

User Manual

Argo Config

V1.7



Confidentiality Notice

Copyright© 2026 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	8
3.1	STATISTICS.....	8
3.2	VIDEO DEVICES	9
3.2.1	Add video devices (Automatic scan/ Manual add).....	9
3.2.2	Edit video devices	12
3.2.3	Delete video device	20
3.2.4	Preview video devices.....	20
3.2.5	Video devices configurations	21
3.2.6	Open device web interface.....	24
3.3	INTERCOMS.....	25
3.3.1	Add Intercoms	25
3.3.2	Edit Intercoms	26
3.3.3	Delete Intercoms	26
3.4	I/O MODULE.....	27
3.4.1	Add I/O module (Auto scan/Manual add).....	27
3.4.2	Edit I/O module.....	29
3.4.2.1	Advantech/ ICPDAS/ Pongee	29
3.4.2.2	Soyal	30
3.4.3	Delete I/O modules	33
3.4.4	Browse I/O modules information and status	33
3.5	SPARK AI DEVICE	34
3.5.1	Add Spark AI Device	35
3.5.1.1	All / Human / Vehicle Detection Devices.....	35
3.5.1.2	LPR Detection Devices.....	35
3.5.1.3	MLPR Detection Devices	35
3.5.1.4	Fire & Smoke Devices	36
3.5.1.5	Generic AI Device.....	38
3.5.1.6	Face Detection.....	39
3.5.1.7	HTTP POST Device	40
3.5.1.8	VLM Device	42
3.5.2	Add Camera to Spark AI Devices	43
3.5.2.1	All/ Vehicle/ Human Detection	43
3.5.2.2	LPR/MLPR Detection.....	44
3.5.2.3	Fire and Smoke Detection.....	45
3.5.2.4	Generic AI	45
3.5.2.5	Face Detection.....	46
3.5.2.6	Spark VLM.....	47
3.5.3	Edit Spark AI Devices.....	48
3.5.3.1	All/Human/Vehicle – Parameter Settings	50
3.5.3.2	Taiwan License Plate Device - Parameter Settings.....	53
3.5.3.3	Multi-country License Plate Device - Parameter Settings-	55



3.5.3.4	Fire and Smoke Detection - Parameter Settings Description.....	57
3.5.3.5	General AI Device - Parameter Settings Description	63
3.5.3.6	Face Detection - Parameter Settings Description.....	64
3.5.3.7	VLM Detection - Parameter Settings Description	65
3.5.4	Delete Spark AI Device Stream Analysis	66
3.5.5	Delete Spark AI Device	66
3.5.6	Edit Common Settings for Spark AI Devices	67
3.5.7	INFO	68
3.6	OTHER SETTINGS.....	69
3.6.1	Database settings	69
3.6.2	License plate recognition upload settings	70
3.6.3	AI Analytics	71
3.6.4	External Network Settings	71
3.6.5	Web server settings.....	72
3.7	STORAGE	73
3.7.1	Add storage	73
3.7.2	Edit storage.....	74
3.7.3	Delete storage	74
3.8	INFORMATION	75
3.8.1	Information	75
3.8.2	Installed services	75
3.9	SERVER.....	76
3.9.1	Primary server and secondary servers.....	76
3.9.2	Add server.....	77
3.9.3	Delete server	80
3.10	VIEW MODE	81
4.	USER MANAGEMENT	82
4.1	PASSWORD SETTINGS	82
4.2	GROUPS.....	83
4.2.1	Create groups.....	83
4.2.2	Set schedules for each group	83
4.2.3	Set permissions for each group:.....	84
4.2.4	Delete group	87
4.3	USER.....	88
4.3.1	Add user	88
4.3.2	Delete User.....	89
4.4	CLIENT CONNECTION INFORMATION	89
5.	HEALTH DOCTOR.....	90
5.1	SYSTEM HEALTH CHECK CONFIGURATION	90
5.2	ADD RESPONSE ACTION.....	91
5.2.1	Send email	92
5.2.2	Line Notify	94
5.3	EDIT RESPONSE ACTION	95
5.4	DELETE RESPONSE ACTION	95
5.5	EXECUTE RESPONSE ACTION	96
6.	EVENT AND MANAGEMENT	97
6.1	ADD/EDIT/COPY/DELETE EVENT	98
6.2	EVENT BEHAVIOR.....	100
6.3	TRIGGER CONDITIONS	101
6.3.1	Add trigger condition	101



6.3.2	Advanced Setting for Trigger Conditions	106
6.3.3	Edit trigger condition	107
6.3.4	Delete trigger condition	107
6.4	RESPONSE ACTION	108
6.4.1	Response action schedule	108
6.4.2	Add response action	109
6.4.3	Edit response action	117
6.4.4	Delete response action	117
6.4.5	Execute response action	117
6.5	SET THE EVENT AS ALARM	118
6.5.1	Edit alarm setting	119
7.	ACCESS CONTROL	123
7.1	ADD/EDIT/DELETE LIST	123
7.2	ACCESS ID.....	124
7.2.1	Add access ID	124
7.2.2	Edit access ID	125
7.2.3	Deactivate/Clear access ID	127
7.2.4	Export/Import access ID.....	128
8.	VIDEO ANALYTICS DATA COLLECTION.....	131
8.1	SENS CAM SETTINGS.....	131
8.1.1	Login settings	131
8.1.2	Image setting	132
8.1.3	Analytics settings	133
8.2	VIDEO ANALYTICS DATA COLLECTION SETTINGS.....	135
8.2.1	Add video analytics parameters.....	135
8.2.2	Set video analytics parameters.....	135
8.2.3	Delete video analytics parameter	136
9.	MATCH DATABASE	137
10.	BACKUP AND RESTORE	138
10.1	BACKUP.....	138
10.2	RESTORE	138
10.3	SCHEDULED BACKUP	139
11.	LICENSE	140
11.1	INFORMATION	140
11.2	MANAGE LICENSE	140
11.3	CHANNEL LICENSE KEY	141
11.4	INTEGRATED DEVICES.....	141
12.	LOG.....	142
12.1	DATA TRACE	142
12.2	SYSTEM LOG.....	144
12.3	DETAILED LOG.....	146
13.	ARGO CLIENT	147
14.	OPTIONS	148
14.1	LANGUAGE	148
14.2	INTERFACE	148



14.3	RENDERING.....	149
14.4	USER INTERACTION MODE.....	151
14.5	WATERMARK.....	152
14.6	SYSTEM.....	153
15.	USER.....	154
15.1	CHANGE PASSWORD.....	154
15.2	LOGOUT/CLOSE.....	154
16.	ABOUT	155
17.	OTHER.....	156
17.1	APPLYING FOR LINE MESSAGE TOKEN	156
17.2	APPLYING FOR GMAIL TWO-STEP VERIFICATION FOR APP PASSWORD.....	160
17.3	APPLYING FOR NGROK ACCOUNT TUTORIAL	162



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

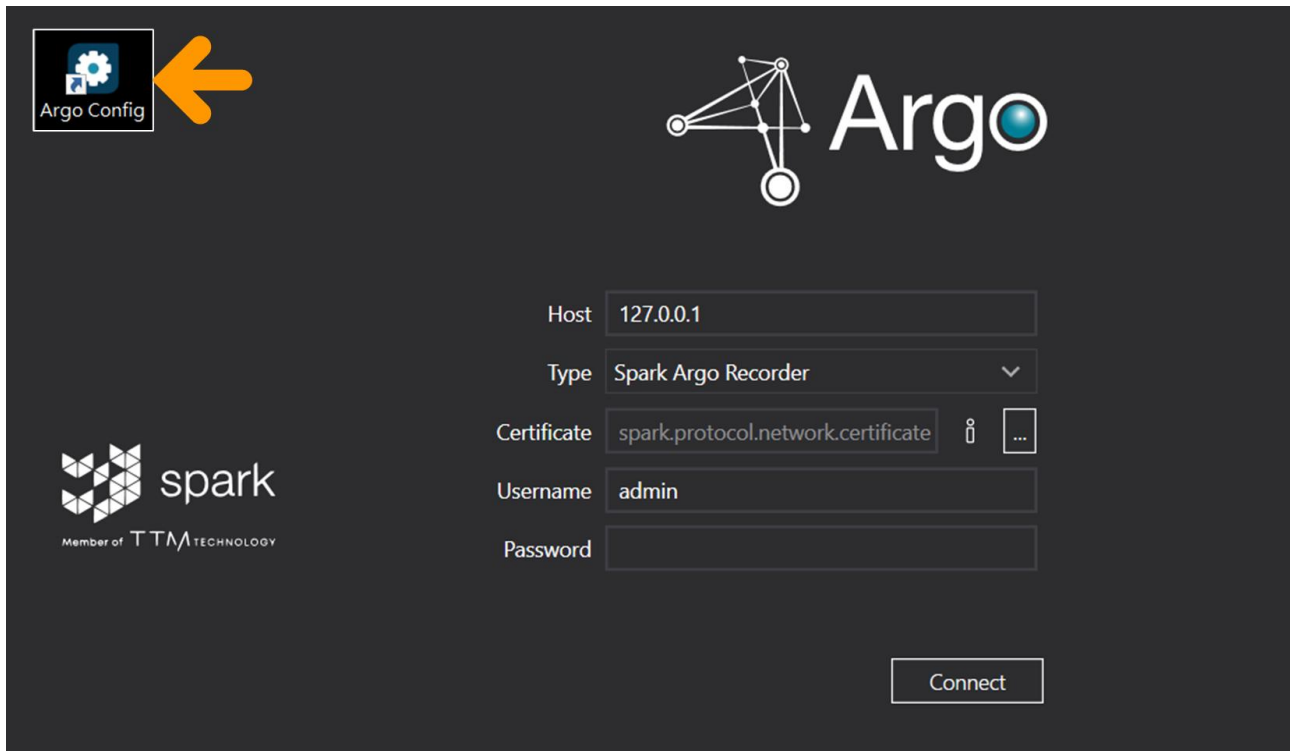
- Spark Client + Config minimum system requirements
CPU: Intel Core i5 @ 2.7GHz RAM 4GB
Disk space: 500 MB free disk space
Graphics Card: 1GHz, 1GB RAM
Screen Resolution: 1920x1080 Network Card Gigabit Ethernet
Operating System: Windows 11 (64-bit)
- Spark Player minimum system requirements
CPU: Intel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



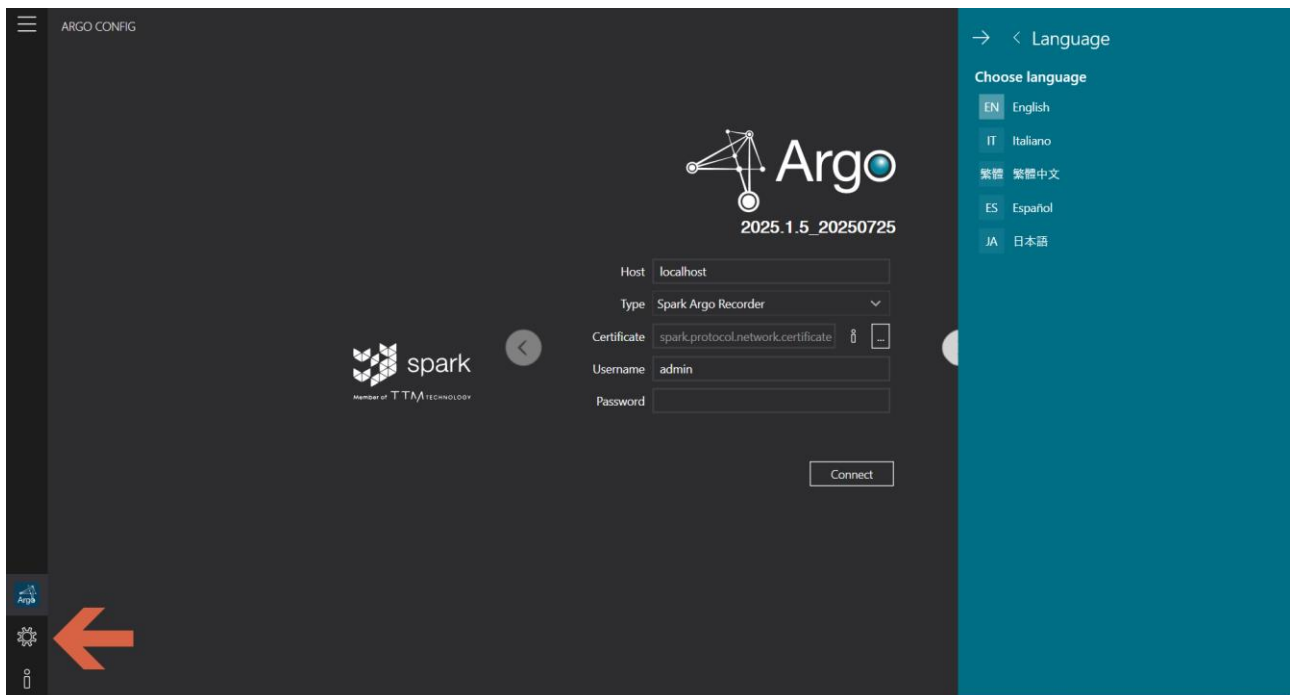
2. START

2.1 Log in

Step1: Double click Argo config to open login window



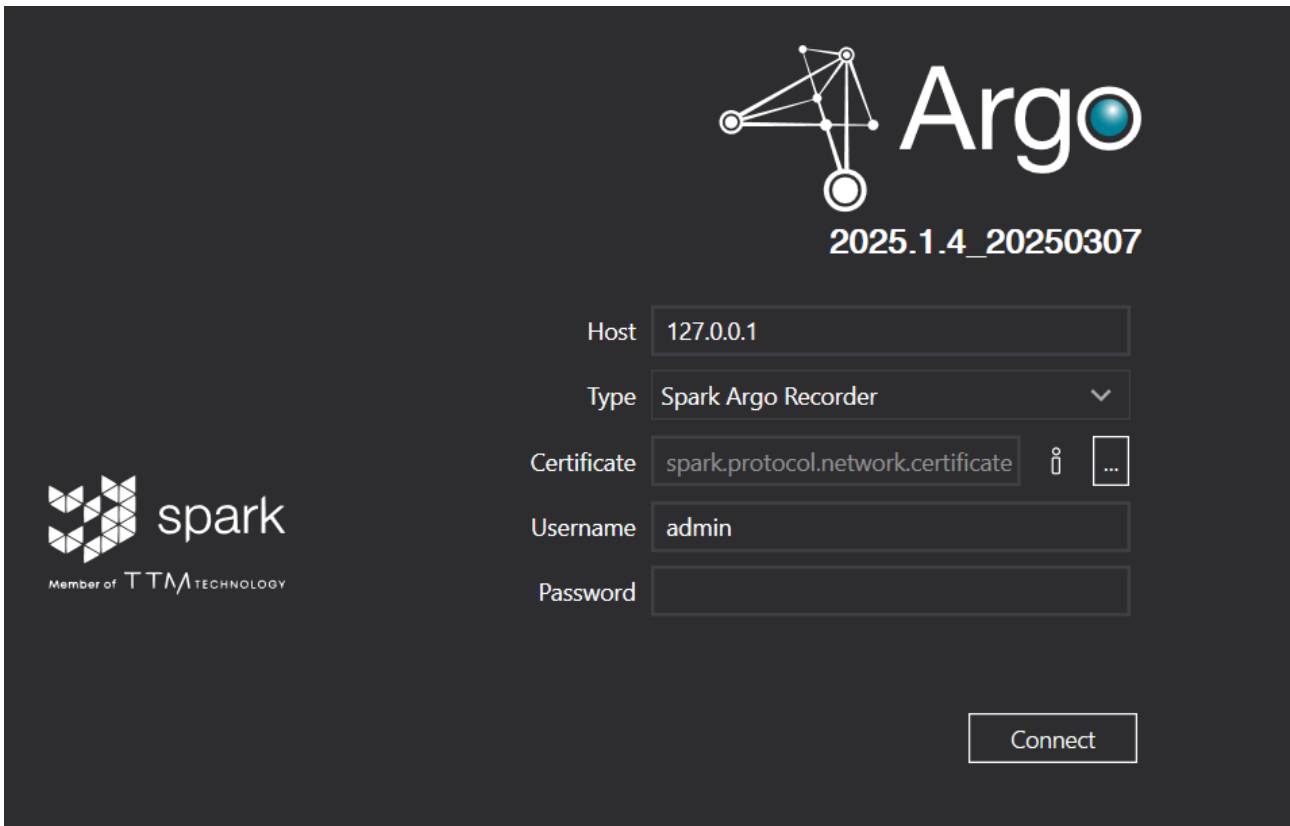
Step2: Select language



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



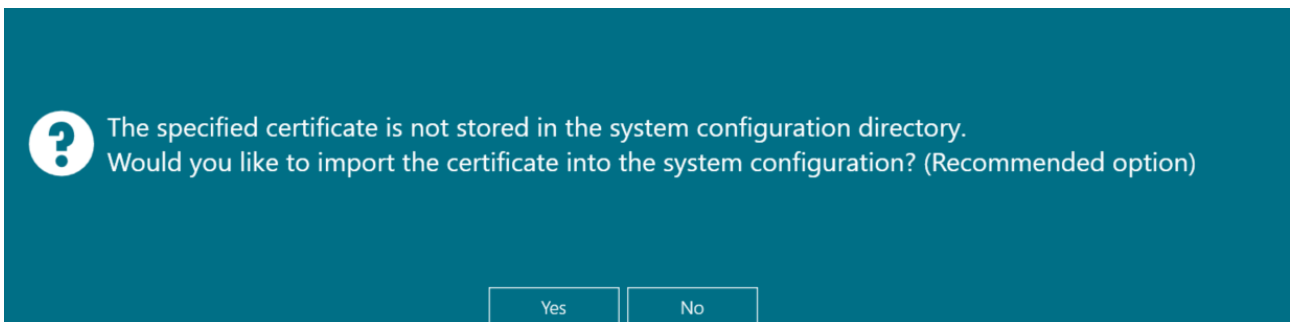
Step3: Log in Argo config



The image shows the Argo login configuration interface. At the top right is the Argo logo and version number 2025.1.4_20250307. On the left is the Spark logo with the text 'Member of TTM TECHNOLOGY'. The main area contains a form with the following fields: Host (127.0.0.1), Type (Spark Argo Recorder), Certificate (spark.protocol.network.certificate), Username (admin), and Password (empty). A 'Connect' button is at the bottom right.

- 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 image shows a dialog box with a teal background. It contains a question mark icon and the text: 'The specified certificate is not stored in the system configuration directory. Would you like to import the certificate into the system configuration? (Recommended option)'. At the bottom are 'Yes' and 'No' buttons.



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.

