
- Select the Detection Type: MLPR.
- Choose the License Key Serial Number that has been uploaded.

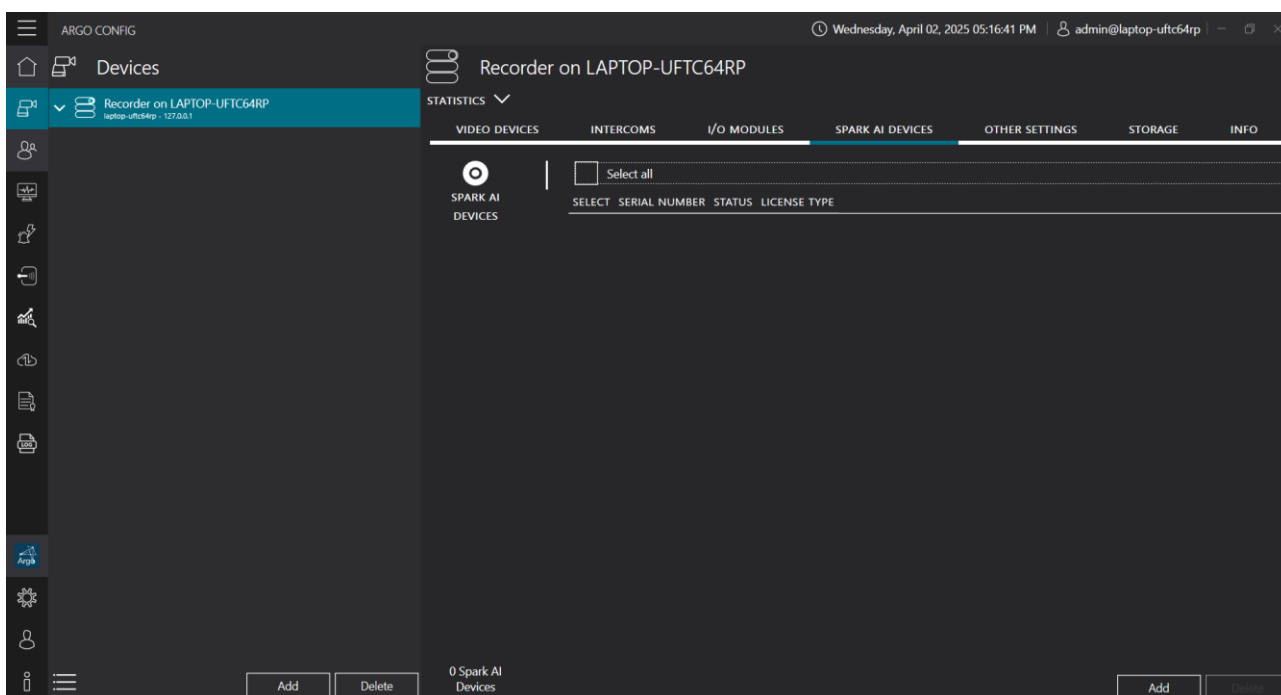


Step2: Upload Recognition Software to the Spark AI Device

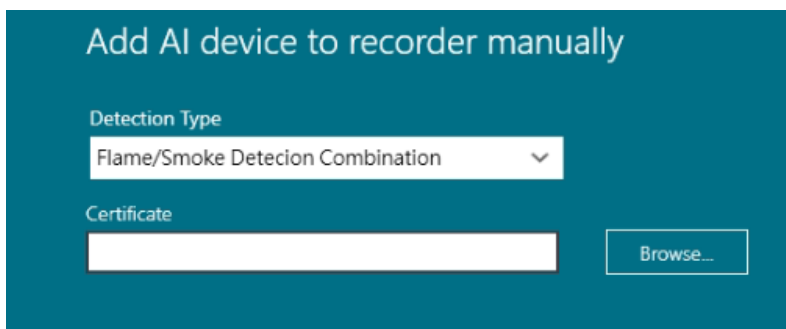


- Click [Add]

3.5.1.4 Fire & Smoke Devices

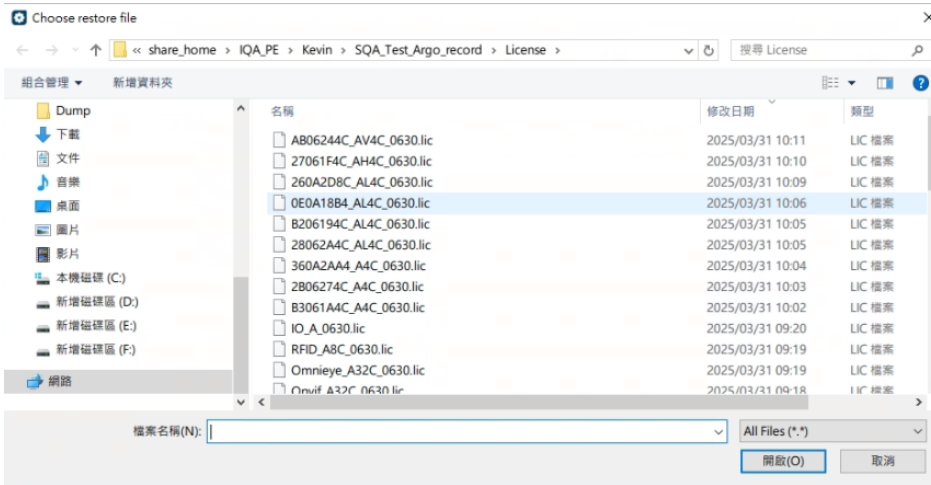


- Step1: Click Browse.

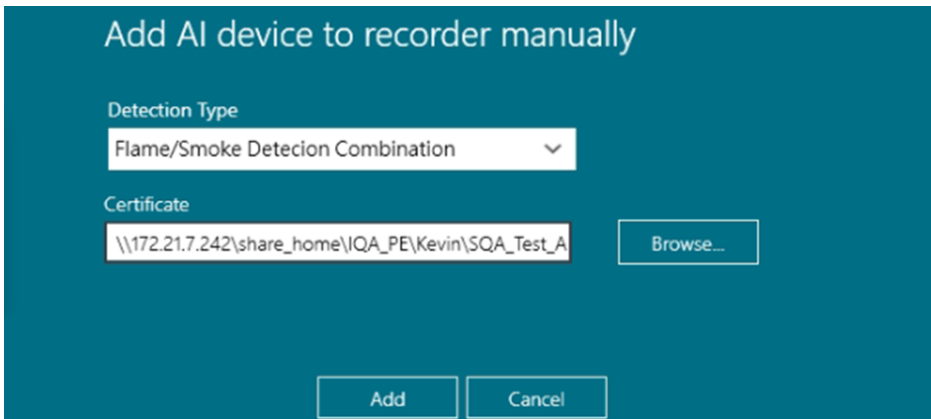




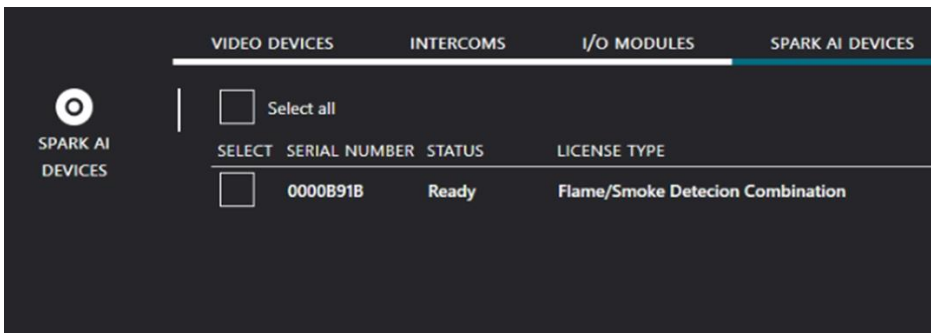
Step2: Select the device certificate to add (the certificate is identified based on the computer's MAC address).



Step3: Click Add to complete the certificate import.



Step4: The Fire & Smoke Detection has been successfully added.

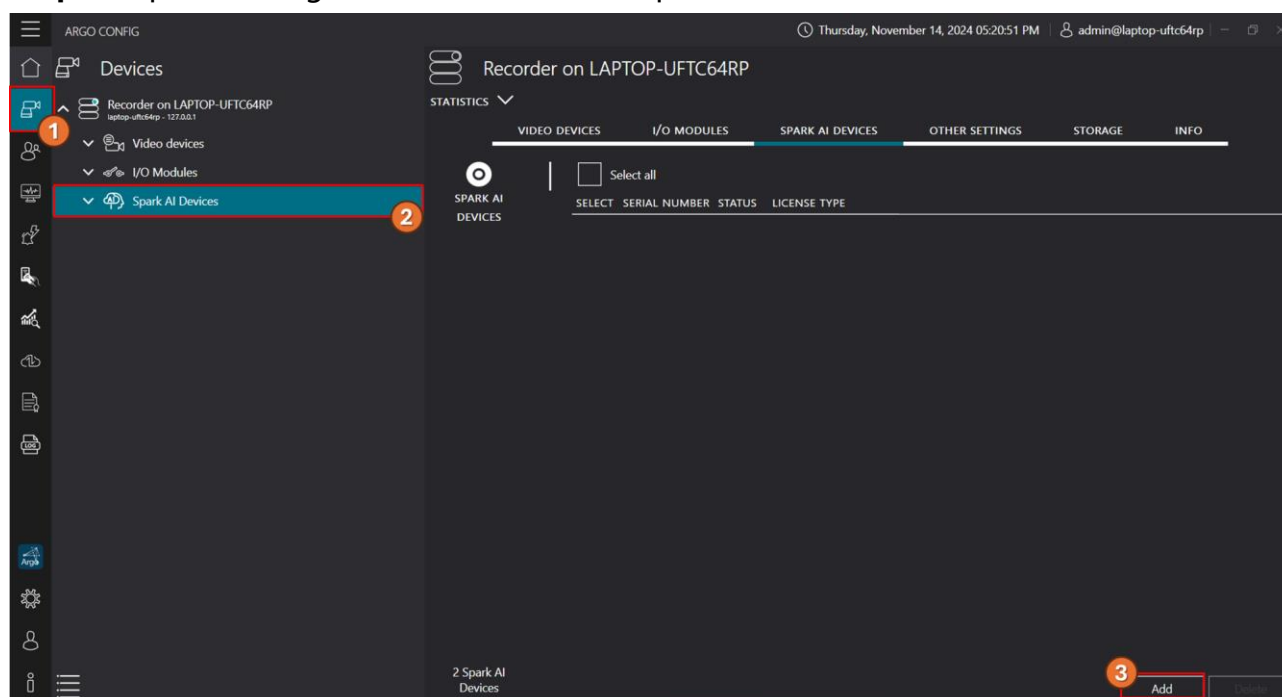




3.5.1.5 Generic AI Device

The Argo Generic AI function supports various intelligent image recognition applications with high flexibility. By integrating AI models, Argo can automatically detect and analyze various objects, providing accurate detection results, enhancing the intelligence of monitoring systems. This function supports custom AI settings, enabling fast, real-time image processing and analysis, and it also supports alarm events to boost the overall efficiency and coverage of security monitoring.

Step1: Upload Recognition Software to the Spark AI Device



- Add AI device to Recorder manually.

Add AI device to recorder manually

Detection Type
Generic AI Detection

Generic AI Detection Class Name
ClassName

Analytics application name
ProgramName.exe

Analytics application Path
Browse...

License serial

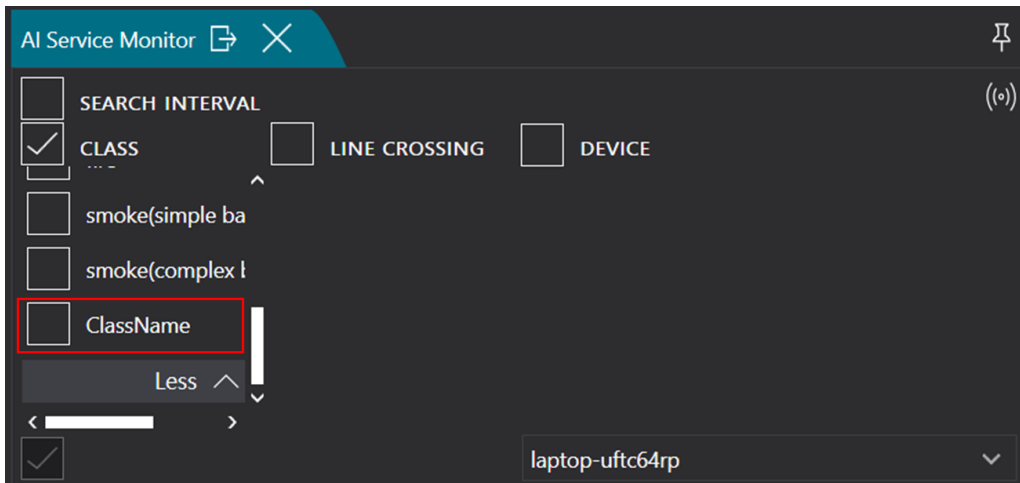
Analytics application Port
31000
The port number must be between 0 and 65535

HTTP Port
9903
The port number must be between 0 and 65535

- Detection Type: Select "Generic AI Detection."

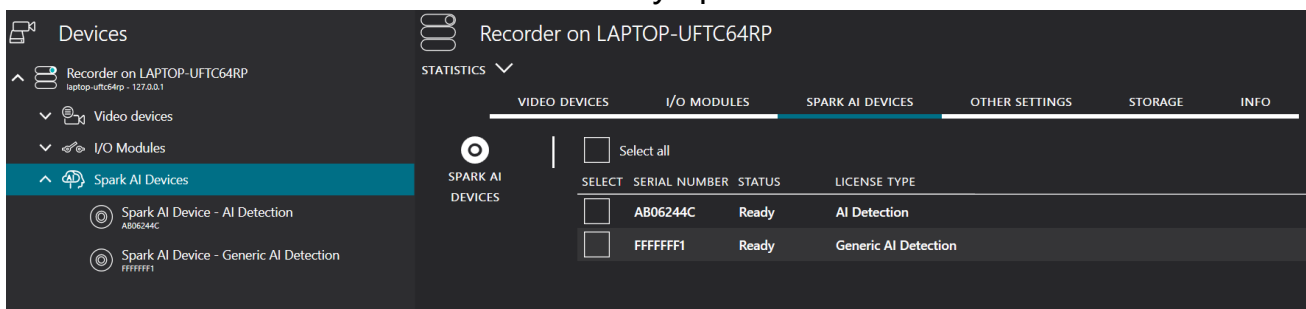


- Generic AI Detection Class Name: Enter the recognition name, such as object detection or flame detection. This category name will be displayed in the Client AI Service Monitor Class list.



- Analytics application Name: Enter the name of the analysis program, such as Program.exe
- Analytics application Path: Browse the program compressed file path.
- License Serial: After obtaining the Spark license, select the Generic AI module license serial number.
- Analytics application Port: Enter the port number (between 0-65535).
- HTTP Port: Enter the HTTP port number (between 0-65535).

- The Generic AI detection is successfully uploaded.



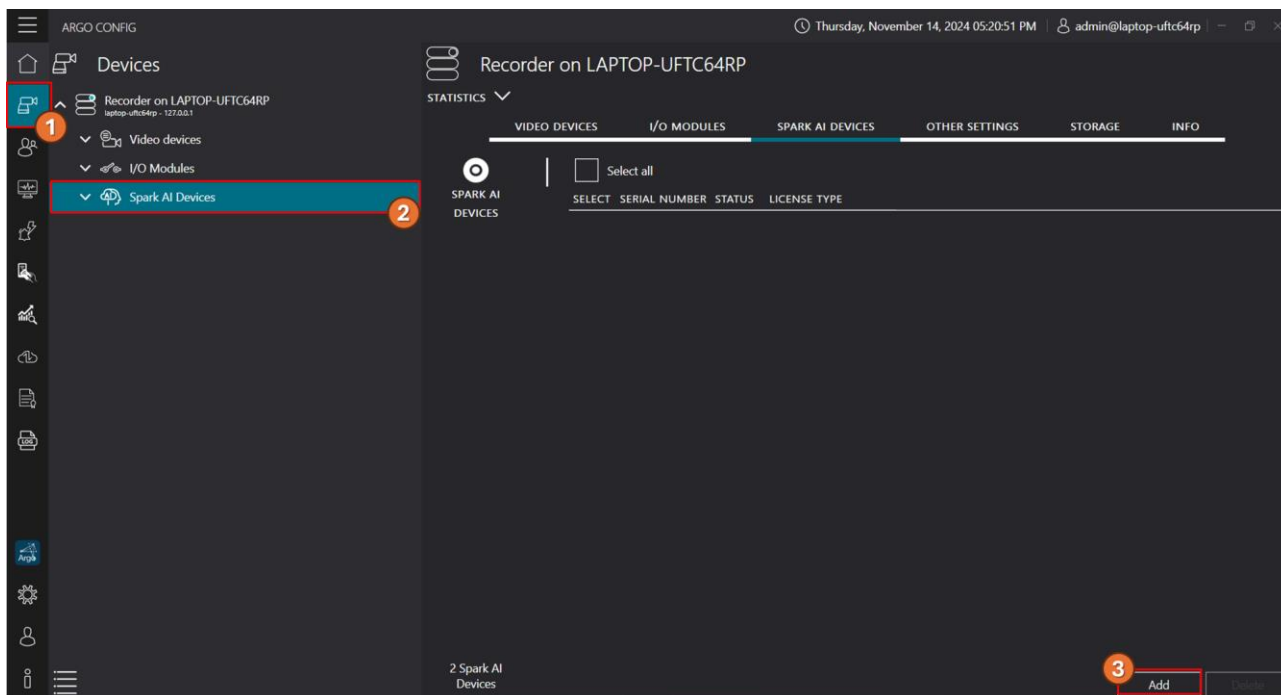
3.5.1.6 Face Detection

- Ensure the license certificate has been successfully uploaded.
- Insert the Spark AI Dongle into the computer: Once connected, the system will automatically add the Spark AI device and display the recognition categories based on the license type.

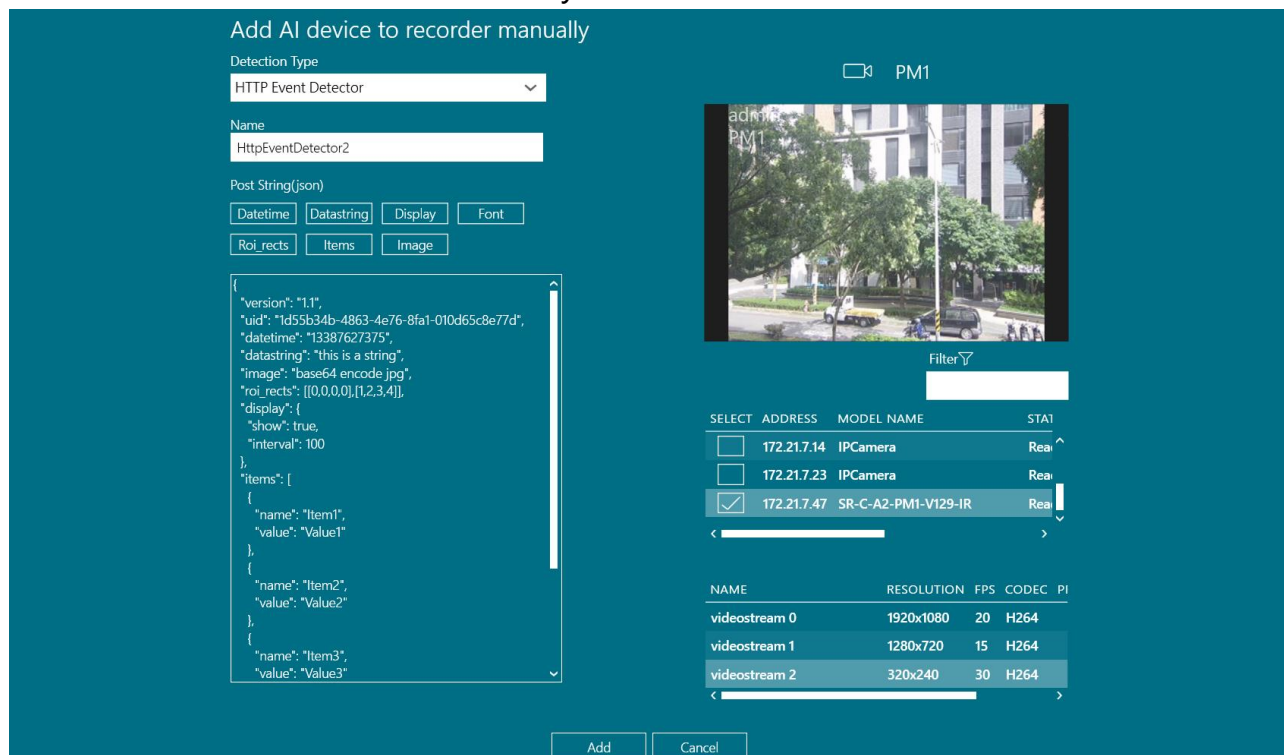


3.5.1.7 HTTP POST Device

Argo can receive events from any third-party device via HTTP POST and display them in the Client's AI Monitoring interface. Additionally, Argo supports overlaying relevant event information as text on the designated camera feed, enabling users to quickly understand the situation.



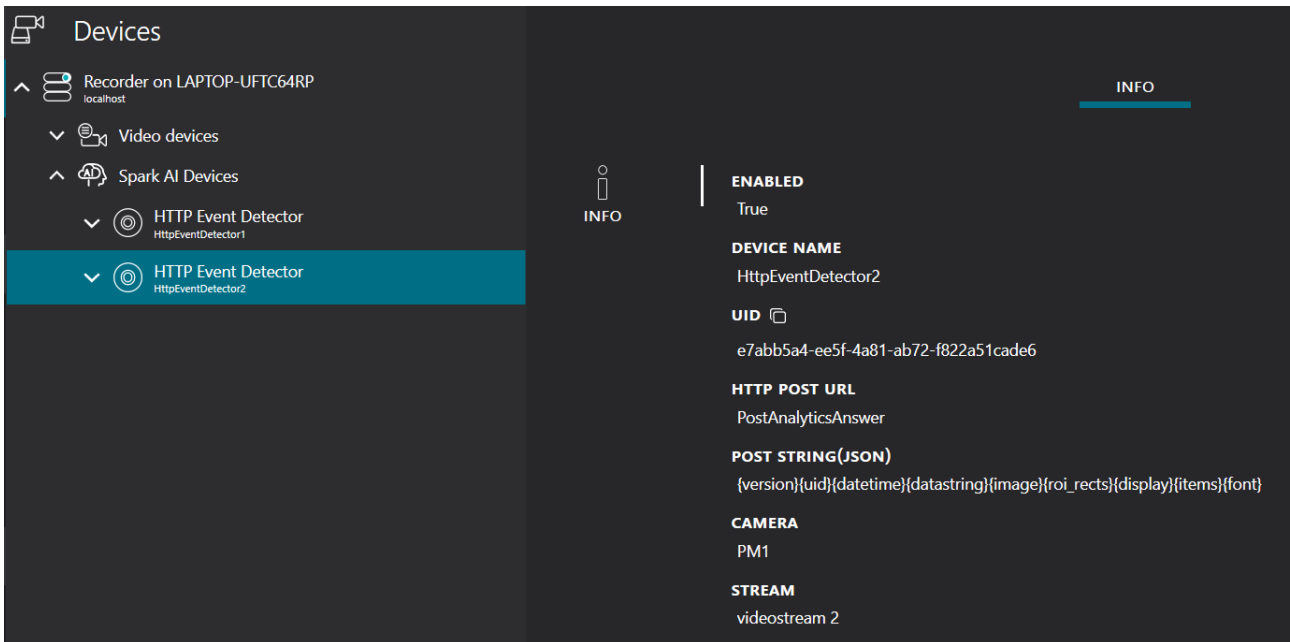
- Add AI device to Recorder manually.



- Detection Type: Select HTTP Event Detector



- Name: Enter a custom name for this detector (e.g., "Access Door Event")
- POST String: Define the expected data content (e.g., keyword or JSON string) that Argo will match when a POST is received



- Get Http POST device information

NOTE: For details on HTTP integration, please refer to the Argo Generic Event v1.1 User Manual Guide.

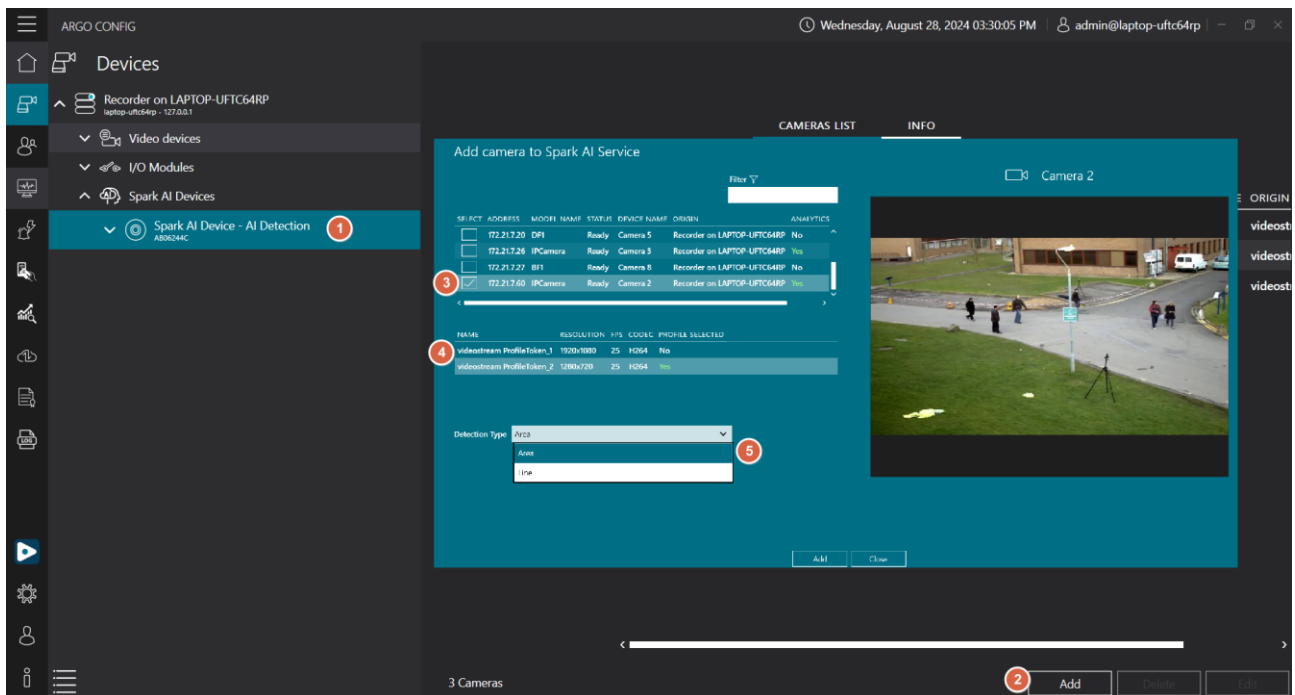


3.5.2 Add Camera to Spark AI Devices

Recommended Camera Stream Resolutions for Optimized Image Analysis.

Detection Type	Resolution	FPS
All Detection	1280x720P	5 FPS
Vehicle Detection	1280x720P	5 FPS
Human Detection	1280x720P	5 FPS
LPR Detection	1920x1080P	10 FPS
Fire and Smoke Detection	1280x720P	15 FPS
Line Crossing Detection	1280x720P	15 FPS

3.5.2.1 All/ Vehicle/ Human Detection



- Select the AI device to be recognized, then click the bottom-right button [Add].
- Check the cameras you want to add to the Spark AI service.
- Select the camera stream: Refer to 3.5.2.
- Choose the detection type: Area or Line Crossing.



- Click [Add] to complete the camera addition.

3.5.2.2 LPR/MLPR Detection

Add camera to Spark AI Service

Filter ▾

SELECT	ADDRESS	MODEL NAME	STATUS	DEVICE NAME	ORIGIN
<input checked="" type="checkbox"/>	123.111.222.123	Generic Camera	Not applicable	Camera 1	Recorder on DESKTOP-K...
<input type="checkbox"/>	172.21.7.160	SR-C-A2-DM1-V13-IR	Ready	玄關	Recorder on DESKTOP-K...
<input type="checkbox"/>	172.21.7.238	SR-C-A2-DF1-F3-IR	Ready	櫃台	Recorder on DESKTOP-K...
<input type="checkbox"/>	172.21.7.239	SR-C-A2-DF1-F3-IR	Ready	大門	Recorder on DESKTOP-K...

NAME	RESOLUTION	FPS	CODEC	PROFILE SELECTED
videostream ProfileToken_1	1920x1080	25	H264	Yes
videostream ProfileToken_2	1280x720	25	H264	Yes

LPR Mode: Lane

Camera 1

Camera 1: 2024/11/01 13:01:20 (UTC+08:00)

Add Close

- Select the image source.
- Select the stream resolution.
- Choose the recognition mode: Lane or Parking.
 - Lane: High-speed recognition mode.
 - Parking: Low-speed recognition mode.



3.5.2.3 Fire and Smoke Detection

The screenshot shows the 'Add camera to Spark AI Service' window. At the top, there is a 'Filter' dropdown and a 'Camera 12' label. A table lists camera options with columns: SELECT, ADDRESS, MODEL NAME, STATUS, DEVICE NAME, and ORIGIN. A red circle '1' highlights the first row. Below the table is a second table with columns: NAME, RESOLUTION, FPS, CODEC, and PROFILE SELECTED. A red circle '2' highlights the second row of this table. At the bottom, there is an 'Add' button and a 'Close' button, with a red circle '3' highlighting the 'Add' button. To the right, a video preview shows a fire scene with the text 'Camera 12' above it.

SELECT	ADDRESS	MODEL NAME	STATUS	DEVICE NAME	ORIGIN
<input type="checkbox"/>	123.111.222.123	Generic Camera	Not applicable	Camera 1	Recorder on DESKTOP-K...
<input type="checkbox"/>	172.21.7.160	SR-C-A2-DM1-V13-IR	Ready	玄関	Recorder on DESKTOP-K...
<input type="checkbox"/>	172.21.7.238	SR-C-A2-DF1-F3-IR	Ready	舞台	Recorder on DESKTOP-K...
<input type="checkbox"/>	172.21.7.239	SR-C-A2-DF1-F3-IR	Ready	大門	Recorder on DESKTOP-K...

NAME	RESOLUTION	FPS	CODEC	PROFILE SELECTED
videostream ProfileToken_1	1920x1080	25	H264	Yes
videostream ProfileToken_2	1280x720	25	H264	Yes

- Select the image source.
- Select the stream resolution: Please refer to 3.5.2 Add Camera to Spark AI Devices
- Click [Add].

3.5.2.4 Generic AI

The screenshot shows the 'Add camera to Spark AI Service' window. At the top, there is a 'Filter' dropdown and a 'Camera 8' label. A table lists camera options with columns: SELECT, ADDRESS, MODEL NAME, STATUS, DEVICE NAME, ORIGIN, and ANALYT. A red circle '1' highlights the third row. Below the table is a second table with columns: NAME, RESOLUTION, FPS, CODEC, and PROFILE SELECTED. A red circle '2' highlights the third row of this table. At the bottom, there is an 'Add' button and a 'Close' button, with a red circle '3' highlighting the 'Add' button. To the right, a video preview shows an office scene with the text 'Camera 8' above it.

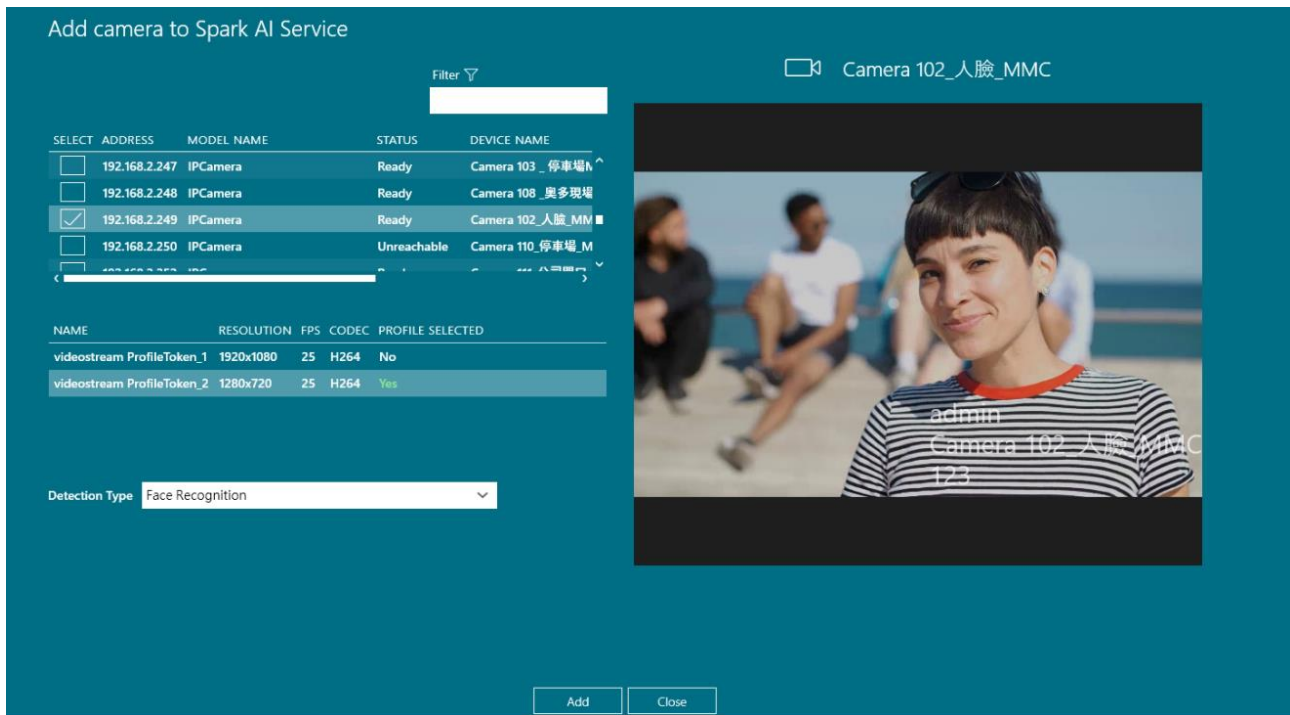
SELECT	ADDRESS	MODEL NAME	STATUS	DEVICE NAME	ORIGIN	ANALYT
<input type="checkbox"/>	172.21.5.10	BM2	Unreachable	Camera 1	Recorder on LAPTOP-UFTC64RP	No
<input type="checkbox"/>	172.21.5.11	BM2	Unreachable	Camera 4	Recorder on LAPTOP-UFTC64RP	No
<input checked="" type="checkbox"/>	172.21.7.27	BF1	Ready	Camera 8	Recorder on LAPTOP-UFTC64RP	No

NAME	RESOLUTION	FPS	CODEC	PROFILE SELECTED
videostream 0	1920x1080	30	H264	No
videostream 1	640x360	7	H264	Yes
videostream 2	320x240	2	JPEG	Yes

- Select the image source.
- Select the stream resolution: Please refer to 3.5.2 Add Camera to Spark AI Devices
- Click [Add].



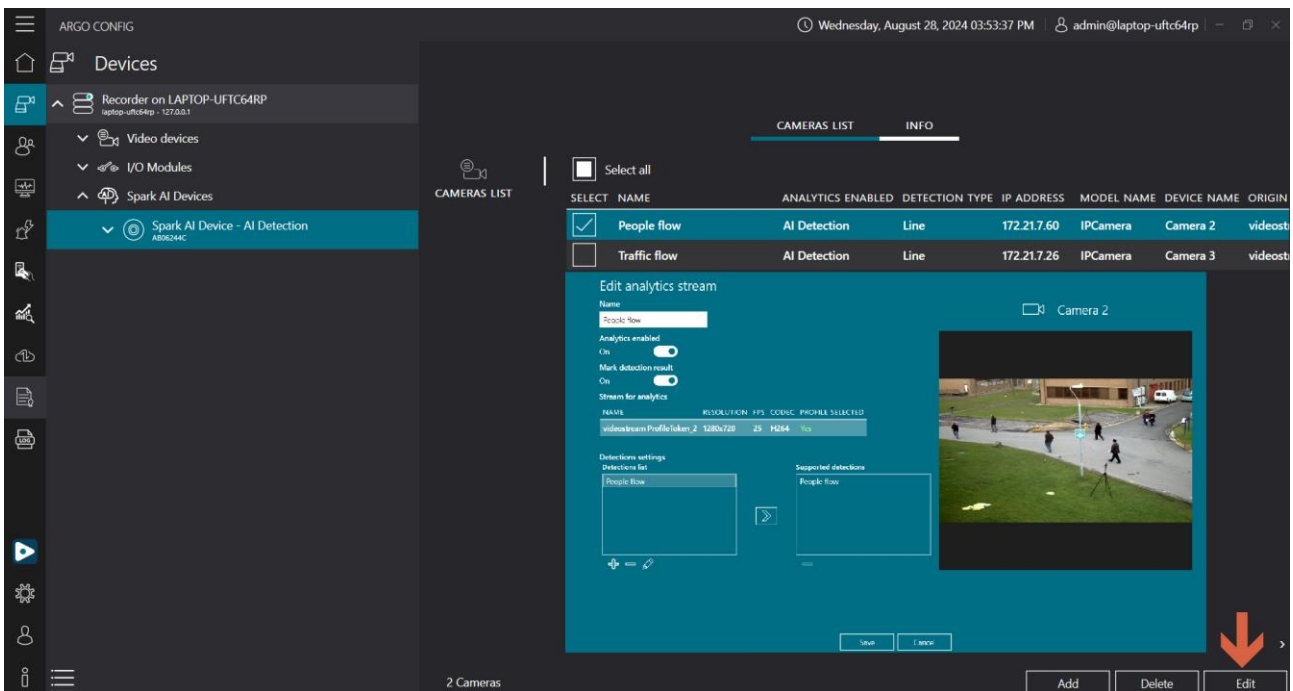
3.5.2.5 Face Detection



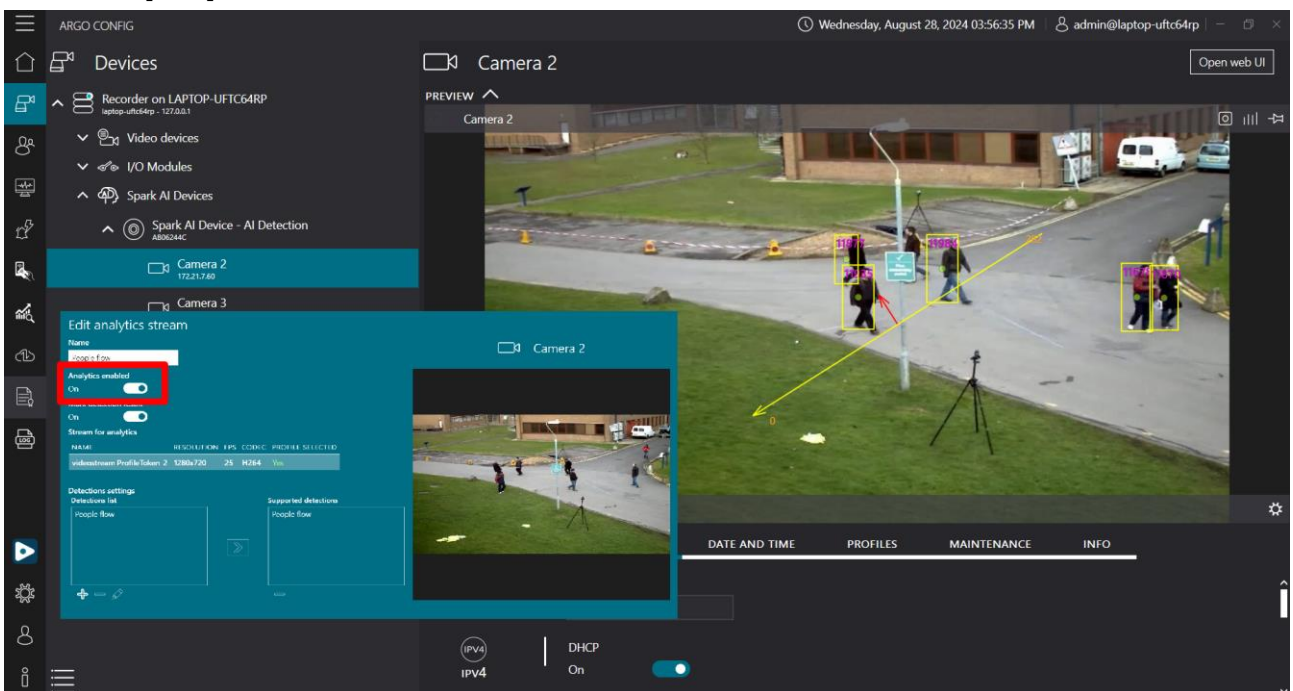
- Select the image source.
- Select the stream resolution: Please refer to 3.5.2 Add Camera to Spark AI Devices.
- Detection Type: Select Face Recognition.
- Click [Add].



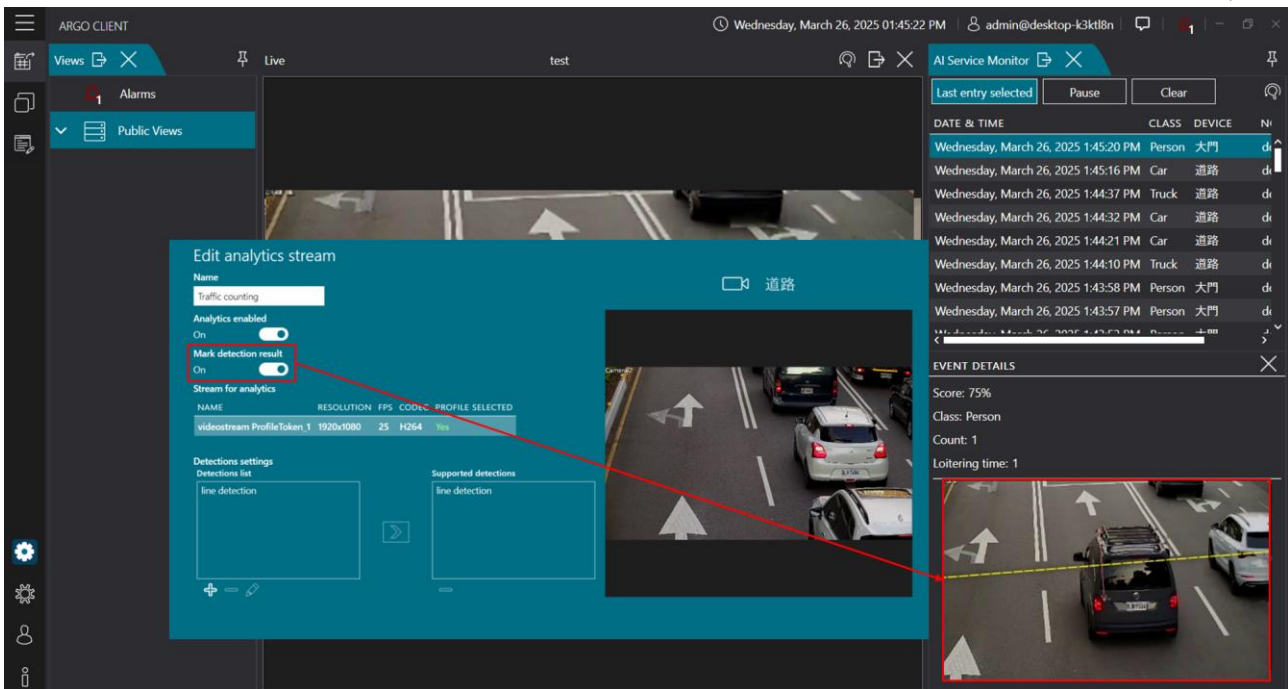
3.5.3 Edit Spark AI Devices



- Select the Spark AI device to edit.
- Check the analysis stream in the list.
- Click [Edit].



- Analysis enabled: Turn on (enabled by default) to activate smart analysis. The detection red box will be visible in the video stream



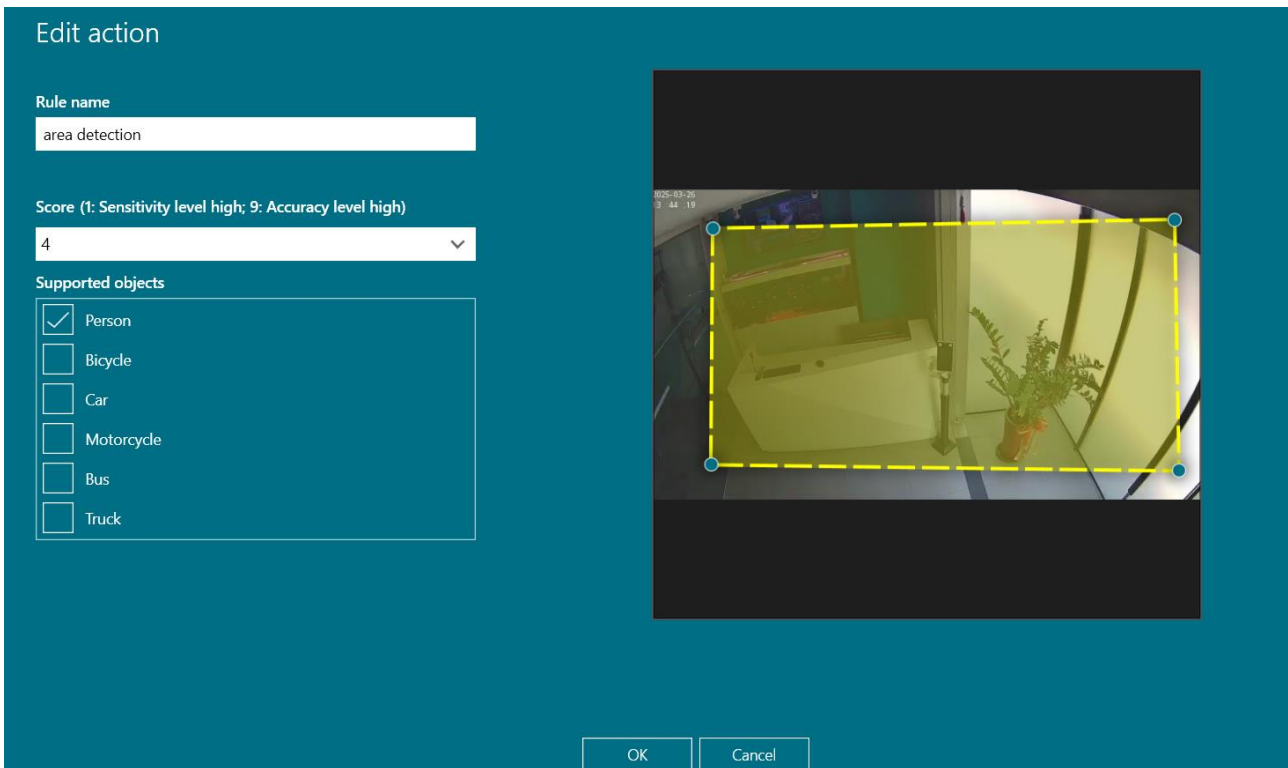
- Mark detection results: Turn on (default is off). Detected objects will be highlighted with a red box and displayed in the AI service monitoring window on the Client.
- Stream for analysis : Displays selected analysis stream information (read-only).
- Detection Settings: Edit region detection settings for the Spark AI service camera.






3.5.3.1 All/Human/Vehicle – Parameter Settings

A. Detection Type: Area

Add selectable region lists:



- Detection Name: Enter the detection area name.
- Score: The Score adjusts sensitivity (lower = higher sensitivity) and accuracy (higher = better accuracy), with a range of 1–9
- Supported objects: Select the object type to detect.
 - A. Human Detection: Pre-set to Person (cannot be changed).
 - B. Vehicle Detection: Options include Bicycle, Car, Motorcycle, Bus, Truck.
 - C. All Detection: Options include Person, Bicycle, Car, Motorcycle, Bus, Truck.
- Live View: Click the yellow detection box. When the four red dots turn green, drag the dots to adjust the detection area.
 - **Pencil Icon** : Add another detection area.
 - **Trash Bin Icon** : Delete the selected detection area.
 - **Pin Icon** : Keep the toolbar pinned for display.
- Add: Click [Add] to finalize the settings.
- Save: Click [OK] to store the settings.



B. Detection Type: Line crossing

Edit action

Rule name
line detection

Center Radius
10 + -

Detection Interval(FPS)
5 + -

Direction
Bidirection

Periodical
00 : 00

Score (1: Sensitivity level high; 9: Accuracy level high)
4




Supported objects

- Person
- Bicycle
- Car
- Motorcycle
- Bus
- Truck

- Rule Name: Enter the detection area name.
- Center Radius: [1–10], adjusts the diameter of the object center that crosses the line. A larger value increases the likelihood of triggering the object detection.
- Detection Interval (FPS): [10–60], sets the time interval for detecting objects crossing the line. This interval controls how soon the next trigger can occur after the first.
- Direction: Options include Bidirectional, Enter, Exit. Reverse: Reverses the direction of entry or exit.
- Periodical: This sets the time for data reset. [00–23] (units: hours), Minute: [00–50] (units: every 10 minutes).
- Score: The Score adjusts sensitivity (lower = higher sensitivity) and accuracy (higher = better accuracy), with a range of 1–9.
- Supported objects: Select the object type to detect.
 - Human Detection: Pre-set to Person (cannot be changed).
 - Vehicle Detection: Options include Bicycle, Car, Motorcycle, Bus, Truck.
 - All Detection: Options include Person, Bicycle, Car, Motorcycle, Bus, Truck.
- Live View: Click the yellow line for line crossing. When the red dots turn green, drag



the dots to adjust the line position..

- **Pencil Icon** : Add another detection area.
 - **Trash Bin Icon** : Delete the selected detection area.
 - **Pin Icon** : Keep the toolbar pinned for display.
- Add: Click [Add] to finalize the settings.
 - Save: Click [OK] to store the settings.

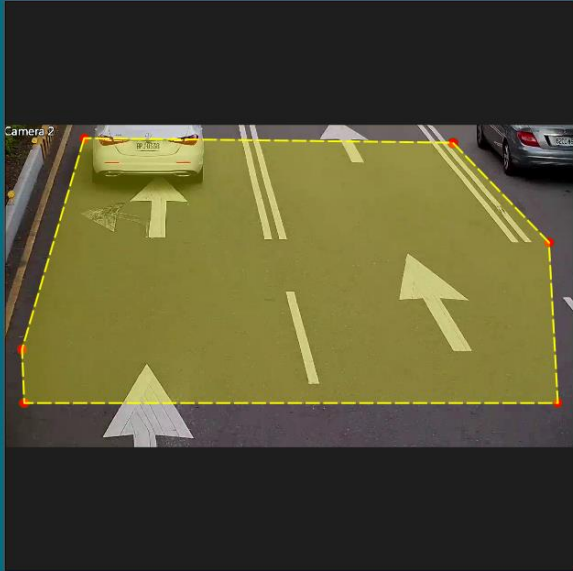


3.5.3.2 Taiwan License Plate Device - Parameter Settings




A. Detection Type: Lane

Edit action

Rule name
area detection|



OK Cancel

- Rule Name: Enter the detection area name.
- Live View: Click the yellow detection box. When the red dots turn green, drag the dots to adjust the detection area.
- Pencil Icon : Add another detection area.
- Trash Bin Icon : Delete the selected detection area.
- Pin Icon : Pin the toolbar for display.
- Save: Click [OK] to finalize the settings.




B. Detection Type: Parking

Edit action




Rule name
area detection1

Recognition Interval (s)
1 + -

Hold Time (s)
20 + -



OK Cancel

- Rule Name: Enter the detection area name.
- Recognition Interval(seconds): The time duration for collecting images.
- Hold Time (seconds): The duration for which the detected license plate is retained, ensuring the same plate is not provided within the set time.
- Live View: Click the yellow detection box. When the red dots turn green, drag the dots to adjust the detection area.
 - Pencil Icon : Add another detection area.
 - Trash Bin Icon : Delete the selected detection area.
 - Pin Icon : Pin the toolbar for display.
- Save: Click [OK] to finalize the settings.



3.5.3.3 Multi-country License Plate Device - Parameter Settings-

Step1: Lane Mode Parameter Editing

The screenshot shows a dialog box titled "Edit action" with a teal background. On the left side, there are four input fields: "Rule name" with the value "mlpr detection1", "Score (1: Sensitivity level high; 9: Accuracy level high)" with the value "9", "Country" with the value "Philippines", and "OCR complexity" with the value "3". On the right side, there is a preview image of a white SUV in a parking lot, with a yellow dashed box around the license plate area. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Settings and adjustments specific to lane mode for multi-country license plate detection.

- Detection Name: Enter the detection area name.
- Score:
 - 1: Higher sensitivity, easier to detect vehicles.
 - 9: Higher accuracy.
- Country: Select the country for license plate recognition as the reference standard.
- OCR Complexity:
 - 1: Uses lower CPU performance for simpler backgrounds.
 - 2 (default): Balanced performance.
 - 3: Uses higher CPU performance for complex scenes and license plates.
- Save: Click Save to finalize the settings.



Step2: Parking Mode Parameter Editing

Edit action

Rule name
mlpr detection1

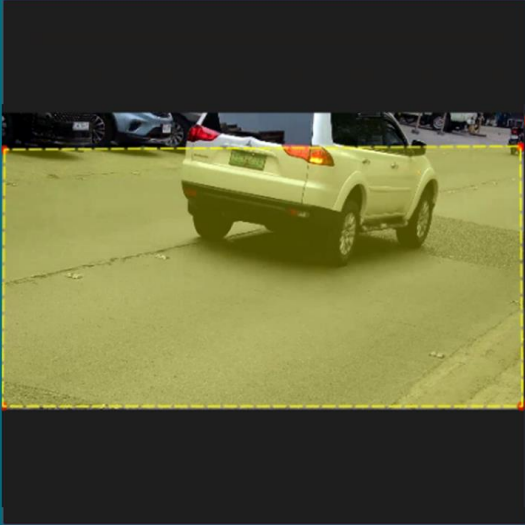
Score (1: Sensitivity level high; 9: Accuracy level high)
9

Country
Philippines




OCR complexity
3

Recognition Interval (s)
1

Hold Time (s)
20

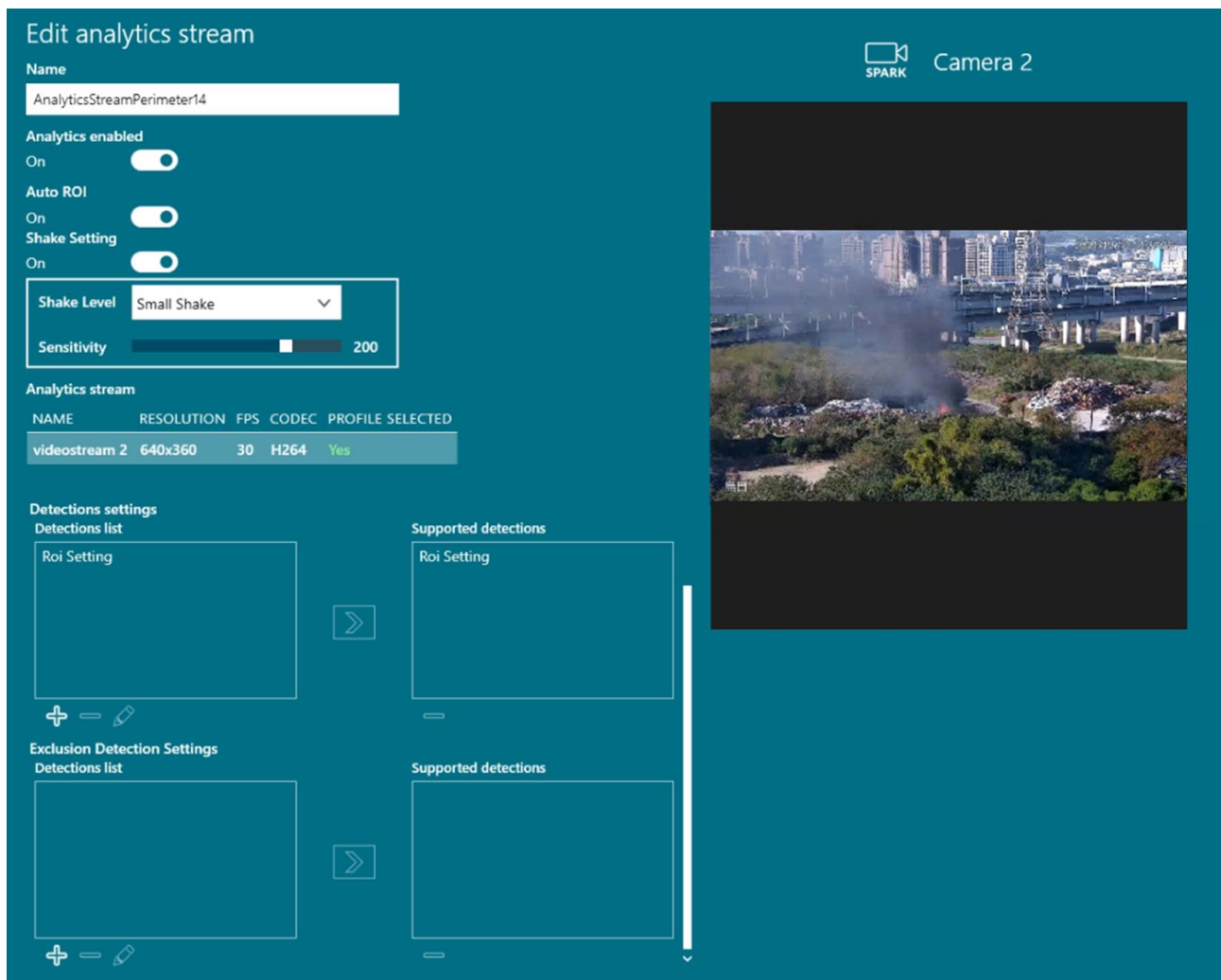


OK Cancel

- Rule Name: Enter the detection area name.
- Country: Select the country for license plate recognition as the reference standard.
- OCR Complexity:
 - 1: Uses lower CPU performance for simpler backgrounds.
 - 2 (default): Balanced performance.
 - 3: Uses higher CPU performance for complex scenes and license plates.
- Recognition Time (seconds): Set the time duration for collecting images of vehicles.
- Hold Time (seconds): Set how long the license plate is retained before being discarded, ensuring the same plate is not detected again within this time.
- Live View: Click the yellow detection box. When the red dots turn green, drag the dots to adjust the detection area.
 - Pencil Icon : Add another detection area.
 - Trash Bin Icon : Delete the selected detection area.
 - Pin Icon : Pin the toolbar for display.
- Save: Click Save to finalize the settings.



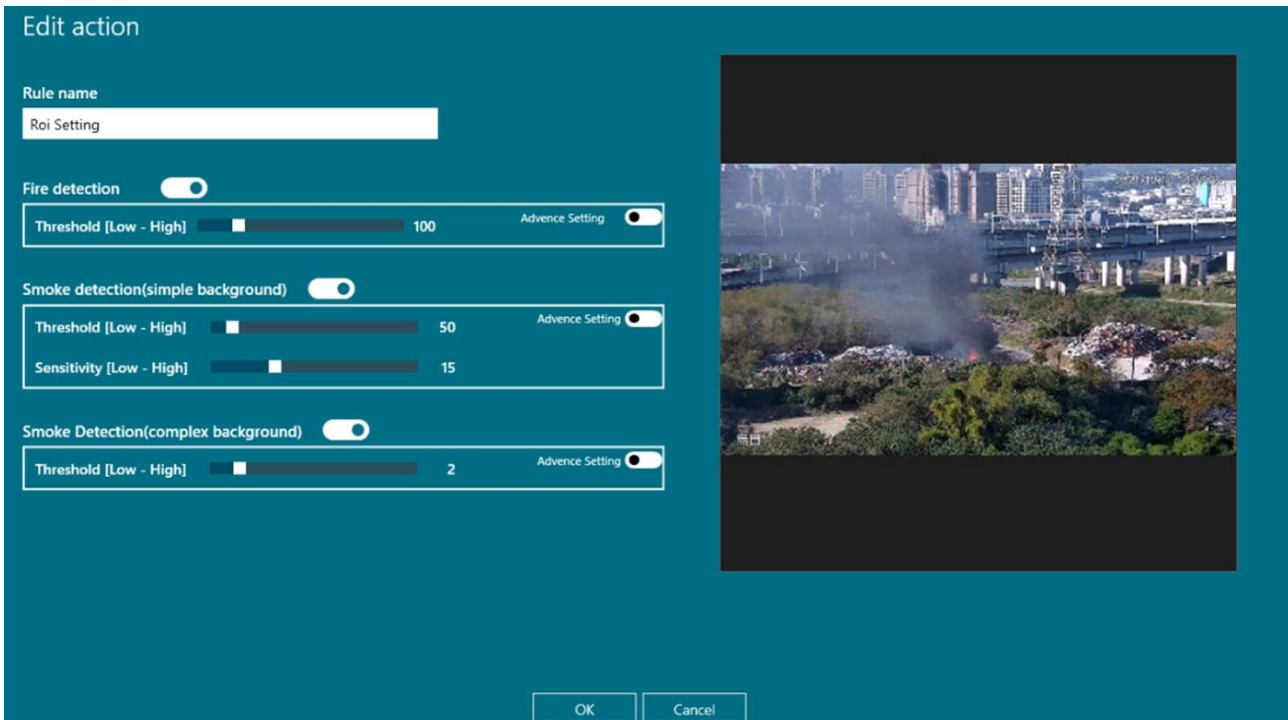
3.5.3.4 Fire and Smoke Detection - Parameter Settings Description



- Auto ROI: Enabled by default, automatically detects the entire screen without manual setup.
- Shake Setting: Options – None, Small Shake, Big Shake (Enabled by default). Adjusts for environmental vibrations to reduce recognition errors.
 - Sensitivity: Range 50–250 (Higher values increase sensitivity).
- Analysis Stream: Displays selected analysis stream information (read-only).
- Detection list: Configure detection regions and parameters.
- Excluded Detections Settings: Define areas to be excluded from detection.



A. Region Detection Settings

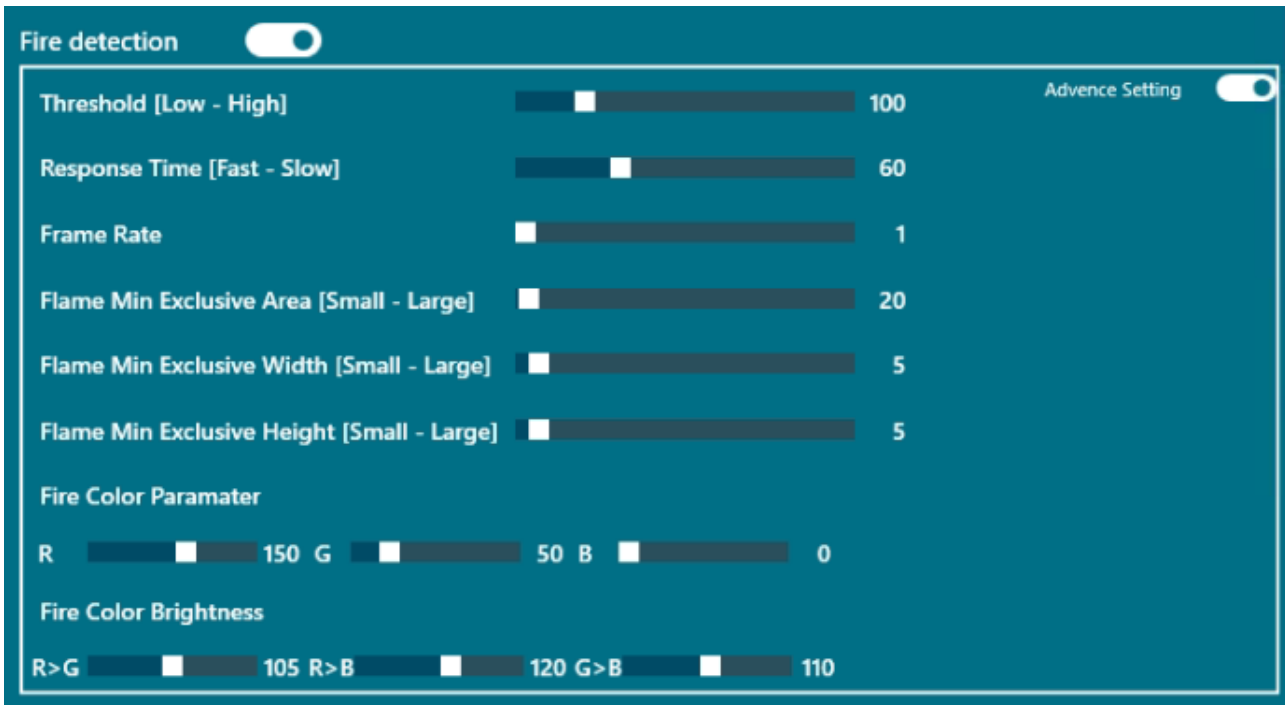


- Fire Detection: Enable/Disable (default: disabled). When enabled, fire detection is activated; when disabled, it is deactivated.
 - Threshold [Low-High]: [1–200]. Higher values require a larger fire to trigger detection.
- Smoke Detection (Simple Background): Enable/Disable (default: disabled). When enabled, smoke detection is activated; when disabled, it is deactivated.
 - Threshold [Low-High]: [10–500]. Higher values require more smoke to trigger detection.
 - Sensitivity [Low-High]: [0–50]. Lower values increase sensitivity, allowing detection of lighter smoke.
- Smoke Detection (Complex Background): Enable/Disable (default: disabled). When enabled, smoke detection is activated; when disabled, it is deactivated.
 - Threshold [Low-High]: [1–9]. Higher values require more smoke to trigger detection.

Note: Advanced Settings: Manufacturer-configured based on the environment; user adjustments may affect accuracy.



(1) Advanced Fire Detection Parameters



Fire Detection: Enable/Disable (default: disabled). Enabling activates fire detection, disabling stops it.

- Threshold [Low-High]: [1~200]. Higher values require larger flames to trigger detection.
- Response Time [Fast-Slow]: [1~200] (default: 60). Lower values increase detection speed.
- Frames Rate: [1~30] (default: 8). Number of frames processed for detection.
- Flame Min Exclusion Area [Small-Large]: [10~1000] (default: 20). Fires smaller than this area will not be detected.
- Flame Min Exclusion Width [Small-Large]: [1~100] (default: 5). Fires narrower than this width will not be detected.
- Flame Min Exclusion Length [Small-Large]: [1~100] (default: 5). Fires shorter than this length will not be detected.
- Fire Color Parameters:
 - R [0~255]: Min red brightness (Indoor: 200, Outdoor: 150).
 - G [0~255]: Min green brightness (Indoor: 100, Outdoor: 50).
 - B [0~255]: Min blue brightness (Indoor & Outdoor: 0).
- Fire Color Brightness:
 - R > G: [10~200] (default: 105).
 - R > B: [10~200] (default: 120).
 - G > B: [10~200] (default: 110).



(2) Advanced Smoke Detection (Simple Background) Parameters

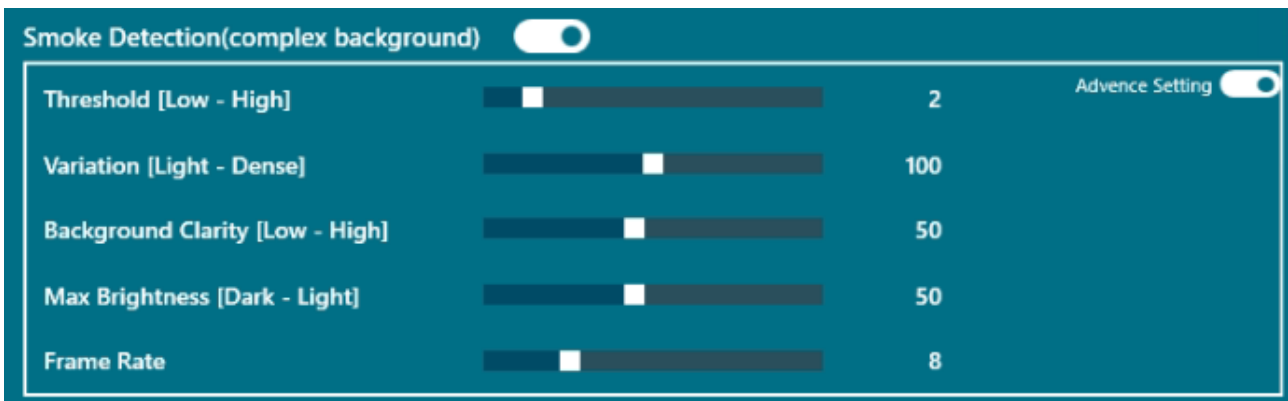
Parameter	Value
Threshold [Low - High]	50
Sensitivity [Low - High]	15
Detection Threshold [Low - High]	100
Response Time [Fast - Slow]	10
Frame Rate	8
Max Brightness [Dark - Light]	255
Min Brightness [Dark - Light]	0
Contrast [Low - High]	30
Texture [Dense - Light]	30

Smoke Detection (Simple Background): Enable/Disable (default: disabled). Enabling activates smoke detection, disabling stops it.

- Threshold [Low-High]: [10~500]. Higher values require larger smoke volumes to trigger detection.
- Sensitivity [Low-High]: [0~50]. Lower values increase sensitivity, allowing detection of lighter smoke.
- Detection Threshold [Low-High]: [1~100] (default: 100). Changes exceeding this value will not be detected.
- Response Time [Fast-Slow]: [1~200] (default: 10). Lower values increase detection speed.
- Frames Rate: [1~30] (default: 8). Number of frames processed for detection.
- Max Brightness [Dark-Bright]: [0~255] (default: 255). Detection starts below this brightness threshold.
- Min Brightness [Dark-Bright]: [0~255] (default: 0). Detection starts above this brightness threshold.
- Contrast [Low-High]: [0~255] (default: 0). Detection starts above this brightness threshold.
- Texture [Dense-Light]: [10~100] (default: 30). Lower values detect denser smoke.



(3) Advanced Smoke Detection (Complex Background) Parameters

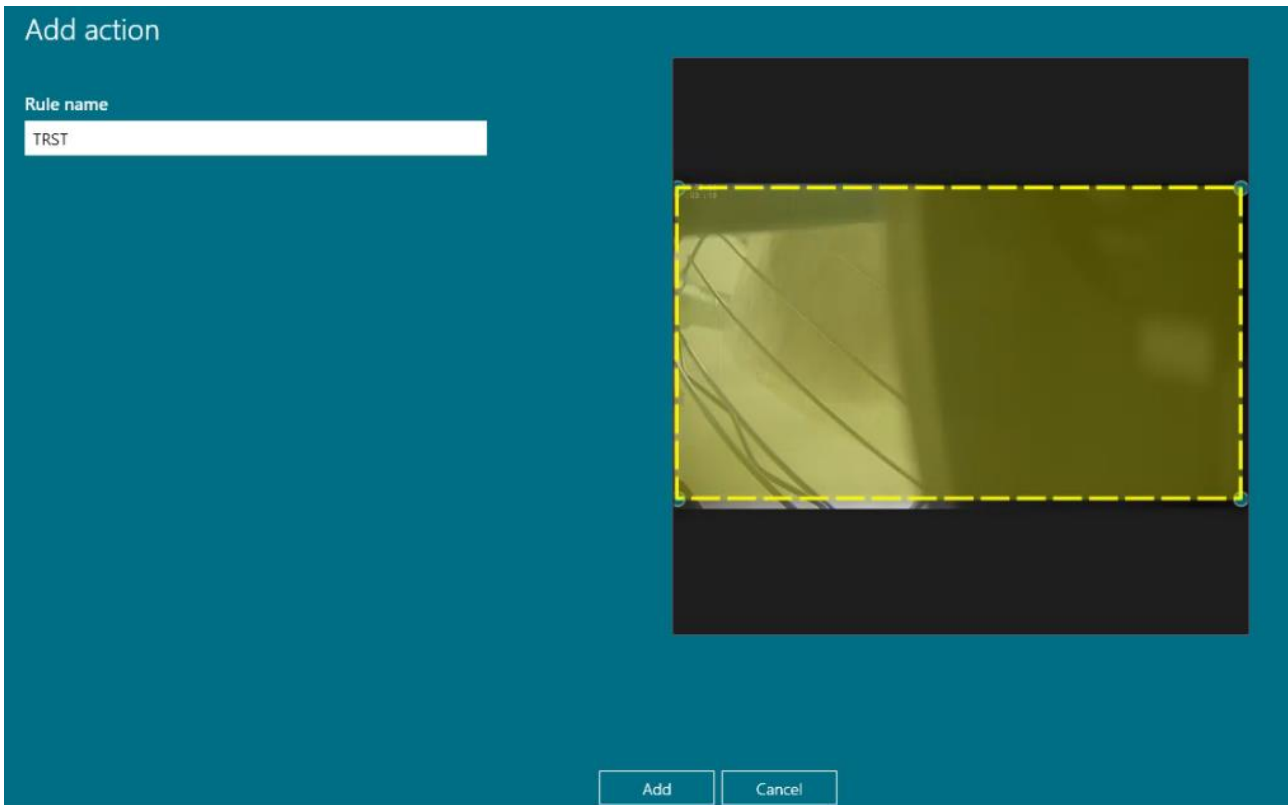


Smoke Detection (Complex Background): Enable/Disable (default: disabled). Enabling activates smoke detection, disabling stops it.

- Threshold [Low-High]: [1~9]. Higher values require larger smoke volumes to trigger detection.
- Variation [Light Smoke - Dense Smoke]: [50~150] (default: 100). Lower values detect denser smoke.
- Background Visibility [Low - High]: [10~100] (default: 50). Detection is disabled below this visibility threshold.
- Max Brightness [Dark - Light]: [10~100] (default: 50). Detection is disabled below this brightness level.
- Frames Rate: [1~30] (default: 8). Number of frames processed for detection.



B. Exclusion Area Detection Settings



- Exclusion Area Detection: Add exclusion area detection settings for Spark AI service cameras to avoid interference sources.
- Click [+] to add a new detection area.
- Rule Name: Enter the detection area name.
- Live Image: Click the yellow detection frame, and the red dots on the corners will turn green. You can drag the dots to adjust the detection area.
 - Pencil Icon: Add another detection area.
 - Trash Bin Icon: Delete the selected detection area.
 - Pin Icon: Pin the toolbar to stay on top.
- Add: Click to complete the settings.
- Save: Click to save the settings.



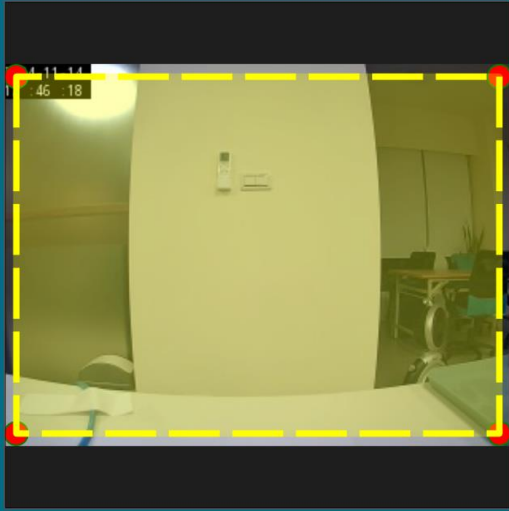
3.5.3.5 General AI Device - Parameter Settings Description

Edit action

Rule name
generic ai detection

Threshold 50

Sensitivity 50



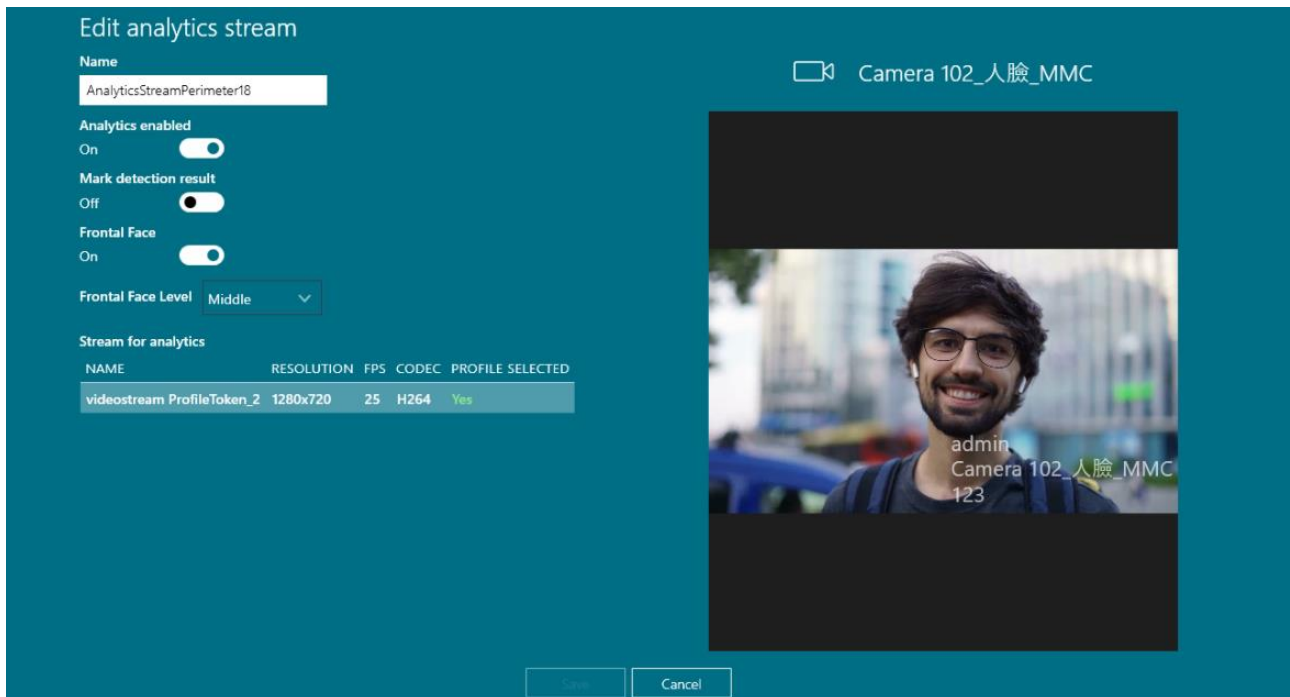
Warning: This change will affect all events referring to this action. Continue?

OK Cancel

- Set Parameters and Draw Detection Area.
 - Threshold: [1~100] Higher values indicate a higher threshold for triggering; lower values indicate a lower threshold.
 - Sensitivity: [1~100] Higher values indicate higher sensitivity in detecting objects; lower values indicate lower sensitivity.
- Save: Click to save the settings.