Change User Password

Username: admin

Old password: [5 masked characters]

New password: [10 masked characters]

Confirm password: [10 masked characters]

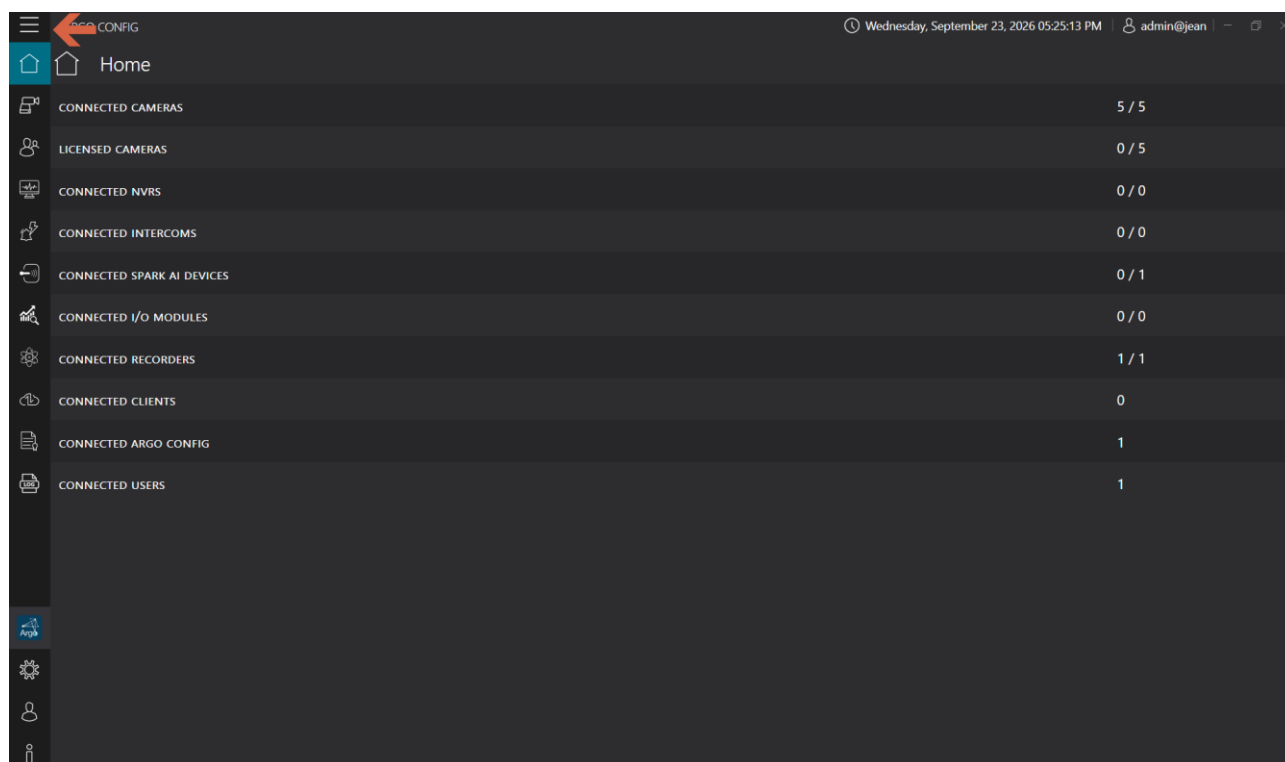
Change password Cancel

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

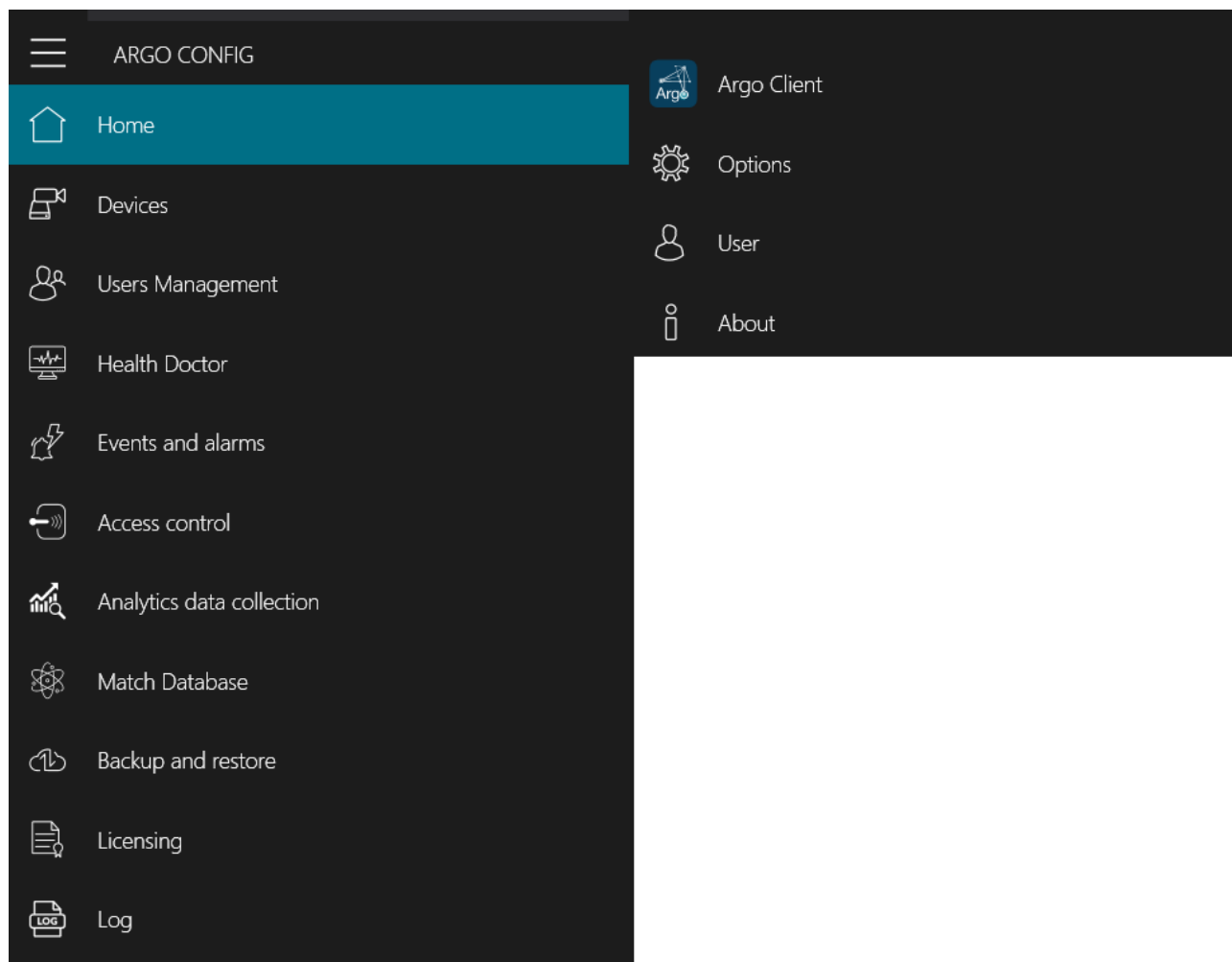
- When using single login interface, users only need to insert the changed password to log in.
- When using quick login interface, users must change the default password to the changed password to log in.



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/Match Database/Licensing/Log/Argo client/Options/User/ About



3. DEVICES

3.1 Statistics

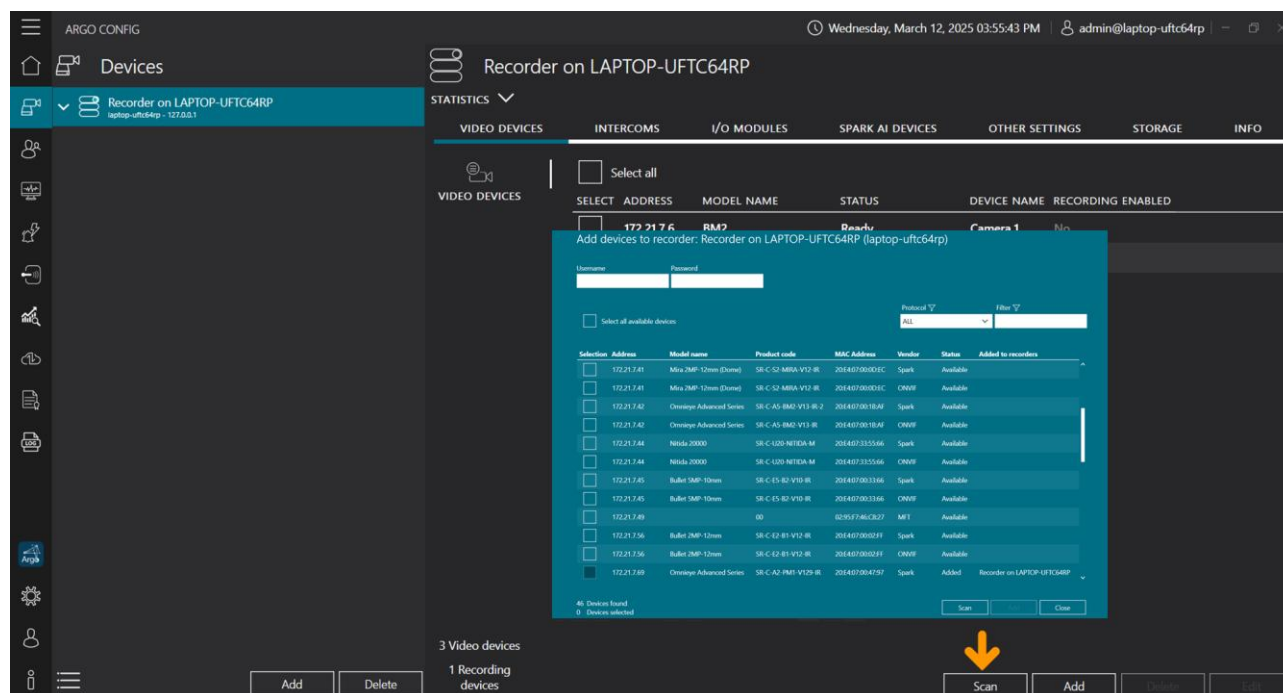
- Click on **[System overview]**
- Browse device status on Statistics: CPU/memory/Storage/Device



3.2 Video Devices

3.2.1 Add video devices (Automatic scan/ Manual add)

A. Automatic scan



- 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

The screenshot shows the ARGO CONFIG web interface. A modal dialog titled "Add device to recorder manually" is open. It contains the following fields: "Brand" (a dropdown menu with "ONVIF" selected), "Name" (a text input), "Device Index" (a text input with "0"), "Username" (a text input), "Password" (a text input), "Address IP, DNS" (a text input), "Port (0 or empty value means default)" (a text input with "0"), and a "Disable IP range" toggle switch which is currently turned off. Below the toggle is a text input for "End IP Address". At the bottom of the dialog are "Add" and "Cancel" buttons. An orange arrow points to the "Add" button. In the background, the "VIDEO DEVICES" section of the interface is visible, showing a list of devices and a status bar at the bottom with "Add" and "Delete" buttons.

- 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
 0

Username Password

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

Disable IP range ☒

End IP Address

RTSP URL

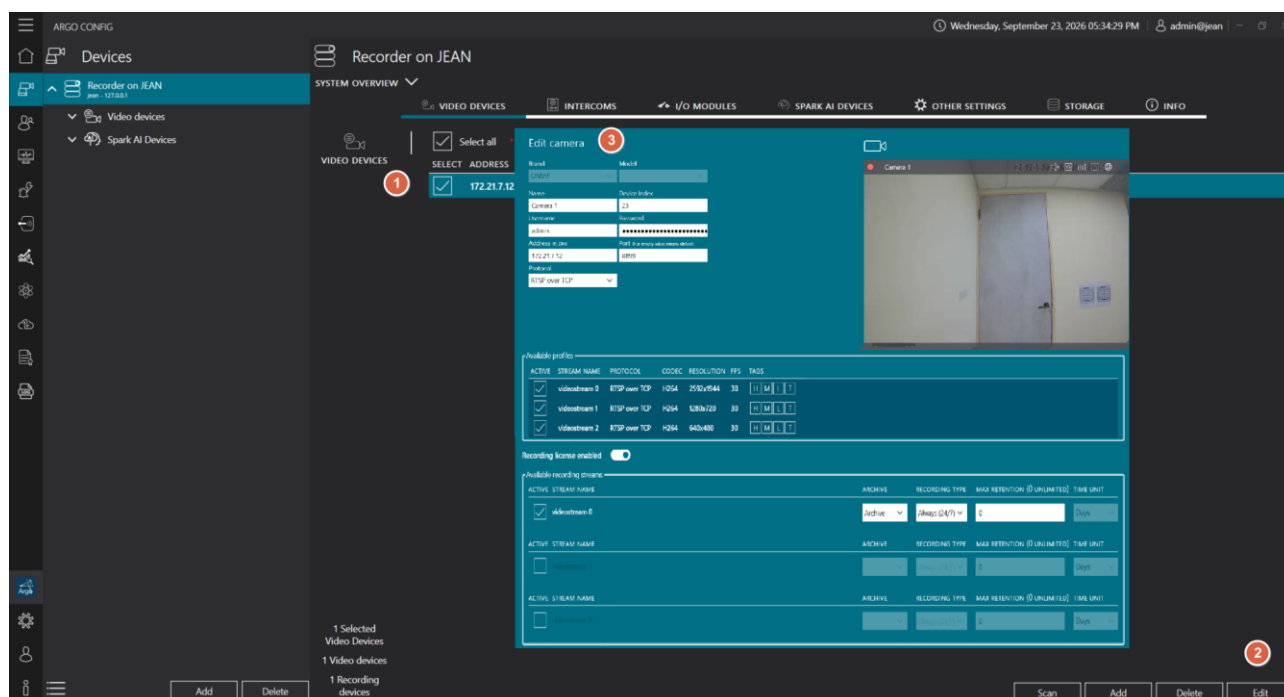
ACTIVE	URL
☐	rtsp://\$USERNAME:\$PASSWORD@\$IPADDRESS:\$RTSPPORT/media1.amp
☐	rtsp://\$USERNAME:\$PASSWORD@\$IPADDRESS:\$RTSPPORT/media2.amp
☐	rtsp://\$USERNAME:\$PASSWORD@\$IPADDRESS:\$RTSPPORT/media3.amp

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' s IP address or DNS.
- RTSP Port: Default is 0.
- Username: Enter the device' s 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).

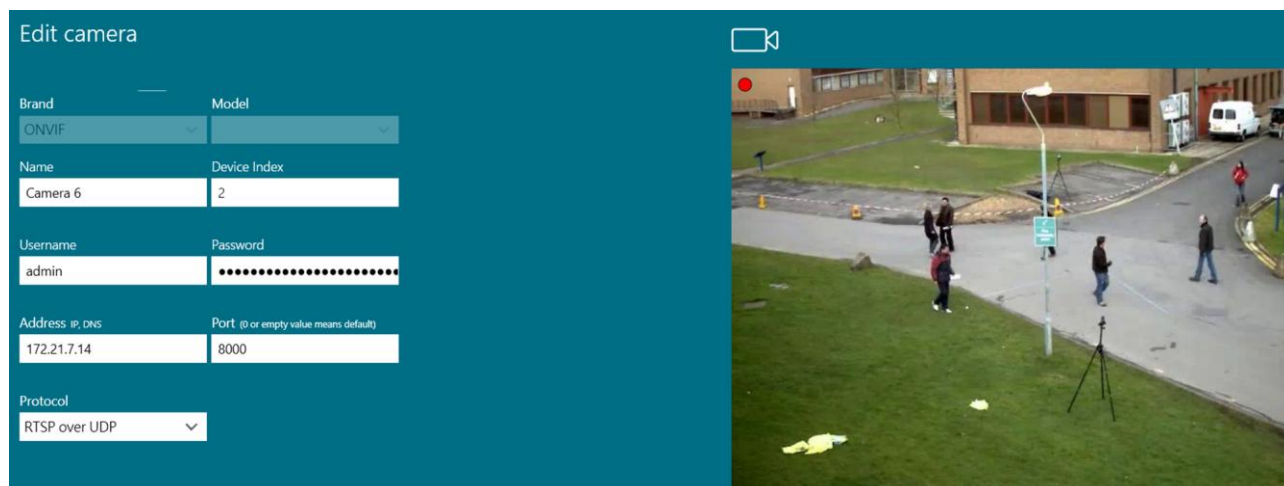


3.2.2 Edit video devices



- 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

Available profiles						
ACTIVE	STREAM NAME	PROTOCOL	CODEC	RESOLUTION	FPS	TAGS
☒	videostream 0	RTSP over TCP	H264	1920x1080	30	☐ H ☐ M ☐ L ☐ T
☒	videostream 1	RTSP over TCP	H264	1280x720	5	☐ H ☐ M ☐ L ☐ T
☒	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
☒	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 RETENTION
☐	videostream ProfileToken_2		Always (24/7)	0

Edit days

Monday	☐	Saturday	☐
Tuesday	☐	Sunday	☐
Wednesday	☐		
Thursday	☐		
Friday	☐		

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.



Recording on event : AI_2.120_Object ▾

Pre-recording time : Seconds 0 + -

Post recording : Seconds 0 + -

- 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.