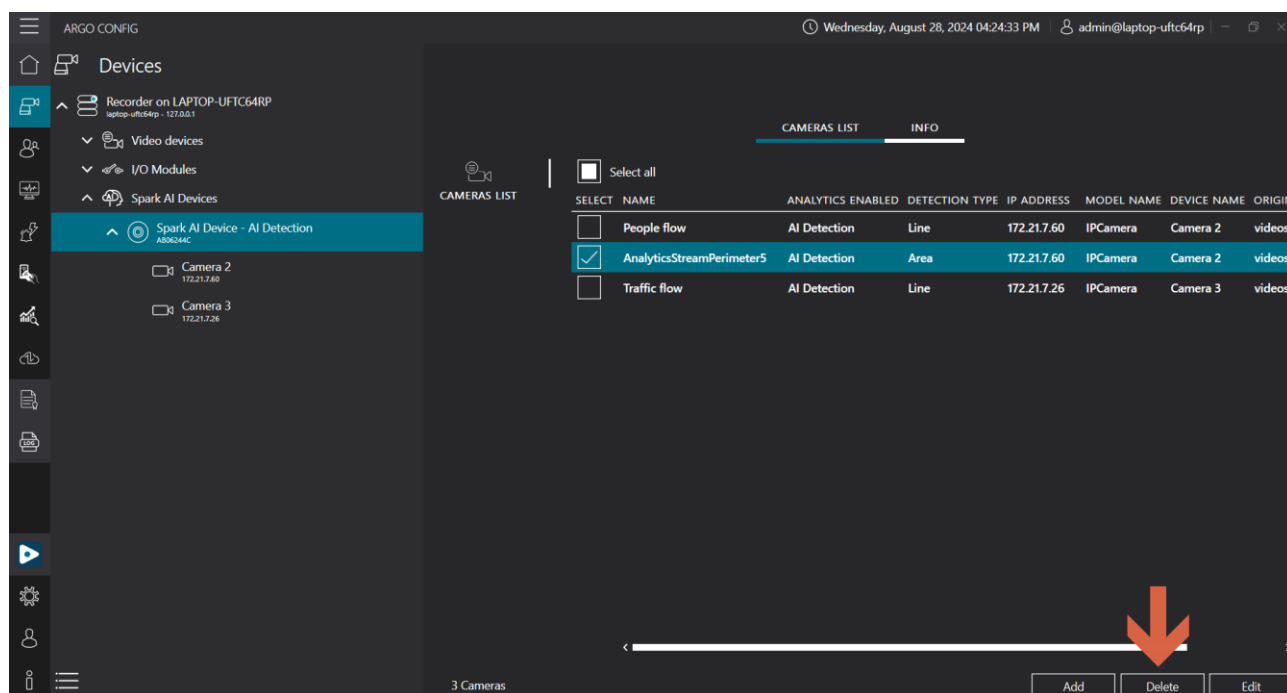
3.5.3.6 Face Detection - Parameter Settings Description



- Analysis enabled: Turn on (enabled by default) to activate smart analysis. The detection red box will be visible in the video stream
- Mark detection results: Turn on (default is off). Detected objects will be highlighted with a red box and displayed in the AI service monitoring window on the Client.
- Frontal Face: Turn on (default is off)
 - Frontal Face Level: [Low, Medium, High] Higher levels apply stricter rules for frontal face detection.
- Stream for analysis : Displays selected analysis stream information (read-only).

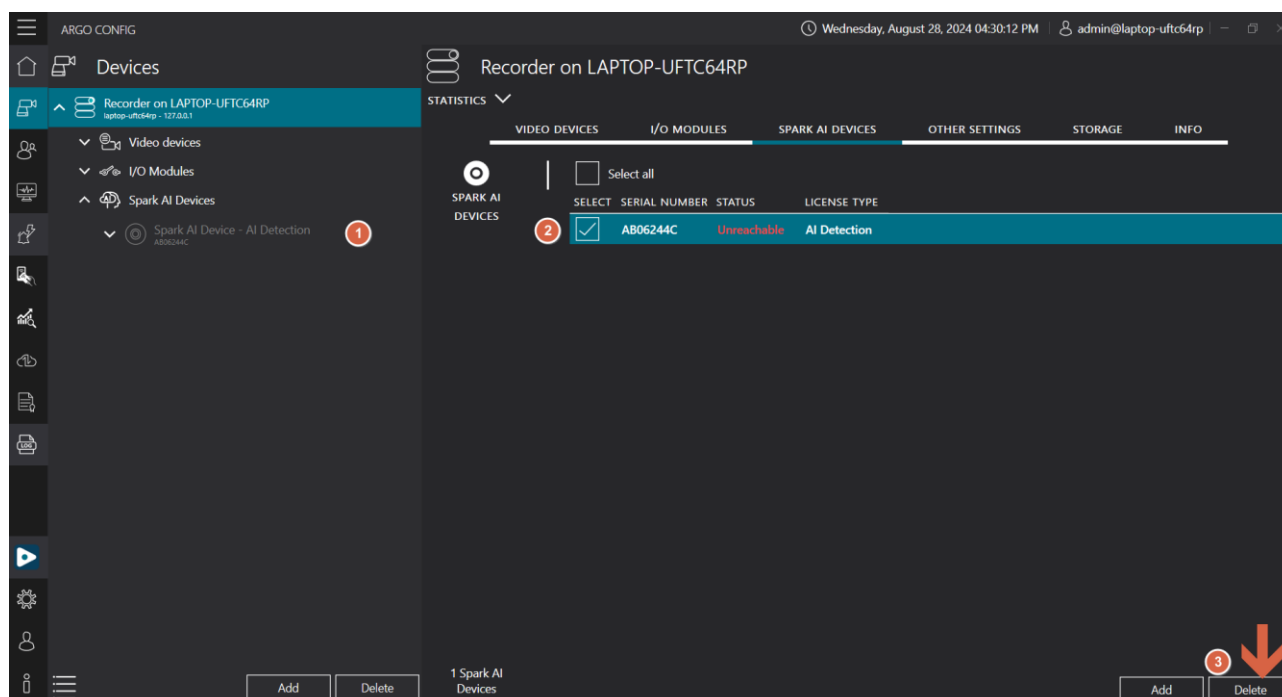


3.5.4 Delete Spark AI Device Stream Analysis



- Select the Spark AI device to edit.
- Check the analysis stream from the list.
- Click [Delete].

3.5.5 Delete Spark AI Device



- Ensure the Spark AI device is in an offline status.
- Select the Spark AI device you wish to delete.
- Click [Delete].

Note: When deleting, the Spark AI key must be offline first.



3.5.6 INFO

The screenshot shows the 'Recorder on DESKTOP-6KBNS5A' interface. The left sidebar lists device categories: Video devices, Intercoms, I/O Modules, and Spark AI Devices. Under Spark AI Devices, several options are listed, with 'Spark AI Device - AI Detection' (ID: 83061A4C) selected. The right panel shows the 'INFO' tab with the following details:

PROPERTY	VALUE
SERIAL NUMBER	B3061A4C
LICENSE TYPE	AI Detection
COUNT	8

Browse Spark AI Detection Device Information :

- Serial Number: The AI device identification number.
- License Key Type: The detection recognition category.
- Count: The number of channels the AI device can recognize.



3.6 Other settings

3.6.1 Database settings

The screenshot shows the 'OTHER SETTINGS' tab in the Spark Recorder interface. On the left, there is a 'DATABASE OPTIONS' menu with a database icon. The main area is divided into sections for different databases and a storage path table.

AI DataBase

Split file interval: 3 Days (with +/- controls)
Retention days: 30 Days (with +/- controls)

ALPR DataBase

Split file interval: 3 Days (with +/- controls)
Retention days: 30 Days (with +/- controls)

Event Manager DataBase

Split file interval: 3 Days (with +/- controls)
Retention days: 30 Days (with +/- controls)

Metadata DataBase

Split file interval: 3 Days (with +/- controls)
Retention days: 30 Days (with +/- controls)

DB Storage Path

SELECT	TYPE	DRIVE	MAX SIZE	FREE SPACE
<input checked="" type="radio"/>	disk	C:\	237.23 GB	24.22 GB

- A. AI Database: Records usage data related to AI functions in Spark Recorder.
 - B. ALPR Database: Records usage data related to license plate recognition functions in Spark Recorder.
 - C. Event Management Database: Records usage data related to event management functions in Spark Recorder.
 - D. Metadata Database: The real-time data dashboard and advanced analytics report features in Spark Recorder are based on recorded data logs.
 - File Split Interval: Interval of time for database record files. Click [+] / [-] to increase/decrease the number of days.
 - Retention Days: When the database record file storage space is full, specify the number of hours/days of recording files to retain before the current day. Click [+] / [-] to increase/decrease the number of days.
- Note: File split interval ranges from 1 to 100 days, retention days range from 3 to 1000 days.**
- E. DB Storage Path: Directory on the hard drive where the database can be stored in Spark Recorder.



3.6.2 License plate recognition upload settings

LPR UPLOAD SETTING

LPR FTP uploading

Enable

Path
ftp://127.0.0.1 (ftp://ip address)

Username

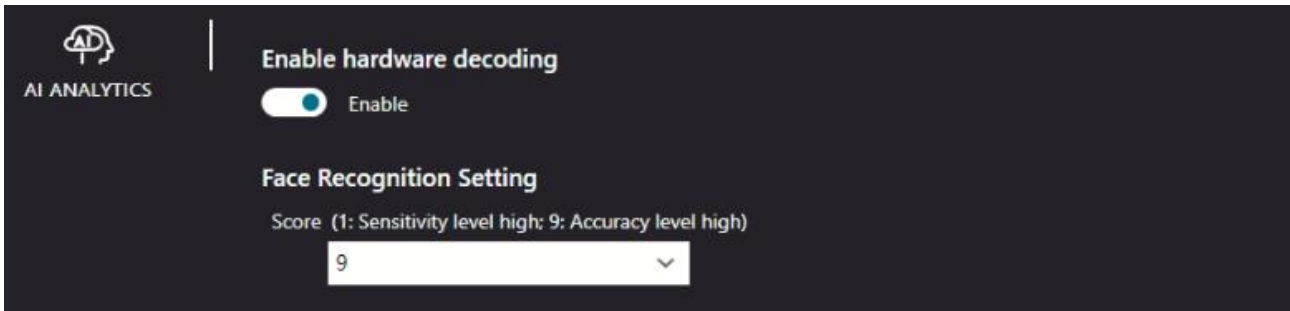
Password

Temporary Folder
C:\ProgramData\Spark\jpeg_tmp

- License plate recognition upload settings:
- Once enabled, license plate recognition data will be uploaded via FTP.
- Path: insert the path in the format ftp://ip address.
- Username: insert the FTP username.
- Password: insert the FTP password.
- Local temporary folder: insert the path of the temporary folder [default value 20842].

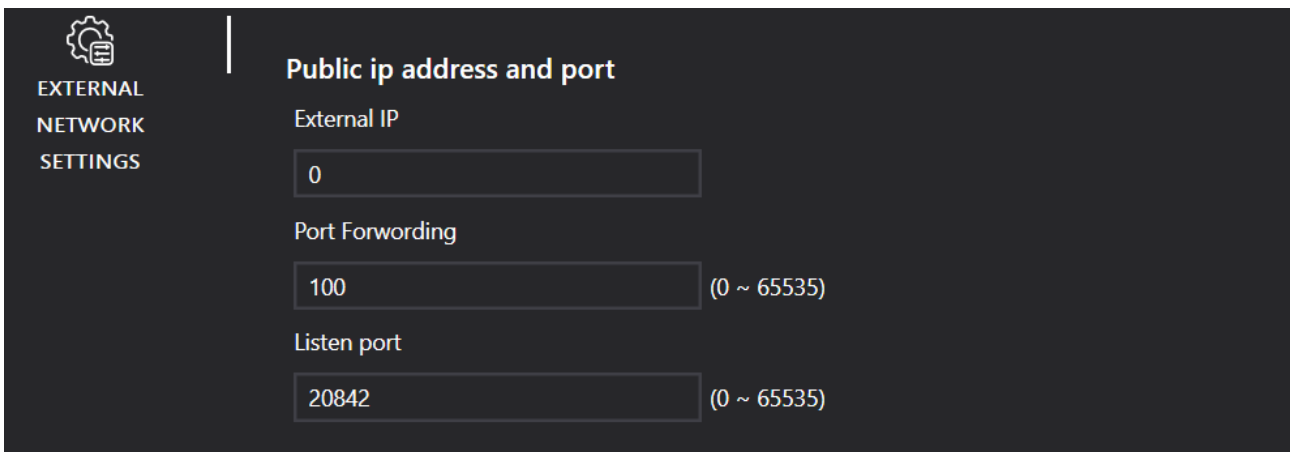


3.6.3 AI Analytics



- Enable Hardware Decoding: Enables hardware decoding for Spark AI intelligent analysis to accelerate multi-stream video processing, improving the number of frames analyzed per second and overall performance.
- Face Recognition Threshold Setting [1~9]: Configures the recognition score threshold for Spark AI face recognition. A higher score indicates stricter detection criteria and improved accuracy.

3.6.4 External Network Settings



- External address: the local WAN (Wide Area Network) IP address used for external communication.
- Communication Forwarding Port: insert the port number used as the external communication port to the router.

Port Range: 0 to 65535 [Default value: 20842]

- Listening Port: insert the port number used by Argo to receive data.

Port Range: 0 to 65535 [Default value: 20842]

Note:

A. The WAN IP address can be checked using <https://www.whatismyip.com.tw/tw/>

B. The router must support Port Forwarding functionality to set up port forwarding.



- C. It is recommended to disable the computer firewall to ensure this function operates correctly.
- D. Use NGROK forwarding service for communication port redirection settings.



3.6.5 Web server settings

Web Server

Enable

HTTP Port
80 (80, 1025 ~ 65535)

HTTPS Port
5555 (443, 1025 ~ 65535)

Certificate File(.pem)

Private Key File(.pem)

Certificate Information

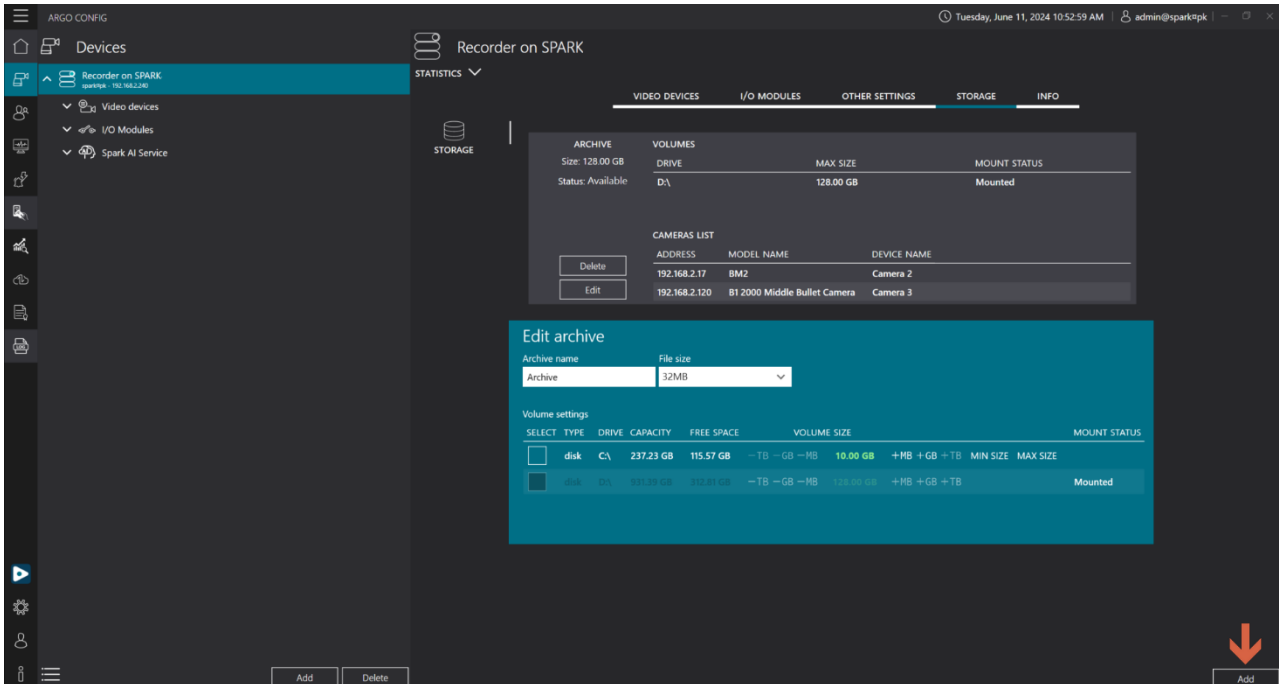
ISSUED TO	ISSUED BY	ISSUED ON	EXPIRES ON
Spark Argo Web	Spark Argo Web	Mar 20 05:09:58 2025 GMT	Apr 19 05:09:58 2025 GMT

- Enable to view the monitoring screen via the web server.
 - HTTP Port: Enter the port.
Range: 80 (default), 1025~65535.
 - HTTPS Port: /: Enter the port.
Range: 443 (default), 1025~65535.
 - Certificate File (.pem): Upload a certificate file for encrypted transmission.
 - Private Key File (.pem): Upload a private key file for encrypted transmission.
- Note: Both the certificate and private key files must be uploaded to successfully enable HTTPS encryption.**
- Certificate Information: The certificate information will be displayed after successful upload.

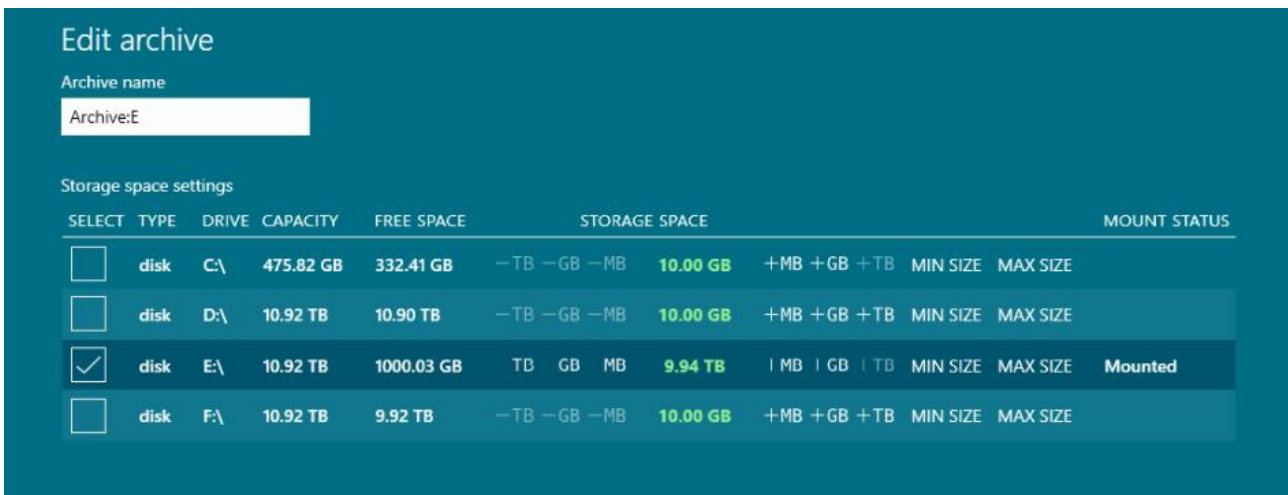


3.7 Storage

3.7.1 Add storage



- Click on the bottom right **[Add]**
- File name: insert name the recording file
- File size: select file size (32/64/128MB)
- Volume settings: select the hard drive(s) you want to add to the storage space



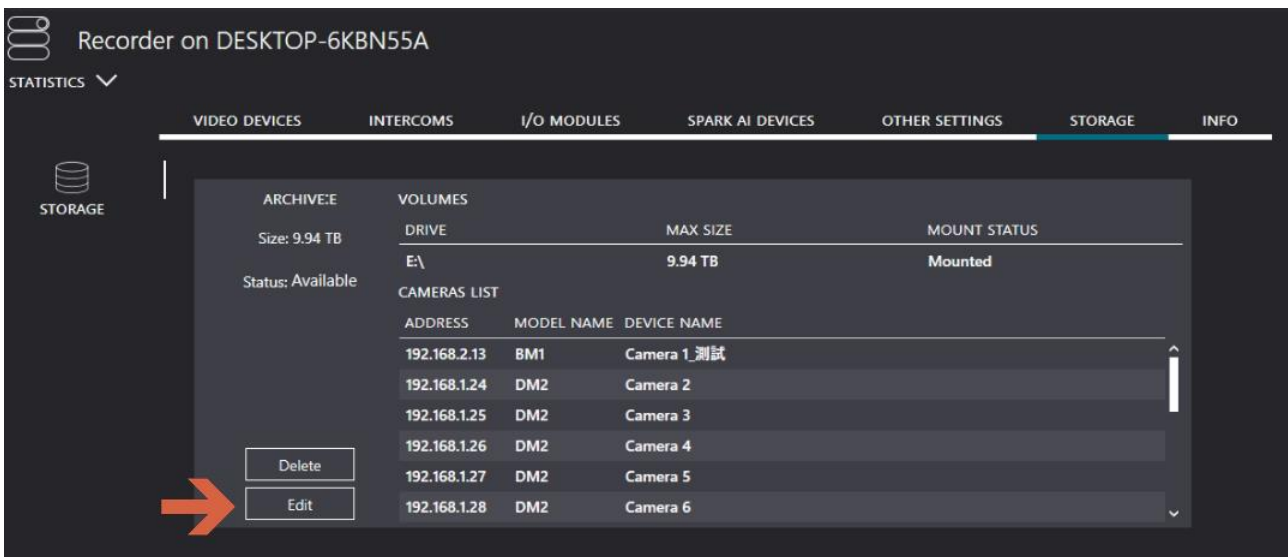
- Disk Partition Size: Click **[+]** to increase recording storage space, click **[-]** to decrease recording storage space.

Note: 1. The minimum size for disk partition is 10GB, and the maximum size is the capacity of the hard drive itself.

2. At least 500MB of disk space needs to be reserved to properly allocate storage space.



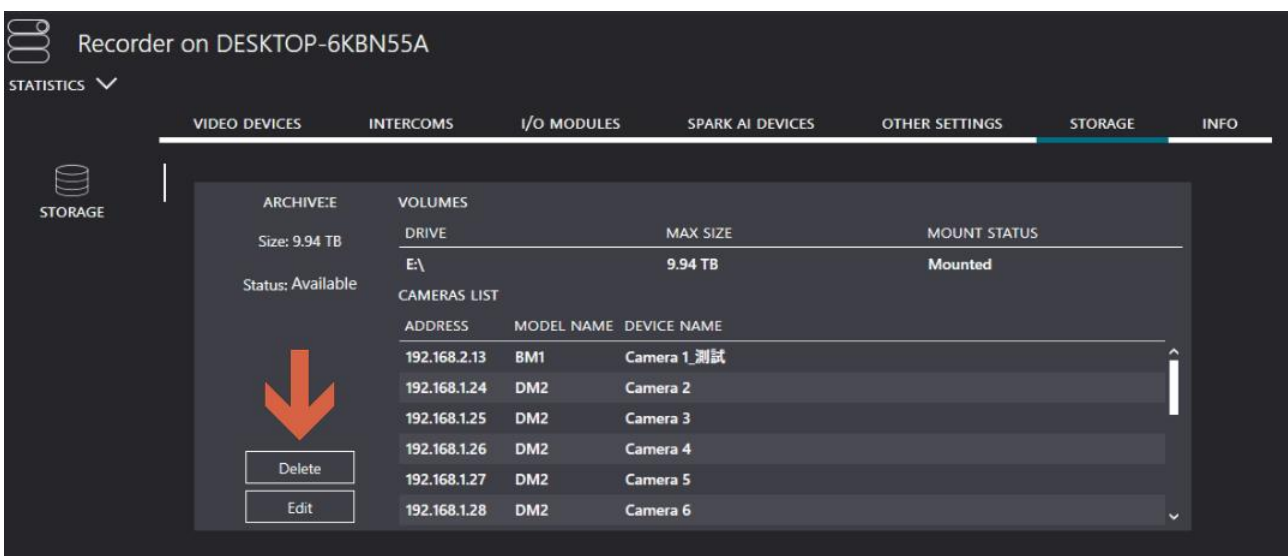
3.7.2 Edit storage



Select the storage space you want to edit and then click on **[Edit]**, tick the box to edit the disk.

Note: Editing the archive size may cause breaks in streams recording.

3.7.3 Delete storage

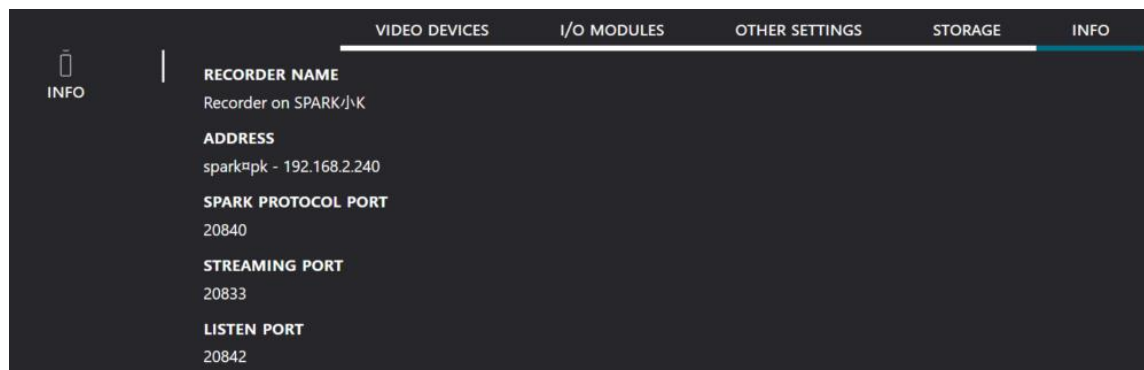


- Select the storage space you want to delete and then click on **[Delete]**.



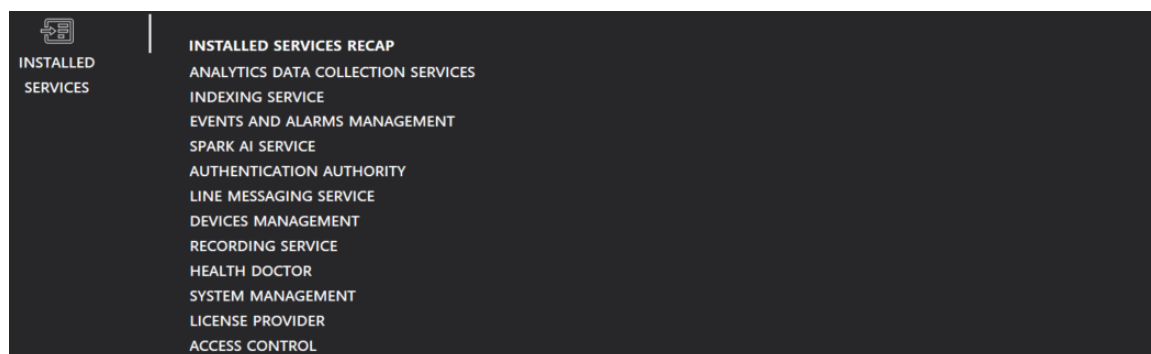
3.8 Information

3.8.1 Information



- Browse the recorder name/address/SPARK protocol port/streaming port/listening port.

3.8.2 Installed services

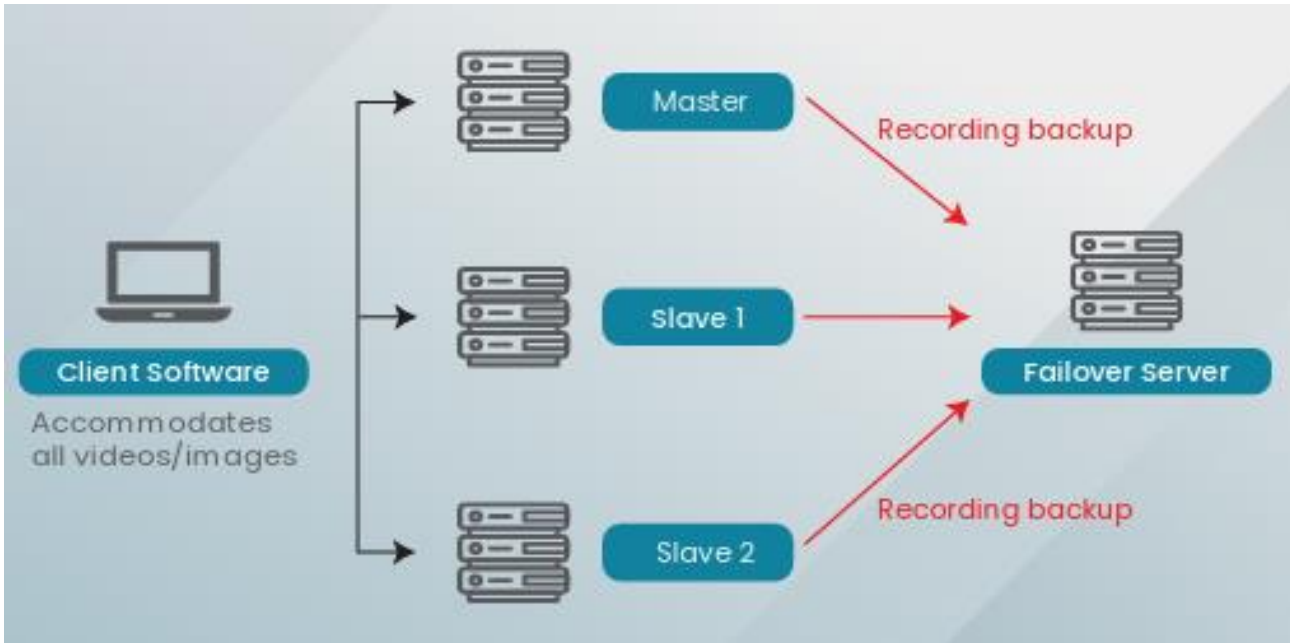


- Installed services content



3.9 Server

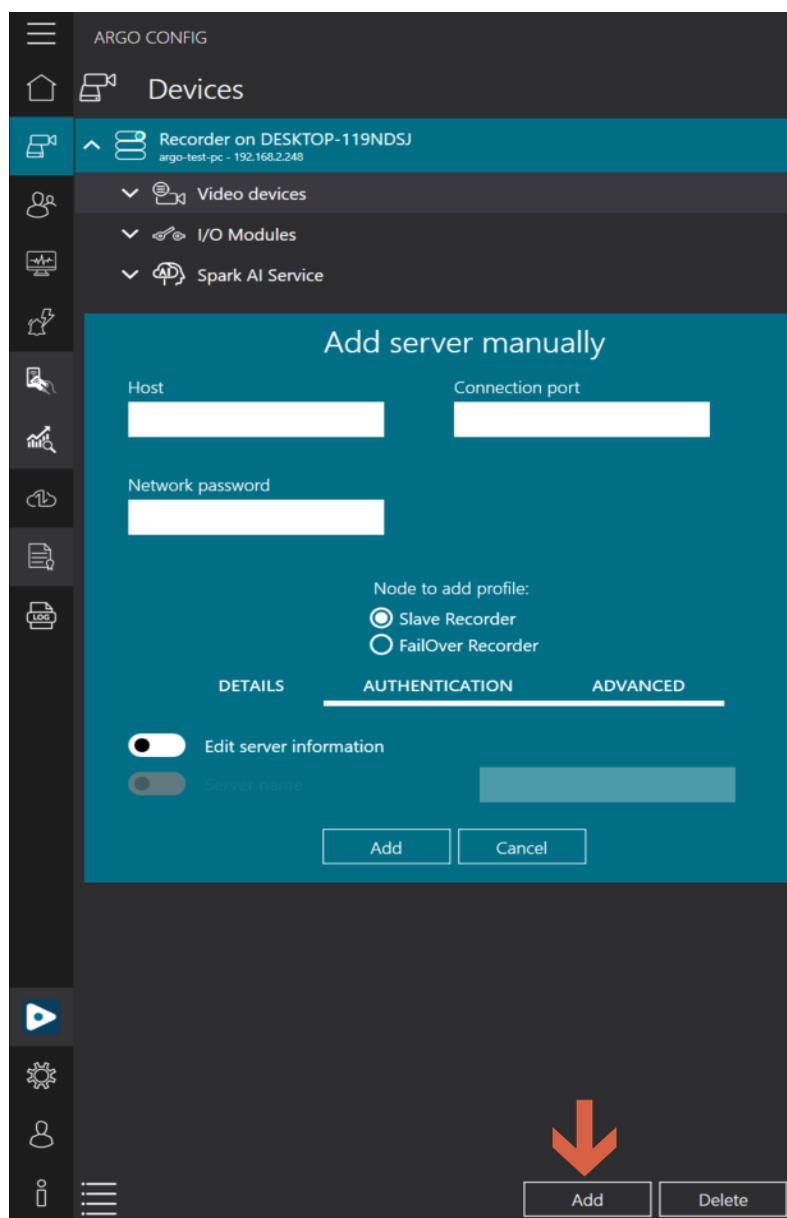
3.9.1 Primary server and secondary servers



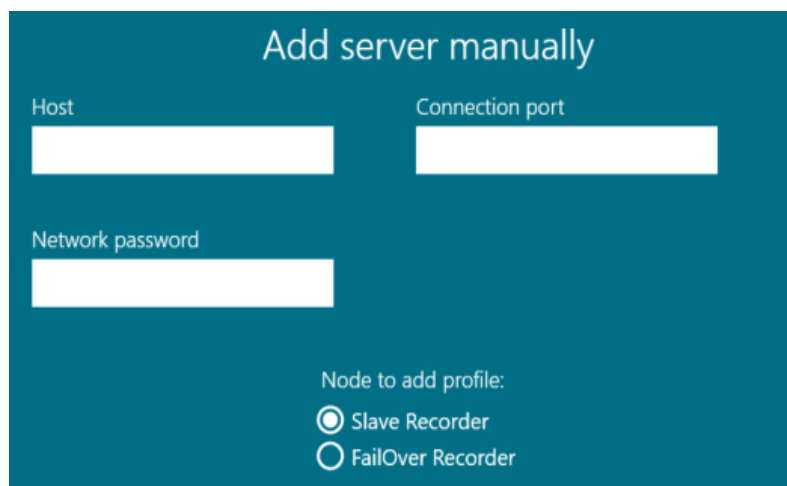
- Mechanism: having primary server and secondary servers allows unified remote monitoring of multiple servers through the primary server.
- Add secondary servers/failover server or delete server, follow below steps:



3.9.2 Add server



- Click **[Add]**





Step 1. Insert server information

- Server: Insert server IP address
- Connection port: insert connection port (main port)
- Password: insert server password

Step 2. Select server type

- Server type: secondary server / failover server
- Secondary server: add other servers to the device list for unified management.
- Failover server: If the primary server loses connection, the failover server will take its place to ensure continuous recording without any loss of video records.

Step 3. Edit server settings

a. Details

The screenshot shows the 'DETAILS' tab of a server configuration interface. At the top, there are three tabs: 'DETAILS', 'AUTHENTICATION', and 'ADVANCED'. Under 'DETAILS', there is a toggle switch for 'Edit server information' which is currently turned on. Below this is a 'Server name' label next to a text input field. At the bottom of the section are two buttons: 'Add' and 'Cancel'.

- Edit server information: enable to edit server name.

Note: You can modify parameters related to inviting network nodes, but using this feature may involve risks.

b. Permissions

The screenshot shows the 'Permissions' section of the server configuration interface. It features three toggle switches: 'Leave authentication authority enabled (if available)', 'Enable authentication authority mirroring (if supported)', and 'Enable authentication authority shadowing (if supported)'. Below the second toggle is a dropdown menu labeled 'Selected authentication authority to monitor for mirroring' with the selected option being 'Authentication authority on Recorder on DESKTOP-119NDSJ (argo-test-pc)'. Each toggle has a descriptive text block explaining its function.

- Allow Authentication Service: When enabled, if the main control machine fails to authorize, the server can authenticate users to access.



c. Advanced

DETAILS AUTHENTICATION ADVANCED

No direct connection to the server

The invited node is behind a network that changes the node address time to time not allowing the other nodes to resolve the invited node address. Checking this option the other nodes on the network will avoid to contact the invited node directly but will wait for the invited node to connect to the network by itself

Use specified address for master

The master server is behind a NAT network and use this following address as its public address.

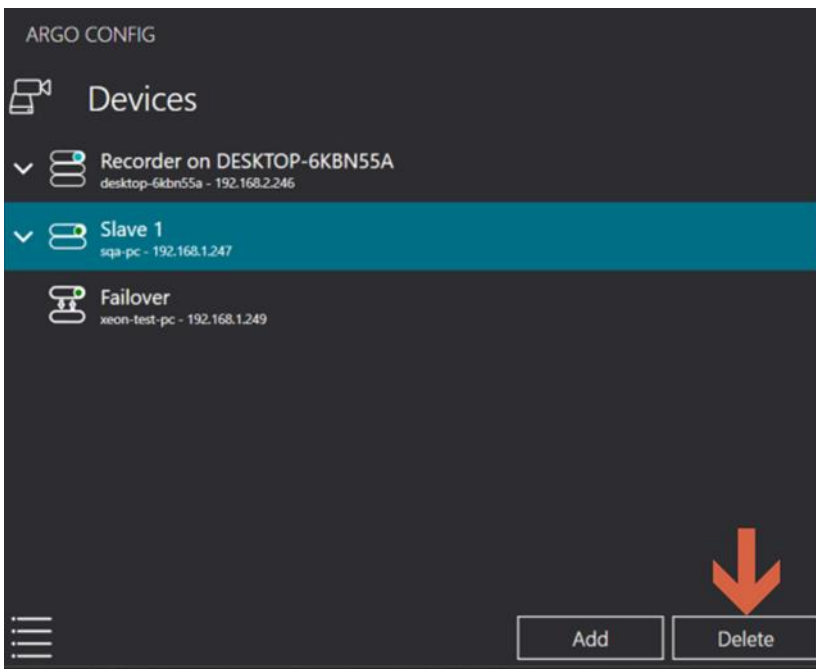
Import directory service config to master

Master will import slave's quad and emap settings after slave is added to network.

- No direct connection with server: enable to prevent other servers from directly contacting this server's network address.
Note: The address of the server may change periodically, so other servers cannot use a fixed address to contact it.
- Use a specific address for the main control machine: enable to input the external WAN IP address to allow devices outside the local network to connect to this server's network address.
- Import directory service config to the master: Enables the replication of electronic maps and viewing layouts from slave servers to the master server's Client.



3.9.3 Delete server



- Click **[Delete]**



3.10 View mode

The image displays two side-by-side screenshots of the ARGO CONFIG interface, illustrating different viewing modes for device management.

Left Screenshot: Hierarchy mode

- Header: ARGO CONFIG, Devices, Hierarchy mode
- Selected device: Recorder on SPARK小K (192.168.2.240)
- Tree structure:
 - Video devices
 - Camera 1 (192.168.2.232)
 - Camera 2 (192.168.2.17)
 - Camera 3 (192.168.2.120)
 - Camera 4 (192.168.2.235)
 - Camera 5 (192.168.1.247)
 - I/O Modules
 - I/O Module 1 (192.168.2.9)
 - I/O Module 2 (192.168.2.19)
 - Spark AI Service
 - Spark AI Device - Human Detection (20062C4C)
 - Camera 3 (192.168.2.120)
 - Camera 5 (192.168.1.247)

Right Screenshot: List mode

- Header: ARGO CONFIG, Devices, List mode
- Filters: Device type (All), Filter
- Table:

ADDRESS	DEVICE TYPE	MODEL NAME	DEVICE NAME
192.168.2.232	Omnieye Advanced Series	BM2	Camera 1
192.168.2.17	Omnieye Advanced Series	BM2	Camera 2
192.168.2.120	Spark Camera	B1 2000 Middle Bullet Camera	Camera 3
192.168.2.235	ONVIF Camera	SR-C-A2-DF1-F3-IR	Camera 4
192.168.1.247	ONVIF Camera	IPCamera	Camera 5
192.168.2.9	ICPDAS I/O Module	tET-PD2POR2	I/O Module 1
192.168.2.19	Pongee I/O Module	UHF101	I/O Module 2
192.168.2.240	Recorder	Recorder on SPARK小K	Recorder on S
	Spark AI Device	SR-VMS-USBKEY	Spark AI Key(z

- Different viewing modes available for the devices: hierarchy mode / list mode



4. USER MANAGEMENT

4.1 Password settings

1. Configure users password

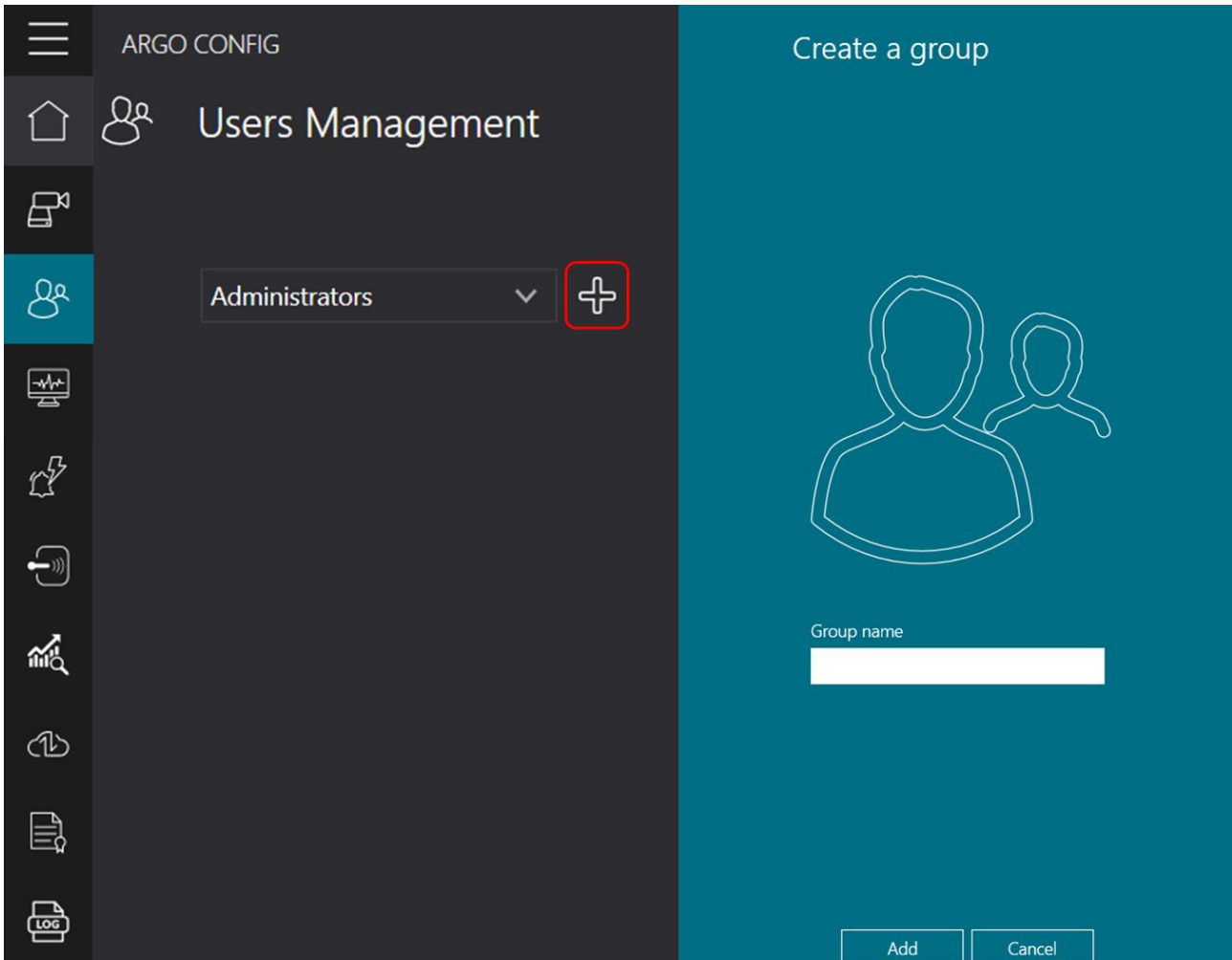
- Password duration rule
Maximum number of days of validity: when the password usage reaches the maximum validity period, it expires and requires resetting. The range of days is from 5 to 100 days.
Reminder message for password expiry: receive a reminder N days before the password expires. The range of days for reminders is from 1 to 100 days.
- Password length rule: set the minimum password length. The range of length can be from 5 to 100 characters.
- Password complexity rule: set advanced password rules to increase password complexity.
- Complexity: lowercase characters / uppercase characters / numerals / special characters.



4.2 Groups

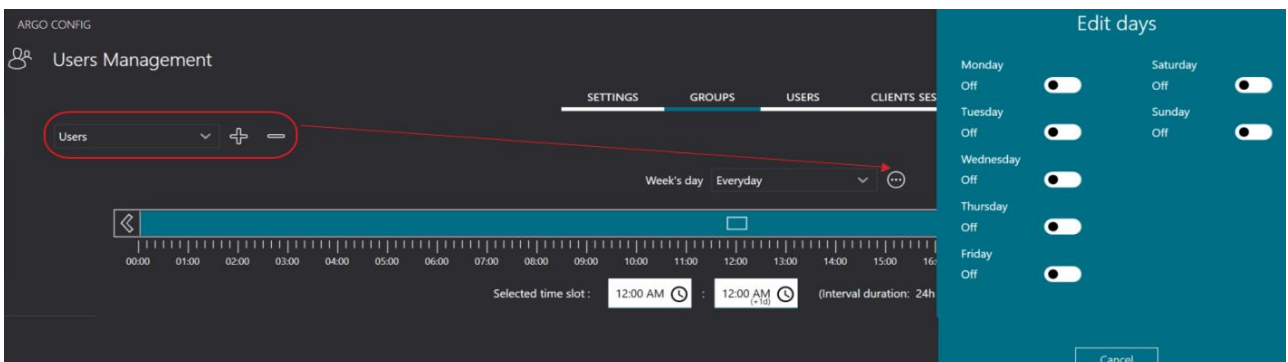
4.2.1 Create groups

- Create groups to classify user access schedules and permissions.



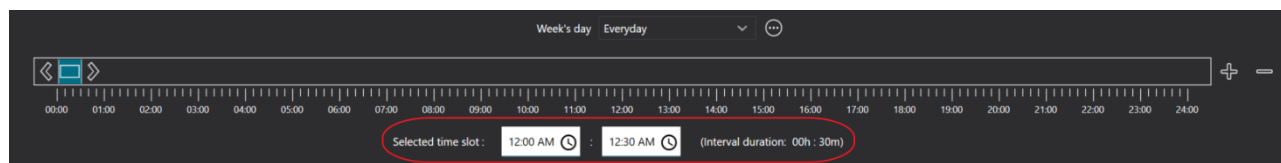
- Click [+]
- Group name: insert name for user group

4.2.2 Set schedules for each group





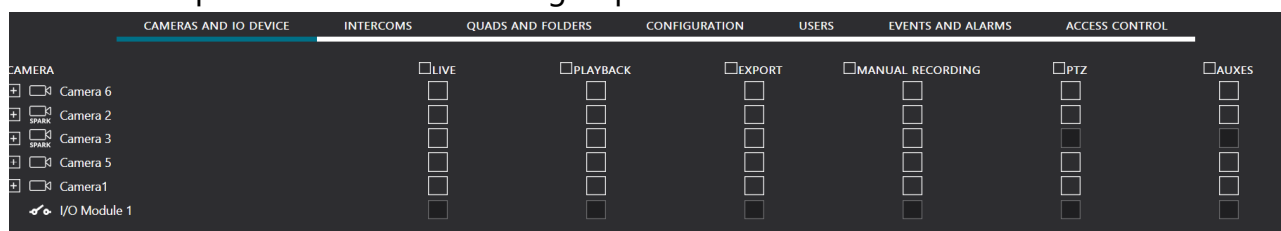
- Edit schedule: default is set everyday. Click [...] to select specific day of the week



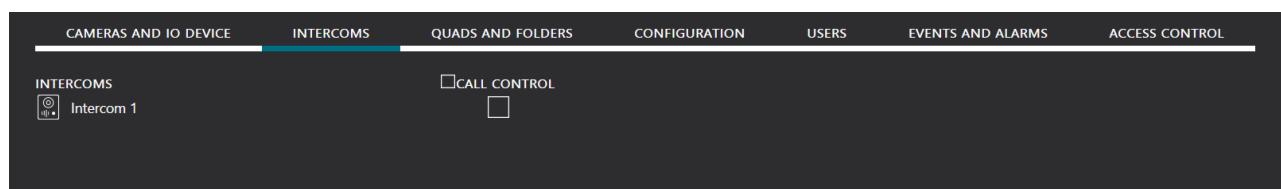
- Add time slot: Click [+] and adjust time slot by dragging left/right or inputting desired time
 - Delete time slot: select the time slot you want to delete and click [-]
 - Edit time slot: adjust the time slot by dragging left/right or inputting desired time
- Note: minimum time interval is 1 hour, maximum is 24 hours.

4.2.3 Set permissions for each group:

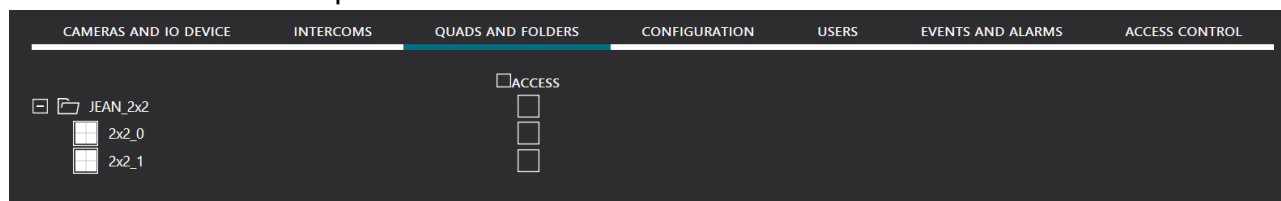
- Allocate permissions for different groups



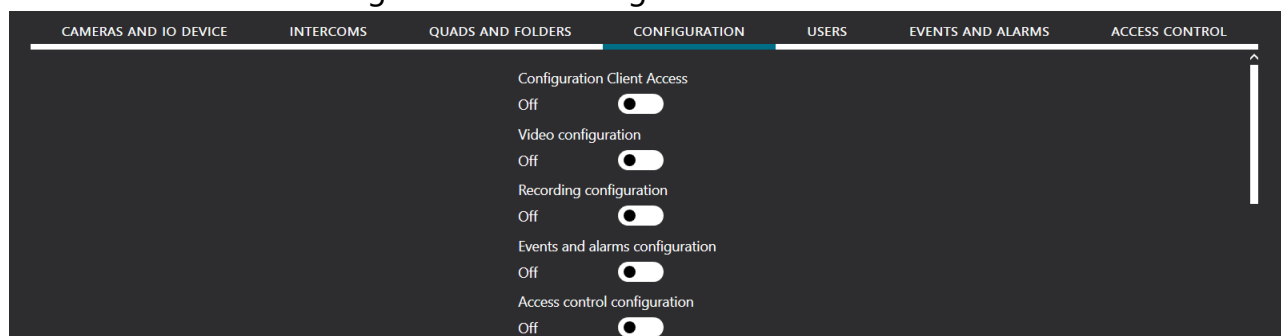
- Cameras: select the camera, I/O modules or devices that the group can manage. Function includes: live, playback, export, manual recording, PTZ, Auxes(I/O output).



Intercoms: Select this option to allow to use intercom call controls.



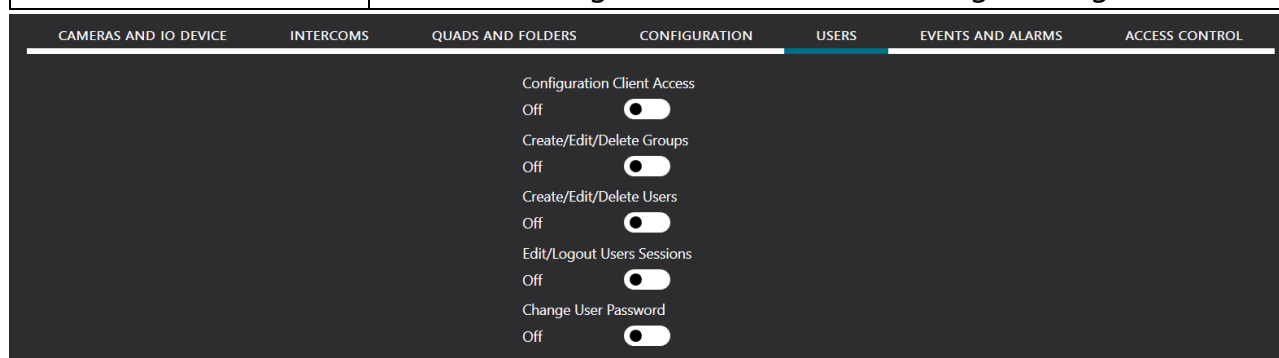
- Quad grants: select the screens that the group can view. Once enabled, the group can view these monitoring screens in the Argo Client.





- Configuration grants: enable/disable configurations that the group can manage.

Option	Description
Configuration Client Access	When disabled, users of the selected group will not be able to access Argo Config.
Video configuration	When disabled, users of the selected group will not be able to access video configuration on Argo Config.
Recording configuration	When disabled, users of the selected group will not be able to access recording configuration on Argo Config.
Events and alarms configuration	When disabled, users of the selected group will not be able to access events and alarms configuration on Argo Config.
Access control configuration	When disabled, users of the selected group will not be able to access access control configuration on Argo Config.
Video analytics configuration	When disabled, users of the selected group will not be able to access video analytics configuration on Argo Config.
Logs visualization	When disabled, users of the selected group will not be able to access log on Argo Config.
Backup and restore operations	When disabled, users of the selected group will not be able to perform backup or restore on Argo Config.
Licenses configuration	When disabled, users of the selected group will not be able to access the license page on Argo Config.
Maps Configuration & Access	When disabled, users of the selected group will not be able to access or configure maps on Argo Config.
Quads Configurations	When disabled, users of the selected group will not be able to access or configure live view format on Argo Config.

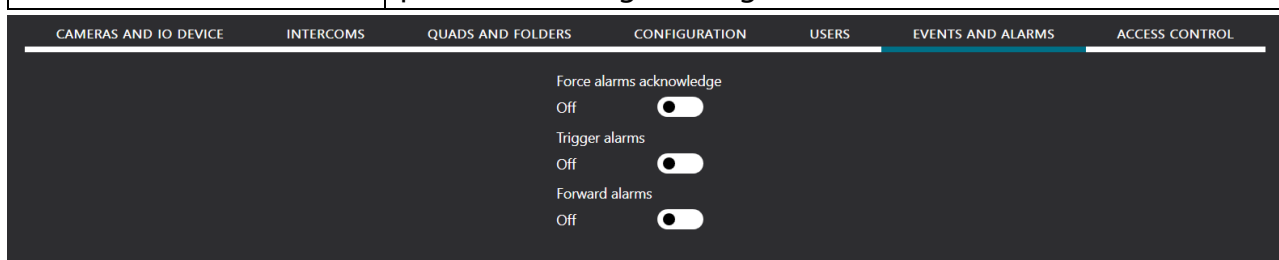


- User grants: set user configuration that the group can manage.

Options	Description
Configuration Client Access	When disabled, users of the selected group will not be able to access Argo Config.

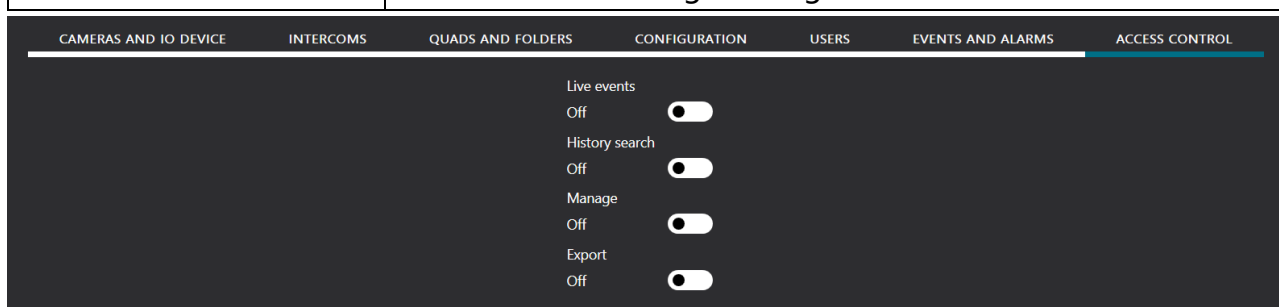


Options	Description
Create/Edit/Delete Groups	When disabled, users of the selected group will not be able to create/edit/delete groups on Argo Config.
Create/Edit/Delete Users	When disabled, users of the selected group will not be able to create/edit/delete users on Argo Config.
Edit/Logout User Sessions	When disabled, users of the selected group will not be able to edit/logout other users' sessions on Argo Config.
Change User Password	When disabled, users of the selected group will not be able to password on Argo Config.



- Event and alarm grants: set event and alarm configuration that the group can manage.

Options	Description
Force alarms acknowledge	When disabled, users of the selected group will not be able to force alarm acknowledgment on Argo Config.
Trigger alarms	When disabled, users of the selected group will not be able to manually trigger alarm on Argo Config.
Forward alarms	When disabled, users of the selected group will not be able to forward alarm on Argo Config.



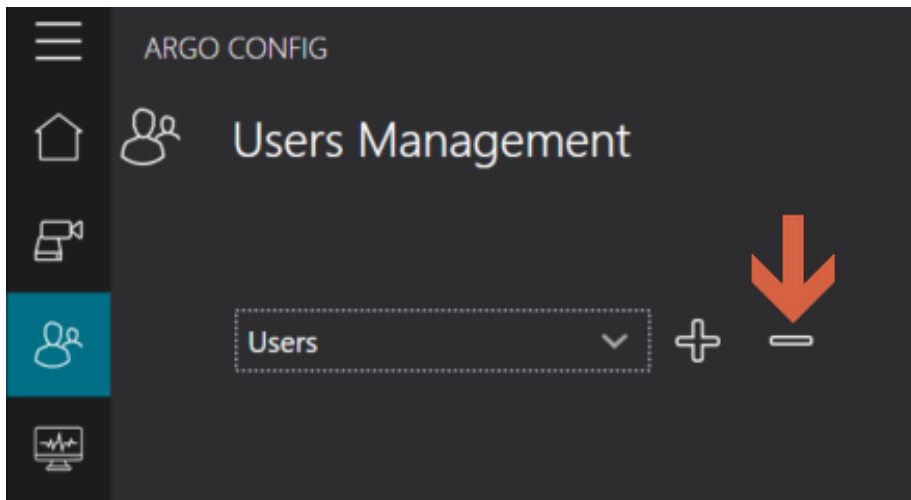
- Access control: set access control configuration that the group can manage.

Options	Description
Live events	When disabled, users of the selected group will not be able to live view access control events on Argo Client.
History search	When disabled, users of the selected group will not be able to search for the record of the accessed ID on Argo Client.



Options	Description
Manage	When disabled, users of the selected group will not be able to manage ID with access permission on Argo Config.
Export	When disabled, users of the selected group will not be able to export the list of ID with access permission on Argo Config.

4.2.4 Delete group

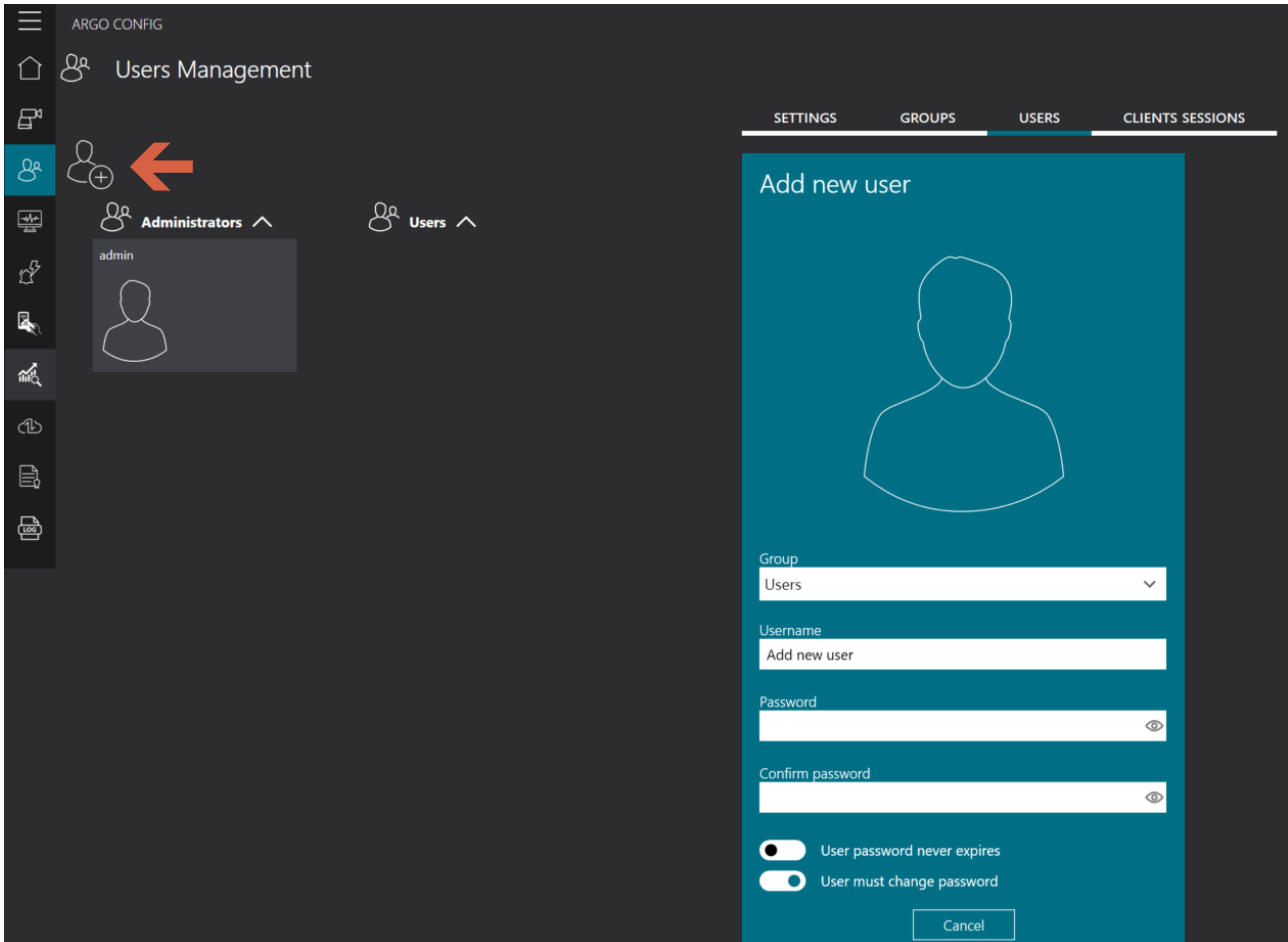


- Select group and click [-]



4.3 User

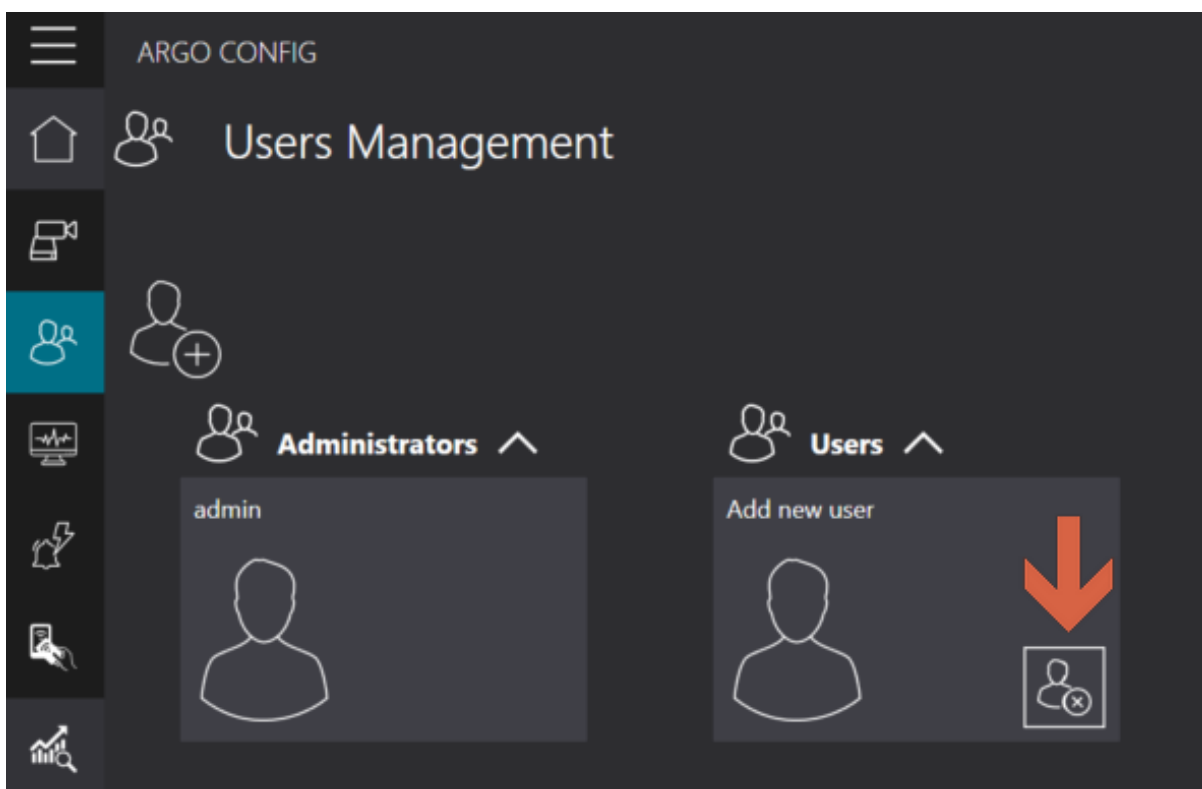
4.3.1 Add user



- Click [+]
- Group: select the group to which the user belongs. Default options include User Group/Administrator Group.
- Username: set user's account name, with a minimum length of 5 characters.
- Password: set the user's login password.
- Confirm password: re-enter the password for confirmation.
- User password never expires: when enabled, the user's password is not subject to password expiration rules.
- User must change password: when enabled, the user must change the password upon login.



4.3.2 Delete User



- Click on the user you want to delete, then click on the [X] button at the bottom right corner.

4.4 Client connection information

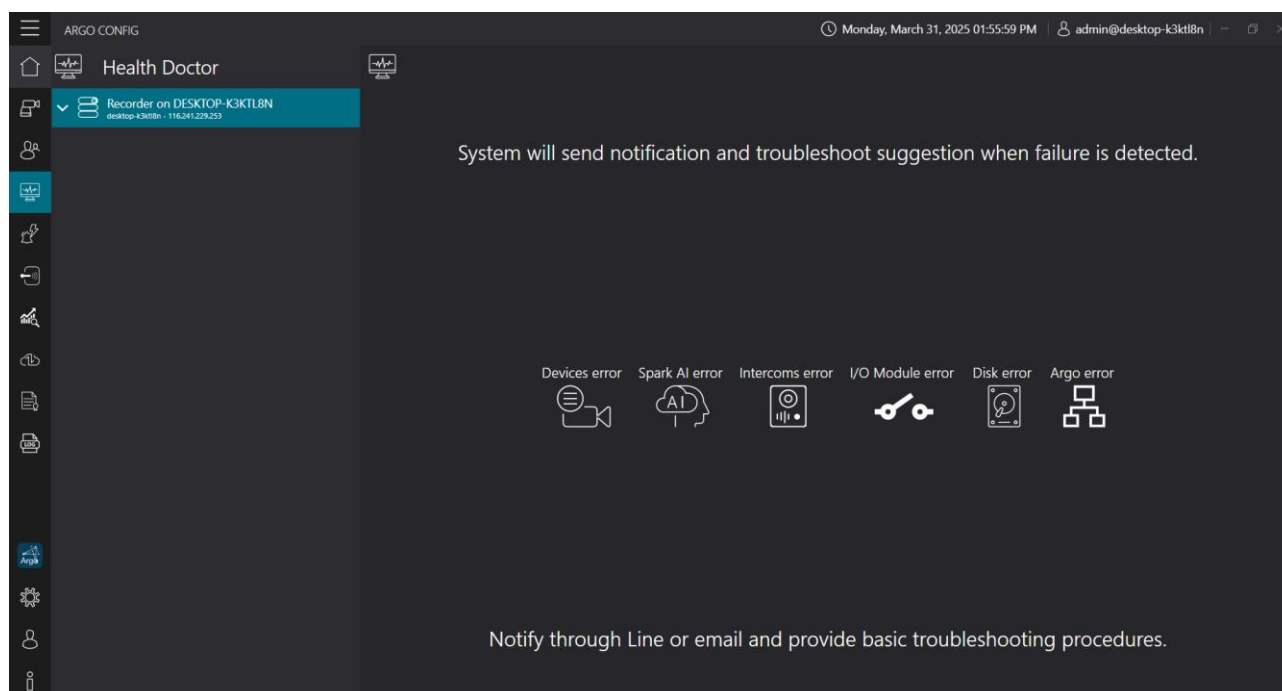
- View and disconnect users connected to Argo Client

USERNAME	GROUP	CLIENT MACHINE	IP ADDRESS	TYPE	CONNECTION TIMESTAMP
admin	Administrators	Unknown	sparkpk	Argo Client	7:28:11 PM Tuesday, June 11, 2024

- Username: users currently logged into Argo client
 - Group: group to which the user currently logged into the Argo Client system belongs.
 - Client server: hostname connected to Argo Config for using the Argo Client system.
 - IP address: IP address of the server
 - Type: login type
 - Connecting time: the time when the user logged into the Argo Client system.
- Note: If no user is logged into the Argo Client system, the Client Connection Information will not be displayed.

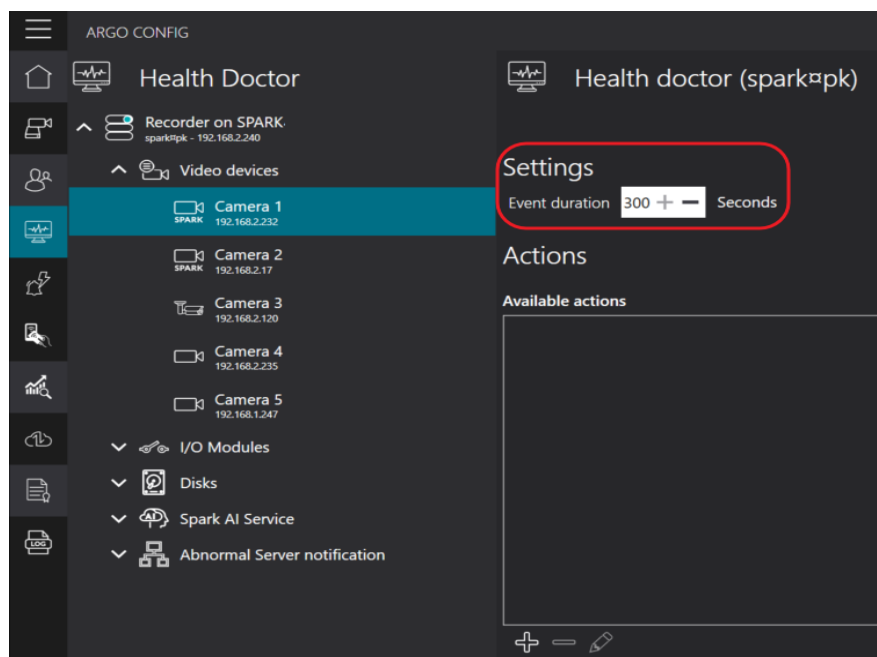


5. HEALTH DOCTOR



- System health check will automatically execute user-defined actions when the device encounters abnormalities or disconnections.
- Device type: video device / Spark AI device / I/O module / HDD / Server abnormal

5.1 System health check configuration



- Event duration: The system will continuously send abnormal notifications at intervals based on the configured number of seconds while the event persists, ranging from 1 to 300 seconds.



Note1: Server abnormal notification needs server confirmation, hence it will not follow the event duration setting.

Note2: Notification Sequence: The first notification will be received 5 minutes after the server is offline, and a notification will be sent every hour.

5.2 Add response action

The screenshot shows the 'Add action' dialog box. On the left, the 'Settings' panel shows 'Event duration' set to 5 seconds. Below it, the 'Available actions' list is empty. A red arrow points to a plus sign icon at the bottom of the 'Available actions' list. The main 'Add action' panel on the right has the following fields: 'Action name' (text input), 'Action category' (dropdown menu set to 'Send email'), 'Select email account' (dropdown menu), 'To' (text input with 'Cc' and 'Bcc' buttons), and 'Subject' (text input). At the bottom of the 'Add action' panel are 'Add' and 'Cancel' buttons.

- Click [+]
- Response action name: insert response action name
- Response action duration: set the duration for which the response action should last, ranging from 0 to 300 seconds.
Note: this function is only supported when the I/O module output is enabled under the condition that there is an alarm for this event.
- Response action delay time: After the trigger condition is met, the response action occurs after a delay of N seconds, ranging from 0 to 300 seconds.
Note: this setting is only supported for setting the output time of the I/O module.
- Response action type



5.2.1 Send email

The image shows two side-by-side screenshots from a software interface. The left screenshot, titled 'Add action', contains the following fields: 'Action name' (text input), 'Action category' (dropdown menu set to 'Send email'), 'Select email account' (dropdown menu with a blue '...' button), 'To' (text input with 'Cc' and 'Bcc' buttons), and 'Subject' (text input). At the bottom are 'Add' and 'Cancel' buttons. An orange arrow points to the 'Select email account' dropdown. The right screenshot, titled 'Email accounts', shows a list of 'Configured email accounts' (currently empty) with a '+' and '-' icon below it. Below the list is a form to add a new account with fields: 'Name' (text input with 'Gmail' entered), 'SMTP server name' (text input with 'smtp.gmail.com:587' entered), 'Username' (text input with 'test' entered), 'Password' (password input with dots and an eye icon), 'Email displayed name' (text input with 'Spark_Alarm_gmail' entered), and 'Email address' (text input with 'sparksqa888@gmail.com' entered). At the bottom are 'OK' and 'Cancel' buttons.

- Select email account: click [...] to add/delete sender email accounts
- To: insert recipient email address
- Subject: insert email subject
- Email content: The content of the email for device disconnection or abnormality is predefined.

a. Add email account

- Click on [+] at the bottom left of the default account field
- Name: name of the default email account
- SMTP server name: Enter the SMTP protocol of the email service system (refer to the list below)
- Account: insert the email account
- Password: insert the email password

Note: email password is the application password after two-step verification, not the original email password. For G-mail, please refer to obtaining the Gmail email application password.

- Email address: insert sender' s email address

b. Delete email account

- Select the email address you want to delete and click [-]



c. SMTP server name: SMTP server corresponding to each email service

Email service	SMTP server name	Email service	SMTP server name
Gmail	smtp.gmail.com	Zoho mail	smtp.zoho.com
Outlook	smtp.office365.com	Naver mail	smtp.naver.com
iCloud Mail Server	smtp.mail.me.com	Yandex mail	smtp.yandex.com
Yahoo mail	smtp.mail.yahoo.com	Proton mail	127.0.0.1
Hotmail/Live.com	smtp-mail.outlook.com	AOL mail	smtp.aol.com

Note: If the email service you are using is not listed in the SMTP server list above, please search with the keywords "email service platform name" and "smtp server name".



5.2.2 Line Notify

Add action

Action name

Action category
Line notify ▼

Photo Send Interval(second)
150 + -

Token

- Interval (seconds): set the interval time for sending images.
- Token: paste your Line Notify token.
- Line notification content: the content of the email for device disconnection or abnormalities is default.

Default content: device is experiencing issues and temporarily unavailable. Please perform simple troubleshooting. We will notify you again once the system is back up and running.



5.3 Edit response action

Actions

Available actions

mail

Edit action

Action name
mail

Action category
Send email

Select email account
Gmail

To
spark@spark-security.com.yw

Subject
spark_notify

Body

Duplicate OK Cancel

- Select the response action and then click

5.4 Delete response action

Actions

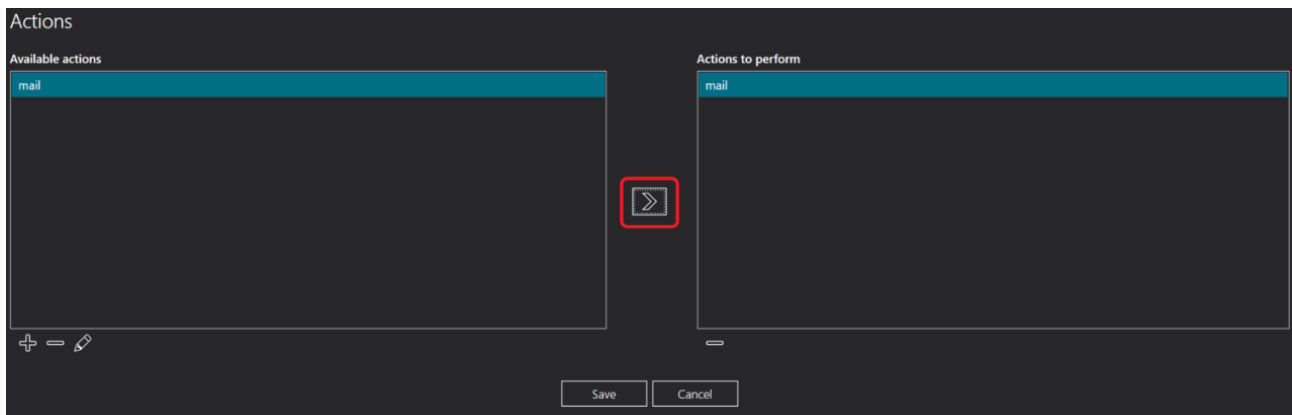
Available actions

mail

- Select the response action and then click [-]



5.5 Execute response action



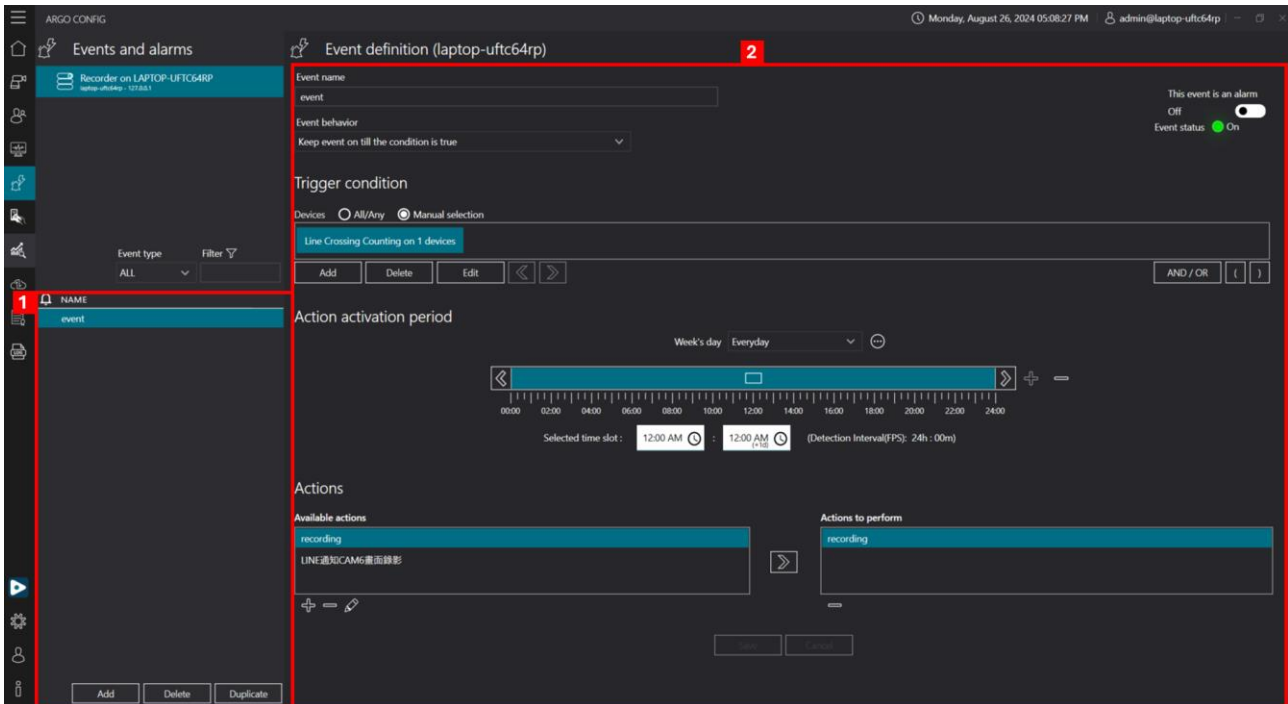
- Apply the executed response behavior: select the response behavior you want to apply, and click [>]
- Delete the executed response behavior: select the executed response behavior you want to delete and click [-]



6. EVENT AND MANAGEMENT

User Management and Event & Alarm Configuration

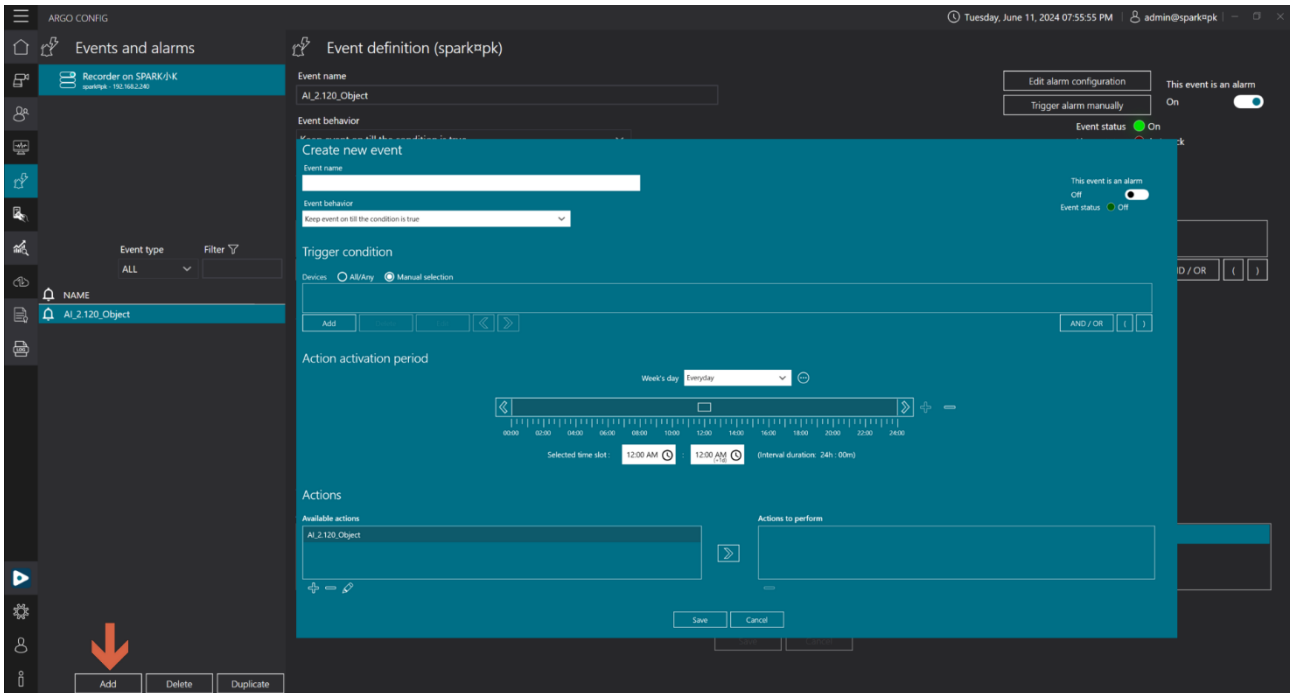
1. **Event Overview:** A summary of event settings. A 🛎 icon indicates whether the event is set as an alarm.
2. **Event Definition:** Configurations related to event name, alarm settings, trigger conditions, and actions.