ACTIVE	STREAM NAME	ARCHIVE	RECORDING TYPE	MAX RETENTION (0 UNLIMITED)	TIME UNIT	EDGE RECOVER
☒	videostream 0	Archive ▾	Always (24/7) ▾	0	Days ▾	Recover from ▾
☐	videostream 1	Archive ▾	Always (24/7) ▾	0	Days ▾	Recover from ▾

- 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

OMNIEYE SECURITY

Live View | Playback | Configuration | English

Advanced Configuration

- Encode
- Image
- Lens Control
- Video
- Network
- System**
- Account
- Event Source
- Video Analytics
- Event Setting

Date & Time | Audio | Firmware | Initialization | OSD | Events

Basic Setting

Current Server time
2024/06/07 16:44:38

Synchronization Mode

- ☐ Manually setting Date and Time
Date: 2024/05/23 Time: 10:40:57
- ☒ Synchronize with PC
Date: 2024/06/07 Time: 16:44:38
- ☐ Synchronize with NTP Server

Time Zone Setting

Time Zone GMT+8

- 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

Live View | Playback | Configuration | English

Advanced Configuration

- Encode
- Image
- Lens Control
- Video
- Network
- System
- Account
- Event Source**
- Video Analytics
- Event Setting

Alarm | Audio | Defocus | Motion | Network | **Schedule** | Tamper | mSD healthiness

Basic Setting

Enable ☒ Mode Regular Trigger Interval 5 (5~3600)Sec

Handlers

Alarm Out	Audio	Snapshot	Recording
☐ 1	Audio Out ☐ Audio Sound 1	☐ Store to Edge ☐ Store to FTP	☒ Edge Record

Email

Enable ☐
Subject

- 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

Live View | Playback | Configuration | English

Alarm Out | Email | FTP | Record Setting | SD Card | Snapshot | Sound | HTTP Generic Event

Advanced Configuration

- Encode
- Image
- Lens Control
- Video
- Network
- System
- Account
- Event Source
- Video Analytics
- Event Setting**

Basic Setting

Record Type: Video

Record Status: Continuous

Clip Size: 50 (50~100 MB)

Record Codec: 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

Live View | Playback | Configuration | English

Alarm Out | Email | FTP | Record Setting | **SD Card** | Snapshot | Sound | HTTP Generic Event

Advanced Configuration

- Encode
- Image
- Lens Control
- Video
- Network
- System
- Account
- Event Source
- Video Analytics
- Event Setting**

Basic Setting

Overwrite: On (Reserve 120MB)

Status: Working normally

Capacity: 234059(MB)

Free Space: 194333(MB)

Encrypted Mode: Off

SD Format: **Format**

Download SD File

June 2024

Select All ☐ No Folder name

- 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	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

ARGO CONFIG

Recorder on LAPTOP-UFTC64RP

STATISTICS

VIDEO DEVICES INTERCOMS I/O MODULES SPARK AI DEVICES OTHER SETTINGS STORAGE INFO

VIDEO DEVICES

Select all

SELECT	ADDRESS	MODEL NAME	STATUS	DEVICE NAME	RECORDING ENABLED
☐	172.21.7.6	RM2	Ready	Camera 1	No

Add devices to recorder: Recorder on LAPTOP-UFTC64RP (laptop-uftc64rp)

Username Password

☐ Select all available devices

Protocol V Filter V

All

Selection	Address	Model name	Product code	MAC Address	Vendor	Status	Added to recorders
☐	172.21.7.41	Mira 2MP-12mm (Exire)	SR-C-S2-MIRA-V12-B	20E4D70D03EC	Spark	Available	
☐	172.21.7.41	Mira 2MP-12mm (Exire)	SR-C-S2-MIRA-V12-B	20E4D70D03EC	CHW	Available	
☐	172.21.7.42	Omnieye Advanced Series	SR-C-A5-IM2-V13-B-2	20E4D70D18AF	Spark	Available	
☐	172.21.7.42	Omnieye Advanced Series	SR-C-A5-IM2-V13-B	20E4D70D18AF	CHW	Available	
☐	172.21.7.44	Nitida 20000	SR-C-U20-NITEA-M	20E4D73355A6	Spark	Available	
☐	172.21.7.44	Nitida 20000	SR-C-U20-NITEA-M	20E4D73355A6	CHW	Available	
☐	172.21.7.45	Bullet 2MP-10mm	SR-C-E5-B0-V10-B	20E4D70D13A6	Spark	Available	
☐	172.21.7.45	Bullet 2MP-10mm	SR-C-E5-B0-V10-B	20E4D70D13A6	CHW	Available	
☐	172.21.7.49		00	029577A6C827	MIT	Available	
☐	172.21.7.56	Bullet 2MP-10mm	SR-C-E2-B1-V12-B	20E4D70D03FF	Spark	Available	
☐	172.21.7.56	Bullet 2MP-10mm	SR-C-E2-B1-V12-B	20E4D70D03FF	CHW	Available	
☒	172.21.7.69	Omnieye Advanced Series	SR-C-A2-IM2-V12-B	20E4D70D4797	Spark	Added	Recorder on LAPTOP-UFTC64RP

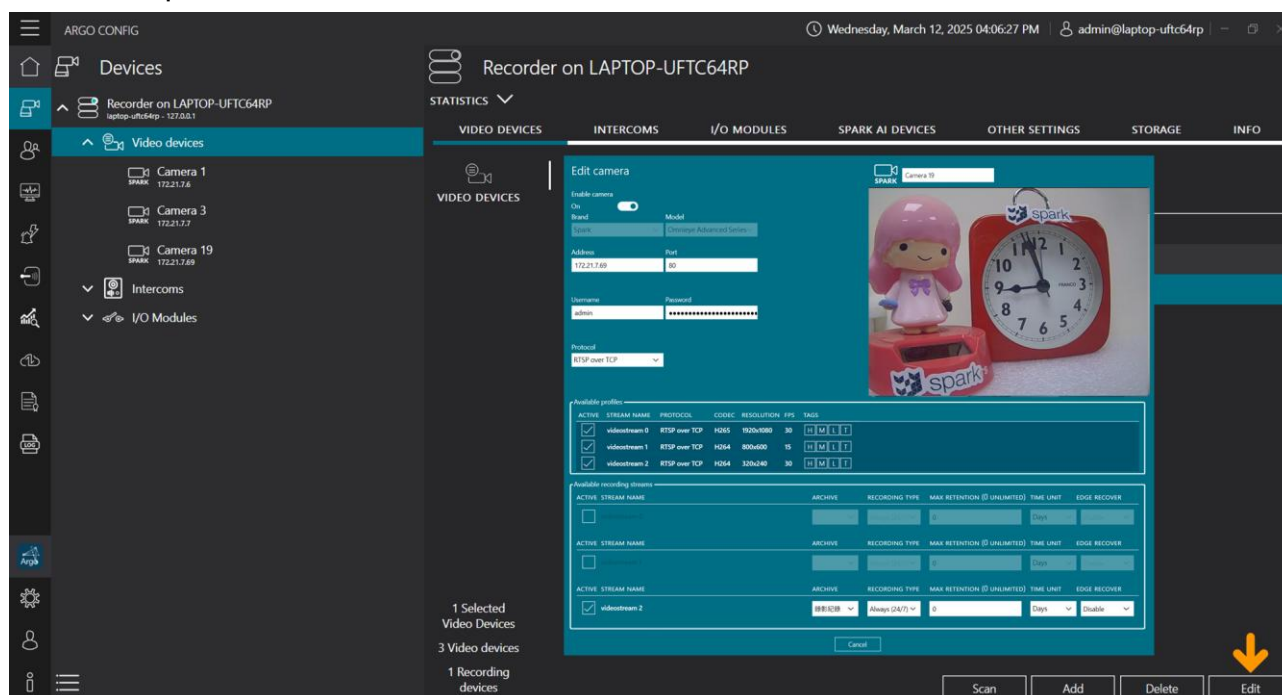
3 Video devices
1 Recording devices

Add Delete

Scan Add



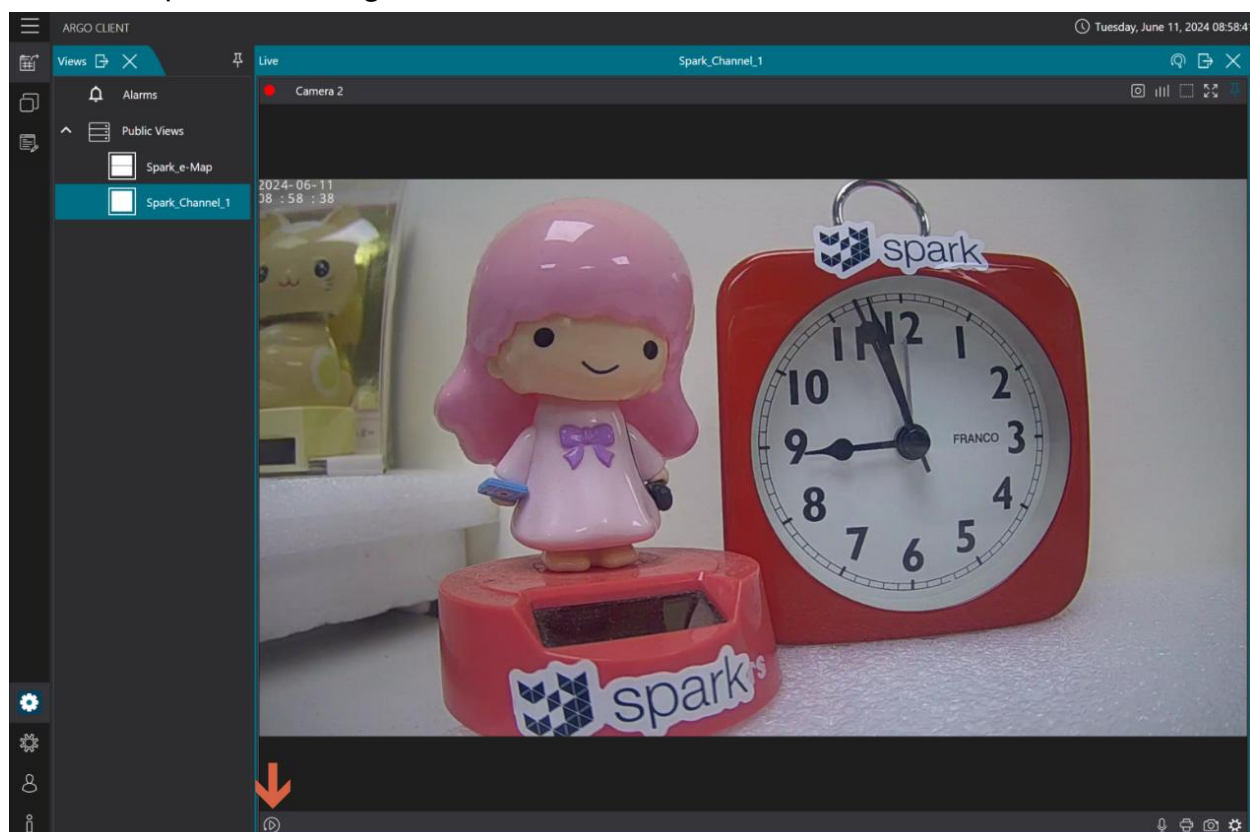
Step 7. Edit device - video devices



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

c. Argo Client system configuration

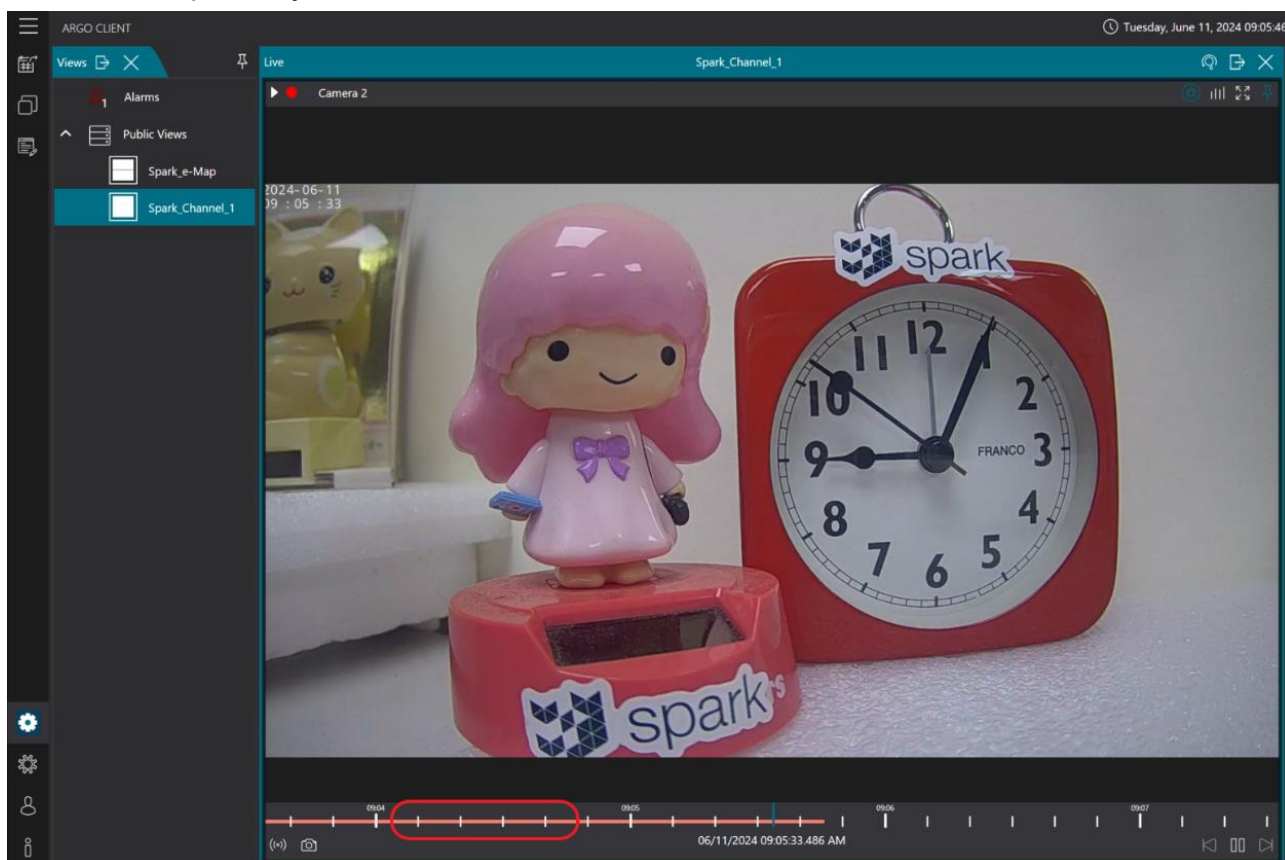
Step 8. monitoring interface





- 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

ARGO CONFIG

Wednesday, March 12, 2025 04:36:19 PM | admin@laptop-uftc64rp

Recorder on LAPTOP-UFTC64RP

STATISTICS

VIDEO DEVICES INTERCOMS I/O MODULES SPARK AI DEVICES OTHER SETTINGS STORAGE INFO

VIDEO DEVICES

Select all * Only modify up to 32 cameras at a time! *

SELECT	ADDRESS	MODEL NAME	STATUS	DEVICE NAME	RECORDING ENABLED
☒	172.21.7.6	BM2	Ready	Camera 1	No
☐	172.21.7.7	DF1	Ready	Camera 3	No
☐	172.21.7.69	PM1	Ready	Camera 19	Yes

1 Selected Video Devices
3 Video devices
1 Recording devices

Add Delete Scan Add Delete Edit

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

3.2.4 Preview video devices

SPARK

Camera 2

PREVIEW

Camera 2

2024-06-11 09:13:23 AM

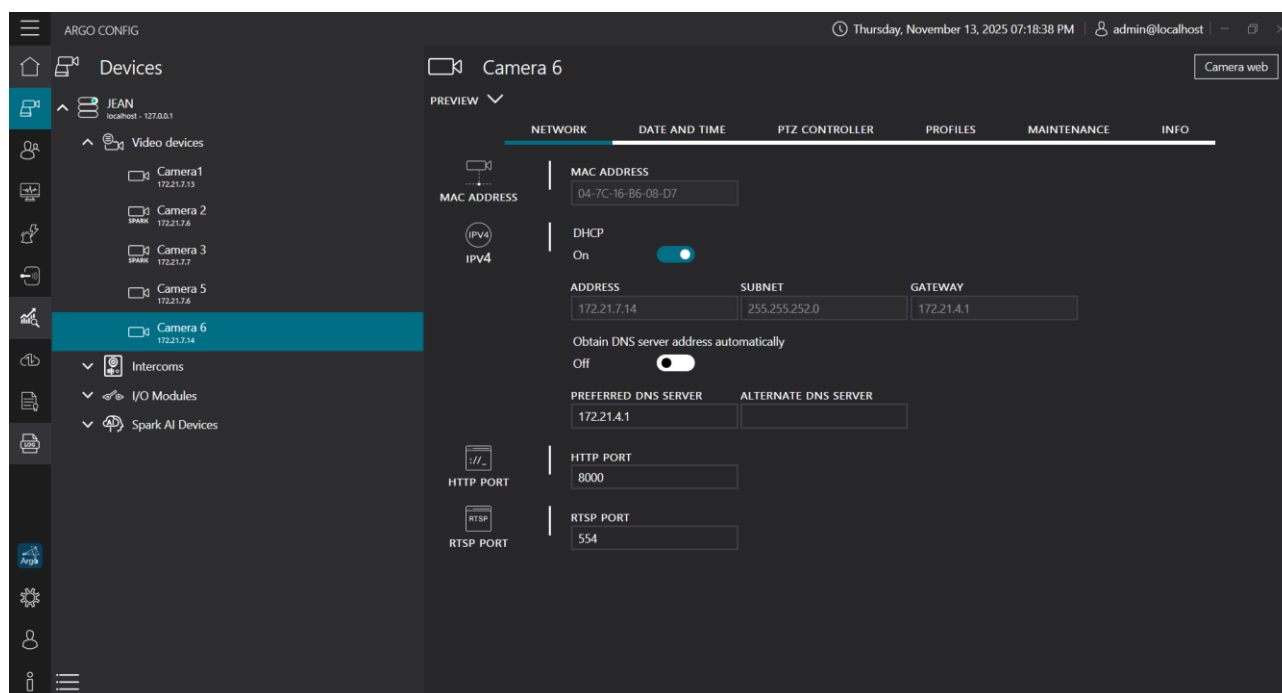
MAC ADDRESS 20:e4:07:00:47:7a

NETWORK DATE AND TIME PROFILES ANALYTICS MAINTENANCE INFO

B. Click **[Preview]**

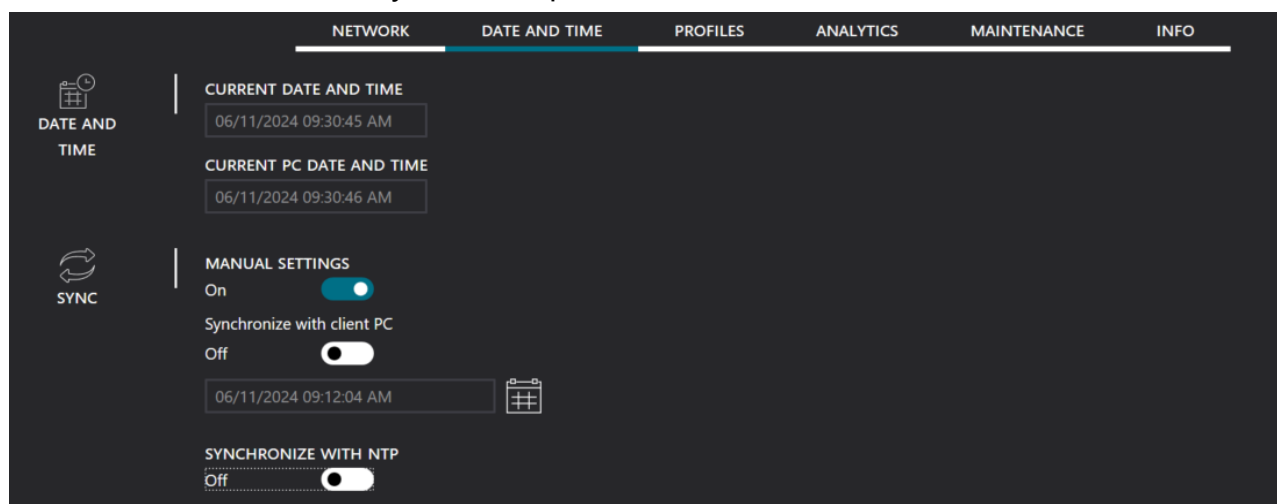


3.2.5 Video devices configurations



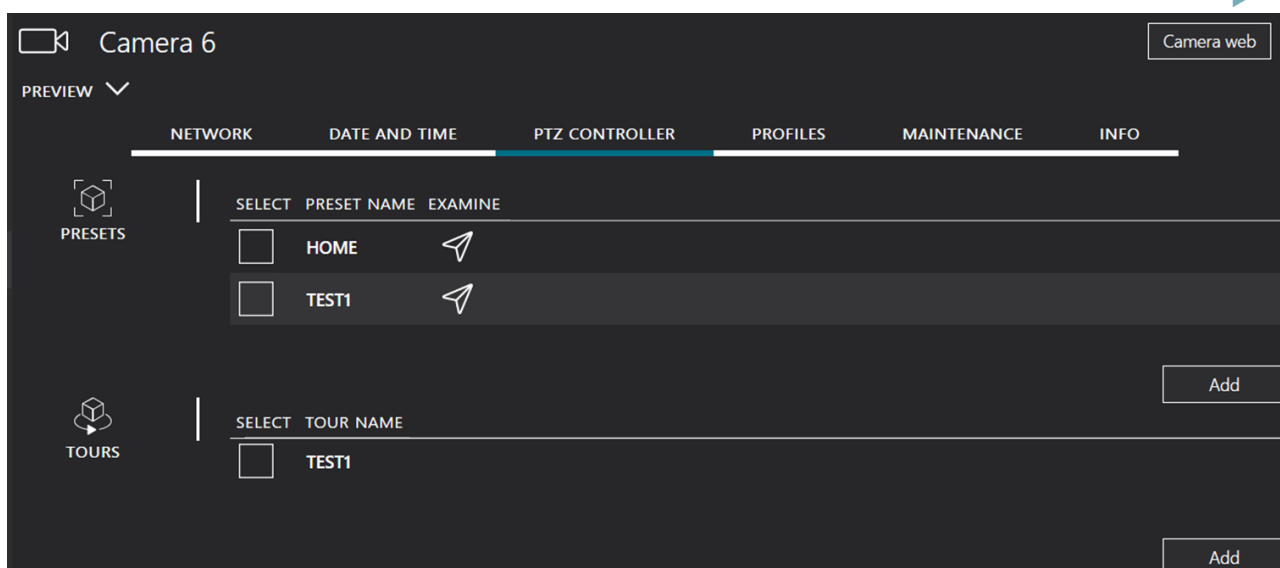
A. Network: edit device network settings

- 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.