6.1 Add/Edit/Copy/Delete Event

A. Add event



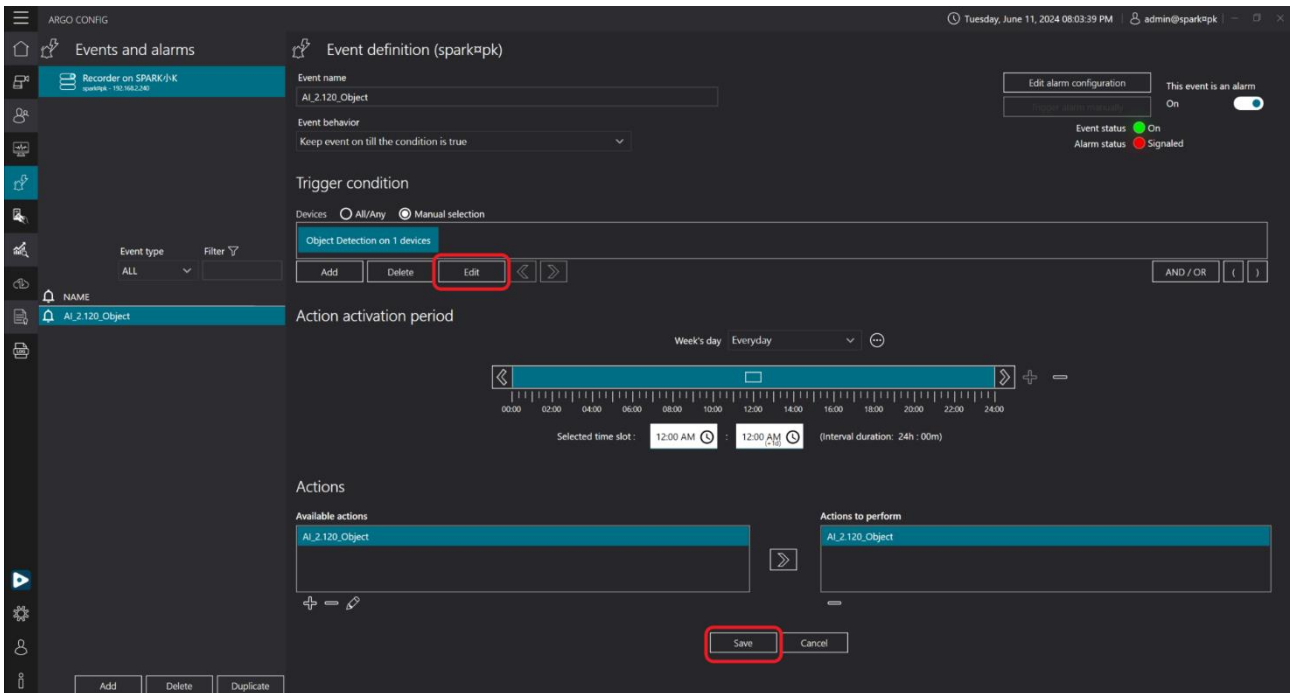
- Click **[Add]**

Type	Description
Event behavior	Defines the activation behavior of the event
This event is an alarm	When enabled, the event is classified as an alarm
Trigger condition	Defines the conditions that trigger the event
Action activation period	Defines the schedule for triggering response actions
Actions	Defines the actions taken in response to the event.

- Event name: insert name of the event
- Event behavior: select event behavior
 - Keep event on till the condition is true
 - Keep event active for X seconds from the condition trigger
 - Keep event on for X seconds after the trigger condition ends
 - Keep event active for X seconds and raise event again if condition still trigger

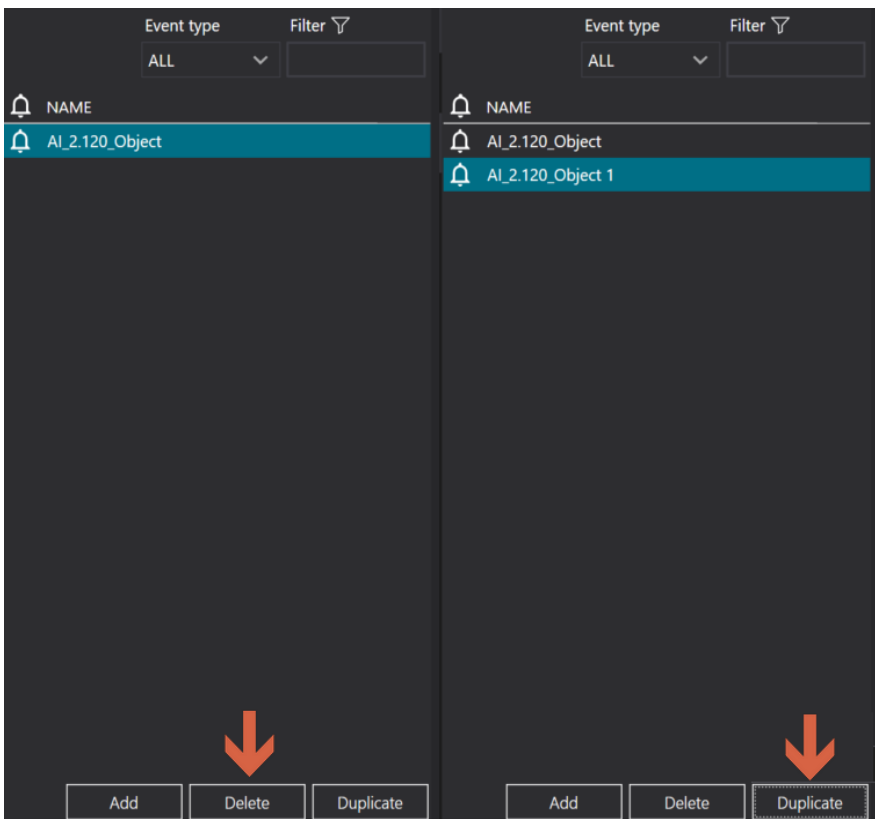


B. Edit event



- Select the event you want to edit, proceed with the editing and click **[Save]**

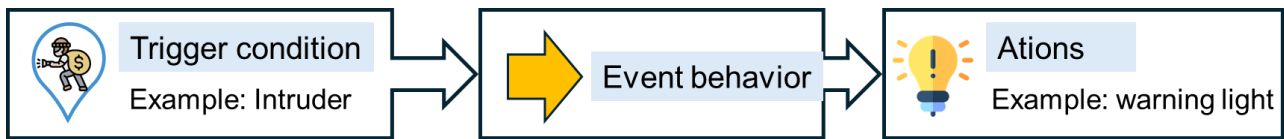
C. Copy/Delete Event


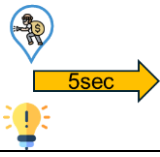

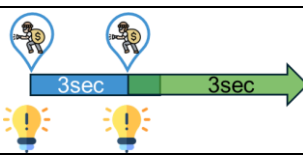


- Select the event you want to copy and click **[Copy]**
- Select the event you want to delete and click **[Delete]**



6.2 Event behavior

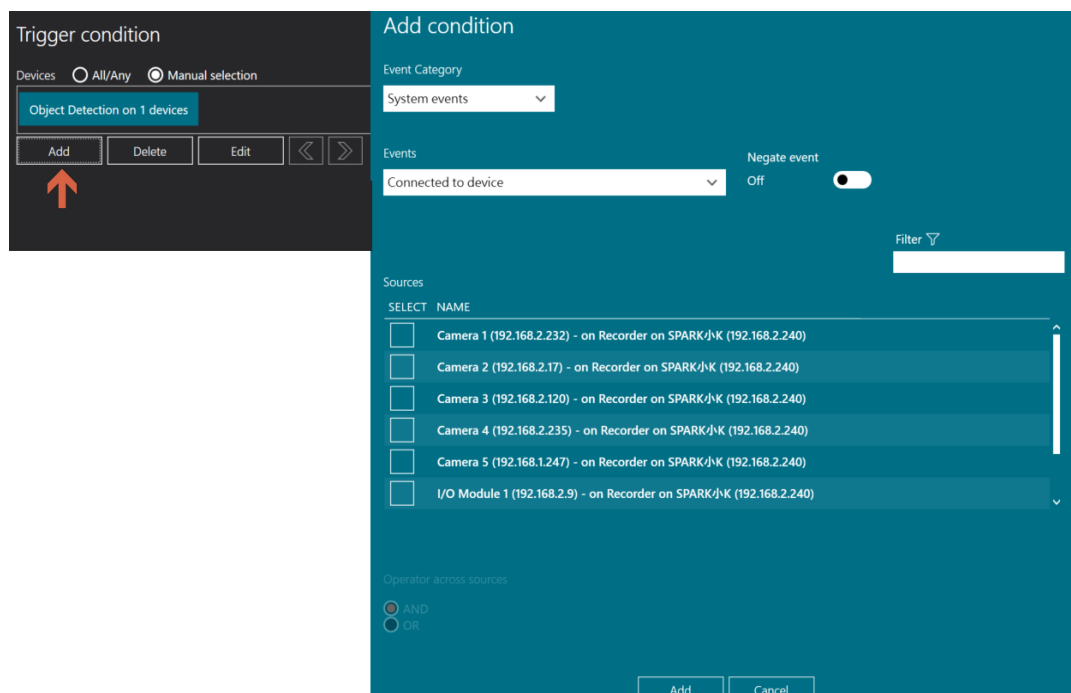


Type	Event Behavior Description	Case Description
Keep event on till the condition is true	 <p>Each trigger is recorded as a single event.</p>	Intruder enters the area, the warning light activates immediately.
Keep event active for X seconds from the condition trigger	 <p>After the trigger ends, the event continues for 5 seconds before concluding.</p>	Intruder enters the area, the warning light activates immediately and maintains the event for 5 seconds.
Keep event on for X seconds after the trigger condition ends	 <p>If no additional triggers occur within the 5-second continuation period, the event concludes.</p>	Intruder enters the area and remains, the warning light activates immediately until the intruder leaves the area. After the trigger ends, the event continues for 5 seconds
Keep event active for X seconds and raise event again if condition still trigger	 <p>If the event is triggered again within the 3-second continuation period after the initial trigger ends, the event restarts, and the event behavior resets</p>	Intruder enters the area, the warning light activates immediately. If the intruder re-enters the area within the detection time of 3 seconds, the event is re-triggered and restarted



6.3 Trigger conditions

6.3.1 Add trigger condition



- Click **[Add]**
- Event Categories: system event, event and alarms, I/O, camera video analytics, access control, Spark AI services (refer to below table)
- Event: select event trigger conditions (refer to below table)
- Negative event: event triggered when the trigger condition is not met
- Source: Devices and settings related to triggering event trigger conditions
- Actions between event sources: When selecting two or more sources, you can choose between "All" (AND) or "Any" (OR) to trigger the event.

- System Event

Event	Description
Disk online status	Triggers when disk is working normally.
Memory load critical	Triggers when memory usage reaches 80%.
Memory load	Triggers when memory usage reaches defined %.
CPU usage critical	Triggers when CPU usage reaches 80%.
CPU usage	Triggers when CPU usage reaches defined %.



Event	Description
Connected to device	Triggers when device is connected. Enable Negate event to receive alarm when device is disconnected.
Device licensed	Triggers when device license is activated.
Backup	Triggers when server is making backup.

- **Event and alarm**

Event	Description
Alarm has been assigned	Triggers when select source is assigned.
Alarm has been assigned by	Triggers when select source is assigned by defined user/group.
Alarm has been managed	Triggers when selected source is managed.
Alarm has been managed by	Triggers when selected source is managed by defined user/group.

- **I/O**

Event	Description
I/O output status	Triggers when I/O output status is active.
I/O input status	Triggers when I/O input status is active.
Audio output streaming status	Triggers when the audio output status is turned on.

- **Access Control**

Event	Description
Category signaled for Plate Detection	Triggers an event when a license plate is detected.
ID detected in the designated list	Triggers when an ID present in category is detected.
Allowed ID detected in the designated list	Triggers when an ID present in category and allow list is detected.
Denied Allowed ID detected in the designated list	Triggers when an ID present in category and deny list is detected.
Expired Allowed ID detected in the designated list	Triggers when an ID present in category and expired list is detected.



- Spark AI Services

Event	Description
License status	Triggers when Spark AI service license status is abnormal
Line crossing counting	Triggers an event when an object crosses a line and reaches the set threshold (1-128 seconds).
Line crossing detection	Triggers an event when an object crosses a line.
Loitering detection	Triggers when loitering is detected for the set duration (1-128 seconds)
Object detection	Triggers when object (inc. people) is detected
People density	Triggers when target density reaches the set value (1-128).
Smoke and Fire detection	Triggers when smoke is detected
HTTP POST detection	Triggered when the device receives an HTTP POST event

- Camera video analytics

Event	Description
Tampering	Triggers when tampering is detected
Motion	Triggers when motion is detected
Audio	Triggers when audio is detected
Tripwire	Triggers when line crossing behavior is detected.
People density	Triggers when crowd gathering is detected.
Perimeter	Triggers when an intruder is detected.
Temperature	An event is triggered when the camera detects a specified temperature.(Currently supported only by TBT cameras.)

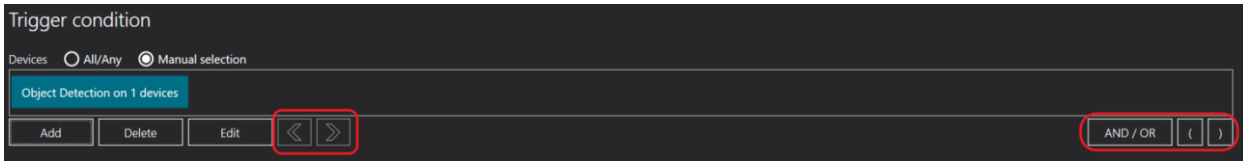
Note: If the system does not have the device, the event will not have that event option.

- Intercom service

Event	Description
Intercom Status	<ul style="list-style-type: none">- Outdoing: Triggers an event when the Client initiates a call to the intercom.- Incoming: Triggers an event when the intercom initiates a call to the Client.- Talking: Triggers an event when a call is in progress.- Idle: Triggers an event when the intercom is idle.



6.3.2 Advanced Setting for Trigger Conditions

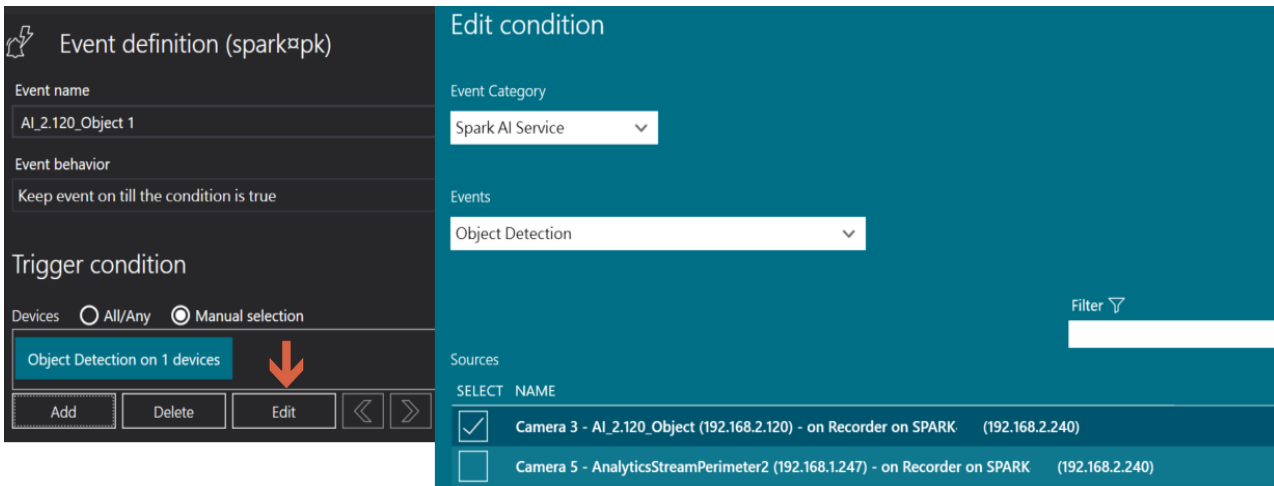


- Click [**<**] or [**>**] to adjust the order of trigger conditions.
- Click [**AND/OR**] or [**(**] or [**)**] to adjust the setting of whether the trigger conditions are met or not.

Examples:

1. A and B: The event is triggered only if both conditions A and B are met.
2. A or B: The event is triggered if either condition A or condition B is met.
3. (A AND B) OR C: The event is triggered if either both conditions A and B or condition C is met.

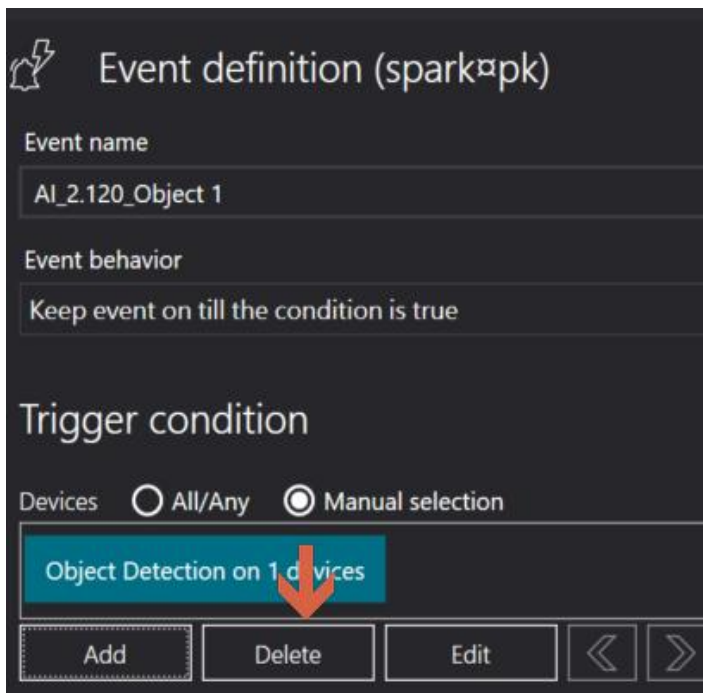
6.3.3 Edit trigger condition



- Select the trigger condition you want to edit and click [**edit**]



6.3.4 Delete trigger condition






- Select the trigger condition you want to delete and click **[delete]**

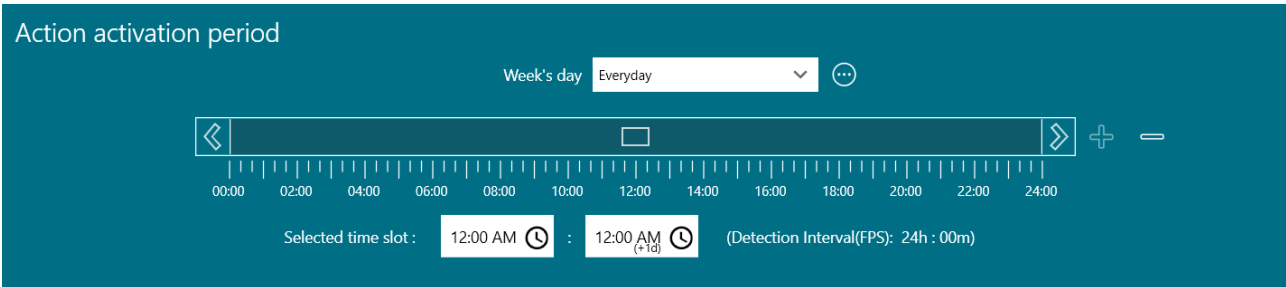


6.4 Response action


6.4.1 Response action schedule

The system can activate different responses based on specific time periods.

- Day Selection: Click  to choose either "Daily" or specific days of the week (Monday to Sunday).
- Time Periods: Use the timeline tool   to add or remove detection intervals.



Action activation period

Week's day Everyday 

00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00

Selected time slot: 12:00 AM : 12:00 AM (+1d) (Detection Interval(FPS): 24h : 00m)

- Add time slot: Click [**+**] and adjust time slot by dragging left/right or inputting desired time
- Delete time slot: select the time slot you want to delete and click [**-**]
- Edit time slot: adjust the time slot by dragging left/right or inputting desired time



6.4.2 Add response action

Edit action

Action name
Light

Action category
Aux output

Action duration
10 + -

Actions delay time
2 + -

Select an aux output
門口警報 - I/O output 0 (172.21.7.72) - Recorder on DESKTOP-K3KTL8N (d▼)

Set aux output new status
Off

Here is the translation of the table for response action types

Type	Description
Start Recording	The selected camera begins recording when the event occurs.
I/O Output	Triggers an I/O output when the event occurs.
Go to Preset	Moves a PTZ camera to a predefined position when the event occurs.
Start Tour	Starts a preset patrol route for a PTZ camera when the event occurs.
Send Email	Sends an email notification when the event occurs.
LINE Message	Sends a LINE notification when the event occurs. A single event supports only one LINE group and cannot notify multiple groups.
LED Display	Displays a message on an LED board when the event occurs.
HTTPS Event Post	Sends an HTTPS post to third-party devices when the event occurs.



A. Start recording

The screenshot shows the 'Add action' configuration interface. The 'Action name' field contains 'Test'. The 'Action category' dropdown is set to 'Start recording'. The 'Select a camera' dropdown is set to 'Camera 1 (172.21.5.10) - Recorder on LAPTOP-UFTC64RP (laptop-uftc64rp)'.

- Select camera: select camera for executing event response behavior.

Note:

1. In non-alarm situations : Start recording when the event is triggered, stop recording when the event ends.
2. In alarm situations: Start recording when the event is triggered, stop recording when the alarm is cleared.

B. I/O output

The screenshot shows the 'Add action' configuration interface for 'Aux output'. The 'Action name' field contains 'Test'. The 'Action category' dropdown is set to 'Aux output'. The 'Action duration' and 'Actions delay time' are both set to 0 with increment/decrement buttons. The 'Select an aux output' dropdown is set to 'Camera 1 - I/O output 0 (172.21.5.10) - Recorder on LAPTOP-UFTC64RP (laptop-uftc64rp)'. At the bottom, there is a toggle switch for 'Set aux output new status' which is currently turned 'On'.

- Select AUX output: choose the I/O module device to apply.
- Set new AUX output state: enable/disable the new state of AUX output.



C. Go to preset

Add action

Action name
Test

Action category
Go to preset

Actions delay time
0 + -

Select a PTZ camera
Camera 1 - PTZ controller 0 (172.21.5.10) - Recorder on LAPTOP-UFTC64RP (laptop-uftc64rp)

Select preset

- Select a PTZ camera: choose a camera with PTZ functionality.
- Select preset: choose a preset position already configured in the camera.

D. Start tour

Add action

Action name
Test

Action category
Start tour

Actions delay time
0 + -

Select a PTZ camera
Camera 1 - PTZ controller 0 (172.21.5.10) - Recorder on LAPTOP-UFTC64RP (laptop-uftc64rp)

Select tour to start

- Select a PTZ camera: choose a camera with PTZ functionality.
- Select start tour: select a tour already configured in the camera.



E. Send email

The image shows two overlapping dialog boxes. The left dialog, titled 'Add action', has fields for 'Action name' (Test), 'Action category' (Send email), 'Actions delay time' (0), 'Select email account' (NewEmailAccount), 'To', 'Subject', and 'Body'. The right dialog, titled 'Email accounts', has a 'Configured email accounts' list with 'Gmail' selected, and fields for 'Name', 'SMTP server name', 'Username', 'Password', 'Email displayed name', and 'Email address'. An orange arrow points to the '...' button in the 'Select email account' field of the 'Add action' dialog.

- Select email account: click [...] to add/delete sender email accounts
 - To: insert recipient email address
 - Subject: insert email subject
 - Email content: insert email content
- a. Add email account
- Click on [+] at the bottom left of the default account field
 - Name: name of the default email account
 - SMTP server name: Enter the SMTP protocol of the email service system (refer to the list below)
 - Account: insert the email account
 - Password: insert the email password
 - Email Display Name: Enter the display name of the sender.
 - Email Address: Enter the sender's email address.
- b. Delete email account
- Select the email address you want to delete and click [-]



c. SMTP server name: SMTP server corresponding to each email service

Email service	SMTP server name	Email service	SMTP server name
Gmail	smtp.gmail.com	Zoho mail	smtp.zoho.com
Outlook	smtp.office365.com	Naver mail	smtp.naver.com
iCloud Mail Server	smtp.mail.me.com	Yandex mail	smtp.yandex.com
Yahoo mail	smtp.mail.yahoo.com	Proton mail	127.0.0.1
Hotmail/Live.com	smtp-mail.outlook.com	AOL mail	smtp.aol.com
		Mail.com	smtp.mail.com

Note: If the email service you are using is not listed in the SMTP server list above, please search with the keywords "email service platform name" and "smtp server name" Please refer to obtaining password.

F. Line Message

- Interval (seconds): set the interval time for sending images.
- Token: paste your Line Message token.
- Line notification content: insert content of the email for device disconnection or abnormalities is default.



G. LED display

Add action

Action name

Action category

Actions delay time
 + -

IP Address

Content
For ex: {lpr(licenseplate)}{RGB(0,255,0)}{CLEAR(10000)}{EFFECT(0)}

- IP address: insert LED display IP address
- Content (sample): {lpr(licenseplate)}{RGB(0,255,0)}{CLEAR(10000)}{EFFECT(0)}

Please refer to the syntax explanation below

`{lpr(licenseplate)}{RGB(0,255,0)}{CLEAR(10000)}{EFFECT(0)}` Avoid
Tailgating{RGB(255,0,0)}

`{lpr(licenseplate)}` => Replaced with the detected license plate.
`{RGB(Red,Green,Blue)}` => Specifies the corresponding text color.
If not specified, default is RGB(255,0,0) red. Refer to the "color code chart."
`{CLEAR(10000)}` => displays the text for 10000 milliseconds
If not specified, the text will not be cleared.
`{EFFECT(0)}` => Specifies the display effect of the string.



H. HTTPS Event Sending

Add action

Action name

Action category

Actions delay time
 + -

URL

Content
For ex: time={time}&event={EventName}

URL : Uniform Resource Locator, insert the desired "link" or "web address",


E.g.: <https://192.168.X.X:8080/> or <https://www.xxxx.com>

Content: insert {time} to print the time of event triggering.

insert {Event Name} to print the name of the event triggered.



6.4.3 Edit response action

- Select response action and click 

6.4.4 Delete response action

- Select response action and click [-]

6.4.5 Execute response action

- Apply the executed response behavior: select the response behavior you want to apply, and click [>] and save
- Delete the executed response behavior: select the executed response behavior you want to delete and click [-] and save




6.5 Set the event as alarm

The image shows two screenshots of the Argo Client interface. The left screenshot is titled "Create new event" and shows a form with fields for "Event name", "Event behavior" (set to "Keep event on till the condition is true"), "Trigger condition" (with "Manual selection" selected), "Action activation period" (set to "Everyday" with a time slot from 12:00 AM to 12:00 AM), and "Actions" (with "LINE MESSAGE" selected). A red box highlights the "This event is an alarm" toggle switch, which is currently set to "Off". A red arrow points from this toggle to the right screenshot. The right screenshot is titled "Edit alarm configuration" and shows the same "This event is an alarm" toggle switch, now set to "On". A red circle with the number "2" is next to the "Edit alarm configuration" button, and a red circle with the number "1" is next to the "This event is an alarm" toggle switch.




- This event is an alarm: Enable the alarm to record the event.
- Click **[Edit Alarm Settings]**.

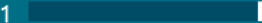


6.5.1 Edit alarm setting

Set the event as an alert to enable event management and lookup through the notification bell  in the Client interface.


Alarm configuration

Alarm category
System   



Alarm priority
Highest Lowest
1  100
100

Related devices




ADDRESS	DEVICE NAME	MODEL NAME	STATUS	NODE
---------	-------------	------------	--------	------





Alarm procedure

Alarm recipients (leave empty to send alarm to all users)






Alarm options

- User note is mandatory
- Auto-acknowledge alarm after   seconds since alarm has been triggered
- Can be triggered manually
- Play a sound on client machine when an alarm occurs
- Use event scheduler

A. Alarm type

Alarm category

System   

- Add labels to alarm for classification. Click [+/-] to add/delete alarm categories. The default categories are Critical and System.



B. Alarm priority



- Drag to adjust alarm priority level

C. Related devices

ADDRESS	DEVICE NAME	MODEL NAME	STATUS	NODE
172.21.7.6	Camera 1 - videoinput 0 - on recorder laptop-uftc64rp	BM2	Ready	laptop-uftc64rp
172.21.7.7	Camera 3 - videoinput 0 - on recorder laptop-uftc64rp	DF1	Ready	laptop-uftc64rp
172.21.7.69	Camera 19 - videoinput 0 - on recorder laptop-uftc64rp	PM1	Unreachable	laptop-uftc64rp

SELECT	ADDRESS	DEVICE NAME	MODEL NAME	STATUS	NODE
<input checked="" type="checkbox"/>	172.21.7.6	Camera 1 - videoinput 0 - on recorder laptop-uftc64rp	BM2	Ready	laptop-uftc64rp
<input type="checkbox"/>	172.21.7.7	Camera 3 - videoinput 0 - on recorder laptop-uftc64rp	DF1	Ready	laptop-uftc64rp
<input type="checkbox"/>	172.21.7.69	Camera 19 - videoinput 0 - on recorder laptop-uftc64rp	PM1	Unreachable	laptop-uftc64rp

- Click and select related devices
- Select the relevant devices.
- Save the settings. Once linked, the associated camera feed will be displayed in the Client when an alert notification is triggered.

D. Alarm handling procedure

Users can provide a **Standard Operating Procedure (SOP)** to guide monitoring personnel in responding to triggered alerts. Click to manage the procedure.



E. Alarm recipients

- Leave blank to send the alarm to all users and groups
- Click **[+]** to add groups/users as alarm recipients
- Click **[-]** to remove groups/users from alarm recipients

F. Alarm options

- User note required: when enabled, Argo client alarm recipients must fill in the user note field to close or forward alarms.
- Auto-close alarm: when enabled, the alarm will automatically close N seconds after being triggered, with a range of 1-300 seconds.

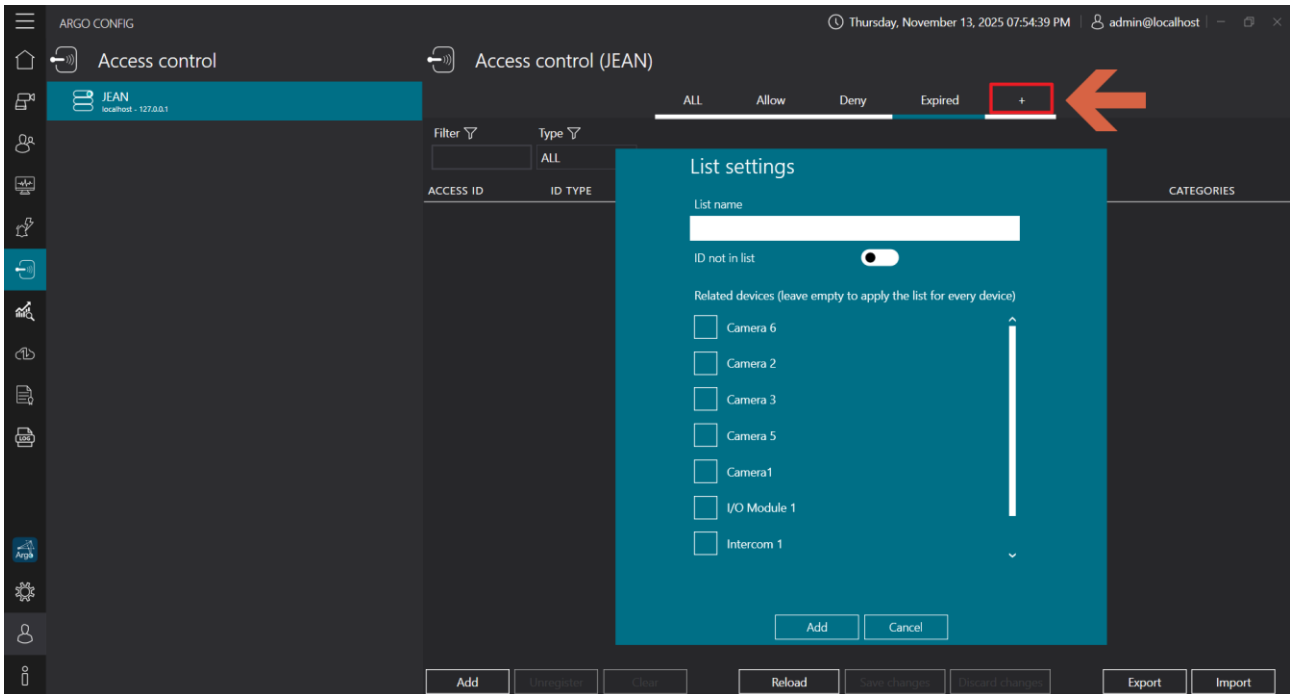
- Manually Triggerable: When enabled, you can click **[Manually Trigger Alarm]** to test the Argo Client's alarm sending functionality.
- Sound Alert on Alarm Trigger: When enabled, a sound will be emitted from the Argo Client host when an alarm is triggered.



7. ACCESS CONTROL

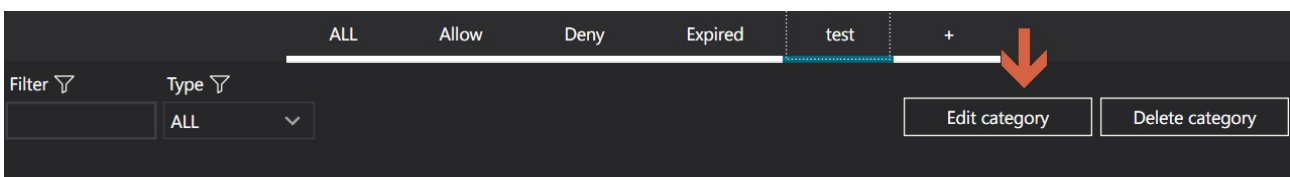
7.1 Add/Edit/Delete list

A. Add list



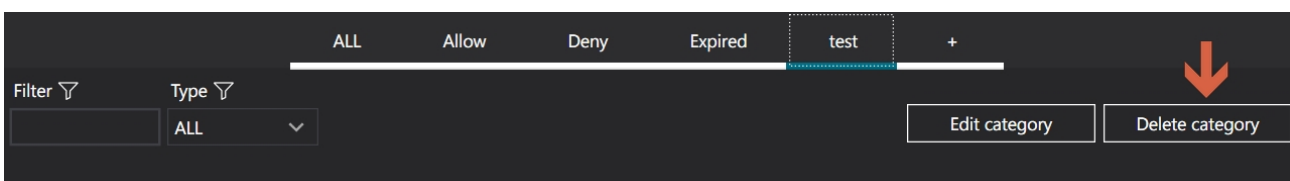
- Click [+] to add a new category to the access service list.
 - List: name the category of the access service list
 - ID not in the list: IDs not in this list are the access standards
 - Related devices: select the devices to be used for this access service list
- Note: leave empty to apply the list for every device

B. Edit list



- Click [**Edit list**] to edit the list

C. Delete list



- Click [**Delete list**] to delete list



7.2 Access ID

7.2.1 Add access ID

The screenshot shows the ARGO CONFIG software interface. The main window is titled 'Access control (master)'. On the left, there is a sidebar with a list of devices: 'Recorder on DESKTOP-9C43ST0', '台灣油維科 Slave 1', and '台灣油維科 Slave 2'. The main area shows a table with columns for 'Filter' and 'Type'. Below the table, there is a red arrow pointing to the 'Add' button. The 'Add' dialog box is open, showing the following fields: 'Access id', 'Id type', 'Begin of overall validity', 'End of overall validity', 'Begin of daily validity', and 'End of daily validity'. The 'Add' button is highlighted in the dialog box.

- Select [**List category**] and click [**Add**]
- Access ID: insert access ID, the system will use this ID as the basis for identifying vehicle entry and exit.
Note: insert an alphanumeric combination without "-" such as: ABC1234.
- Access type: select ID category
LPR: for license plate recognition, insert the license plate number in this field.
RFID: high-frequency RFID (e-tag), insert the RFID number here.
- Effective Date (Start): ID effective start date.
- Effective Date (End): ID effective end date.
- Daily Valid Time (Start): ID daily valid entry and exit start time.
- Daily Valid Time (End): ID daily valid entry and exit end time.
- Note: You can enter ID notes as needed (optional).



7.2.2 Edit access ID

The screenshot shows the 'Access control (master)' interface. On the left, there is a sidebar with navigation icons. The main area displays a list of access IDs. The selected ID 'FHC8637' is highlighted in blue. The edit form for this ID is shown on the left side of the main area. The form includes the following fields:

- Access id: FHC8637
- Id type: LPR
- Begin of overall validity: 6/11/2024 12:00:00 AM
- End of overall validity: 6/12/2024 10:00:00 AM
- Begin of daily validity: 12:00 AM
- End of daily validity: 12:00 AM (+1d)
- Notes: (empty)

At the bottom of the form, there are buttons for 'Add', 'Unregister', 'Clear', 'Reload', 'Save changes', 'Discard changes', 'Export', and 'Import'. A red arrow points to the 'Save changes' button.