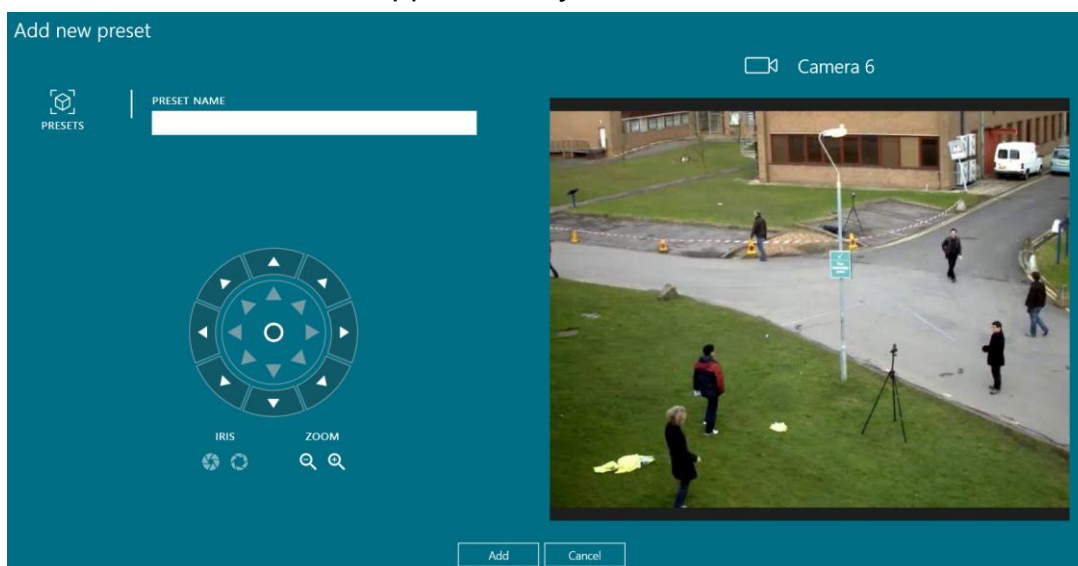
B. Date and time: Edit device date and time settings.

- 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.

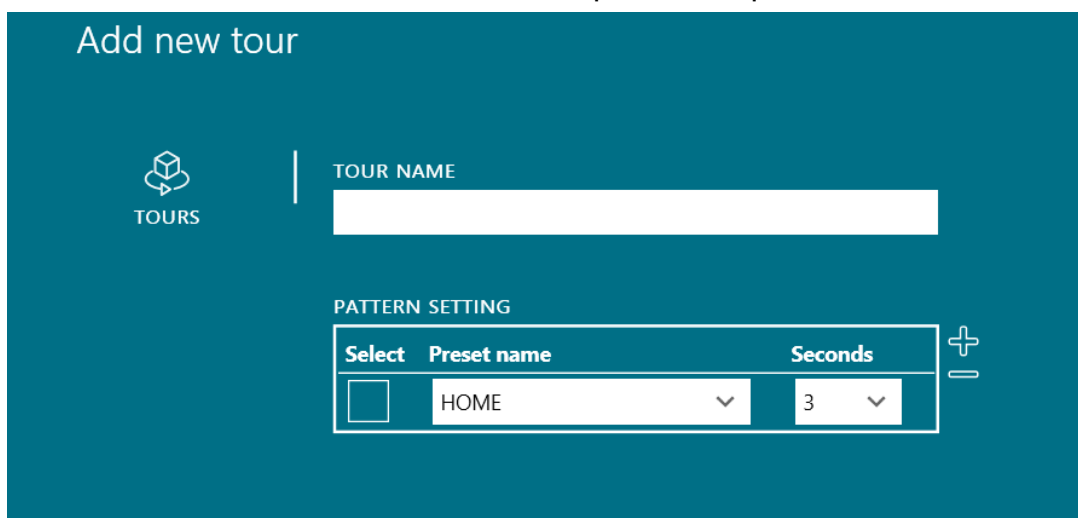


C. PTZ controller: Edit Preset and Tour.

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



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

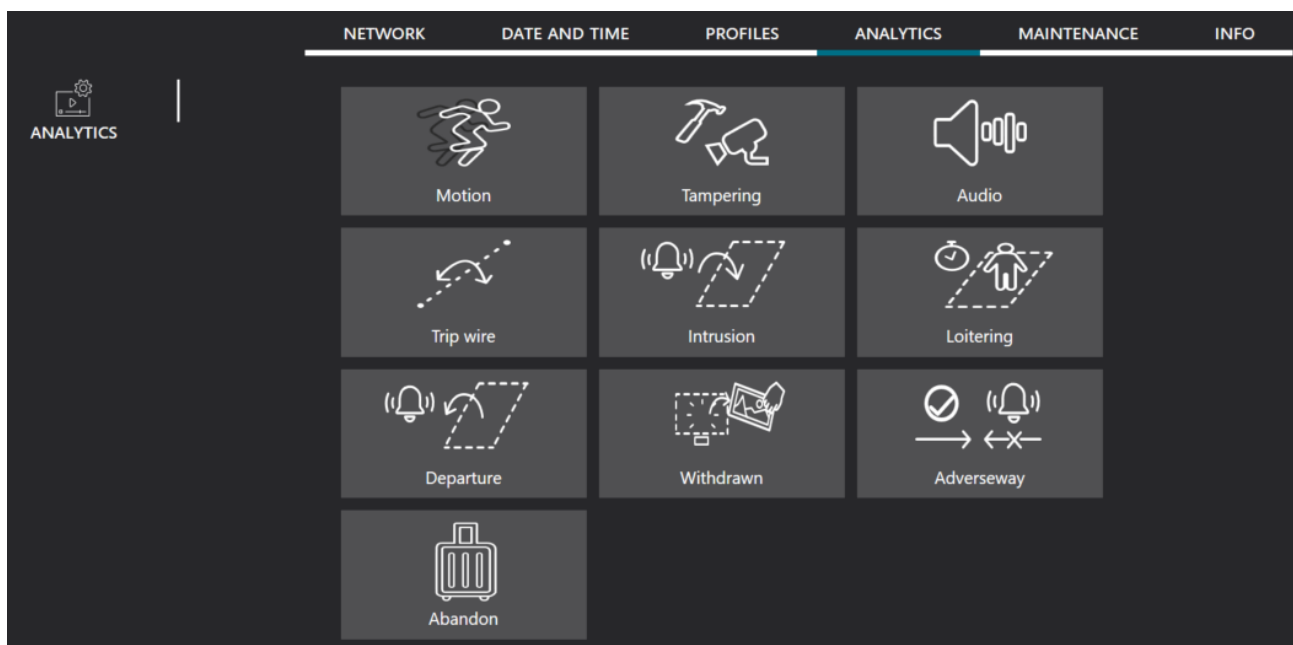


- Add Tour: Configure a patrol route based on the preset positions already created.

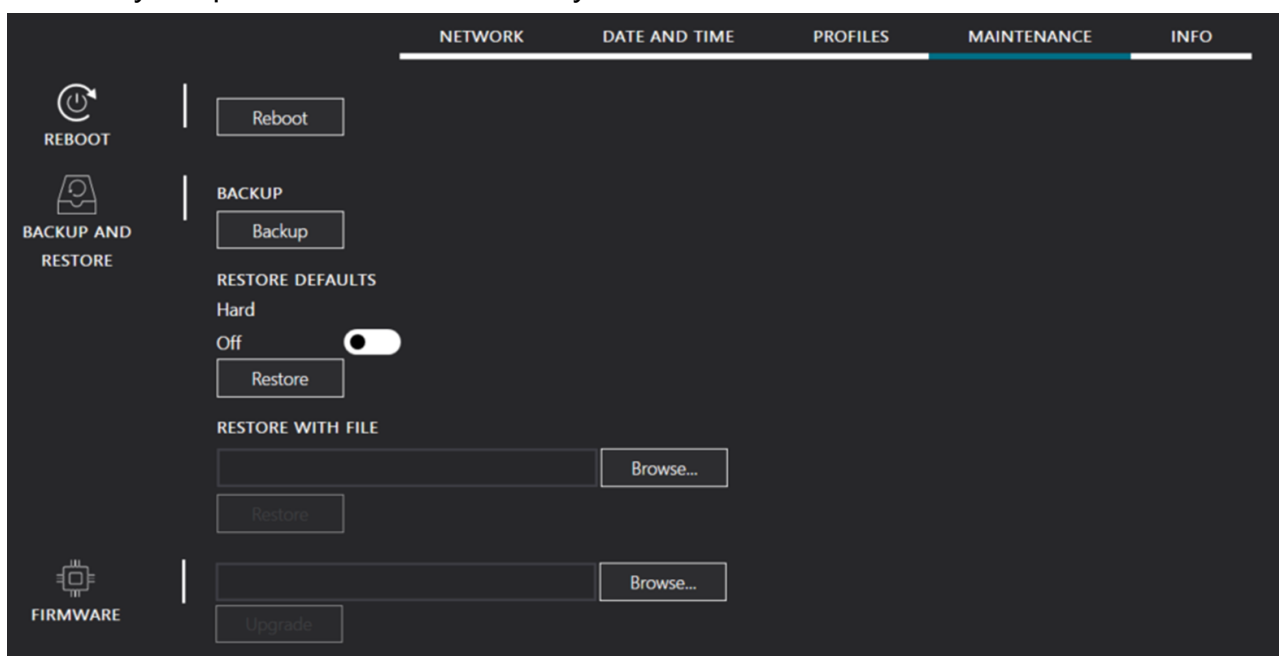


	NETWORK	DATE AND TIME	PROFILES	ANALYTICS	MAINTENANCE	INFO
 PROFILES						
SELECT	STREAM NAME	PROTOCOL	CODEC	RESOLUTION	FPS	ENABLED
☐	videostream 0	RTSP over TCP	H264	1920x1080	30	Yes
☐	videostream 1	RTSP over TCP	H264	1280x720	5	Yes
☐	videostream 2	RTSP over TCP	H264	320x240	30	Yes

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



E. Analytics: preview device video analytics status.

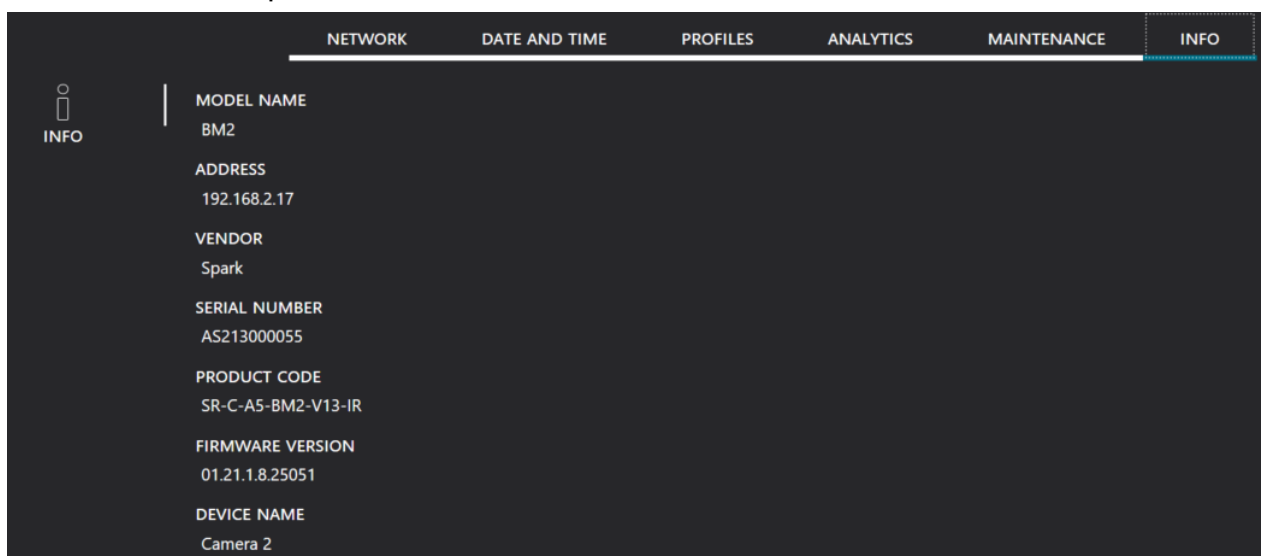


F. Maintenance: edit device maintenance settings.

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

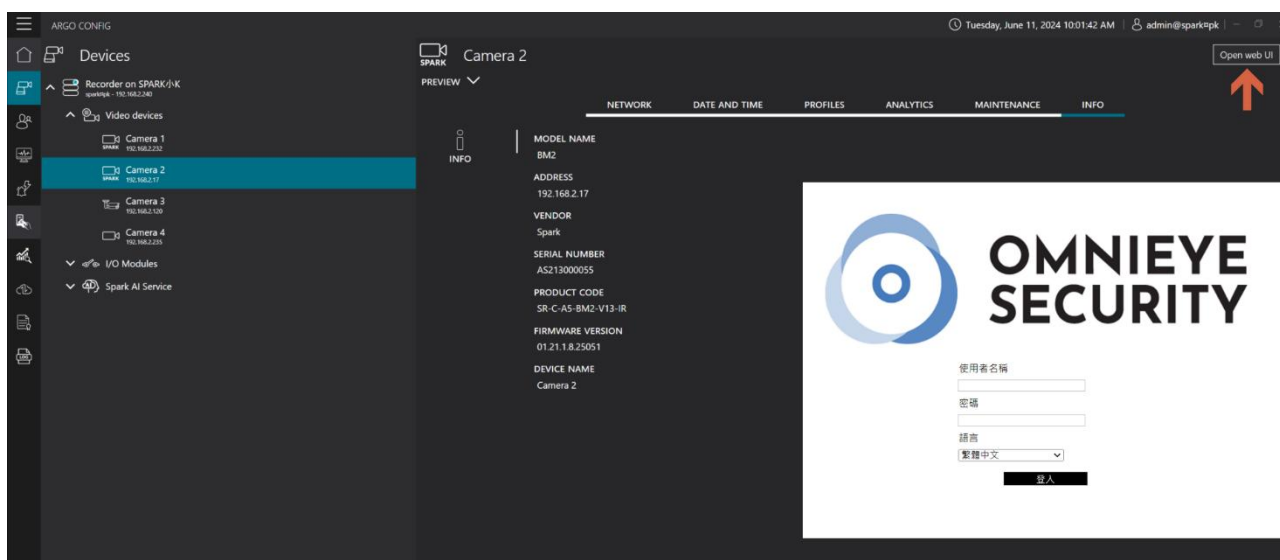


- Firmware: Update firmware version of the camera.



G. Info: browse device information

3.2.6 Open device web interface



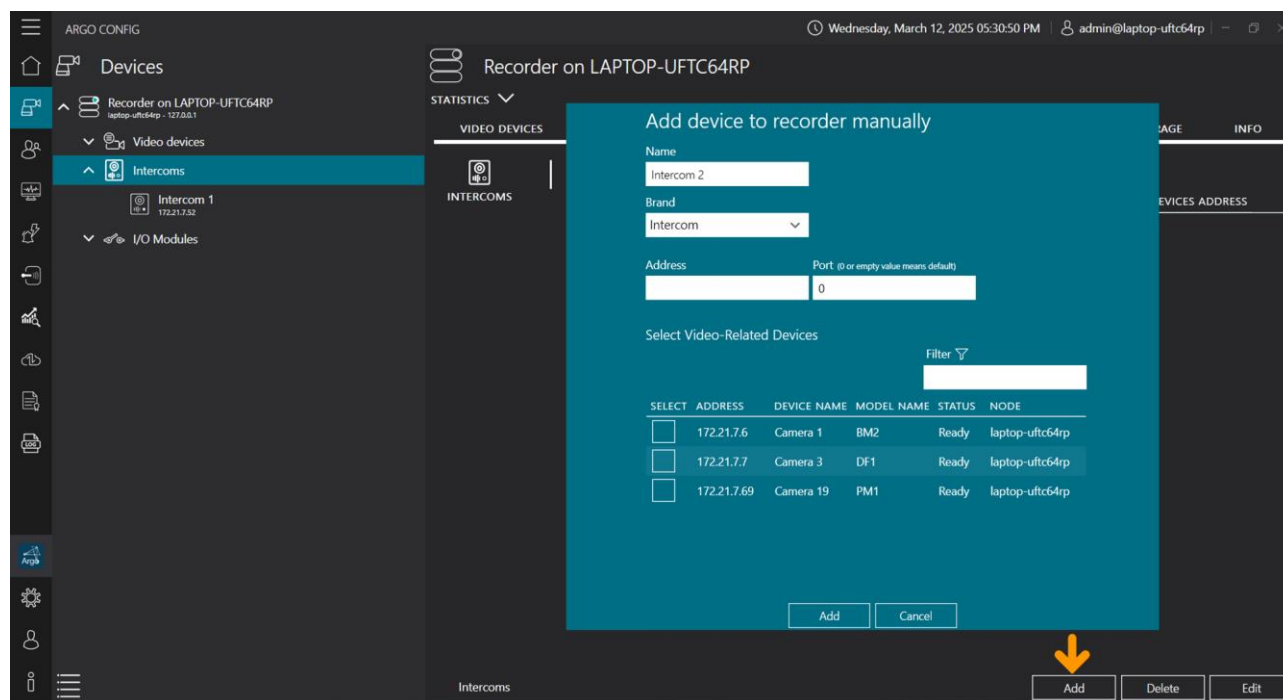
- Click on **[Open Web UI]**
- Username: insert username
- Password: insert password
- Language: select language



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

The screenshot shows the 'Edit intercom' dialog box in the ARGO CONFIG application. The dialog is titled 'Edit intercom' and contains the following fields and options:

- Enabled:** A toggle switch currently set to 'On'.
- Name:** A text field containing 'Intercom 1'.
- Brand:** A dropdown menu showing 'Intercom'.
- Address:** A text field containing '172.21.7.52'.
- Port:** A text field containing '0'.
- Select Video-Related Devices:** A section with a filter input and a table of available devices.