- Select the access ID you want to edit, proceed to edit and then and click **[Save]**
- Access ID: cannot be modified.
- Access type: cannot be modified.
- Effective Date (Start): ID effective start date.
- Effective Date (End): ID effective end date.
- Daily Valid Time (Start): ID daily valid entry and exit start time.
- Daily Valid Time (End): ID daily valid entry and exit end time.
- Note: You can enter ID notes as needed (optional).



7.2.3 Deactivate/Clear access ID

A. Deactivate

The screenshot shows the 'Access control (master)' configuration page. The left sidebar is set to 'Access id' for 'ARQ-2991'. The main area displays a table of access IDs. An orange arrow points to the 'Clear' button at the bottom of the interface.

Access ID	Type	Valid From	Valid To	Valid Time	Status
ARQ-2991	LPR	Tuesday, June 11, 2024	Thursday, July 11, 2024	00:00:00 - 24:00:00	Deny
FHC8637	LPR	Tuesday, June 11, 2024	Wednesday, June 12, 2024	00:00:00 - 24:00:00	Allow

- Select access ID you want to deactivate and click [**deactivate**]

B. Clear

The screenshot shows the 'Access control (master)' configuration page. The left sidebar is set to 'Access id' for 'FHC8637'. The main area displays a table of access IDs. An orange arrow points to the 'Clear' button at the bottom of the interface.

Access ID	Type	Valid From	Valid To	Valid Time	Status
ARQ-2991	LPR	Tuesday, June 11, 2024	Thursday, July 11, 2024	00:00:00 - 24:00:00	Deny
FHC8637	LPR	Tuesday, June 11, 2024	Wednesday, June 12, 2024	00:00:00 - 24:00:00	Allow

- Click [**Clear**] to delete all access ID



7.2.4 Export/Import access ID

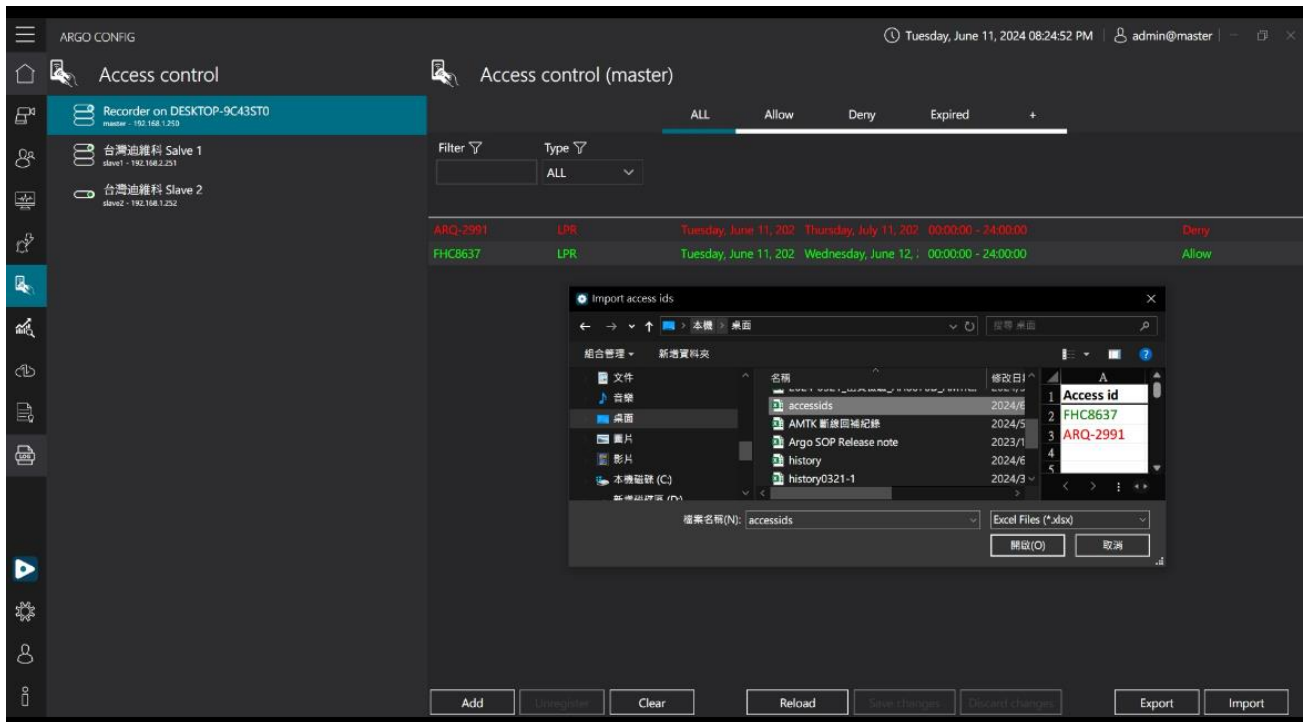
A. Export

A	B	C	D	E	F	G	H
通行ID	通行類別	有效日期(起)	有效日期(迄)	每日有效時間(起)	每日有效時間(迄)	備註	清單
ABC1234	LPR	2024/01/25 00:00:00	2024/02/25 00:00:00	00:00:00	24:00:00		Allowed
ABC1235	LPR	2024/01/25 00:00:00	2024/02/25 00:00:00	00:00:00	24:00:00		Allowed
ABC1236	LPR	2024/01/25 00:00:00	2024/02/25 00:00:00	00:00:00	24:00:00		Allowed
ABC1237	RFID	2024/01/25 00:00:00	2024/02/25 00:00:00	00:00:00	24:00:00		Denied
ABC1238	LPR	2024/01/25 00:00:00	2024/02/25 00:00:00	00:00:00	24:00:00		Denied
ABC1239	LPR	2024/01/25 00:00:00	2024/02/25 00:00:00	00:00:00	24:00:00		Denied
ABC1240	LPR	2023/12/04 00:00:00	2023/12/05 00:00:00	00:00:00	24:00:00		Expired
ABC1241	LPR	2024/01/25 00:00:00	2024/02/25 00:00:00	00:00:00	24:00:00		test, Allowed
10							

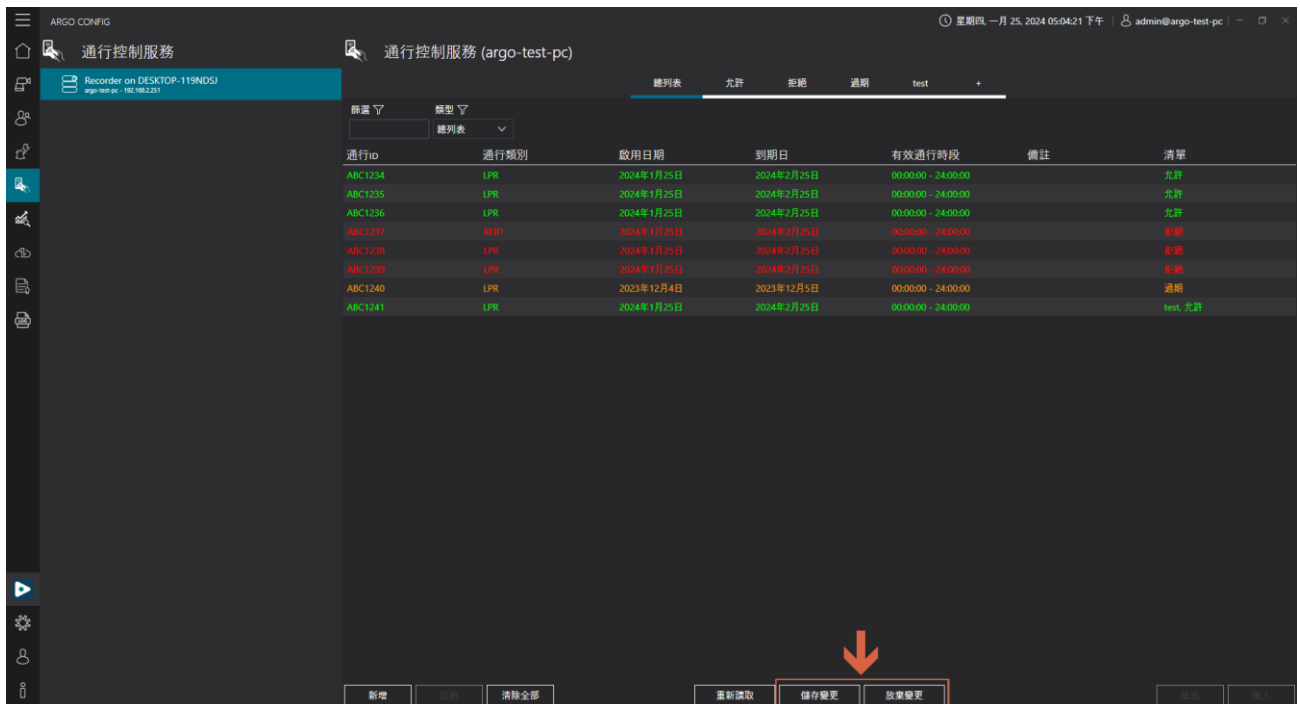
- Click **[Export]** to export the list of access IDs.
- File type: xlsx, csv.
- Note: Before updating or reinstalling the application, make sure to export and backup access ID data to prevent loss.



B. Import



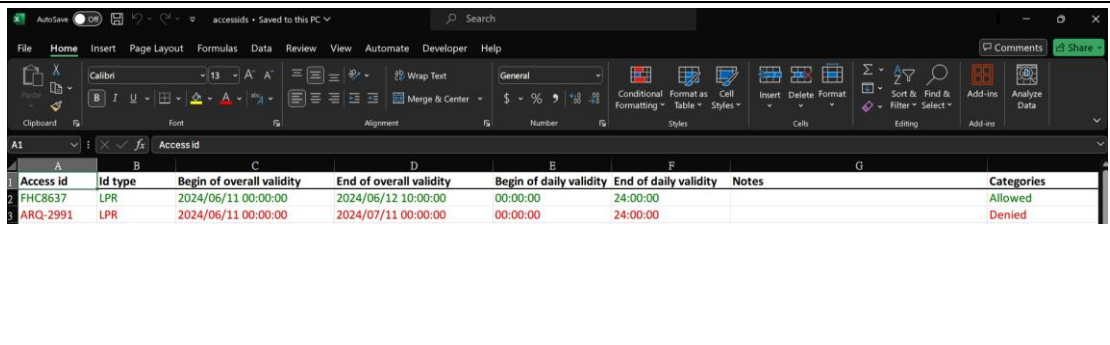
- Click **[Import]** to Import access ID file.



- After importing, click **[Save]** to finalize the process. If you do not wish to save the import results, please click **[Discard Changes]**.
- File type: xlsx, csv.
- Note: It is recommended to add access IDs and export them before importing to ensure that the imported file complies to the file type format.



C. File type sample

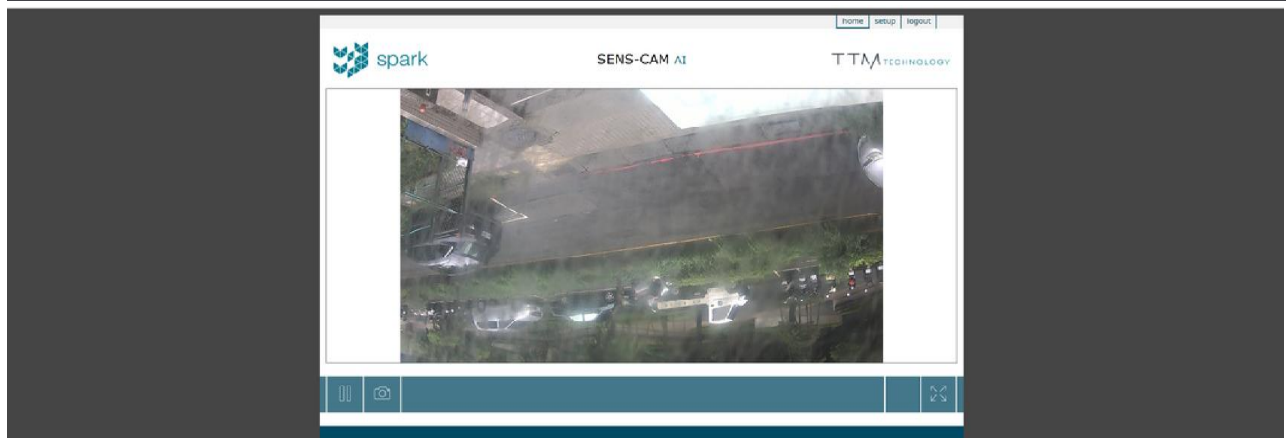
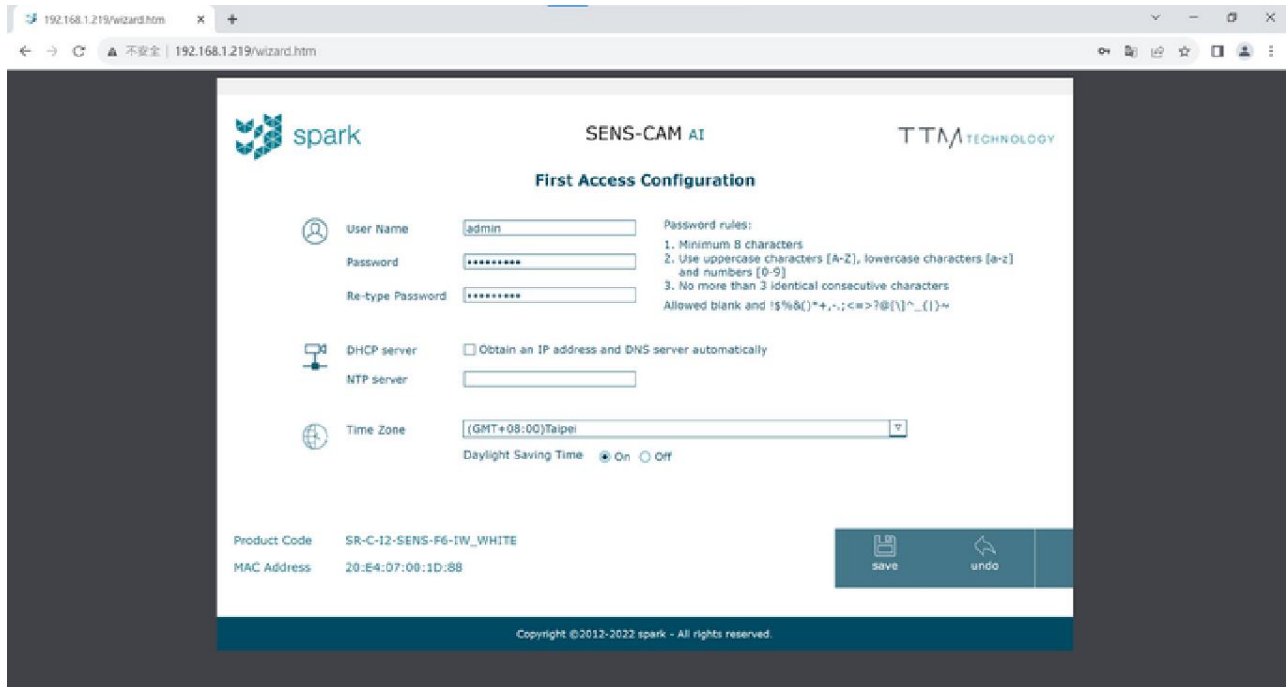
xlsx file	 <table border="1"><thead><tr><th>Access id</th><th>Id type</th><th>Begin of overall validity</th><th>End of overall validity</th><th>Begin of daily validity</th><th>End of daily validity</th><th>Notes</th><th>Categories</th></tr></thead><tbody><tr><td>FHC8637</td><td>LPR</td><td>2024/06/11 00:00:00</td><td>2024/06/12 10:00:00</td><td>00:00:00</td><td>24:00:00</td><td></td><td>Allowed</td></tr><tr><td>ARQ-2991</td><td>LPR</td><td>2024/06/11 00:00:00</td><td>2024/07/11 00:00:00</td><td>00:00:00</td><td>24:00:00</td><td></td><td>Denied</td></tr></tbody></table>	Access id	Id type	Begin of overall validity	End of overall validity	Begin of daily validity	End of daily validity	Notes	Categories	FHC8637	LPR	2024/06/11 00:00:00	2024/06/12 10:00:00	00:00:00	24:00:00		Allowed	ARQ-2991	LPR	2024/06/11 00:00:00	2024/07/11 00:00:00	00:00:00	24:00:00		Denied
Access id	Id type	Begin of overall validity	End of overall validity	Begin of daily validity	End of daily validity	Notes	Categories																		
FHC8637	LPR	2024/06/11 00:00:00	2024/06/12 10:00:00	00:00:00	24:00:00		Allowed																		
ARQ-2991	LPR	2024/06/11 00:00:00	2024/07/11 00:00:00	00:00:00	24:00:00		Denied																		
csv file	<p>accessids - 記事本 檔案(F) 編輯(E) 格式(O) 檢視(V) 說明</p> <p>ACCESS ID; ID TYPE; BEGIN OF OVERALL VALIDITY; END OF OVERALL VALIDITY; BEGIN OF DAILY VALIDITY; END OF DAILY VALIDITY; NOTES; CATEGORIES FHC8637; LPR; 2024-06-11T00:00:00.000Z; 2024-06-12T10:00:00.000Z; 00:00:00; 24:00:00; ; Allowed ARQ-2991; LPR; 2024-06-11T00:00:00.000Z; 2024-07-11T00:00:00.000Z; 00:00:00; 24:00:00; ; Denied</p>																								



8. VIDEO ANALYTICS DATA COLLECTION

8.1 Sens Cam settings

8.1.1 Login settings

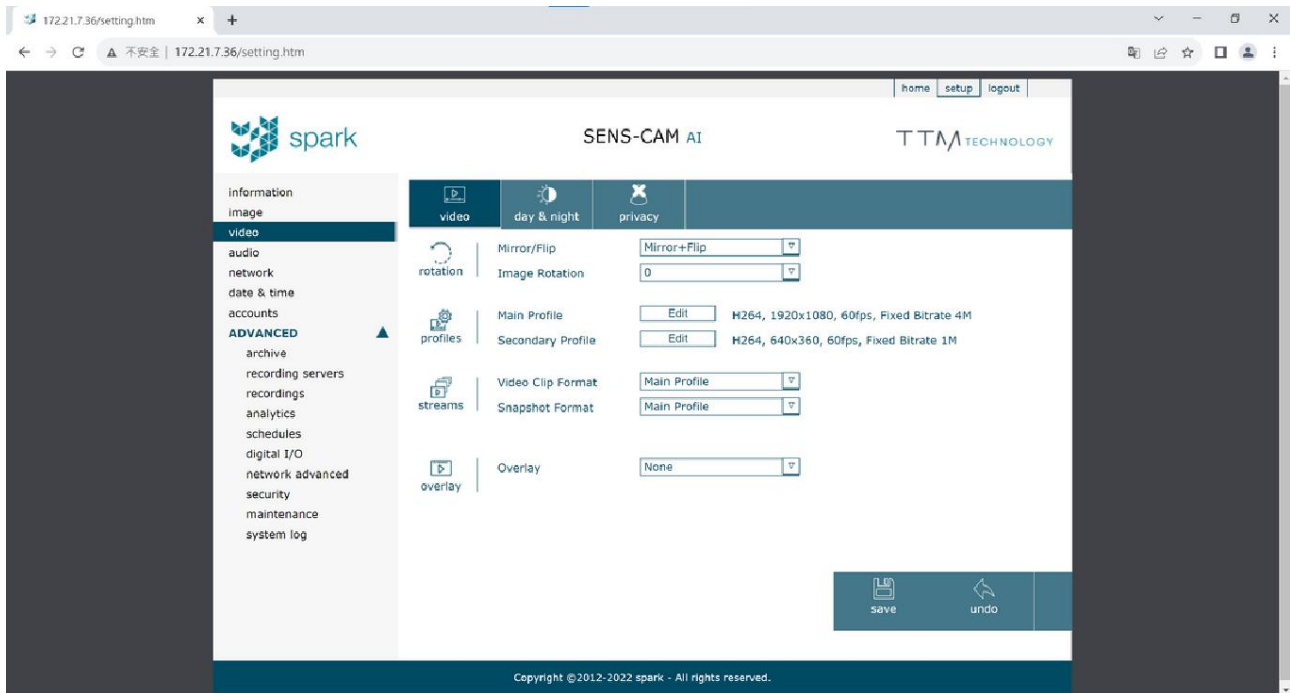


- On the web browser, insert Sens Cam default IP address 192.168.1.219
- User Name: insert username
- Password: insert password
- Re-type Password: retype the password
- DHCP server: if choosing "obtain an IP address and DNS server automatically", please check the assigned IP address through computer network settings. (If not configured, the IP address defaults to 192.168.1.219)
- NTP server: enter the Network Time Protocol of the device platform for time synchronization.
- Time Zone: set the time zone (select GMT+8 for Taiwan).



- After completing the initial login settings, log in again with the new IP address to access the interface.

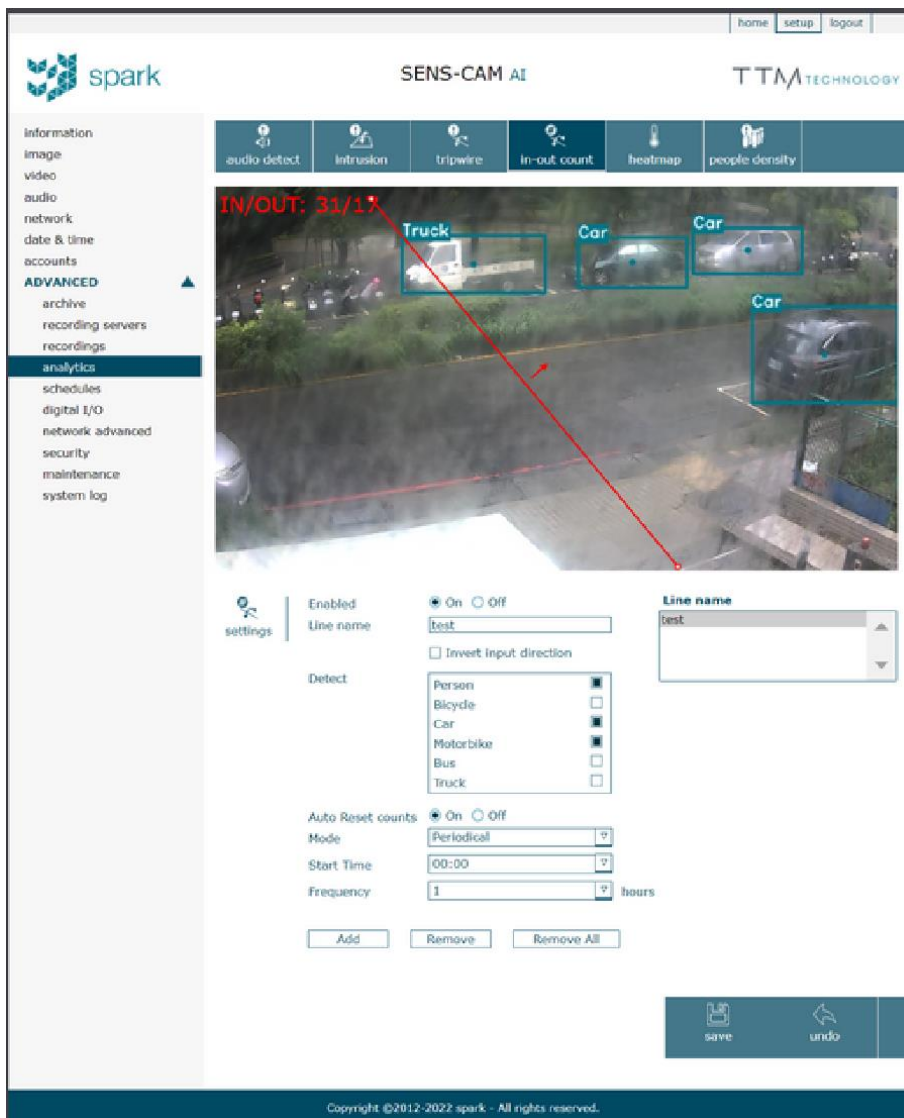
8.1.2 Image setting



- Click on setup and then click video
- rotation: select Mirror/Flip and Image Rotation settings.
- profiles: edit Main Profile (main stream) and Secondary Profile settings.
- streams: select the stream formats for Video Clip Format and Snapshot Format.
- overlay: when enabled, configure the appearance of the overlay on the screen.



8.1.3 Analytics settings



A. Add analytics

- Click setup then click ADVANCED and select analytics
- Enabled: enable to set up analytics
- Line name: insert the name
- Detect: select object to be detected (person, bicycle, car, motorbike, bus, truck)
- Auto Reset counts: When enabled, automatically reset counts at the specified mode and settings.
 1. Mode: select time mode and threshold
 2. Start time: select start time
 3. Frequency: select frequency (in hours)
- Click Add

Note: The example provided is for setting up intelligent analysis for in-out count. For other types of analysis, please configure accordingly.



B. Delete analytics

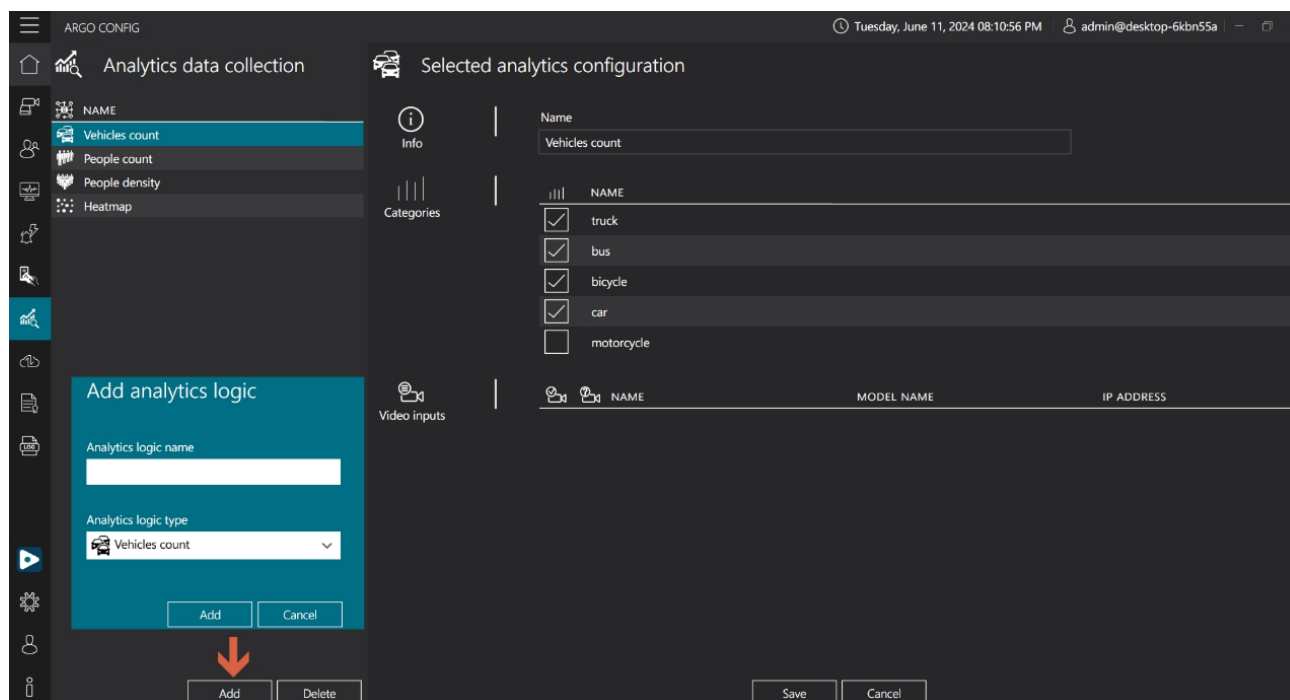
The screenshot displays the SENS-CAM AI analytics interface. At the top, there are navigation links for 'home', 'setup', and 'logout'. The main header includes the 'spark' logo, 'SENS-CAM AI', and 'TTM TECHNOLOGY'. A menu on the left lists various system functions, with 'analytics' highlighted. The central video feed shows a road scene with a red line representing an analytics line. A red arrow points from the 'IN/OUT: 31/17' text to the line. Below the video feed, the settings for the analytics line are displayed, including 'Enabled', 'Line name', 'Detect' (with a list of vehicle types), 'Auto Reset counts', 'Mode', 'Start Time', and 'Frequency'. There are 'Add', 'Remove', and 'Remove All' buttons at the bottom of the settings section. The bottom right corner has 'save' and 'undo' buttons. The footer contains the copyright notice: 'Copyright ©2012-2022 spark - All rights reserved.'

- Select the analytics line name and click “remove” or “remove all” to delete all analytics.



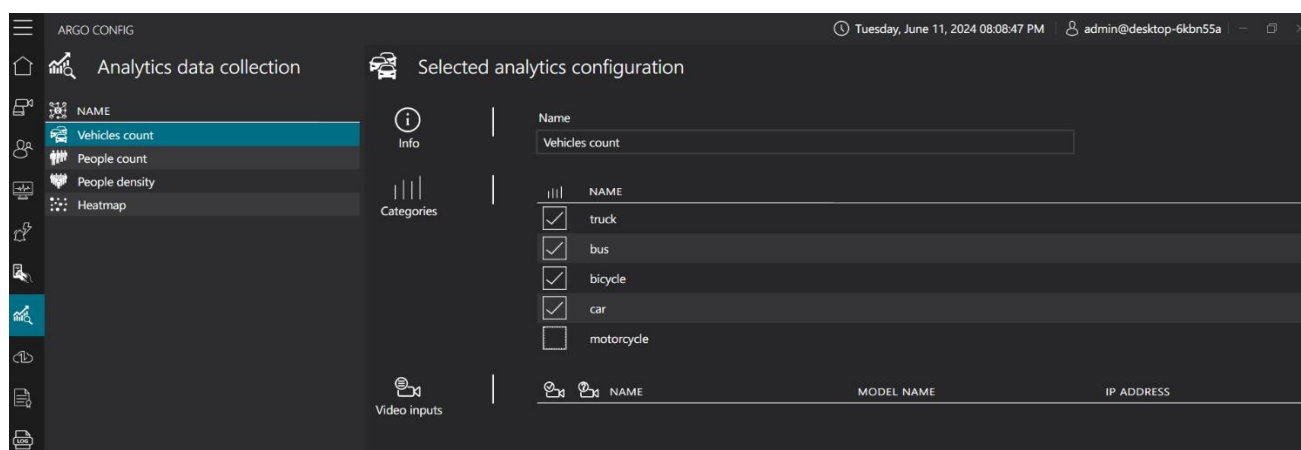
8.2 Video analytics data collection settings

8.2.1 Add video analytics parameters



- Click [Add] to add new parameters
- Name: name the parameter
- Type: select type (vehicle counting / people counting / people density / heatmap / Face Recognition)

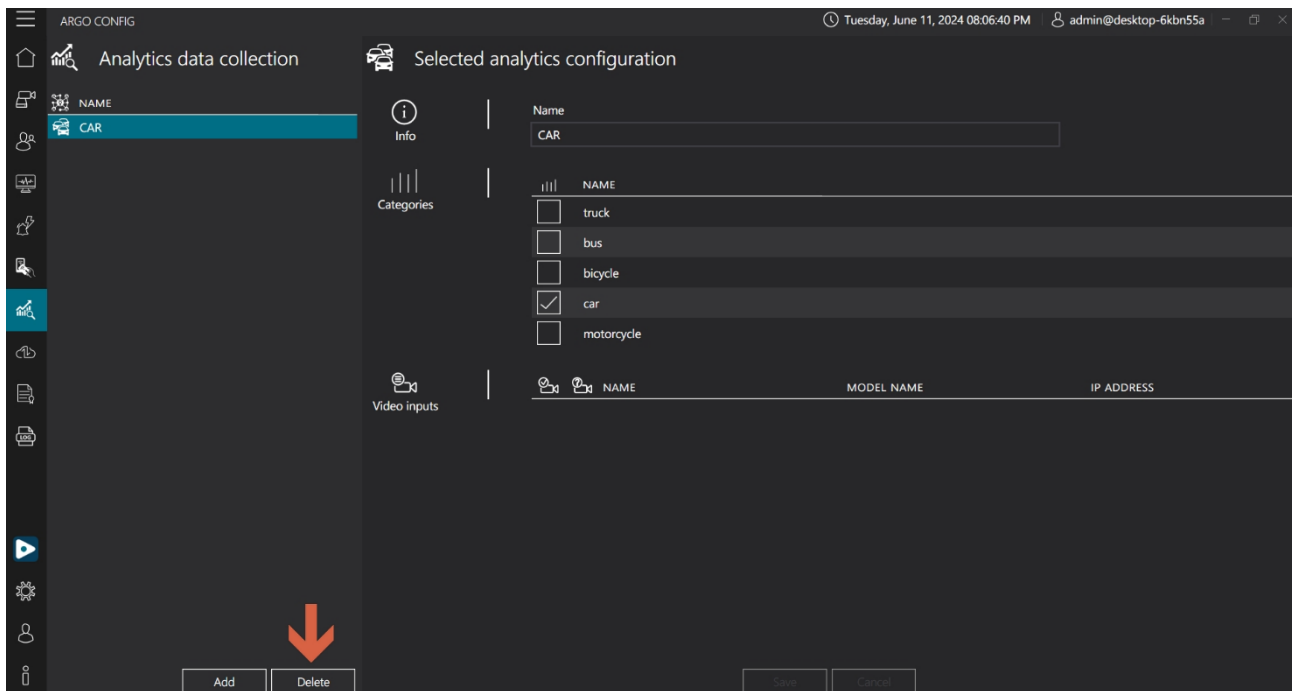
8.2.2 Set video analytics parameters



- Information: displays name of the parameter
- List: select the detection object
- Image input: select Sens cam device



8.2.3 Delete video analytics parameter



- Select the parameter you want to delete and click **[Delete]**



9. BACKUP AND RESTORE

9.1 Backup

ARGO CONFIG Tuesday, June 11, 2024 08:05:00 PM admin@desktop-6kbn55a

Backup and restore

BACKUP RESTORE SCHEDULE BACKUP

Select all available devices

Device type: All Filter

SELECTION	IP ADDRESS	DEVICE NAME	DEVICE TYPE	MODEL NAME	OPTIONS	STATUS
<input type="checkbox"/>		Slave 1	Recorder	Slave 1	<input type="checkbox"/> Events database	Ready
<input checked="" type="checkbox"/>	192.168.1.246	Recorder on DESKTOP-6KBN55A	Recorder	Recorder on DESKTOP-6KBN55A	<input checked="" type="checkbox"/> Events database <input checked="" type="checkbox"/> Licenses	Ready
<input type="checkbox"/>	192.168.1.249	Failover	Recorder	Failover	<input type="checkbox"/> Events database	Ready

Selected backup destination file:
C:\Users\Spark_SQA\Desktop\0102_252_Recorder备份.abkp

Browse... Start backup

- Select the device and the option for backup (event database and license key).
- Click [**Browse**] and select the destination folder for the backup.
- Click [**Start Backup**]

9.2 Restore

ARGO CONFIG Tuesday, June 11, 2024 08:00:38 PM admin@desktop-6kbn55a

Backup and restore

BACKUP RESTORE SCHEDULE BACKUP

Selected backup file to restore:
C:\Users\TMS\Desktop\0611Rest.abkp

Backup file details:
Date and time: 6/11/2024 7:59:57 PM
Description:

Backup file content:
 Select all available devices

SELECTION	IP ADDRESS	DEVICE NAME	DEVICE TYPE	MODEL NAME	OPTIONS	DESTINATION	STATUS
<input checked="" type="checkbox"/>	desktop-6kbn55a	Recorder on DESKTOP-6KBN55A	Recorder	Recorder on DESKTOP-6KBN55A	<input checked="" type="checkbox"/> Events database <input checked="" type="checkbox"/> Licenses	Recorder on DESKTOP-6KBN55A	Connected

Device type: All Filter

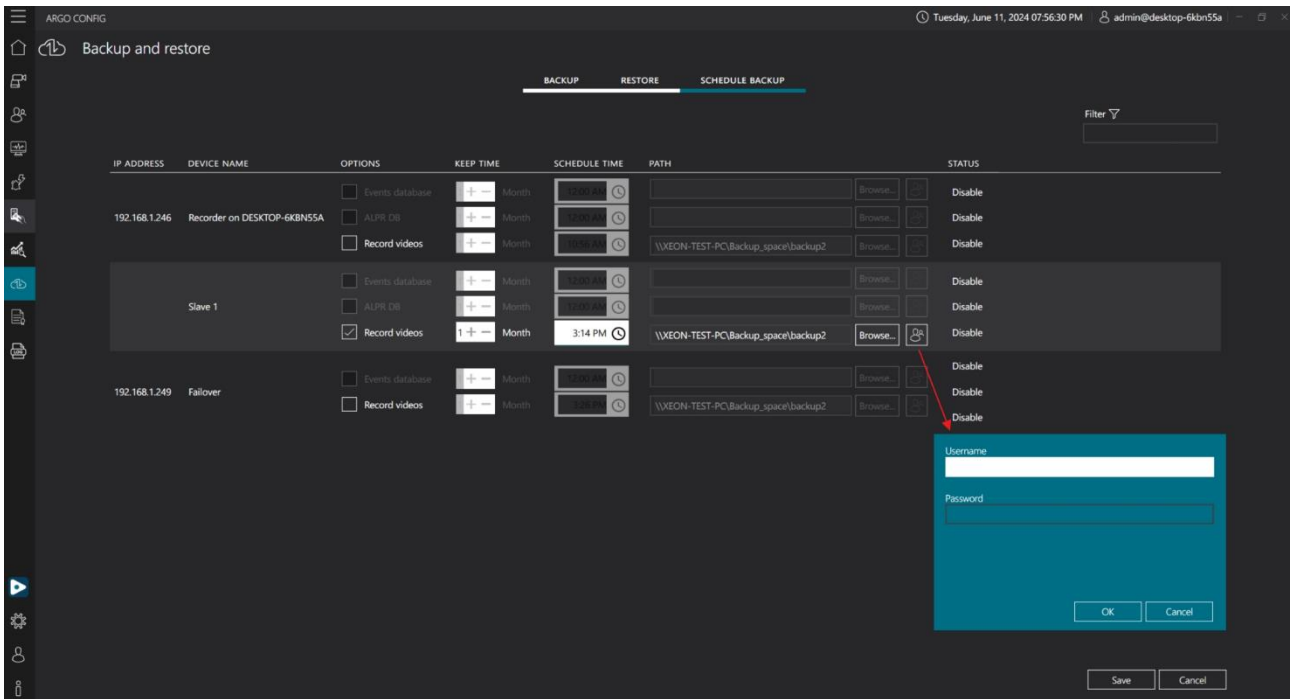
Browse... Start restore

- Click [**Browse**] to select the backup file to restore



- Backup file content: select device and the option for backup (event database and license key).
- Click **[Start Restore]**

9.3 Scheduled backup



- Functions: schedule daily backups of video files during specified times. Backup files are stored in the designated path and retained for one month.



10. LICENSE

ADDRESS	NAME	LICENSE TYPE	STATUS
127.0.0.1	Recorder on LAPTOP-UFTC64RP	Site license	Licensed

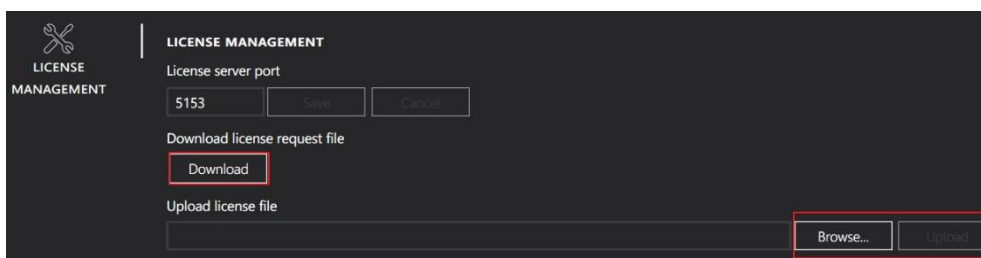
- IP address: current IP address
- Name: server name
- License key type: multiple channel license
- Status: license status

10.1 Information



- License Key Serial Number: Displays the user's license key serial number
Note: If the license key has not been uploaded, the serial number will not be displayed here.