SELECT	ADDRESS	DEVICE NAME	MODEL NAME	STATUS	NODE
☒	172.21.7.6	Camera 1	BM2	Ready	laptop-uftc64rp
☐	172.21.7.7	Camera 3	DF1	Ready	laptop-uftc64rp
☐	172.21.7.69	Camera 19	PM1	Ready	laptop-uftc64rp

At the bottom of the dialog is a 'Cancel' button. In the background, the 'INTERCOMS' table is visible with the following data:

SELECT	ADDRESS	VENDOR	MODEL NAME	STATUS	DEVICE NAME	RELATED DEVICES	RELATED DEVICES ADDRESS
☒	172.21.7.52	Intercom	Intercom	Ready	Intercom 1	Camera 1	172.21.7.6

- 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

The screenshot shows the 'INTERCOMS' table in the ARGO CONFIG application. The table has the following data:

SELECT	ADDRESS	VENDOR	MODEL NAME	STATUS	DEVICE NAME	RELATED DEVICES	RELATED DEVICES ADDRESS
☒	172.21.7.52	Intercom	Intercom	Ready	Intercom 1	Camera 1	172.21.7.6

A yellow arrow points to the 'Delete' button at the bottom right of the interface.

- 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

ARGO CONFIG

Wednesday, August 28, 2024 03:08:31 PM | admin@laptop-uftc64rp

Recorder on LAPTOP-UFTC64RP

STATISTICS

VIDEO DEVICES | I/O MODULES | SPARK AI DEVICES | OTHER SETTINGS | STORAGE | INFO

I/O MODULES

Select all

SELECT	ADDRESS	VENDOR	MODEL NAME	STATUS	DEVICE NAME
☐	172.21.7.21	Advantech	6060	Ready	I/O Module 1
☐	172.21.7.72	Advantech	6060	Ready	I/O Module 2
☐	172.21.7.184	ICPDAS	tET-PD2POR2	Ready	I/O Module 3

Add I/O modules to recorder: Recorder on LAPTOP-UFTC64RP (laptop-uftc64rp)

172.21.7.21

Select	Address	Product code	MAC Address	Vendor	Status	Add to recorder
☐	172.21.7.21	6060	7489-8E48-0810	Advantech	Active	Recorder on LAPTOP-UFTC64RP
☐	172.21.7.72	6060	7489-8E48-0810	Advantech	Active	Recorder on LAPTOP-UFTC64RP
☐	172.21.7.184	HT-2000P02	000B7D6A7C7C	ICPDAS	Active	Recorder on LAPTOP-UFTC64RP
☐	172.21.7.184	HT-2000P02	000B7D6A7C7C	ICPDAS	Active	Recorder on LAPTOP-UFTC64RP
☐	172.21.7.184	HT-2000P02	000B7D6A7C7C	ICPDAS	Active	Recorder on LAPTOP-UFTC64RP
☐	172.21.7.184	HT-2000P02	000B7D6A7C7C	ICPDAS	Active	Recorder on LAPTOP-UFTC64RP

3 I/O Modules

1 Scan Add Delete Edit

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

B. Manual add I/O modules

ARGO CONFIG

Wednesday, August 28, 2024 03:14:17 PM | admin@laptop-uftc64rp

Recorder on LAPTOP-UFTC64RP

STATISTICS

VIDEO DEVICES | I/O MODULES | SPARK AI DEVICES | OTHER SETTINGS | STORAGE | INFO

I/O MODULES

Select all

SELECT	ADDRESS	VENDOR	MODEL NAME	STATUS	DEVICE NAME
☐	172.21.7.21	Advantech	6060	Ready	I/O Module 1
☐	172.21.7.72				
☐	172.21.7.184				

Add device to recorder manually

Name: I/O Module 4

Brand: Advantech

Address: 0

5 Add Cancel

1 Add Delete Edit

- 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
☐	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

Brand

Address Port (0 or empty value means default)

Node Information

Select	Name	Type	Node	Port
☐	Soyal Node	RFID	255	1601
☐	Soyal Node	IO	256	1621

I/O Map Information

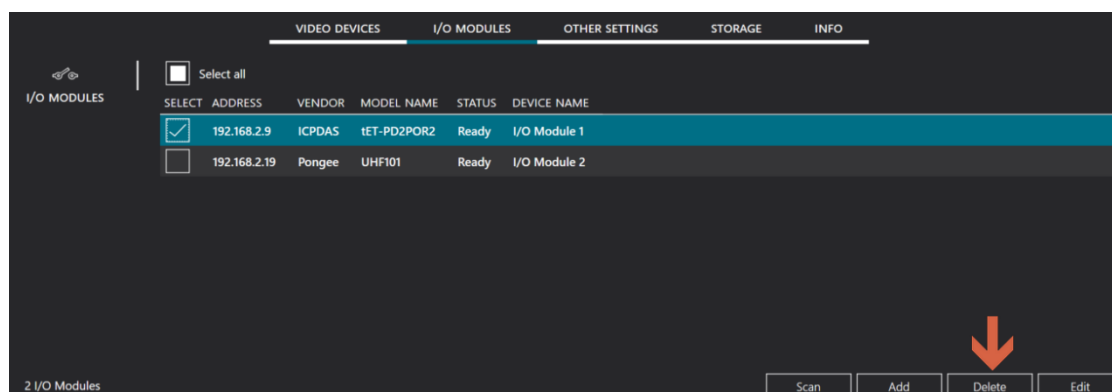
Select	Name	Type	ID
☐	Soyal IO	DI	0
☐	Soyal IO	DO	1

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).

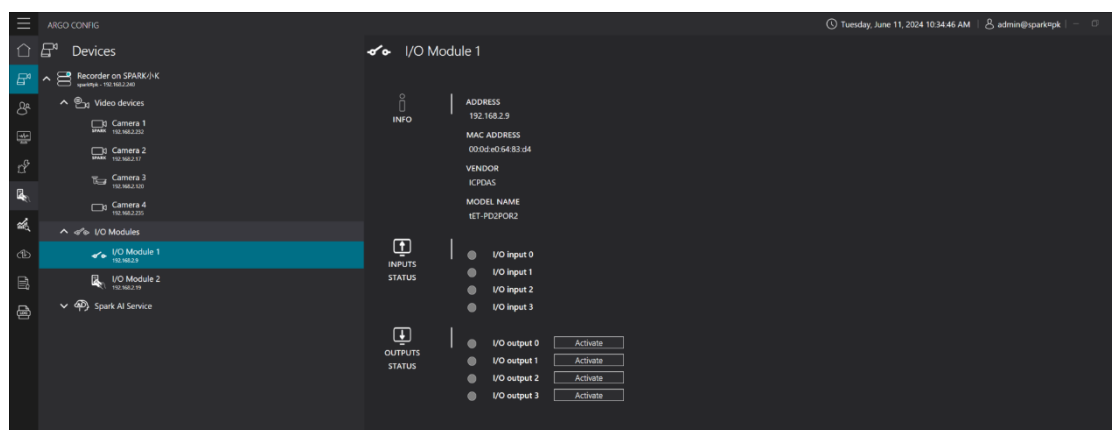


3.4.3 Delete I/O modules



- 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

ARGO CONFIG Tuesday, March 25, 2025 03:51:18 PM admin@desktop-k3ktl8n

Recorder on DESKTOP-K3KTL8N

STATISTICS

VIDEO DEVICES INTERCOMS I/O MODULES **SPARK AI DEVICES** OTHER SETTINGS STORAGE INFO

SPARK AI DEVICES

Select all

SELECT	SERIAL NUMBER	STATUS	LICENSE TYPE
☐	2D06174C	Ready	AI Detection
☐	2B062C4C	Ready	LPR Detection

2 Spark AI Devices

Add Delete



3.5.1 Add Spark AI Device

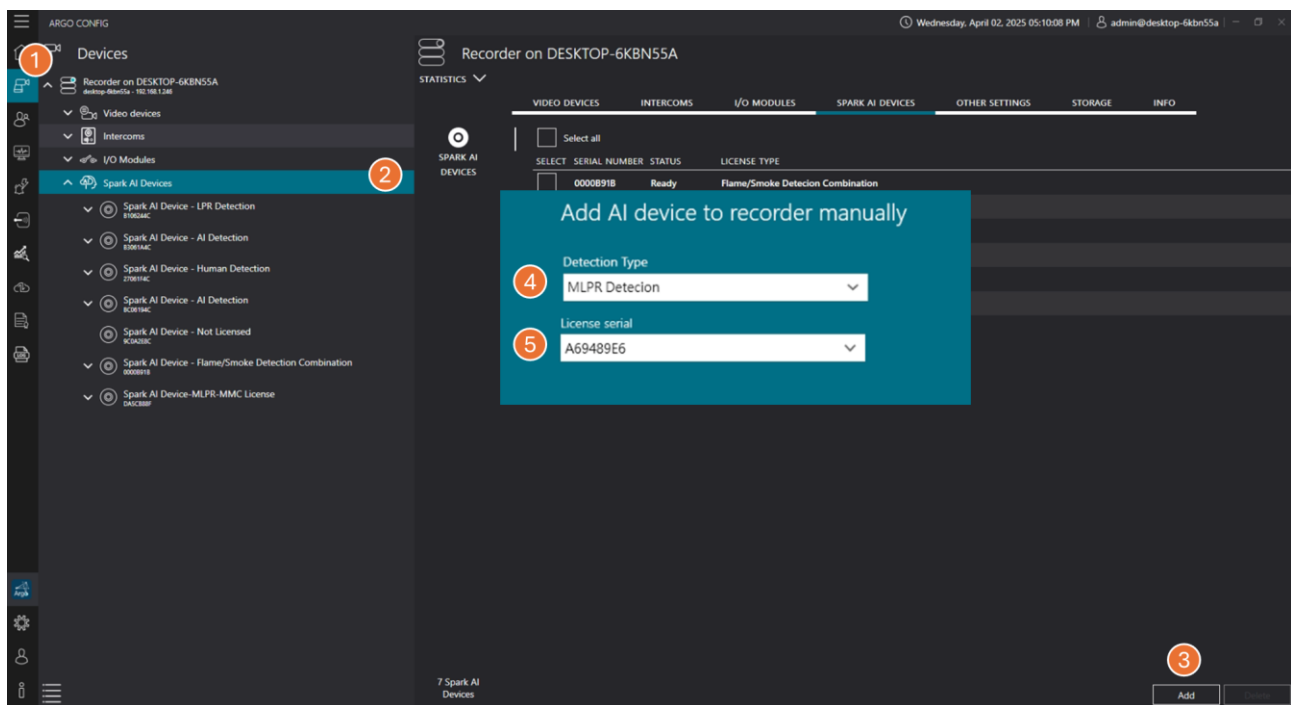
3.5.1.1 All / Human / Vehicle Detection Devices

- 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

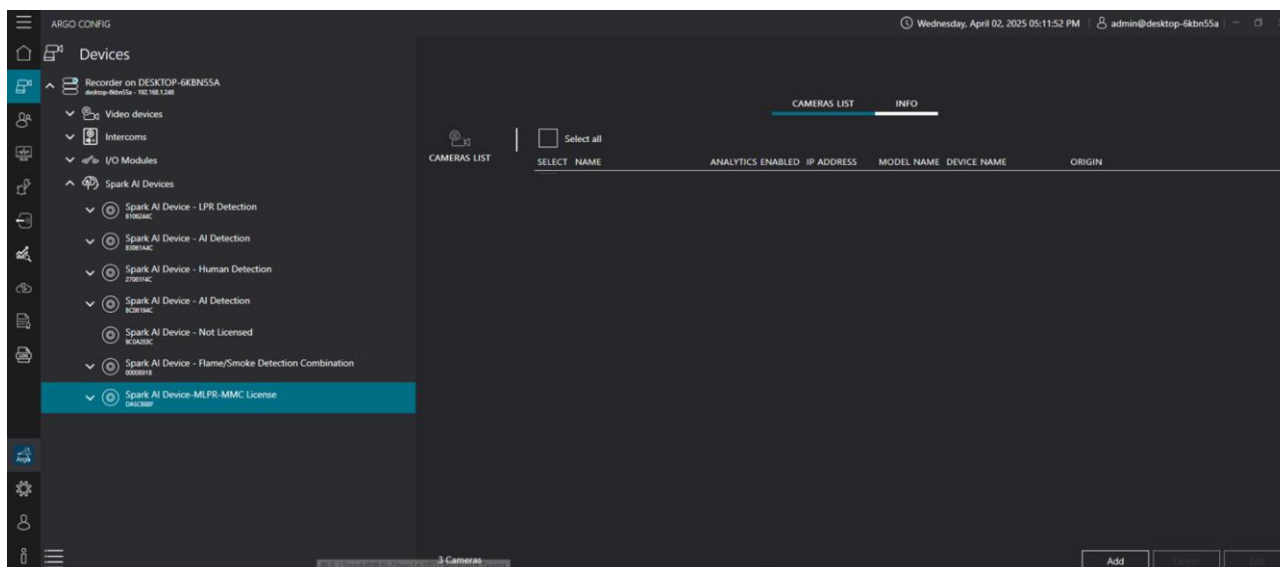


Step1: Add License

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

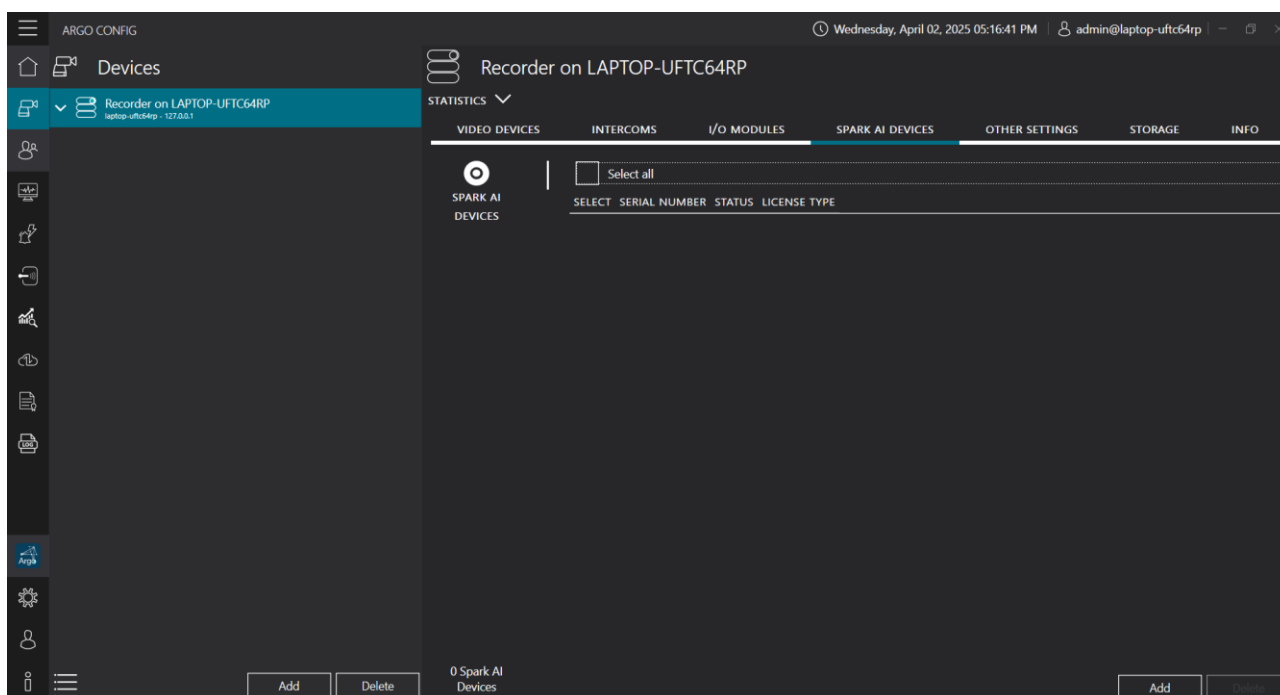


Step2: Upload Recognition Software to the Spark AI Device



- Click [Add]

3.5.1.4 Fire & Smoke Devices



Step1: Click Browse.

Add AI device to recorder manually

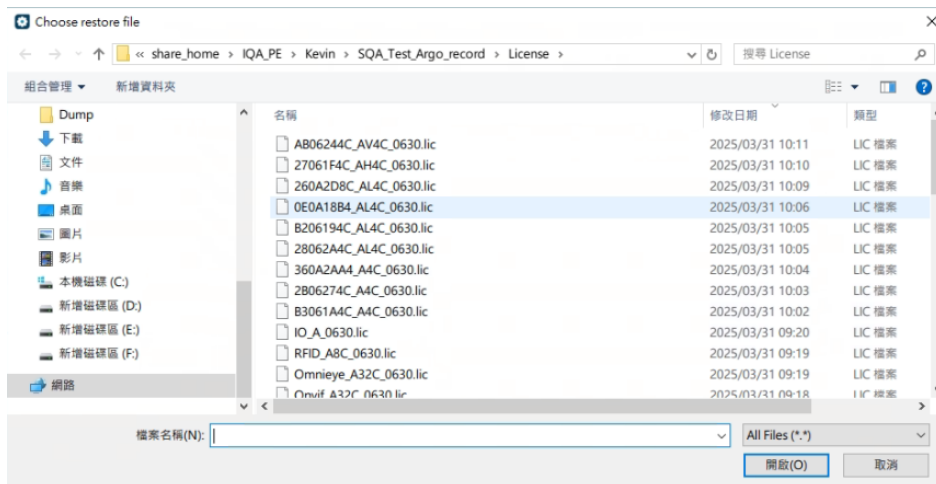
Detection Type
Flame/Smoke Detecion Combination

Certificate

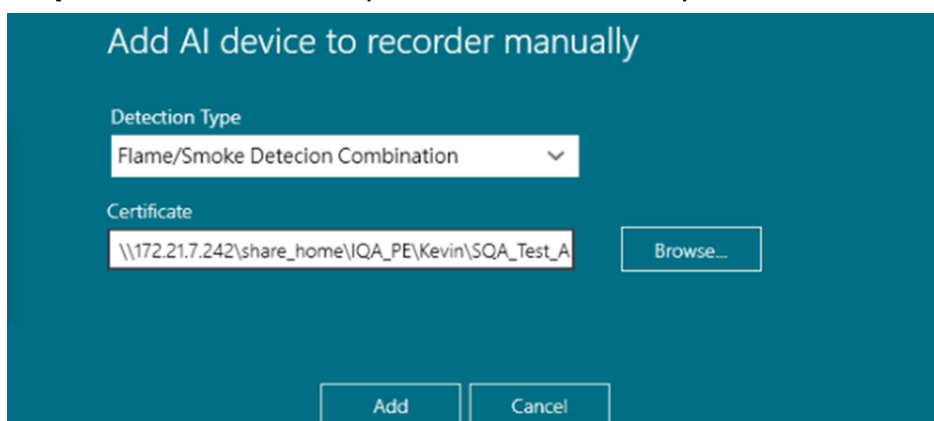
Browse...



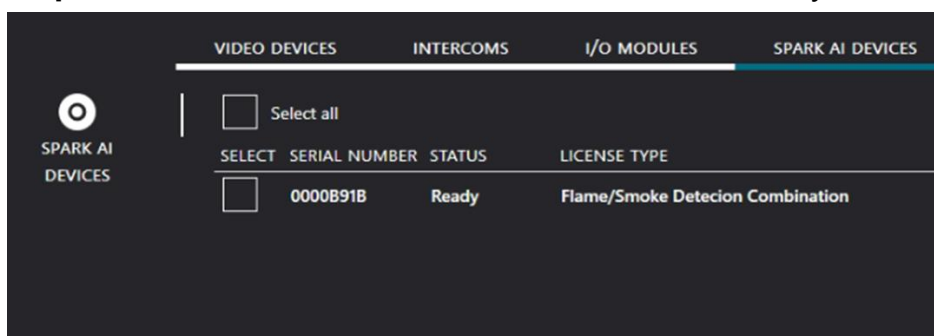
Step2: Select the device certificate to add (the certificate is identified based on the computer's MAC address).



Step3: Click Add to complete the certificate import.



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

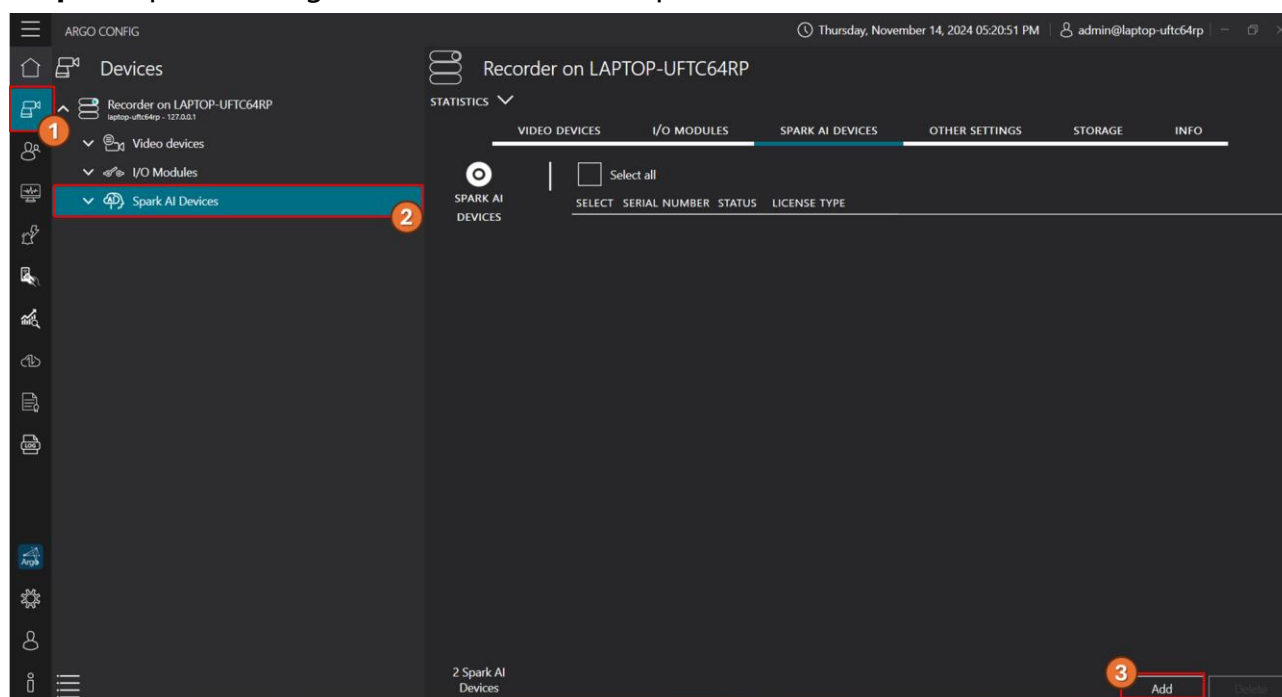




3.5.1.5 Generic AI Device

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

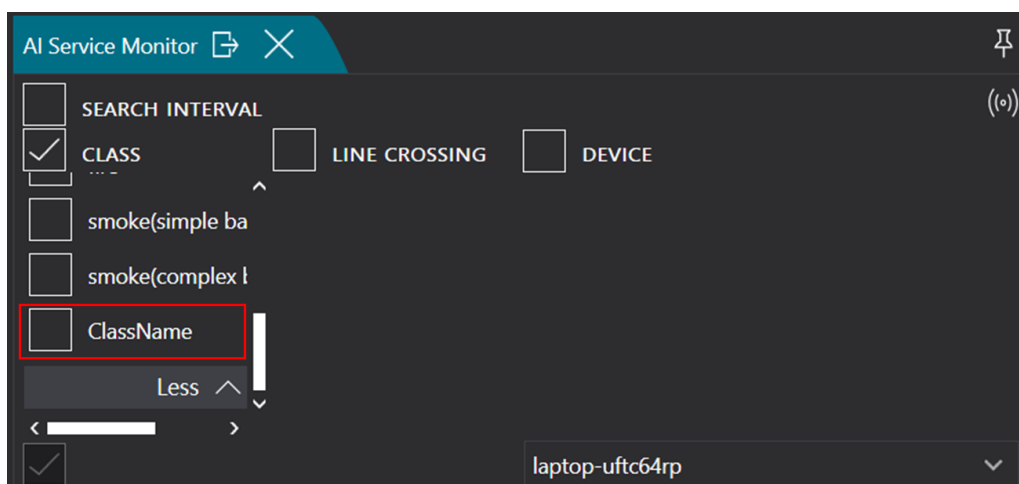
Analytics application Port
31000
The port number must be between 0 and 65535

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

- Detection Type: Select "Generic AI Detection."

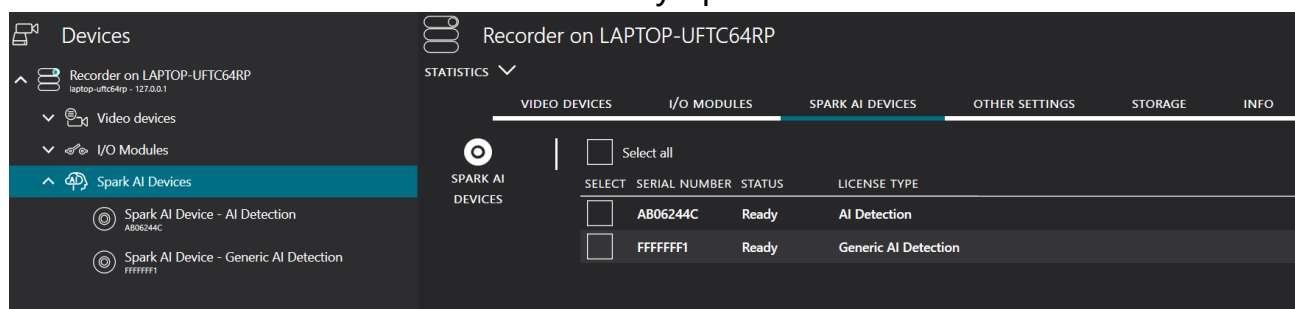


- Generic AI Detection Class Name: Enter the recognition name, such as object detection or flame detection. This category name will be displayed in the Client AI Service Monitor Class list.



- 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.



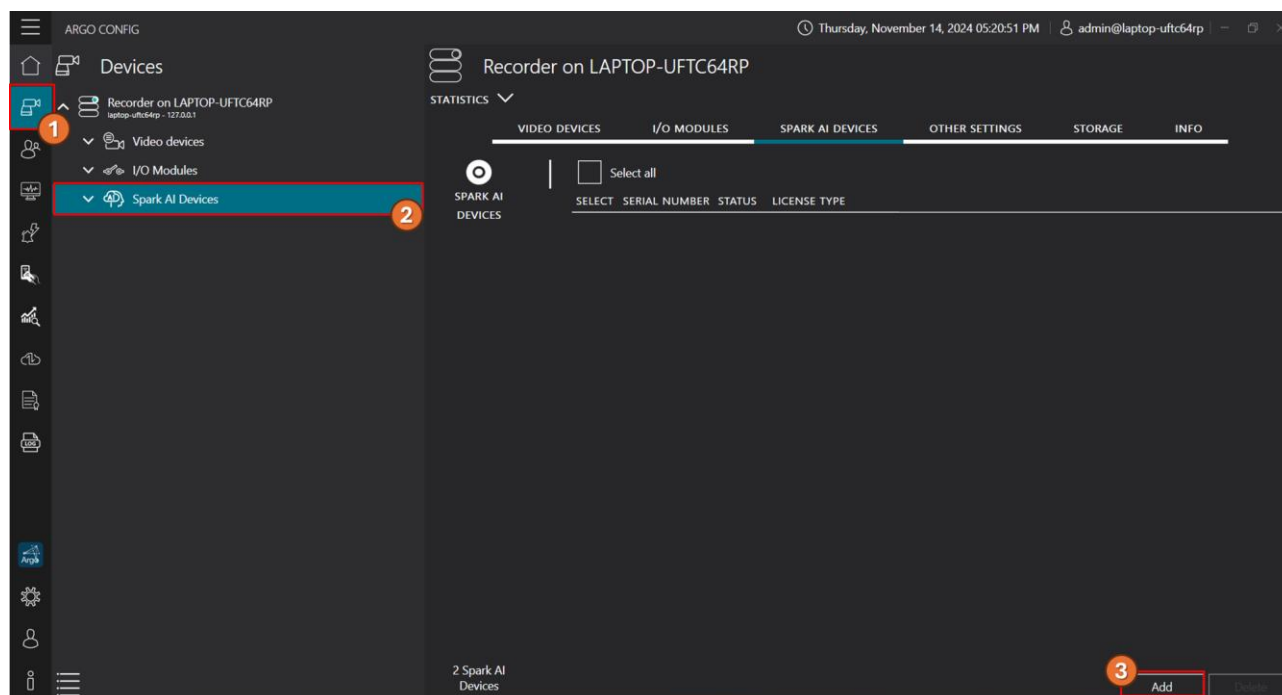
3.5.1.6 Face Detection

- 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.

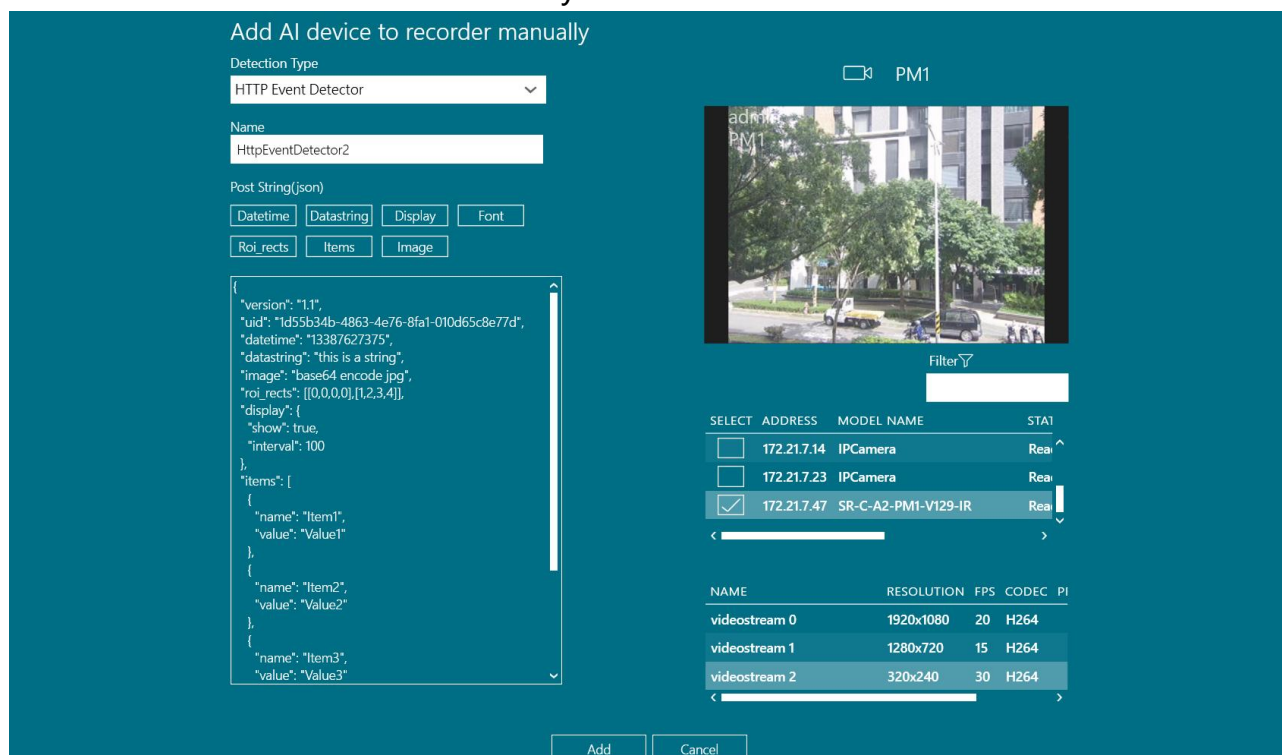


3.5.1.7 HTTP POST Device

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

The screenshot displays the 'Devices' section of the Argo Client interface. On the left, a sidebar lists the following components: 'Recorder on LAPTOP-UFTC64RP', 'Video devices', 'Spark AI Devices', 'HTTP Event Detector' (labeled 'HttpEventDetector1'), and 'HTTP Event Detector' (labeled 'HttpEventDetector2'). The 'HttpEventDetector2' item is selected and highlighted in blue. The main panel on the right shows the configuration details for this selected detector, with an 'INFO' tab active. The configuration includes:

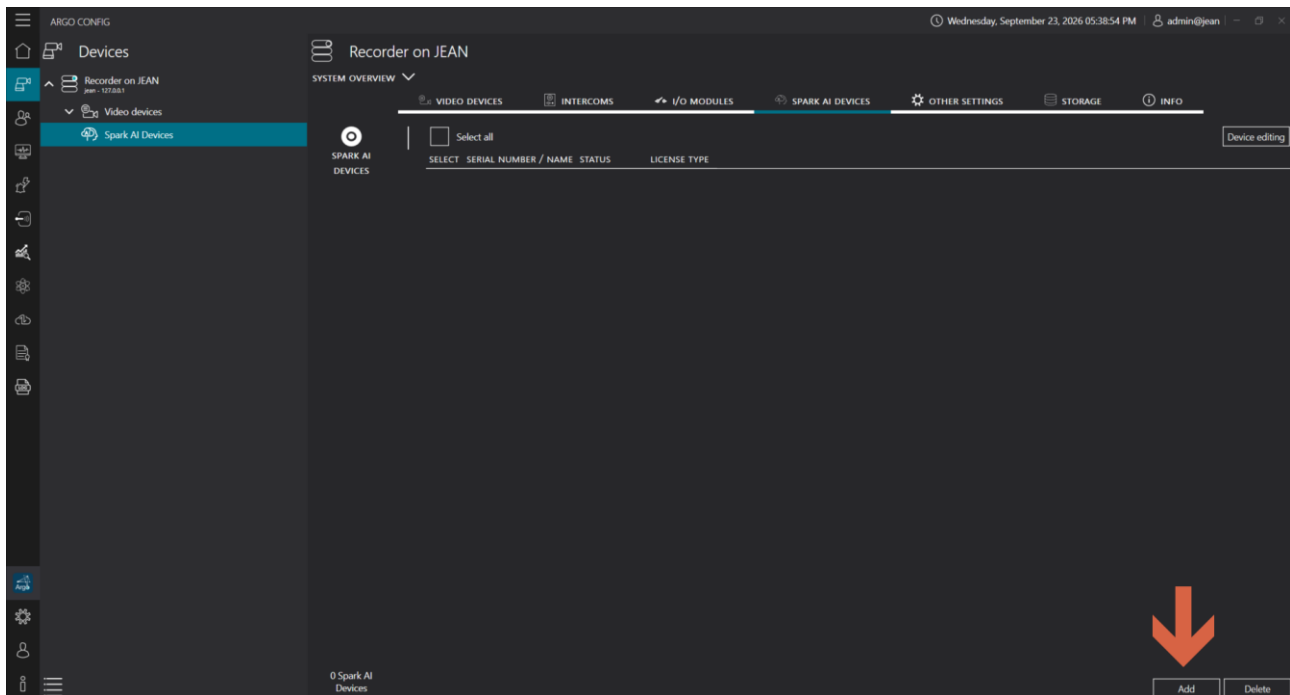
- ENABLED:** True
- DEVICE NAME:** HttpEventDetector2
- UID:** e7abb5a4-ee5f-4a81-ab72-f822a51cade6
- HTTP POST URL:** PostAnalyticsAnswer
- POST STRING(JSON):** {version}{uid}{datetime}{datastring}{image}{roi_rects}{display}{items}{font}
- CAMERA:** PM1
- STREAM:** videostream 2

- Get Http POST device information

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



3.5.1.8 VLM Device



- Confirm that the license certificate has been successfully uploaded.
- Click [Add] in the bottom-right corner.

Add AI device to recorder manually

Detection Type
VLM Detector

Name
VLM1

IP Address
10.10.10.10

Port
0
0 or empty value means default

- Detection Type: Select [VLM Detector].
- Name: Enter a custom device name.
- IP Address: Enter the IP address of the VLM device.
- Port: Default 0 (represents port 5002).



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
Face Detection	1280x720P	10 FPS

3.5.2.1 All/ Vehicle/ Human Detection

The screenshot shows the ARGO CONFIG interface. On the left, the 'Devices' sidebar is expanded, showing 'Spark AI Device - AI Detection' with a red circle 1. The main window displays the 'Add camera to Spark AI Service' dialog. The 'CAMERAS LIST' tab is active, showing a table of cameras. The 'INFO' tab shows a live video feed of a street scene. The 'Add' button is highlighted with a red circle 2. The 'Detection Type' dropdown is set to 'Area' and is highlighted with a red circle 5. The 'Add' button is also highlighted with a red circle 2 at the bottom right of the dialog.