10.2 Manage license



- License key server port: user's license key server port address
- Download license key request file: click **[Download]** and send the user's license key request file to Spark.
- Upload license key: download and unzip the purchased license key file sent by Spark, click **[Browse]**, select the file and click **[Upload]**.



10.3 Channel license key

CHANNELS LICENSE	SUMMARY OF INSTALLED LICENSES PER CHANNEL						
	LICENSE NAME	TYPE	USED	AVAILABLE	TOTAL	EXPIRATION DATE	STATUS
	ONVIF channels license	Permanent	6	82	88	Not applicable	OK
	Omnieye Advanced Series channel license	Permanent	19	69	88	Not applicable	OK
	Brand Series License	Trial	0	8	8	9/26/2024	OK

- Overview of the installed channel license keys: license name / type / in use / available / total / expiry date / status

Note: certain functions cannot be used without adding a license.

10.4 Integrated devices

INTEGRATION LICENSES	SUMMARY OF INSTALLED INTEGRATION LICENSES			
	LICENSE NAME	TYPE	EXPIRATION DATE	STATUS
	AI Service LPR Detection Integration License(B106244C)	Permanent	Not applicable	OK
	I/O Modules activation license	Trial	7/22/2024	OK
	Argo integration license	Trial	8/15/2024	OK
	AI Service Vehicle Detect Integration License(2B06274C)	Trial	8/15/2024	OK
	AI Service Human Detection Integration License(2D06294C)	Trial	8/15/2024	OK
	AI Service Human Detection Integration License(B3061A4C)	Trial	8/15/2024	OK
	AI Service Human Detection Integration License(16041A2C)	Trial	8/15/2024	OK
	AI Service Human Detection Integration License(17041A2C)	Trial	8/15/2024	OK

- Overview of integrated service license keys: license name / type / expiry date / status

Note: certain functions cannot be used without adding a license.



11.LOG

11.1 Data trace

The screenshot shows the 'Log' section of the Argo Config interface. It includes filters for 'LEVEL' (set to ALL), 'FROM' (6/11/2024), and 'TO' (6/11/2024). Below the filters is a table of nodes to select from:

SELECT	NODE	ADDRESS	STATUS
<input checked="" type="checkbox"/>	Recorder on DESKTOP-6KBN55A	desktop-6kbn55a	Online
<input checked="" type="checkbox"/>	Slave 1	localhost	Online
<input checked="" type="checkbox"/>	Failover	xeon-test-pc	Online

Below the node selection is a search bar and a 'Delete' button. The main log area displays a table of log entries:

DATE	LEVEL	MESSAGE	NODE
2024-06-11 09:07:28.841	INFO	User "admin" from xeon-test-pc - 192.168.2.249 started live streaming for stream "videostream 2".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 09:07:28.947	INFO	User "admin" from xeon-test-pc - 192.168.2.249 started live streaming for stream "audiostream 2".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 09:07:28.947	INFO	User "admin" from xeon-test-pc - 192.168.2.249 started live streaming for stream "videostream 2".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 09:07:29.162	INFO	User "admin" from xeon-test-pc - 192.168.2.249 started live streaming for stream "audiostream 2".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 09:07:29.162	INFO	User "admin" from xeon-test-pc - 192.168.2.249 started live streaming for stream "videostream 2".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 09:07:29.282	INFO	User "admin" from xeon-test-pc - 192.168.2.249 started live streaming for stream "videostream 2".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 09:07:29.282	INFO	User "admin" from xeon-test-pc - 192.168.2.249 started live streaming for stream "audiostream 2".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 09:07:29.389	INFO	User "admin" from xeon-test-pc - 192.168.2.249 started live streaming for stream "audiostream 2".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 09:07:29.389	INFO	User "admin" from xeon-test-pc - 192.168.2.249 started live streaming for stream "videostream 2".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)

At the bottom right, there is an 'Export to CSV' button.

A. Search data trace

The screenshot shows the 'Log' section of the Argo Config interface with several annotations:

- A red box highlights the 'LEVEL' dropdown menu, which is currently set to 'ALL'.
- A red box highlights the 'FROM' and 'TO' date input fields, both set to '6/11/2024'. A calendar icon is shown next to each field, indicating that clicking it opens a date picker.
- A red arrow points to the 'Search' input field at the bottom left.

The interface also shows a calendar for June 2024, with the 11th highlighted. The node selection table and log entries are visible below the filters.

- Level: select the level of data trace you want to search
Level types: Full list / INFO / **WARN** / **ERROR** / **SUCCESS**
- Time range: Click on the **[Calendar icon]** to select the time range of the data trace
- Nodes: select the nodes where the data trace is located
Note: select at least one node from the list
- Click **[Search]**



B. Delete data trace

The screenshot shows the 'Log' interface with the following elements:

- Level: A dropdown menu set to 'ALL'.
- Time range: 'FROM' and 'TO' fields both set to '6/11/2024', with calendar icons to the right.
- Nodes: A table with columns 'SELECT', 'NODE', 'ADDRESS', and 'STATUS'. Three nodes are listed: 'Recorder on DESKTOP-6KBN55A', 'Slave 1', and 'Failover', all with checked selection boxes and 'Online' status.
- Buttons: A 'Search' button and a 'Delete' button with a red arrow icon.

- Level: select the level of data trace you want to delete
Level types: Full list / INFO / **WARN** / **ERROR** / **SUCCESS**
- Time range: Click on the **[Calendar icon]** to select the time range of the data trace
- Nodes: select the nodes where the data trace is located
Note: select at least one node from the list
- Click **[Delete]**

C. Export data trace

The screenshot shows a table of log entries with the following columns: DATE, LEVEL, MESSAGE, and NODE. The table contains several rows of log data. At the bottom right, there is an 'Export to CSV' button with a red arrow icon.

DATE	LEVEL	MESSAGE	NODE
2024-06-11 09:07:28.841	INFO	User "admin" from xeon-test-pc - 192.168.2.249 started live streaming for stream "videostream 2".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 09:07:28.947	INFO	User "admin" from xeon-test-pc - 192.168.2.249 started live streaming for stream "audiostream 2".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 09:07:28.947	INFO	User "admin" from xeon-test-pc - 192.168.2.249 started live streaming for stream "videostream 2".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 09:07:29.162	INFO	User "admin" from xeon-test-pc - 192.168.2.249 started live streaming for stream "audiostream 2".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 09:07:29.162	INFO	User "admin" from xeon-test-pc - 192.168.2.249 started live streaming for stream "videostream 2".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 09:07:29.282	INFO	User "admin" from xeon-test-pc - 192.168.2.249 started live streaming for stream "videostream 2".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 09:07:29.282	INFO	User "admin" from xeon-test-pc - 192.168.2.249 started live streaming for stream "audiostream 2".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 09:07:29.389	INFO	User "admin" from xeon-test-pc - 192.168.2.249 started live streaming for stream "audiostream 2".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 09:07:29.389	INFO	User "admin" from xeon-test-pc - 192.168.2.249 started live streaming for stream "videostream 2".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)

- Export the search results of the data trace.
- Click **[Export CSV]**



11.2 System log

DATE	LEVEL	MESSAGE	NODE
2024-06-11 00:00:00.351	INFO	Status of event "systemevent_69d74598-a248-46e0-942a-b2934d65dc36" is now "inactive".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 00:00:00.353	INFO	Status of event "systemevent_69d74598-a248-46e0-942a-b2934d65dc36" is now "active".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 00:00:02.208	INFO	Status of event "systemevent_81e64362-c6a9-41c6-833c-3d9685768767" is now "inactive".	Slave 1 (localhost)
2024-06-11 00:00:02.218	INFO	Status of event "systemevent_81e64362-c6a9-41c6-833c-3d9685768767" is now "active".	Slave 1 (localhost)
2024-06-11 00:00:02.331	INFO	Status of event "systemevent_f2271561-b9fc-4b70-bfca-58c91573be1a" is now "inactive".	Slave 1 (localhost)
2024-06-11 00:00:02.331	INFO	Status of event "systemevent_f2271561-b9fc-4b70-bfca-58c91573be1a" is now "active".	Slave 1 (localhost)
2024-06-11 00:00:04.890	INFO	Status of event "systemevent_0c2c4037-3da4-4c75-90bd-23fe690483bd" is now "inactive".	Slave 1 (localhost)
2024-06-11 00:00:04.890	INFO	Status of event "systemevent_0c2c4037-3da4-4c75-90bd-23fe690483bd" is now "active".	Slave 1 (localhost)
2024-06-11 00:00:04.888	INFO	Status of event "systemevent_69d74598-a248-46e0-942a-b2934d65dc36" is now "inactive".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)

A. Search system log

SELECT	NODE	ADDRESS	STATUS
<input checked="" type="checkbox"/>	Recorder on DESKTOP-6KBN55A	desktop-6kbn55a	Online
<input checked="" type="checkbox"/>	Slave 1	localhost	Online
<input checked="" type="checkbox"/>	Failover	xeon-test-pc	Online

- Level: select the level of the system log you want to search
Level types: Full list / INFO / WARN / ERROR / SUCCESS
- Time range: Click on the **[Calendar icon]** to select the time range of the system log
- Nodes: select the nodes where the system log is located
Note: select at least one node from the list
- Click **[Search]**



B. Delete system log

ARGO CONFIG Tuesday, June 11, 2024 07:17:22 PM admin@desktop-6kbn55a

Log

AUDIT LOG SYSTEM LOG DETAILED LOG

LEVEL: ALL FROM: 6/11/2024 TO: 6/11/2024

Please choose at least a node from the list below:

SELECT	NODE	ADDRESS	STATUS
<input checked="" type="checkbox"/>	Recorder on DESKTOP-6KBN55A	desktop-6kbn55a	Online
<input checked="" type="checkbox"/>	Slave 1	localhost	Online
<input checked="" type="checkbox"/>	Failover	xeon-test-pc	Online

Search [Delete]

- Level: select the level of the system log you want to delete
Level types: Full list / INFO / **WARN** / **ERROR** / **SUCCESS**
- Time range: Click on the **[Calendar icon]** to select the time range of the system log
- Nodes: select the nodes where the system log is located
Note: select at least one node from the list
- Click **[Delete]**

C. Export system log

DATE	LEVEL	MESSAGE	NODE
2024-06-11 00:00:00.351	INFO	Status of event "systemevent_69d74598-a248-46e0-942a-b2934d65dc36" is now "inactive".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 00:00:00.353	INFO	Status of event "systemevent_69d74598-a248-46e0-942a-b2934d65dc36" is now "active".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 00:00:02.208	INFO	Status of event "systemevent_81e64362-c6a9-41c6-833c-3d9685768767" is now "inactive".	Slave 1 (localhost)
2024-06-11 00:00:02.218	INFO	Status of event "systemevent_81e64362-c6a9-41c6-833c-3d9685768767" is now "active".	Slave 1 (localhost)
2024-06-11 00:00:02.331	INFO	Status of event "systemevent_f2271561-b9fc-4b70-bfca-58c91573be1a" is now "inactive".	Slave 1 (localhost)
2024-06-11 00:00:02.331	INFO	Status of event "systemevent_f2271561-b9fc-4b70-bfca-58c91573be1a" is now "active".	Slave 1 (localhost)
2024-06-11 00:00:04.890	INFO	Status of event "systemevent_0c2c4037-3da4-4c75-90bd-23fe690483bd" is now "inactive".	Slave 1 (localhost)
2024-06-11 00:00:04.890	INFO	Status of event "systemevent_0c2c4037-3da4-4c75-90bd-23fe690483bd" is now "active".	Slave 1 (localhost)
2024-06-11 00:00:05.488	INFO	Status of event "systemevent_69d74598-a248-46e0-942a-b2934d65dc36" is now "inactive".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 00:00:05.488	INFO	Status of event "systemevent_69d74598-a248-46e0-942a-b2934d65dc36" is now "active".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 00:00:07.359	INFO	Status of event "systemevent_81e64362-c6a9-41c6-833c-3d9685768767" is now "inactive".	Slave 1 (localhost)
2024-06-11 00:00:07.359	INFO	Status of event "systemevent_81e64362-c6a9-41c6-833c-3d9685768767" is now "active".	Slave 1 (localhost)
2024-06-11 00:00:07.467	INFO	Status of event "systemevent_f2271561-b9fc-4b70-bfca-58c91573be1a" is now "inactive".	Slave 1 (localhost)
2024-06-11 00:00:07.467	INFO	Status of event "systemevent_f2271561-b9fc-4b70-bfca-58c91573be1a" is now "active".	Slave 1 (localhost)
2024-06-11 00:00:10.035	INFO	Status of event "systemevent_0c2c4037-3da4-4c75-90bd-23fe690483bd" is now "inactive".	Slave 1 (localhost)
2024-06-11 00:00:10.035	INFO	Status of event "systemevent_0c2c4037-3da4-4c75-90bd-23fe690483bd" is now "active".	Slave 1 (localhost)

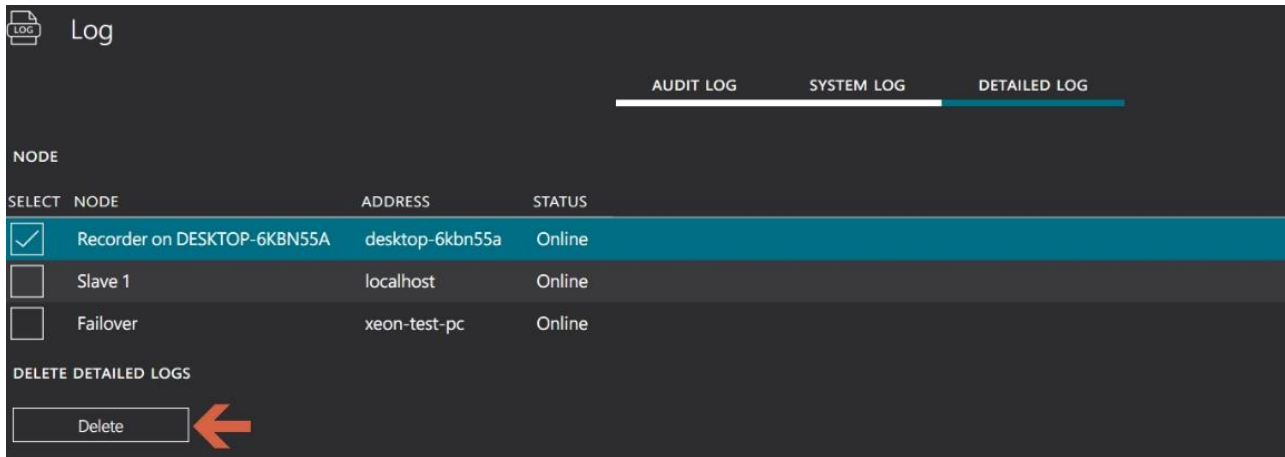
Export to CSV

- Export the search results of the system log.
- Click **[Export CSV]**



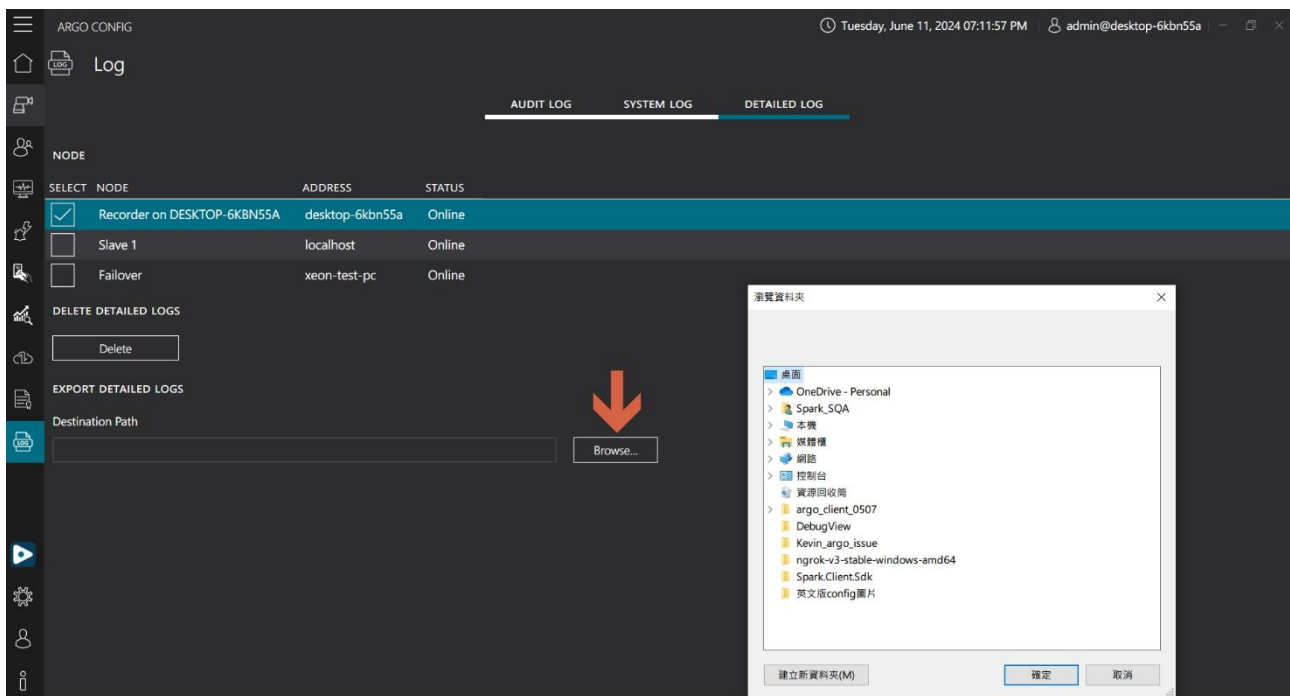
11.3 Detailed log

A. Delete detailed log



- Nodes: select the nodes where the detailed log is located
- Click [**Delete**]

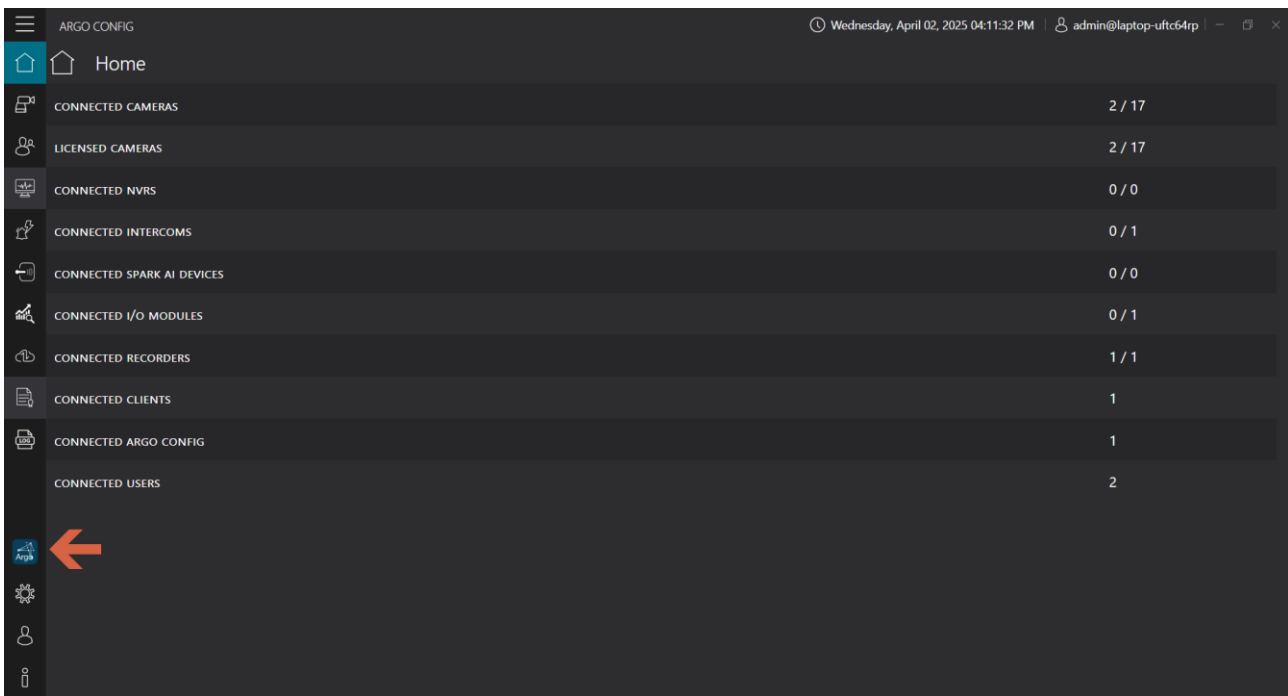
B. Export detailed log



- Nodes: select the nodes where the detailed log is located
- Click [**Browse**] to export folder
- Click [**OK**]



12. ARGO CLIENT

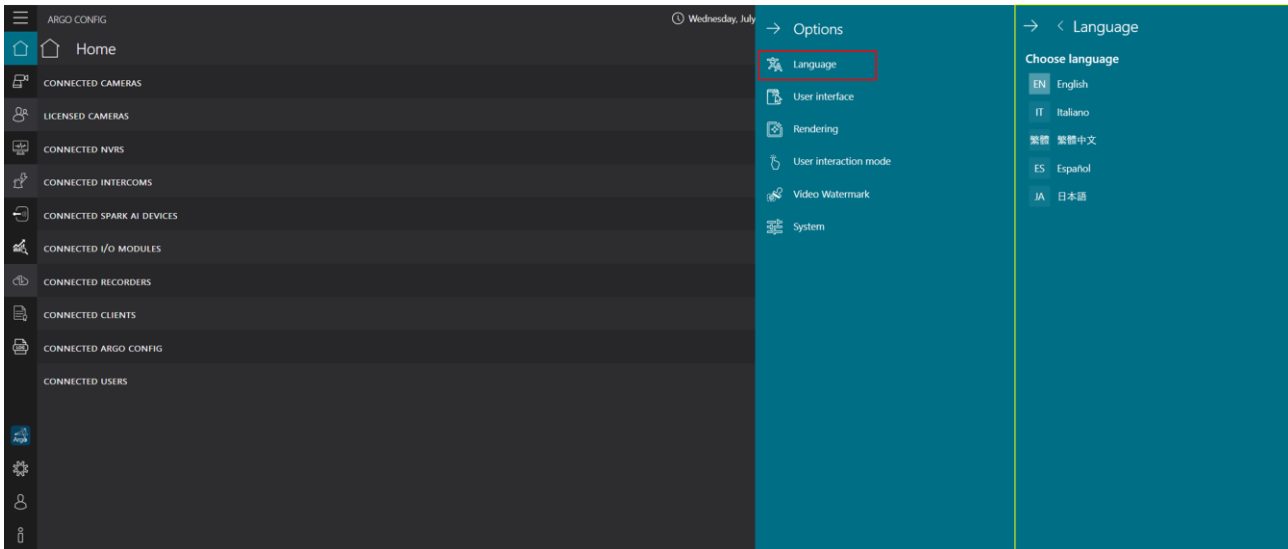


- Click the **[Argo Client icon]** on the bottom left
- Link from Argo Config to Argo Client



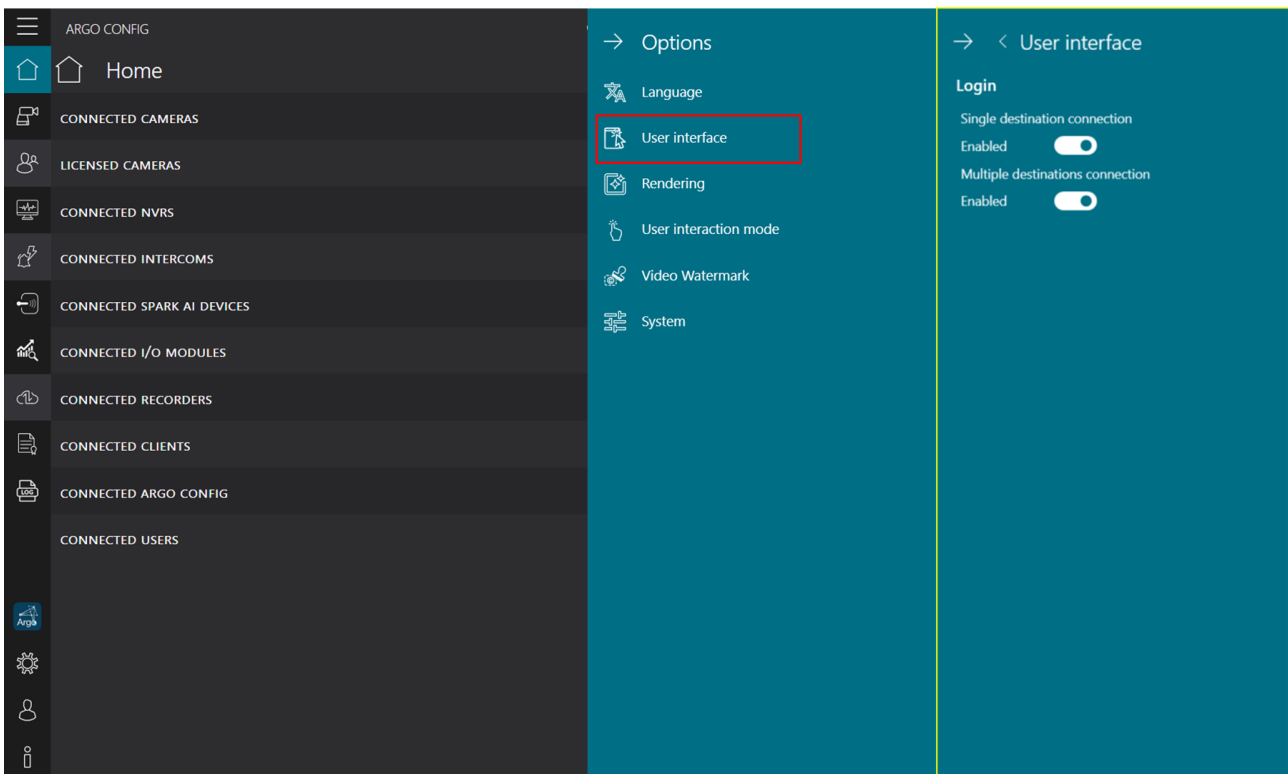
13. OPTIONS

13.1 Language

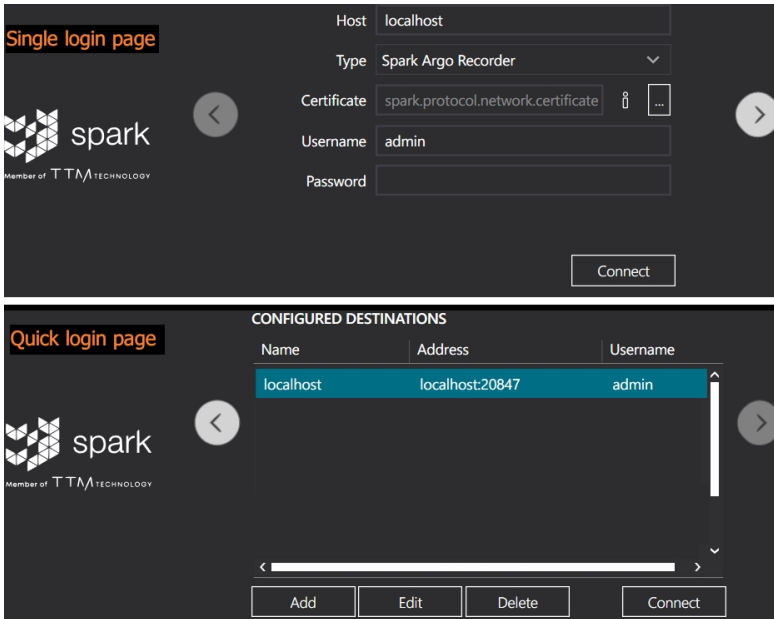


- Click the bottom left **[Gear Icon]** and select **[Language]**.
- Language options: English / Italiano / 繁體中文 / Español / 日本語

13.2 Interface

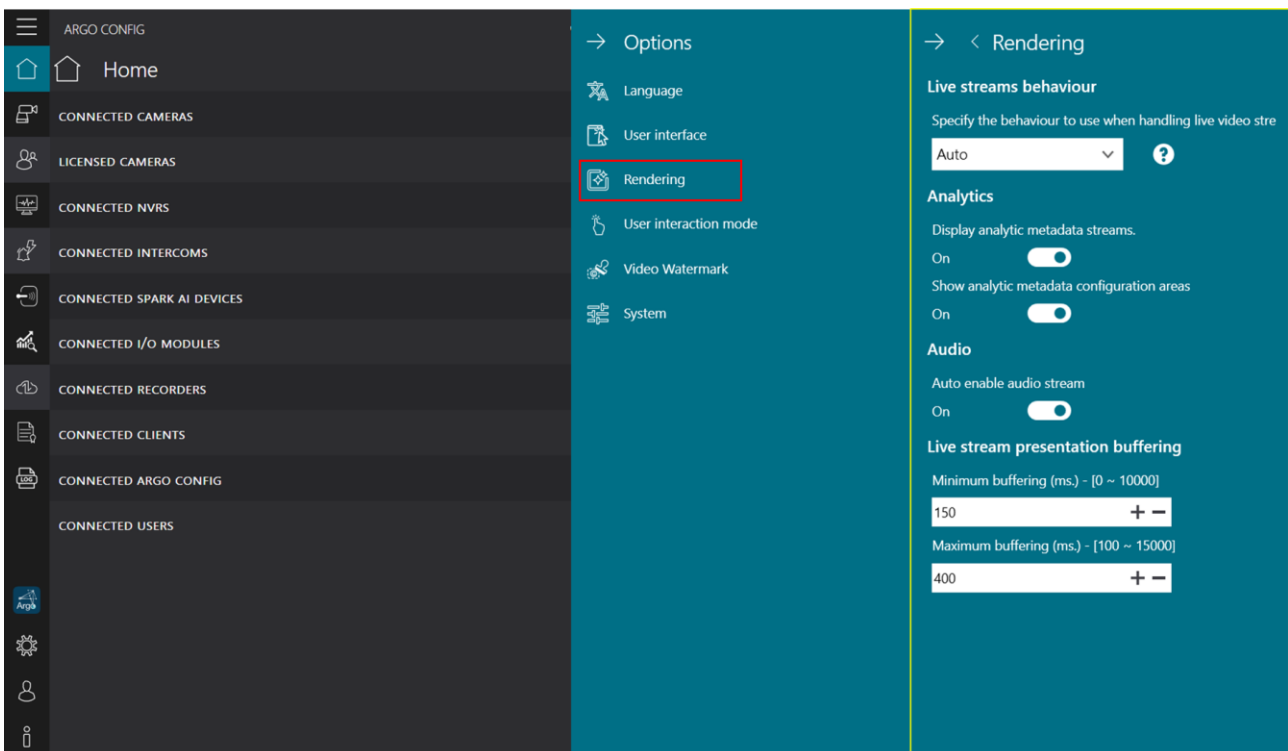


- Click the bottom left **[Gear Icon]** and select **[User Interface]**.



- Log in
Single login page: password is required to log in.
Quick login page: log in without a password for direct connection.

13.3 Rendering

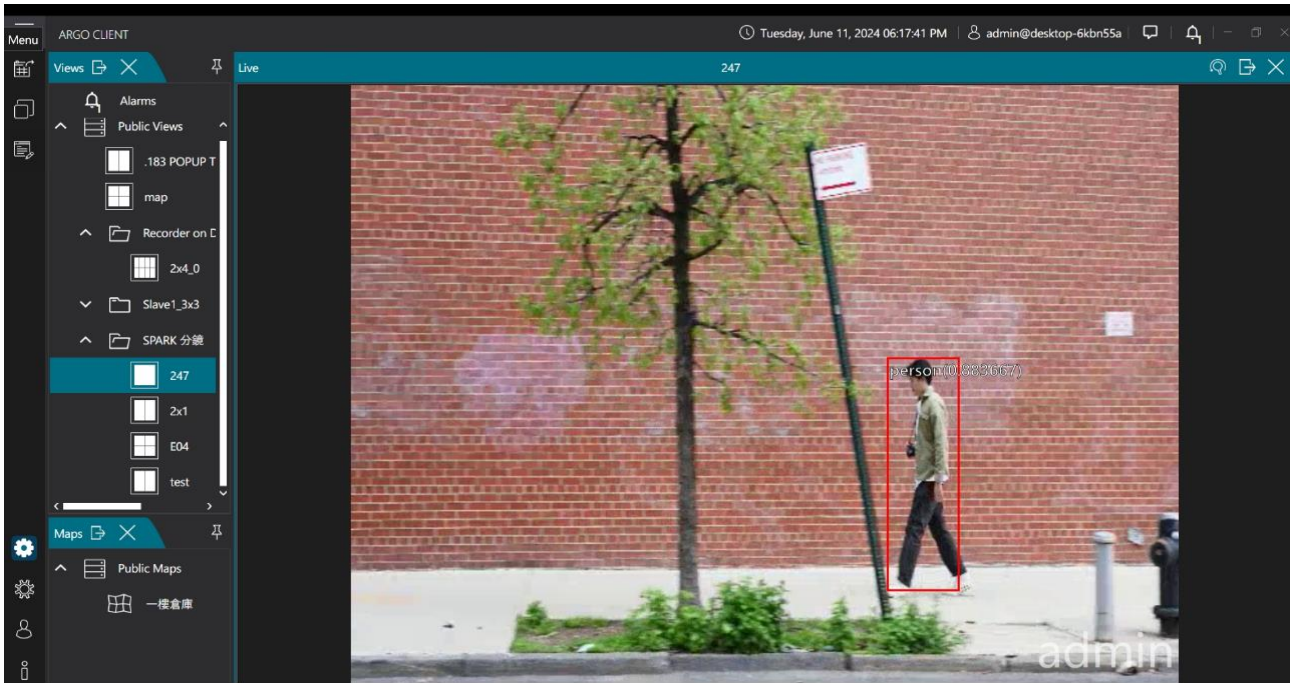


- Click the bottom left **[Gear Icon]** and select **[Rendering]**.
- Real-time streaming behavior
Specify real-time streaming behavior: can be set to auto or highest resolution



- A. Auto: sets the camera to use the lowest available resolution (excluding thumbnail streams) by default.
- B. Highest resolution: sets the camera to use the highest available resolution (excluding thumbnail streams) by default.

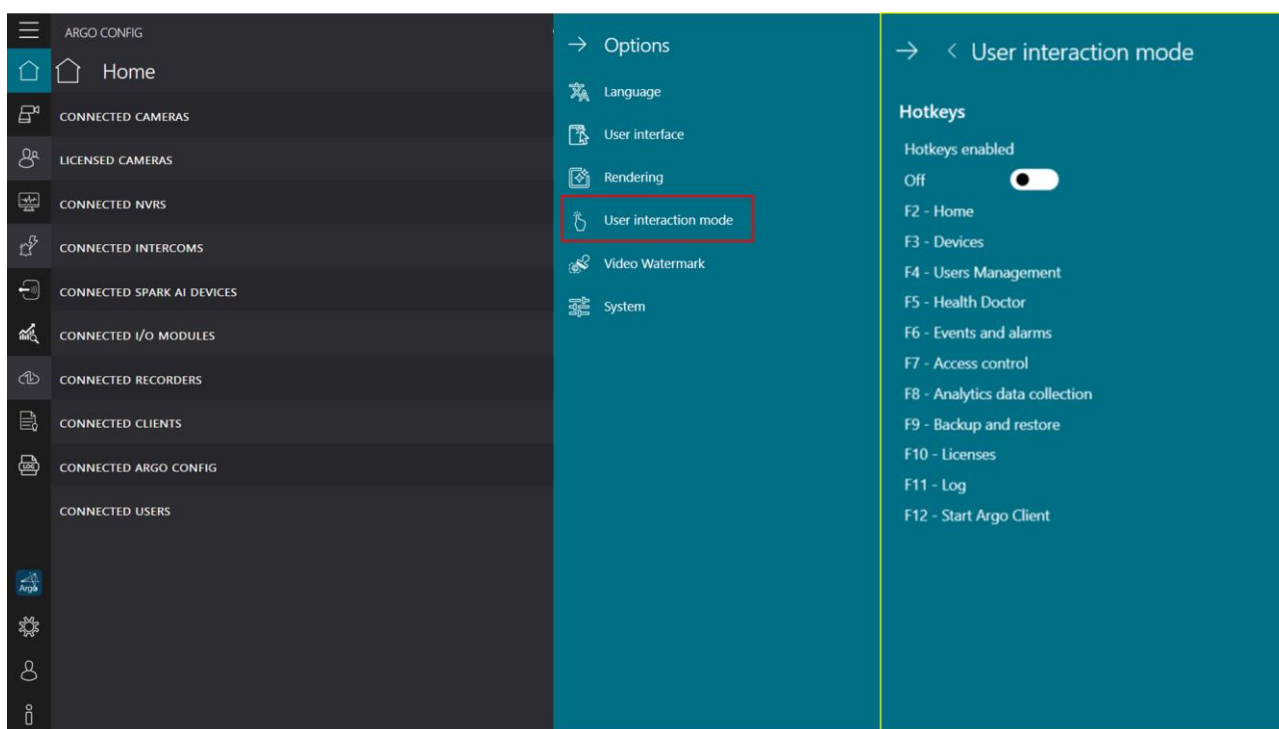
Note: Specifying real-time streaming behavior to Auto typically results in a lower resolution to reduce computer power consumption.



- Video analytics
 - Display detected object: the monitoring screen will display a red frame on detected object.
 - Display detection zone: the monitoring screen will display a red frame on the detection zone.
 - Audio: start audio streaming when viewing the camera: sound will be available when viewing the camera.
 - Real-time stream buffering: edit minimum and maximum buffering time.
 - Minimum buffer time range: 0~10000 milliseconds
 - Maximum buffer time range:100~15000 milliseconds
- Note: for effective video analytics, pre-configuration on the camera's web interface is required.



13.4 User interaction mode

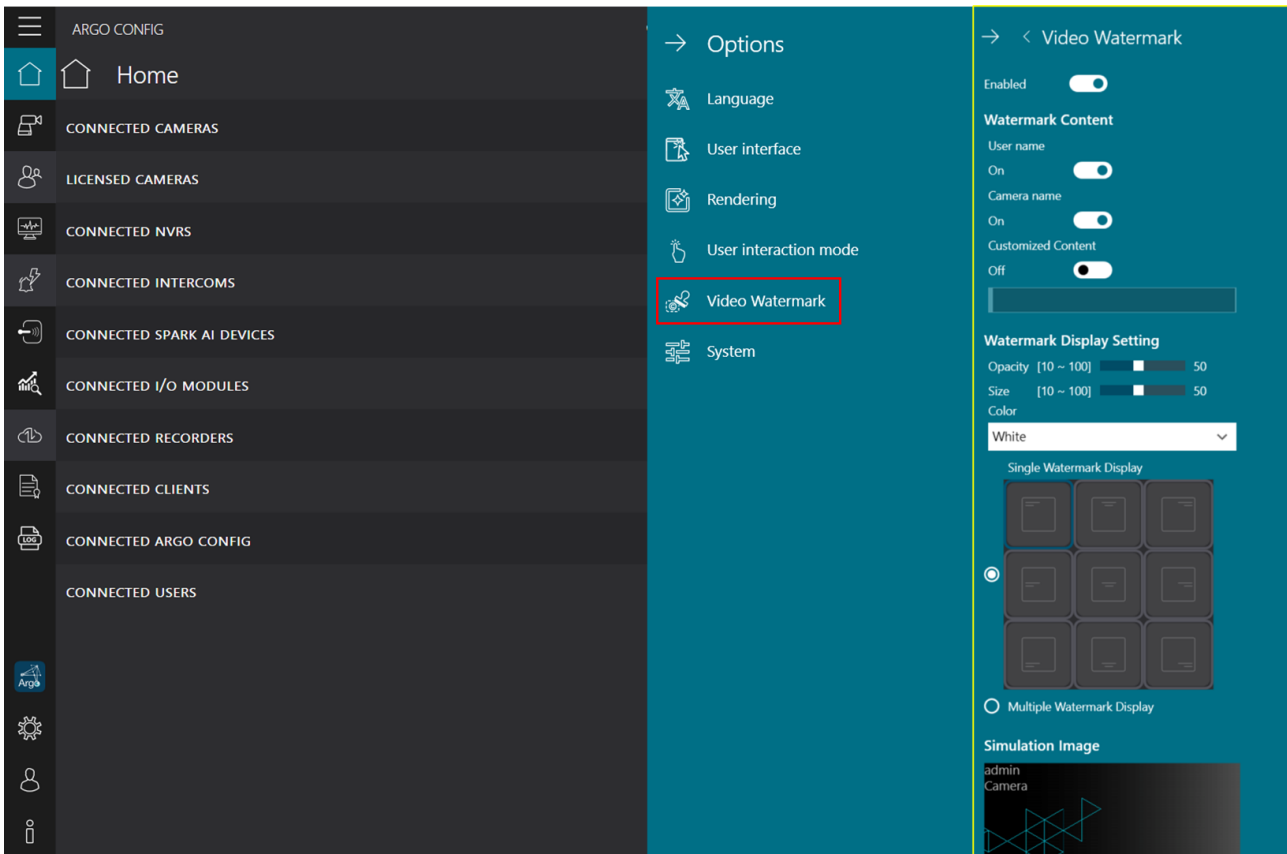


- Click the bottom left **[Gear Icon]** and select **[user interaction mode]**.
- Shortcuts: when enabled, users can use below shortcuts.