SELECT	ADDRESS	MODEL NAME	STATUS	DEVICE NAME	ORIGIN	ANALYTICS
☐	172.21.7.20	DPI	Ready	Camera 5	Recorder on LAPTOP-UFTC64RP	No
☐	172.21.7.26	IPCcamera	Ready	Camera 3	Recorder on LAPTOP-UFTC64RP	Yes
☐	172.21.7.27	BF1	Ready	Camera 6	Recorder on LAPTOP-UFTC64RP	No
☒	172.21.7.60	IPCcamera	Ready	Camera 2	Recorder on LAPTOP-UFTC64RP	Yes

NAME	RESOLUTION	FPS	CODEC	PROFILES SELECTED
videostream ProfileToken_1	1920x1080	25	H264	No
videostream ProfileToken_2	1280x720	25	H264	Yes

Detection Type: Area

Add Close

3 Cameras 2 Add Delete Edit

- 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 ▾

1

SELECT	ADDRESS	MODEL NAME	STATUS	DEVICE NAME	ORIGIN
☒	123.111.222.123	Generic Camera	Not applicable	Camera 1	Recorder on DESKTOP-KC
☐	172.21.7.160	SR-C-A2-DM1-V13-IR	Ready	玄關	Recorder on DESKTOP-KC
☐	172.21.7.238	SR-C-A2-DF1-F3-IR	Ready	櫃台	Recorder on DESKTOP-KC
☐	172.21.7.239	SR-C-A2-DF1-F3-IR	Ready	大門	Recorder on DESKTOP-KC

2

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

3

LPR Mode: Lane

4

Add Close

Camera 1

- 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

Add camera to Spark AI Service

Filter ▾

1

SELECT	ADDRESS	MODEL NAME	STATUS	DEVICE NAME	ORIGIN
☐	123.111.222.123	Generic Camera	Not applicable	Camera 1	Recorder on DESKTOP-KC ^
☐	172.21.7.160	SR-C-A2-DM1-VI3-IR	Ready	玄關	Recorder on DESKTOP-KC
☐	172.21.7.238	SR-C-A2-DF1-F3-IR	Ready	櫃台	Recorder on DESKTOP-KC
☐	172.21.7.239	SR-C-A2-DF1-F3-IR	Ready	大門	Recorder on DESKTOP-KC

2

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

3

Add Close

Camera 12

- 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

Add camera to Spark AI Service

Filter ▾

1

SELECT	ADDRESS	MODEL NAME	STATUS	DEVICE NAME	ORIGIN	ANALYT
☐	172.21.5.10	BM2	Unreachable	Camera 1	Recorder on LAPTOP-UFTC64RP	No
☐	172.21.5.11	BM2	Unreachable	Camera 4	Recorder on LAPTOP-UFTC64RP	No
☒	172.21.7.27	BF1	Ready	Camera 8	Recorder on LAPTOP-UFTC64RP	No

2

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

3

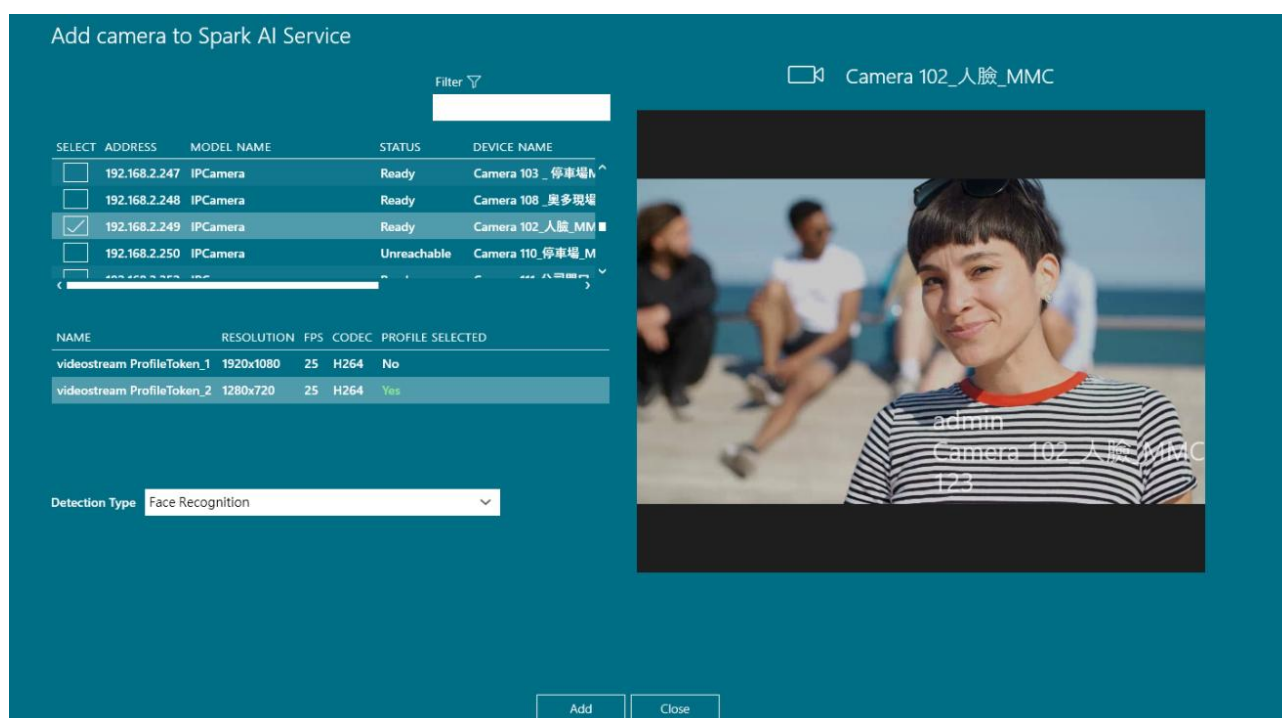
Add Close

Camera 8

- 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].



3.5.2.6 Spark VLM

Edit camera from Spark VLM

Analytics enabled ☒ On

Name
AnalyticsStreamPerimeter7

Source
Spark AI Device

Detection Priority (1 = Highest, 5 = Lowest)
5

Detection Type
Prompt

Prompt
Person Appearance

1F室外大門口



SELECT	NAME	DEVICE NAME	ORIGIN
☐	AnalyticsStreamPerimeter2	spark_ai_key_B10A2DA4	Recorder on DESKTOP-9214I31
☐	AnalyticsStreamPerimeter3	spark_ai_key_B00A2D8C	Recorder on DESKTOP-FUTS800
☒	AnalyticsStreamPerimeter4	spark_ai_key_B10A2DA4	Recorder on DESKTOP-FUTS800
☐	AnalyticsStreamPerimeter5	spark_ai_key_AA0A2E94	Recorder on DESKTOP-FUTS800

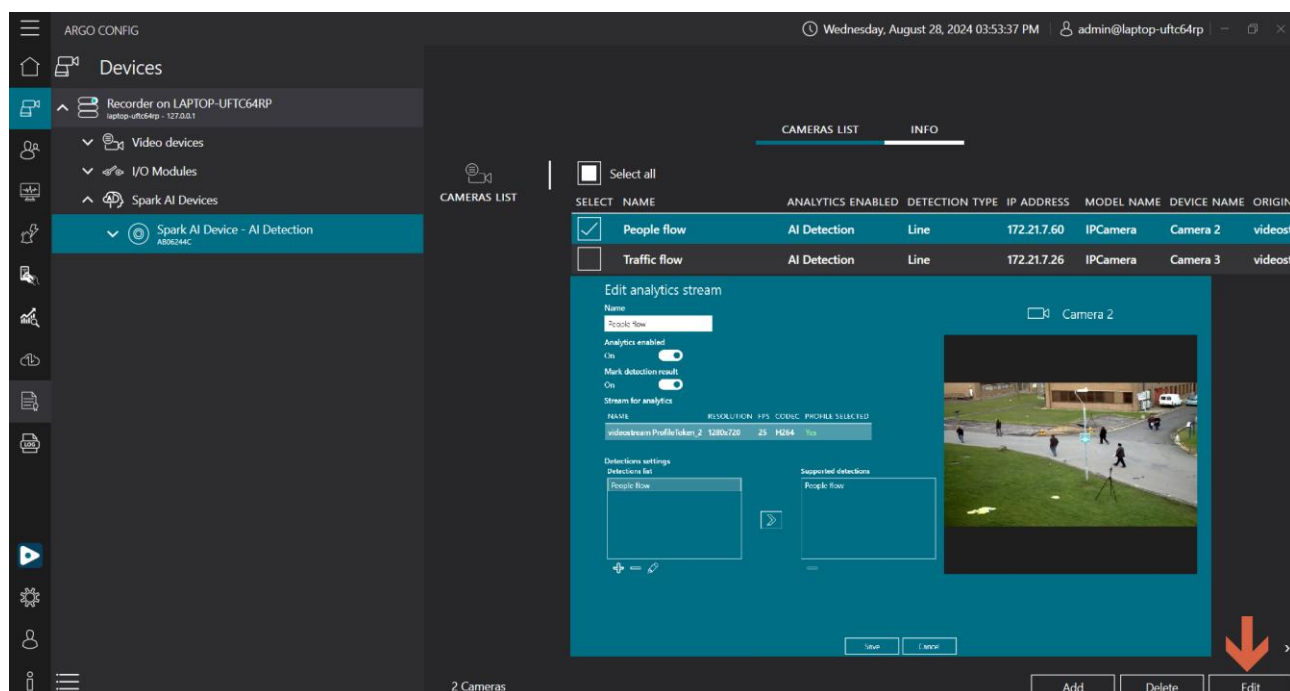
NAME	RESOLUTION	FPS	CODEC
videostream 1	1920x1080	3	H264

Save Cancel

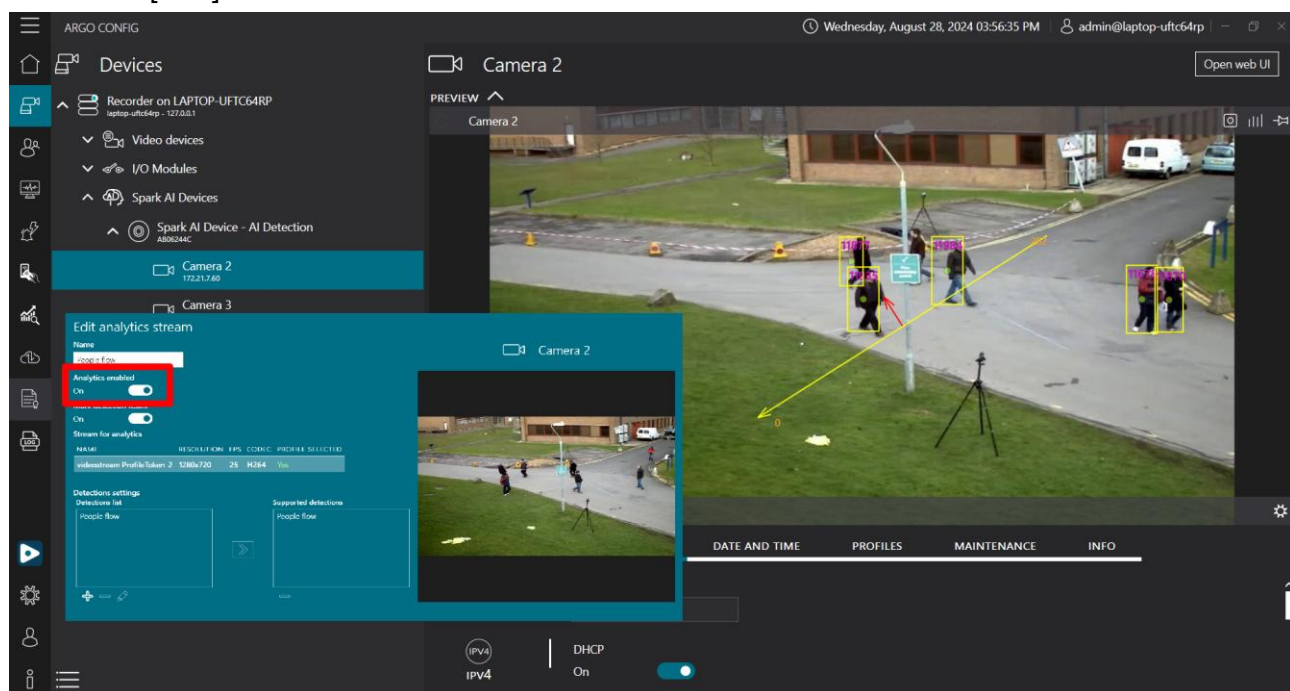
- Analysis enables: Choose whether to enable or disable AI analysis.
- Name: Enter a custom detection name.
- Source: Select the device source for advanced AI analysis.
- Detection Type:
 - Prompt: Built-in detection types, including person appearance (hat, clothing, pants, glasses), fire, and smoke detection.
 - Match Database: Search for objects using reference images. Images must first be added to the Knowledge Base in Config.
- Stream: Select the stream.
- Stream Resolution: Refer to Section Add Camera Analysis Stream.
- Click [Add].



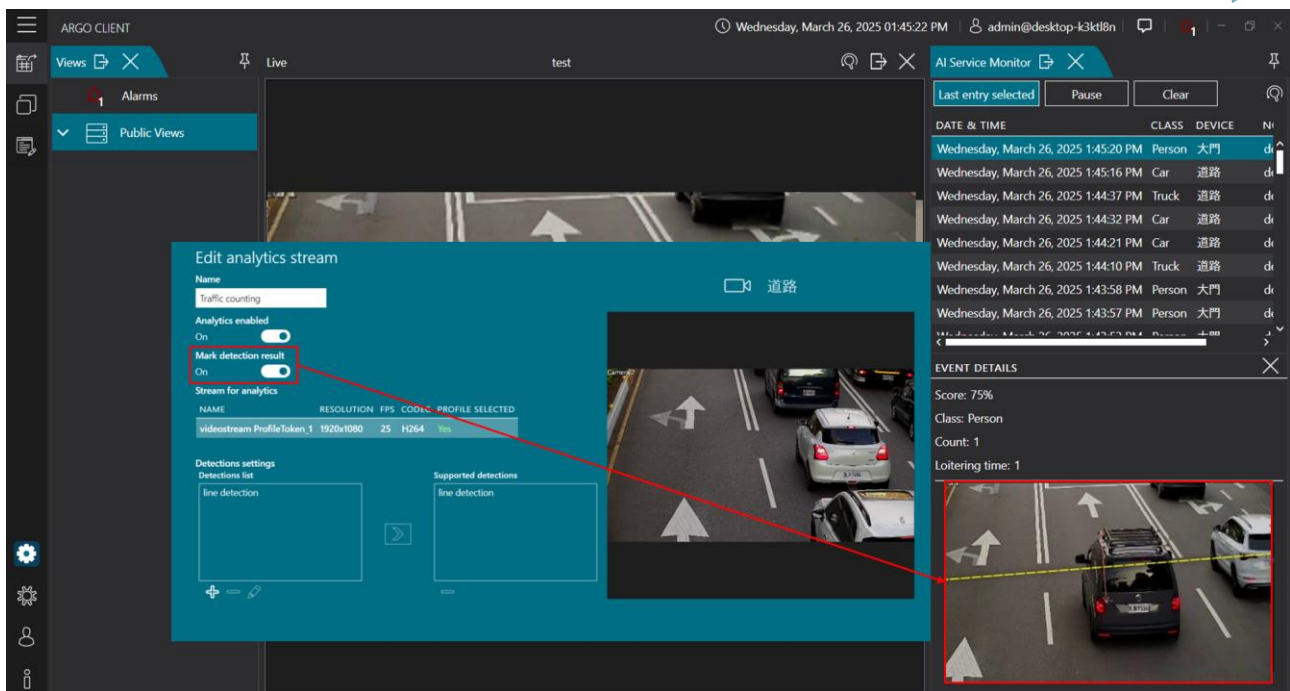
3.5.3 Edit Spark AI Devices



- 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 Reverse

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.
 - 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 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

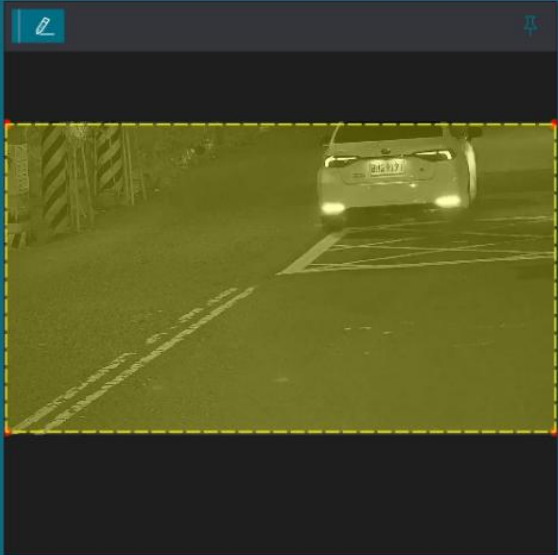
Edit action

Rule name
area detection

License Plate Aspect Ratio Range (Width / Height)
1.4 + - ~ 2.6 + -

Preview



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

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 detection

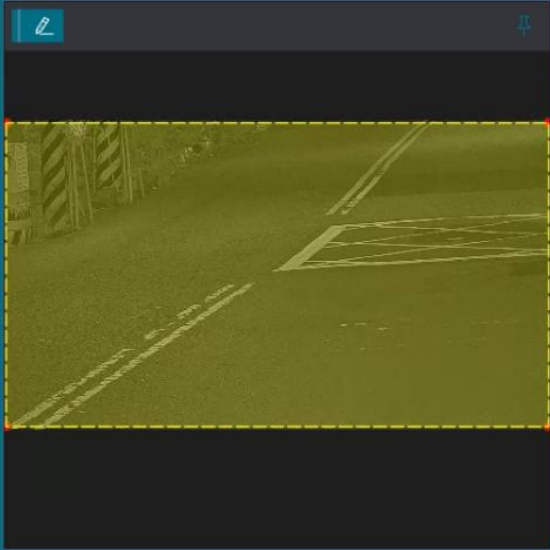
Recognition Interval (s)
1 + -

Hold Time (s)
5 + -

License Plate Aspect Ratio Range (Width / Height)
1.4 + - ~ 2.6 + -

Preview



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.
- License Plate Aspect Ratio Range:
 -  **Minimum [0.1–2.0]:** A lower value allows recognition of more angled or skewed license plates.
 -  **Maximum [2.0–4.0]:** A higher value allows recognition of more elongated license plates.
- 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

Edit action

Rule name
mlpr detection

Score Threshold [Low - High]
70 %

Country
Taiwan

OCR complexity
3

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

OK 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

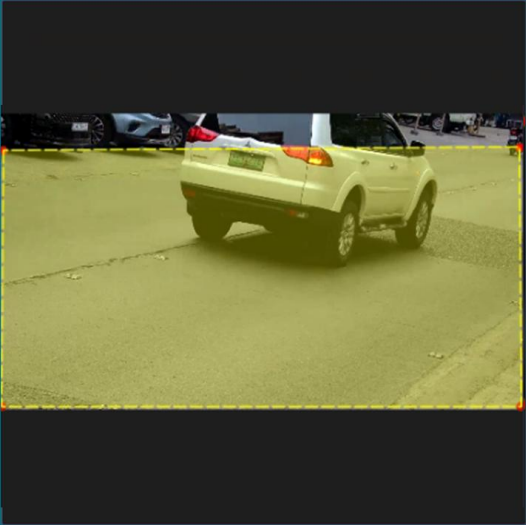
Score (1: Sensitivity level high; 9: Accuracy level high)
9

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

Edit analytics stream

Camera 2

Name: AnalyticsStreamPerimeter14

Analytics enabled: On

Auto ROI: On

Shake Setting: On

Shake Level: Small Shake

Sensitivity: 200

Analytics stream

NAME	RESOLUTION	FPS	CODEC	PROFILE	SELECTED
videostream 2	640x360	30	H264	Yes	

Detections settings

Detections list

Roi Setting

Supported detections

Roi Setting

Exclusion Detection Settings

Detections list

Supported detections

- 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

Edit action

Rule name
Roi Setting

Fire detection ☐

Threshold [Low - High] 100 Advence Setting ☐

Smoke detection(simple background) ☐

Threshold [Low - High] 50 Advence Setting ☐

Sensitivity [Low - High] 15

Smoke Detection(complex background) ☐

Threshold [Low - High] 2 Advence Setting ☐

OK Cancel

- 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 ☐

Threshold [Low - High] 100

Response Time [Fast - Slow] 60

Frame Rate 1

Flame Min Exclusive Area [Small - Large] 20

Flame Min Exclusive Width [Small - Large] 5

Flame Min Exclusive Height [Small - Large] 5

Fire Color Paramater

R 150 G 50 B 0

Fire Color Brightness

R>G 105 R>B 120 G>B 110

Advance Setting ☐

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

Smoke detection(simple background)		50	Advance Setting
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)			Advance Setting
Threshold [Low - High]		2	☐
Variation [Light - Dense]		100	☐
Background Clarity [Low - High]		50	☐
Max Brightness [Dark - Light]		50	☐
Frame Rate		8	☐

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.

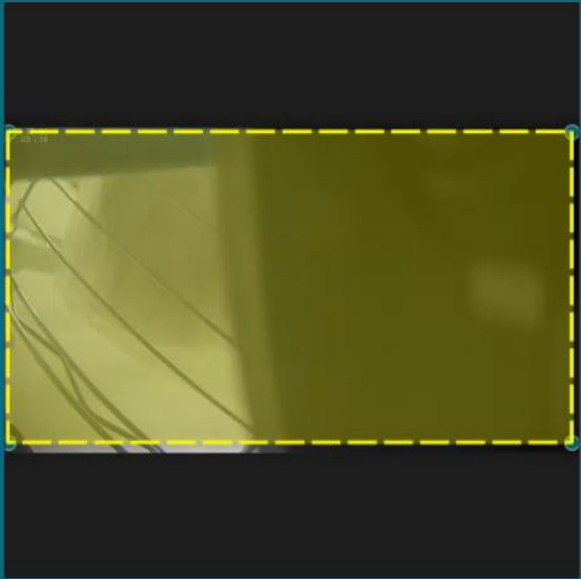


B. Exclusion Area Detection Settings

Add action

Rule name

TRST



Add Cancel

- 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.



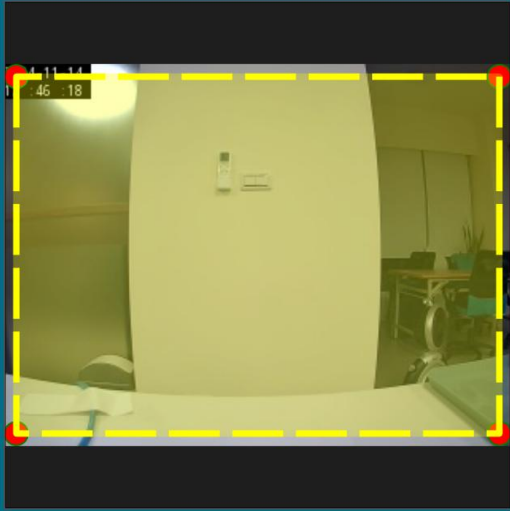
3.5.3.5 General AI Device - Parameter Settings Description

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

Edit analytics stream

Name
AnalyticsStreamPerimeter18

Analytics enabled
On

Mark detection result
Off

Frontal Face
On

Frontal Face Level
Middle

Stream for analytics

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

Camera 102_人臉_MMC

admin
Camera 102_人臉_MMC
123

Save Cancel

- 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).



3.5.3.7 VLM Detection - Parameter Settings Description

Add camera to Spark VLM

Analytics enabled ☒ On

Name
AnalyticsStreamPerimeter1

Source
Spark AI Device

Detection Priority (1 = Highest, 5 = Lowest)
5

Detection Type
Prompt

Prompt
Person Appearance

1F室外大門口



SELECT	NAME	DEVICE NAME	ORIGIN
☐	AnalyticsStreamPerimeter2	spark_ai_key_B10A2DA4	Recorder on DESKTOP-9214I31
☐	AnalyticsStreamPerimeter3	spark_ai_key_B00A2D8C	Recorder on DESKTOP-FUTS800
☐	AnalyticsStreamPerimeter4	spark_ai_key_B10A2DA4	Recorder on DESKTOP-FUTS800
☐	AnalyticsStreamPerimeter5	spark_ai_key_AA0A2E94	Recorder on DESKTOP-FUTS800

NAME	RESOLUTION	FPS	CODEC
videostream 1	1920x1080	3	H264

OK Cancel

- **Enable AI Analysis:** Enable or disable AI analysis.
- **Name:** Enter a detection name.
- **Source:** Select the device source for advanced AI analysis.
- **Detection Type:**
 - **Prompt:** Built-in detection types.
 - ◆ **Person Appearance:** Detects person attributes, including hats, clothing, pants, and glasses.
 - ◆ **Fire and Smoke:** Detects fire and smoke. Two modes are available: **Speed Mode** and **Accuracy Mode (Default)**.
 - **Match database:** Provides image-based object search. Images must first be added to the Reference Image Library in Config.
- **Stream:** Select the stream.
- **Stream Resolution:** Refer to Section 3.5.2, *Add Camera Analysis Stream*.
- Click [OK].



3.5.4 Delete Spark AI Device Stream Analysis

The screenshot shows the 'CAMERAS LIST' tab in the ARGO CONFIG interface. The left sidebar shows the 'Spark AI Device - AI Detection' section. The main area displays a table with the following data:

SELECT	NAME	ANALYTICS ENABLED	DETECTION TYPE	IP ADDRESS	MODEL NAME	DEVICE NAME	ORIGIN
☐	People flow	AI Detection	Line	172.21.7.60	IPCamera	Camera 2	videost
☒	AnalyticsStreamPerimeter5	AI Detection	Area	172.21.7.60	IPCamera	Camera 2	videost
☐	Traffic flow	AI Detection	Line	172.21.7.26	IPCamera	Camera 3	videost

At the bottom right, there are buttons for 'Add', 'Delete', and 'Edit'. A red arrow points to the 'Delete' button.

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

3.5.5 Delete Spark AI Device

The screenshot shows the 'SPARK AI DEVICES' tab in the ARGO CONFIG interface. The left sidebar shows the 'Spark AI Device - AI Detection' section. The main area displays a table with the following data:

SELECT	SERIAL NUMBER	STATUS	LICENSE TYPE
☒	AB06244C	Unreachable	AI Detection

At the bottom right, there are buttons for 'Add' and 'Delete'. A red arrow points to the 'Delete' button.

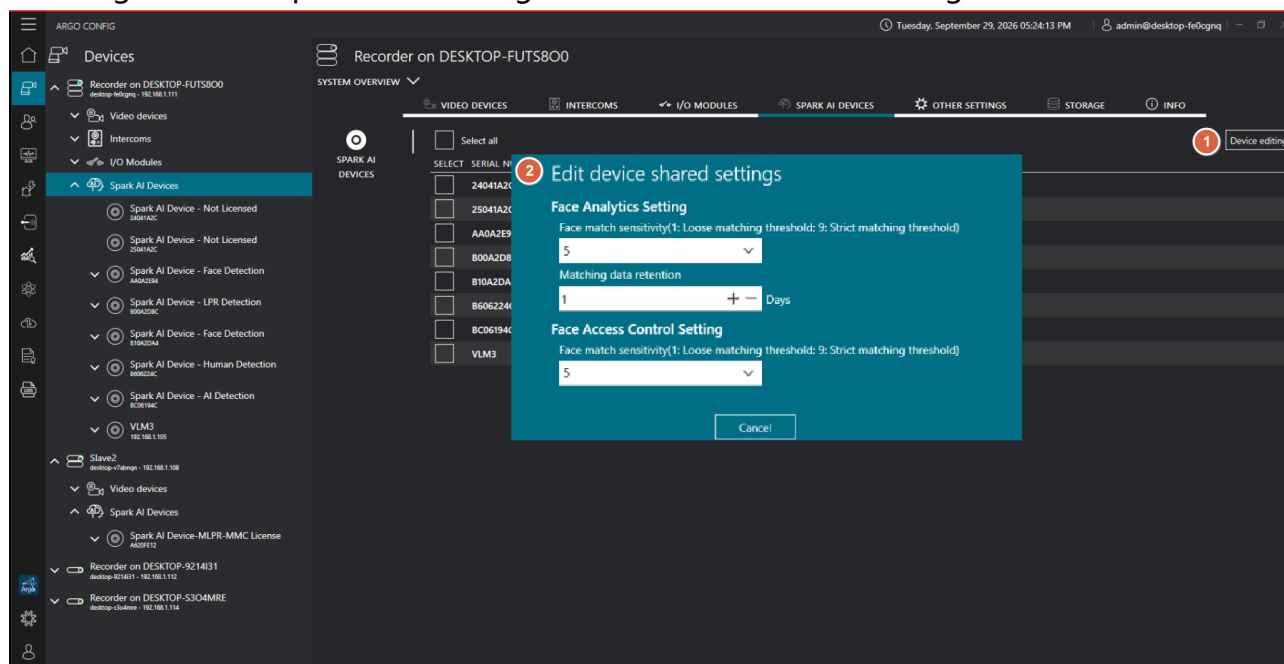
- Ensure the Spark AI device is in an offline status.
- Select the Spark AI device you wish to delete.
- Click [Delete].

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



3.5.6 Edit Common Settings for Spark AI Devices

This function allows you to edit common settings for AI analysis devices of the same type, ensuring consistent parameter configuration and centralized management.



- Click [Device editing].
- Face Analytics Settings
 - Face match Sensitivity: (1–9) Set the sensitivity and matching accuracy. A lower value applies a more lenient matching threshold, while a higher value applies a stricter matching threshold.
 - Matching Data Retention: (1–365 days) Set the number of days to retain matching data.
- Face Access Control Setting
 - Face Similarity Sensitivity: (1–9) Set the sensitivity and matching accuracy. A lower value applies a more lenient matching threshold, while a higher value applies a stricter matching threshold.
- Click [Delete].



3.5.7 INFO

The screenshot displays the Argos Client interface. On the left, a sidebar lists various device categories: Video devices, Intercoms, I/O Modules, and Spark AI Devices. Under Spark AI Devices, several specific devices are listed, including 'Spark AI Device - LPR Detection', 'Spark AI Device - AI Detection' (which is highlighted), 'Spark AI Device - Human Detection', 'Spark AI Device - LPR Detection', 'Spark AI Device - AI Detection', 'Spark AI Device - Flame/Smoke Detection Combination', and 'Spark AI Device-MLPR-MMC License'. The main panel on the right is titled 'INFO' and shows details for the selected 'Spark AI Device - AI Detection' (ID: B3061A4C). The details include: SERIAL NUMBER: B3061A4C, LICENSE TYPE: AI Detection, and COUNT: 8. The interface also has tabs for 'CAMERAS LIST' and 'INFO' at the top right.

Category	Device Name	ID
Spark AI Devices	Spark AI Device - LPR Detection	B1062A4C
Spark AI Devices	Spark AI Device - AI Detection	B3061A4C
Spark AI Devices	Spark AI Device - Human Detection	Z7061F4C
Spark AI Devices	Spark AI Device - LPR Detection	9C0A2B3C
Spark AI Devices	Spark AI Device - AI Detection	8C0E1F4C
Spark AI Devices	Spark AI Device - Flame/Smoke Detection Combination	0000B70B
Spark AI Devices	Spark AI Device-MLPR-MMC License	D45C88BF

Field	Value
SERIAL NUMBER	B3061A4C
LICENSE TYPE	AI Detection
COUNT	8

Browse Spark AI Detection Device Information:

- Serial Number: The AI device identification number.
- License 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 sidebar with 'DATABASE OPTIONS' and a database icon. The main area is divided into four sections for different databases: AI DataBase, ALPR DataBase, Event Manager DataBase, and Metadata DataBase. Each section has two input fields: 'Split file interval' (set to 3) and 'Retention days' (set to 30), both with '+' and '-' buttons to adjust the values. Below these sections is a 'DB Storage Path' table with columns: SELECT, TYPE, DRIVE, MAX SIZE, and FREE SPACE. The table has one row selected, showing 'disk' as the type, 'C:\' as the drive, '237.23 GB' as the max size, and '24.22 GB' as the free space.

SELECT	TYPE	DRIVE	MAX SIZE	FREE SPACE
☒	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://ip address)

Username

Password

Temporary Folder

- 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].

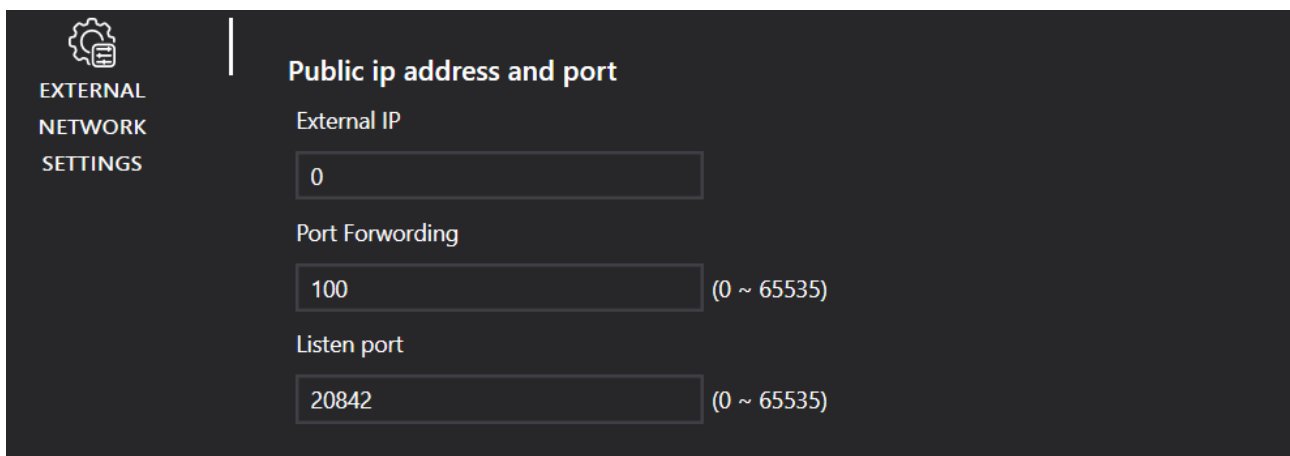


3.6.3 AI Analytics



- 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.

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

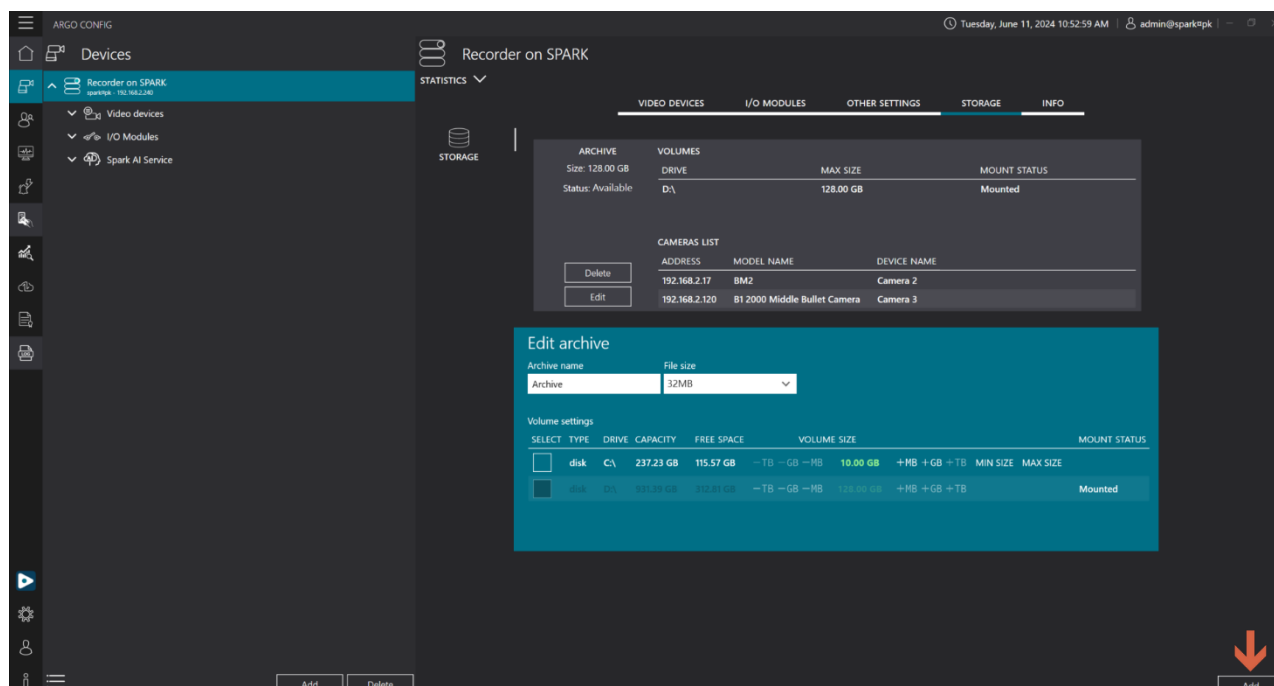
Certificate Information			
ISSUED TO	ISSUED BY	ISSUED ON	EXPIRES ON
argo [redacted].com	G [redacted] In [redacted] R1v1	Jul 8 12:51:30 2026 GMT	Jan 22 12:51:30 2027 GMT

- 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.

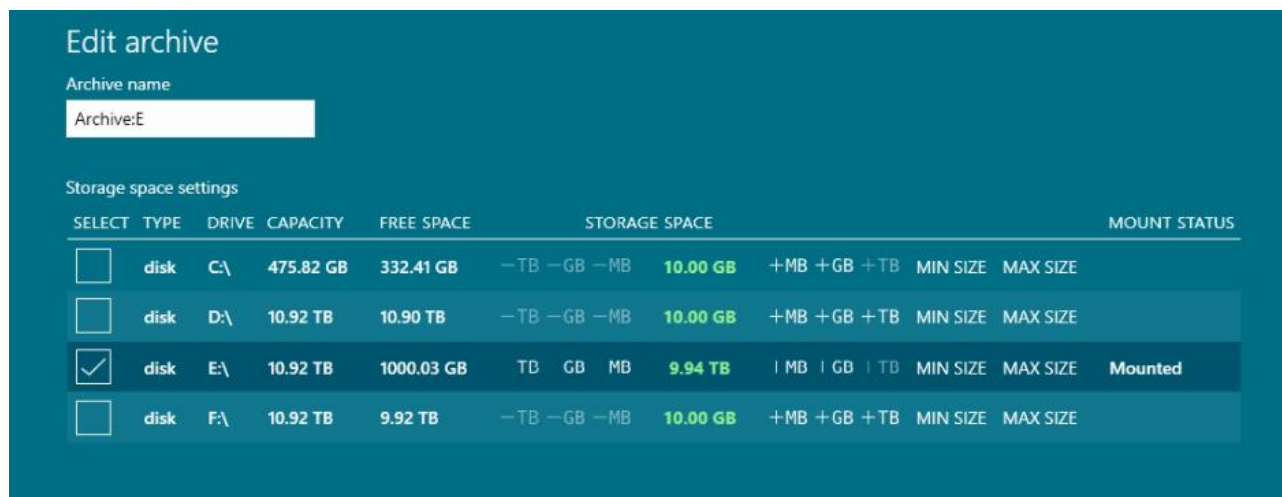


3.7 Storage

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

DRIVE	MAX SIZE	MOUNT STATUS
E:\	9.94 TB	