F2	Home	F8	Video analytics data collection
F3	Device	F9	Backup and restore
F4	User management	F10	License
F5	System health check	F11	Log
F6	Event and alarm	F12	Start Argo Client
F7	Access Control		



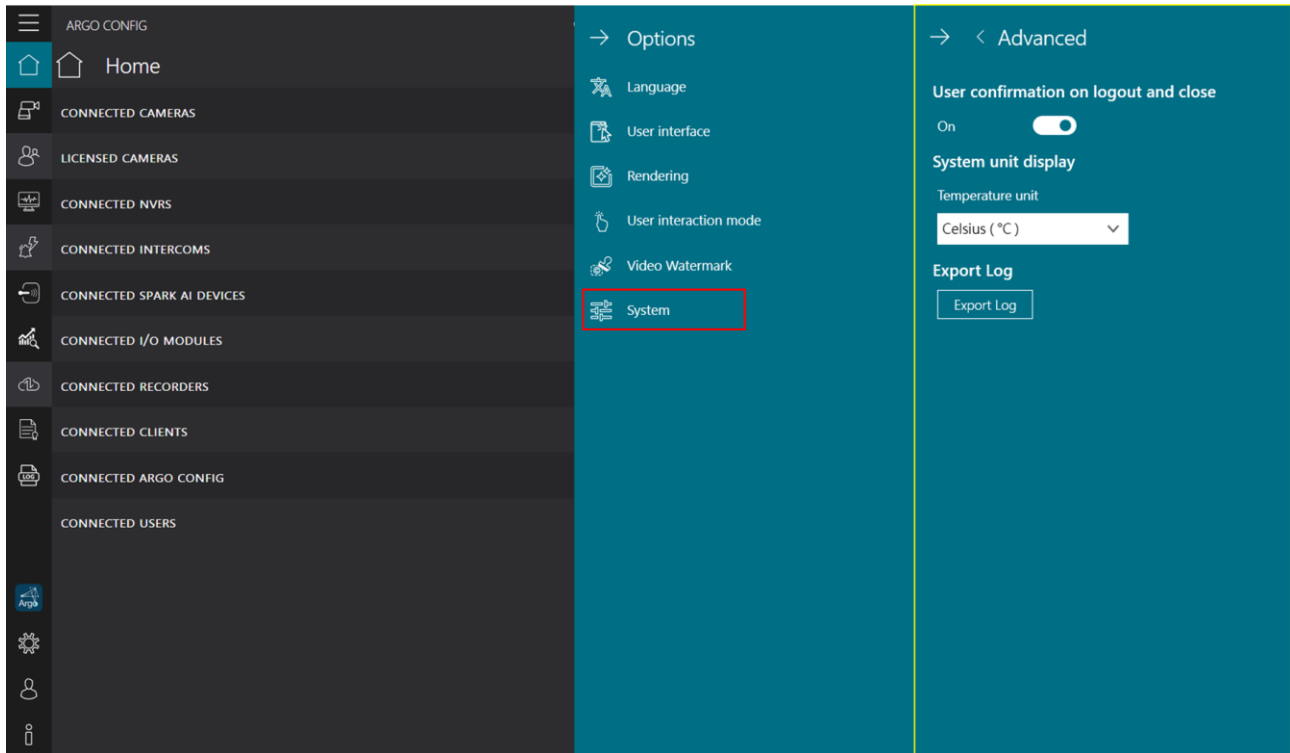
13.5 Watermark



- Click the bottom left **[Gear Icon]** and select **[Watermark]**.
- Watermark content: edit the username and custom content.
Username: when enabled, the watermark will display the username.
Custom content: when enabled, users can custom watermark content.
- Watermark display options:
Edit the text transparency, text size, text color, single watermark display position, or multiple watermarks filling the image.
Text transparency: edit the transparency of the watermark text, ranging from 10 to 100.
Text size: edit the size of the watermark text, ranging from 10 to 100.
Text color: edit the watermark text color, choosing between white or black.
Single watermark display position: display a single watermark at the specified position.
Position options: top left / top center / top right / center left / center / center right / bottom left / bottom center / bottom right (9 positions in total)
Multiple watermarks filling the image: display watermarks at all nine positions, filling the image with watermark content.
Watermark preview: preview the watermark settings.



13.6 System



- Click the bottom left [**Gear Icon**] and select [**Advanced**].
- Logout/close program confirmation
Enabled: a confirmation prompt will be displayed when logging out or closing the program.
- System Unit display
Temperature Unit: Select from Celsius, Fahrenheit, or Kelvin.
- Export log: Click [**Export logs**] to export complete system program log



14. USER

14.1 Change password

The screenshot shows the 'Change User Password' dialog box. The title bar includes an information icon and the text 'Change User Password'. A sidebar on the left contains icons for 'Argo', 'Change password', 'Logout', and 'Close'. The main area features three input fields: 'Username' (containing 'admin'), 'Old password', 'New password', and 'Confirm password', each with a visibility icon. Below the fields is a warning message: 'WARNING: CAPS LOCK is active'. At the bottom are two buttons: 'Change password' and 'Cancel'.

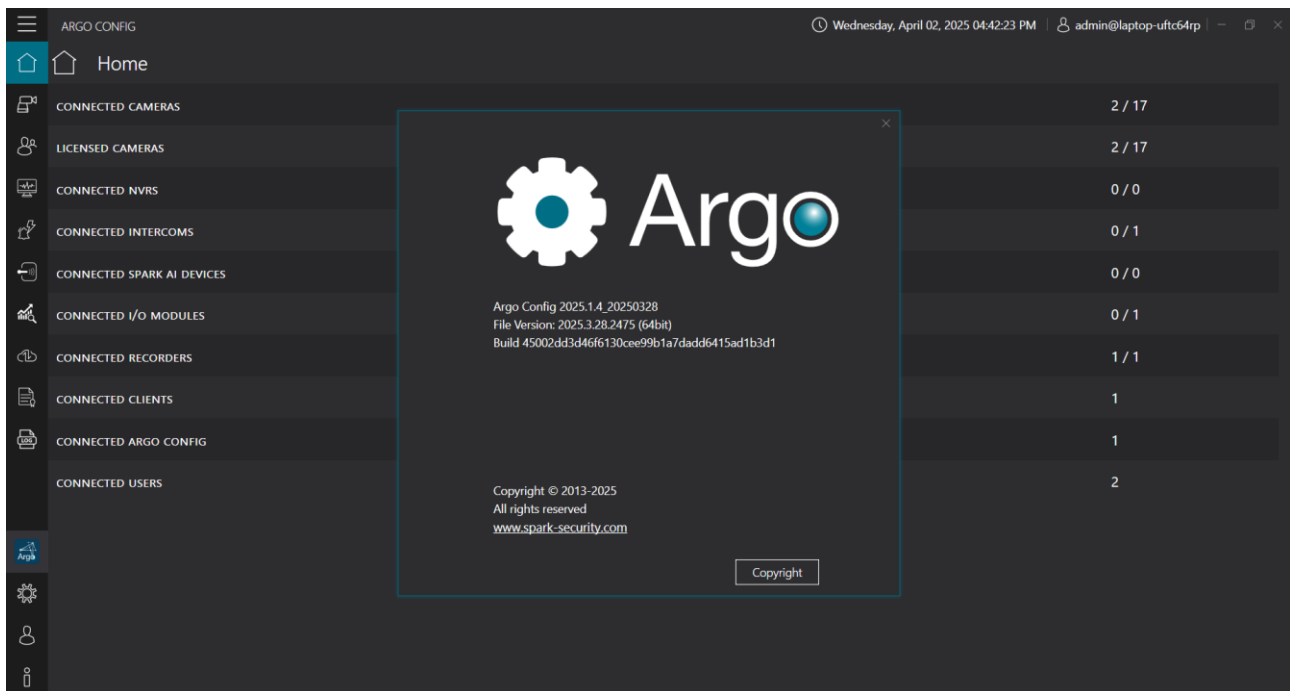
- Click on **[User]** then click **[change password]**. After changing password, click **[change password]** to confirm.
- Username: usernames cannot be modified.
- Old password: insert username old password
- New password: insert new password
- Retype password: retype the password

14.2 Logout/Close

- Logout: click **[logout]** to logout of Argo Config and return to the login page.
- Close: click **[close]** to close Argo Config.



15. ABOUT



- Click on the bottom left [i] to browse the system program version.
- Click www.spark-security.com to access Spark official website
- Click [**Copyright**] to browse detailed copyright information.



16. OTHER

16.1 Applying for LINE message token

Step1: Click on <https://developers.line.biz/en/services/line-login/> to access the official LINE Business Account page.

Step2: Register for LINE Business ID

To create a LINE Official Account, you need to register for LINE Business ID (opens new window). You can register for LINE Business ID using your LINE account or email address.

LINE Business ID

Sign up with LINE account

or

Sign up with email

Already have an account?

By signing up and using LINE Business ID, you agree to the [Terms of Use](#).

[About LINE Business ID](#)

English ▾

[Help](#) [Terms of Use](#) © LY Corporation

Step3: Fill in the entry form



Create a LINE official account

• Required

Login info

Username Sample [Log out](#)

Service region Zambia

Account info

Account name • 0/20

This name will appear on the LINE friend list and chat screen.

Email address • 16/240

Company or owner's country or region

This country/region info will be displayed where users can see, such as on your account profile.

•

Company name 0/100

Industry •



Step4: Check your LINE Official Account

The screenshot shows the 'LINE Official Account Manager' interface. At the top left, it says 'LINE Official Account Manager'. On the right, there is a user profile icon and the text 'Sample accou...'. Below this, there are two tabs: 'Accounts' (selected) and 'Groups'. On the left sidebar, there is a 'Create new' button. The main content area is titled 'Accounts' and shows 'Accounts (1)'. There is a search bar labeled 'Account name' with a green search icon. Below the search bar is a table with the following data:

Account name	Friends	Role	Plan
Sample channel	0	Administrator	コミュニケーション

At the bottom of the table, there is a pagination control showing '< 1 >'. At the bottom left of the page, there is a 'Hide menu labels' button. At the bottom right, there is a copyright notice '© LINE Corporation'.

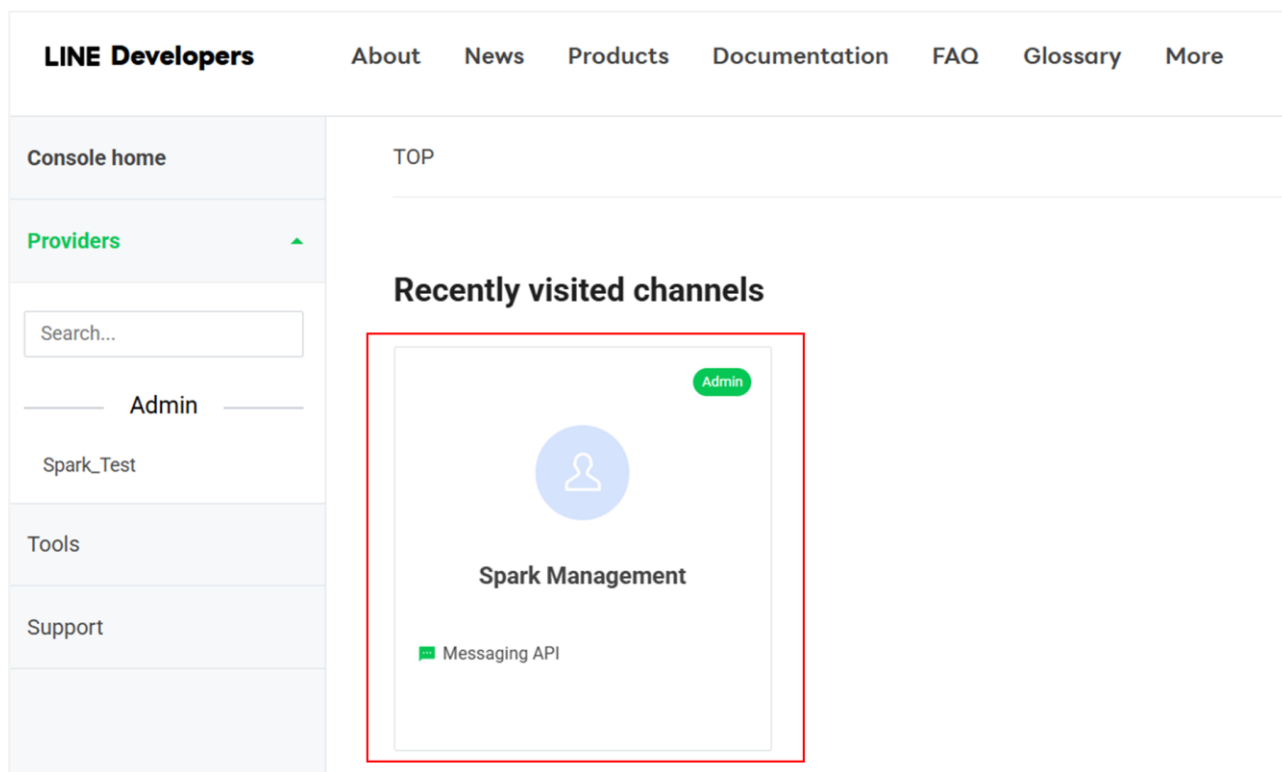
Step5: Enable the Messaging API for your LINE Official Account

To link your LINE Official Account with the Messaging API, go to the LINE Official Account Manager (opens new window) and enable the Messaging API. This creates a channel.

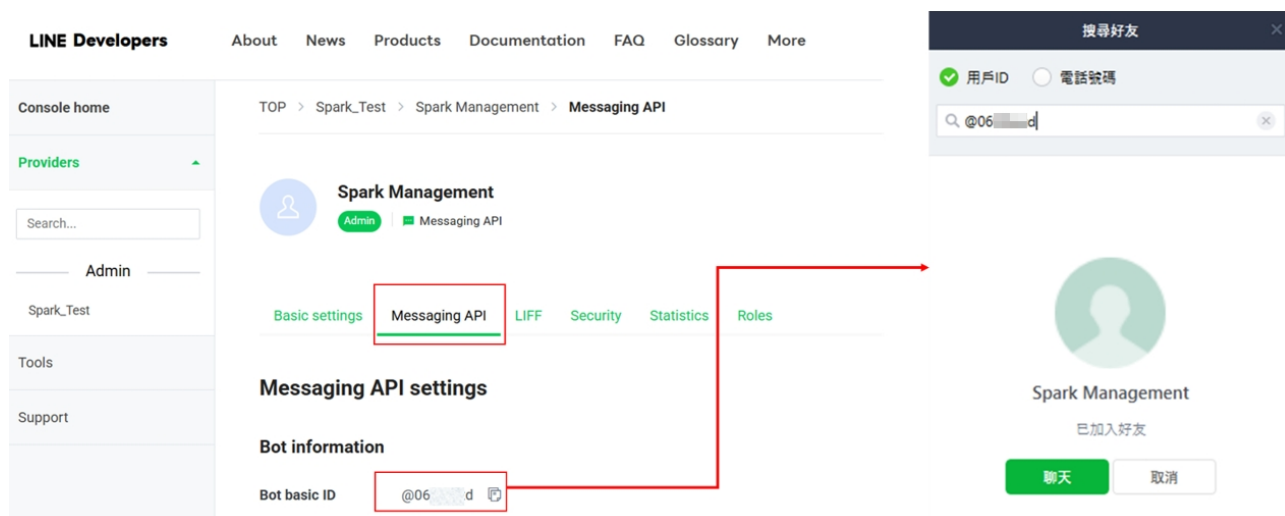
The screenshot shows the homepage of the LINE Developers website. The top navigation bar includes 'LINE Developers', 'About', 'News', 'Products', 'Documentation', 'FAQ', 'Glossary', and 'More'. On the right side of the navigation bar, there is a search icon, a globe icon, and a 'Console' button highlighted with a red box. Below the navigation bar is a large hero image of a woman looking at a laptop. The text 'Connect with {/LINE Developers}' is overlaid on the image. At the bottom left of the hero image, there is a link '/ Start Console >'. The overall design is clean and modern.



Step6: Select the LINE account to which you want to send notifications.



Step7: Click on [Messaging API], and obtain the ID to add the LINE account as a friend.



Step8: Scroll down to the bottom of the page and locate the "Channel Access Token" section. Click [Issue].

Channel access token

Channel access token (long-lived) ?

Issue



Step9: Copy the Channel Access Token to obtain the authentication token.

Channel access token

Channel access token (long-lived) ⓘ

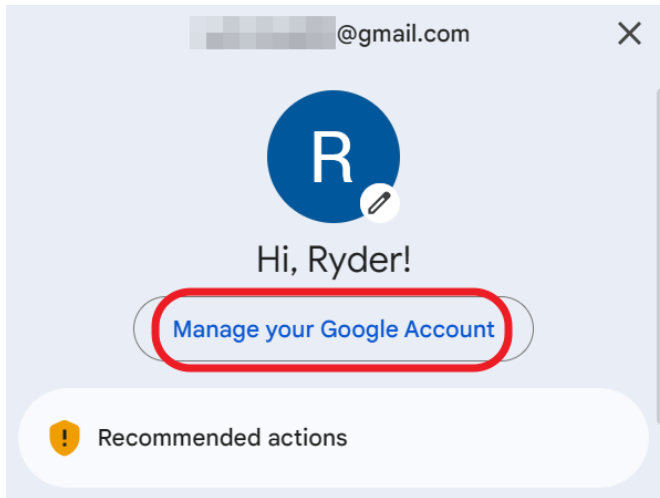
69z8U EAICw	7LC2Fd7vBL6H3tB4trzFVupwWFn/VFUApEdH/XIOQnJx2GTZjF4UxsQeQBzPmjP inyilFU=		Reissue
----------------	---	---	-------------------------

Note: It is recommended to copy and save the token in a memo or text file for easy access when integrating with Argo later.

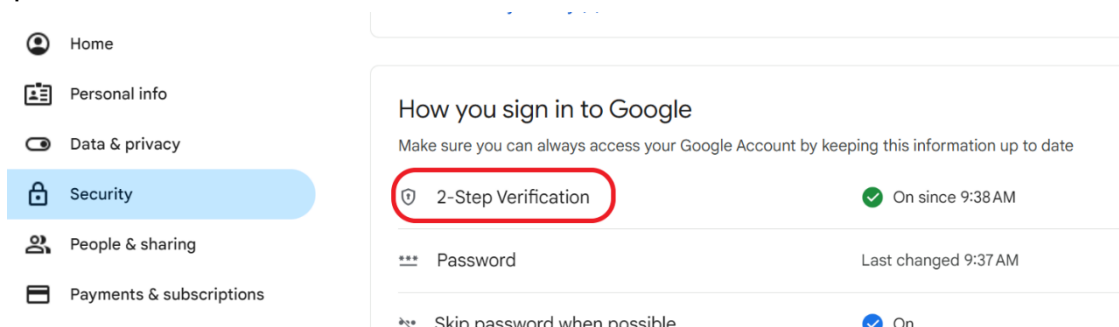


16.2 Applying for Gmail Two-Step Verification for App Password

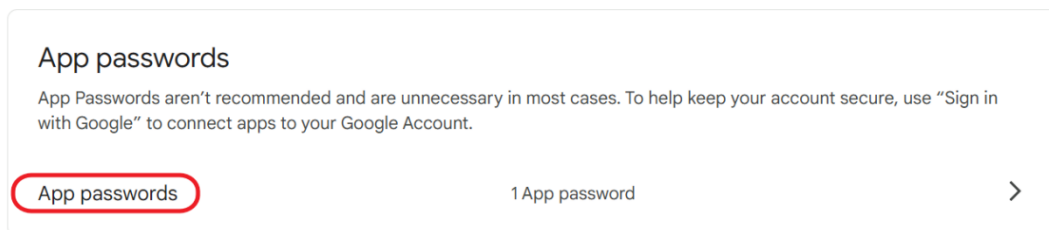
Step1: Go to the Gmail homepage, click on "Manage your Google Account."



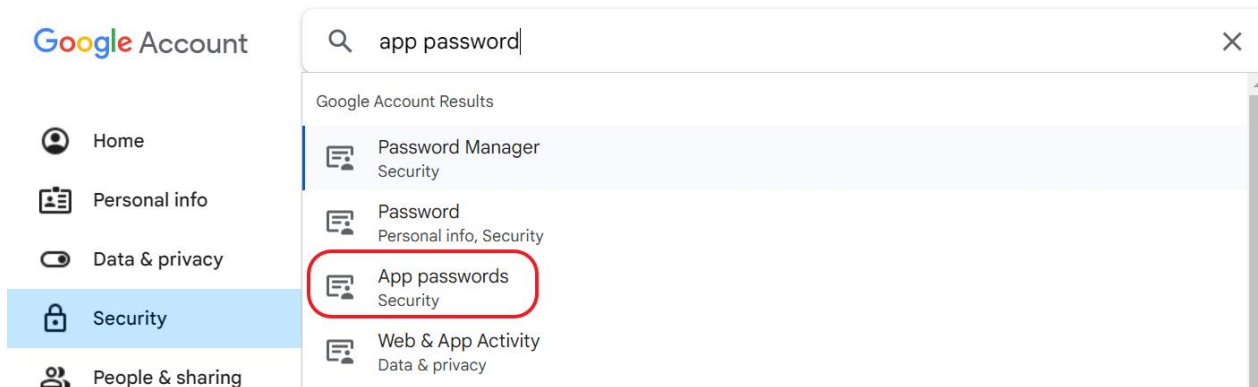
Step2: Click on "Security" to enter two-step verification, then enter your account password.



Step3: On the two-step verification page, click on application password



If the application password does not display correctly, key-in the application password in the search field to set up.



Step4: Create an application name.

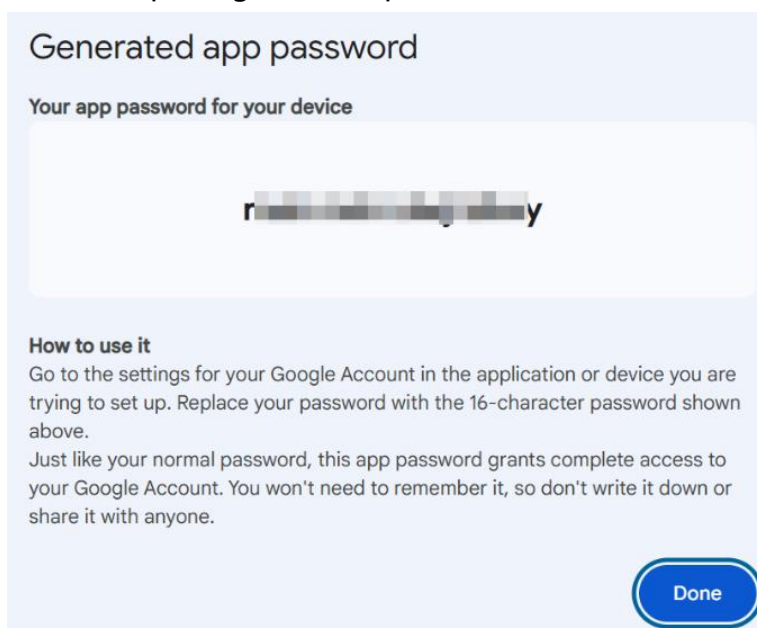
Your app passwords

To create a new app specific password, type a name for it below...

App name
Argo|

Create

Step5: Backup the generated password, then click Finish to complete the setup process.



Note: This password serves as the email password.

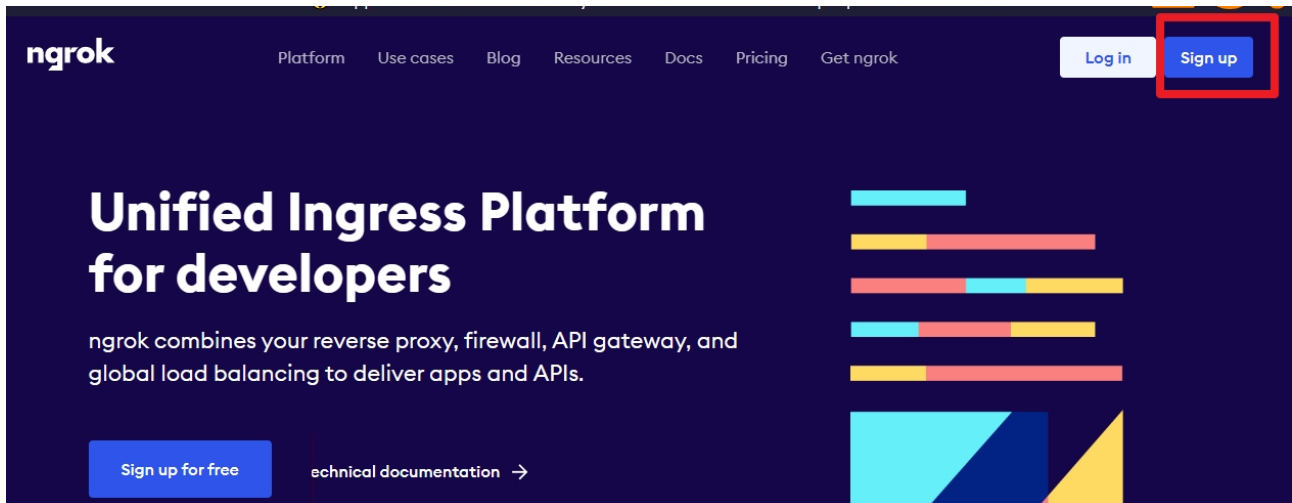


16.3 Applying for Ngrok Account Tutorial

Requires Application on a Computer

Step 1: Use Google or Edge to search for Ngrok and go to the official Ngrok website at <https://ngrok.com/>.

Step 2: Click "Sign Up" to start the process.



Step 3: Enter Ngrok name, email, and password to log in.


ngrok

Sign up

Name

Email

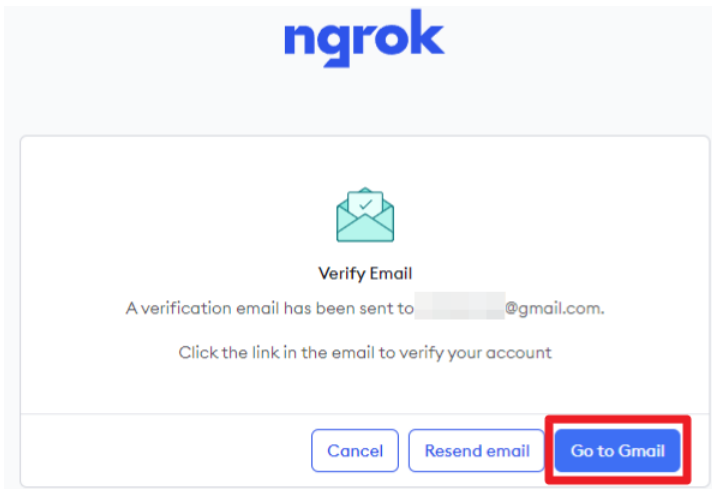
Password

我不是機器人  reCAPTCHA
隱私權 - 條款

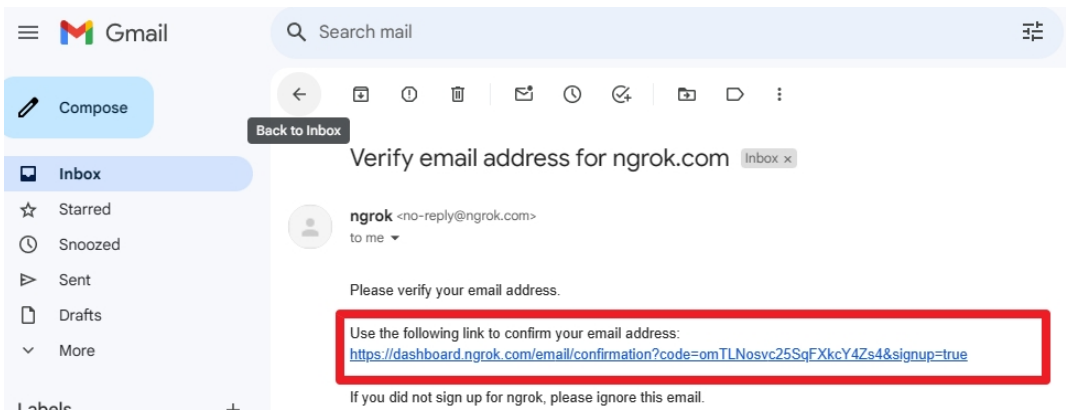
I accept the [terms of service](#) and [privacy policy](#)



Step 4. Go to the email inbox to confirm the account.

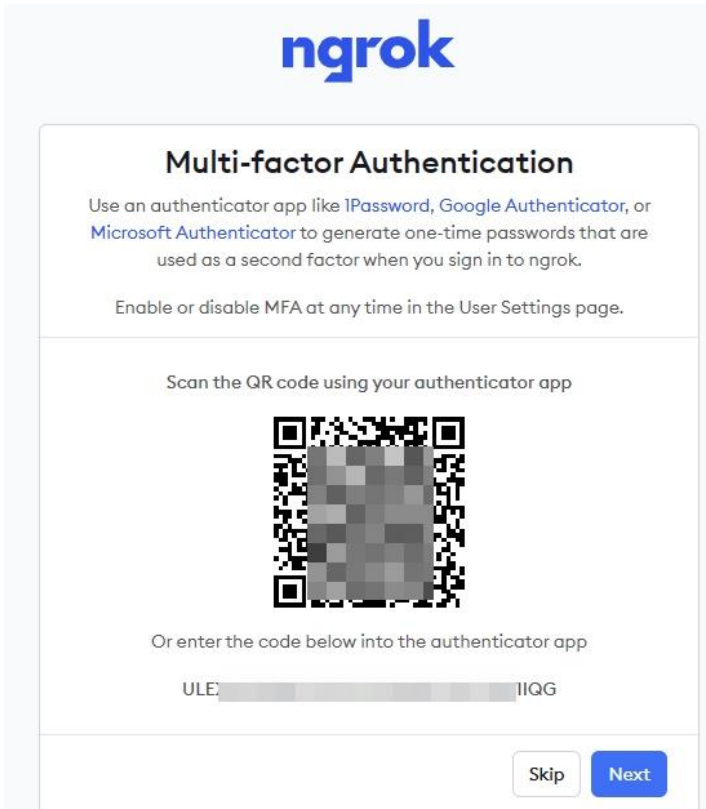


Step 5. Click the link in the email to confirm the account.

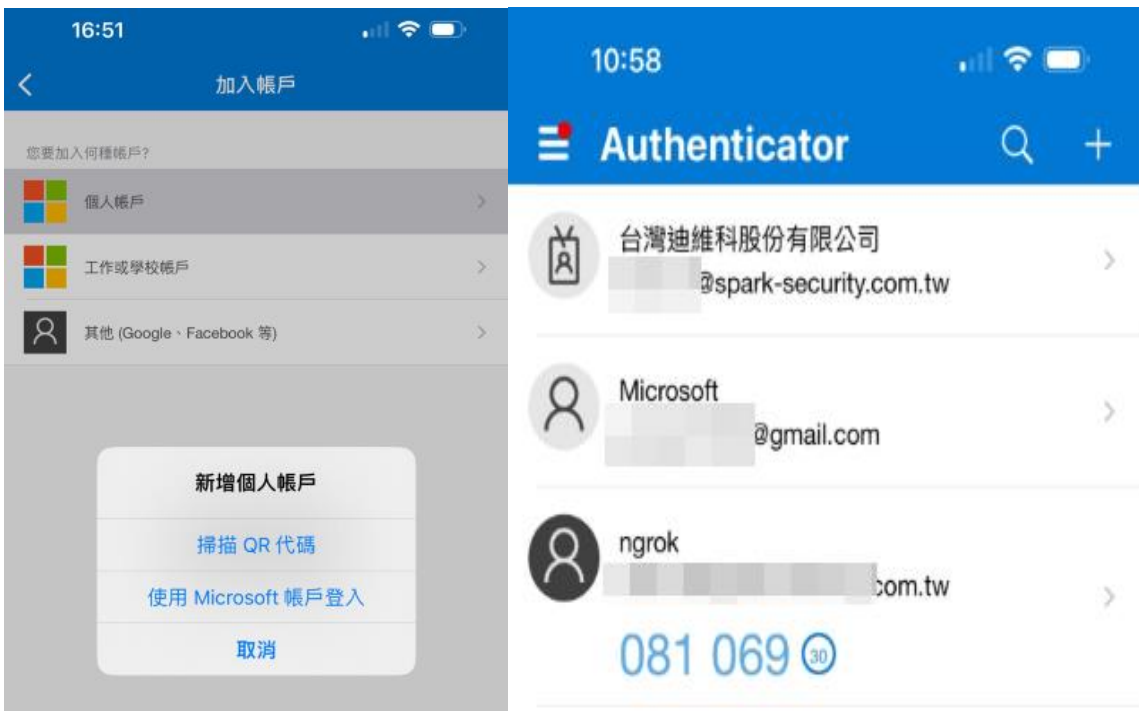


Step 6. Ngrok will display a QR code and authentication code. It is recommended to use a smartphone to scan the QR code for authentication. Click "Next" to proceed.

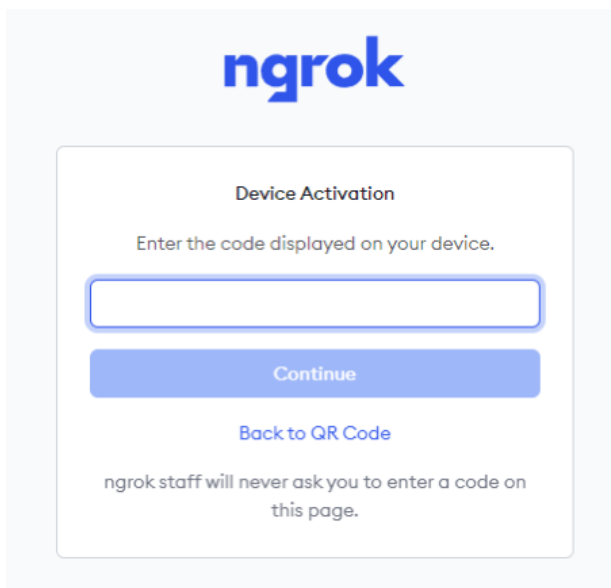
Note: Please complete Step 6 before clicking "Next". You can use the Microsoft Authenticator app or Google Authenticator app to scan for authentication.



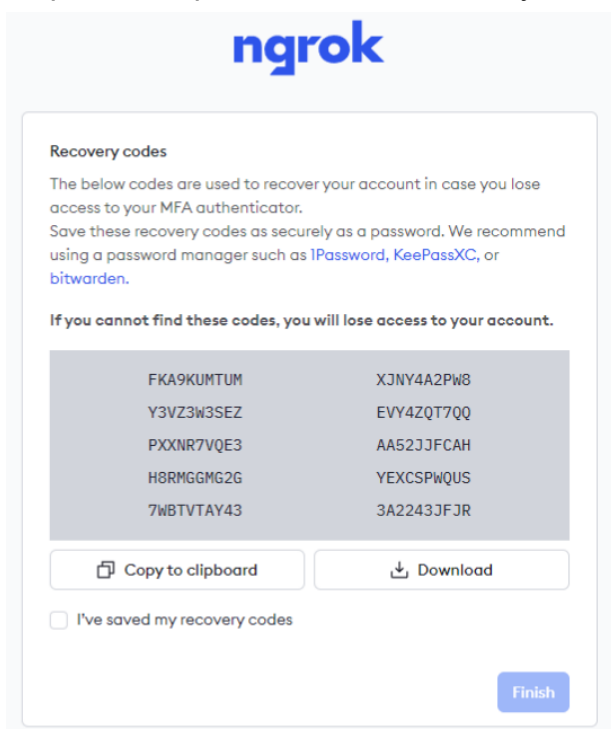
Step 7. Open the Authenticator app and scan the QR code to obtain a six-digit authentication code.



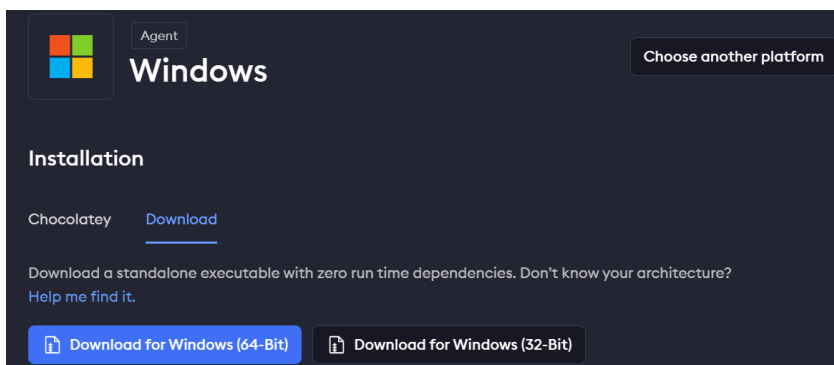
Step 8. Enter the six-digit code generated by the Authenticator app and click "Continue".



Step 9. Backup and store the recovery code for future account management.



Step 10. Download the Ngrok program file.



Step 11. After logging into Ngrok, copy the authentication configuration command and grant permission.



Installation

[Chocolatey](#) Download

Install ngrok via Chocolatey with the following command:

```
choco install ngrok
```

Run the following command to add your authtoken to the default ngrok.yml configuration file.

```
ngrok config add-authtoken 2a2e[REDACTED]_4GVnoDNex5U3KGhkKB1ff
```

Step 12. Open ngrok.exe executable file and paste the authentication configuration command, then press Enter.

```
D:\Download\ngrok-v3-stable-windows-amd64>ngrok config add-authtoken 2a2e[REDACTED]_4GVnoDNex5U3KGhkKB1ff
```

Step 13. Enter **ngrok.exe http 20842** and press Enter to obtain the URL for port forwarding (highlighted in red).

```
ngrok is a command line application, try typing 'ngrok.exe http 80' at this terminal prompt to expose port 80.
D:\Download\ngrok-v3-stable-windows-amd64>ngrok.exe http 20842
```

```
ngrok (Ctrl+C to quit)
Try our new Traffic Inspector Dev Preview: https://ngrok.com/r/ti
Session Status      online
Account             [REDACTED]@gmail.com (Plan: Free)
Version             3.10.0
Region              Japan (jp)
Latency             35ms
Web Interface       http://127.0.0.1:4040
Forwarding           https://7c37-1-171-31-44.ngrok-free.app -> http://localhost:20842
Connections
  ttl   opn   rt1   rt5   p50   p90
   0    0    0.00 0.00 0.00 0.00
```

Step 14. Paste the forwarding port URL into the IP address field of the External Network Settings in Argo, then click "Save" to complete the setup.

EXTERNAL NETWORK SETTINGS

Public ip address and port

External IP

Port Forwarding
 (0 ~ 65535)

Listen port
 (0 ~ 65535)



spark

HQ

Via Antonio Gramsci, No. 86/A
42124 Reggio Emilia, Italy
Tel. +39 0522 929850
info@spark-security.com

Asia office

No. 45, Aikou 2nd Rd., Zhubei City,
302053 Hsinchu County, Taiwan
Tel. +886 3 575 2786
info@spark-security.com.tw

For more information,
please visit us at www.spark-security.com.tw

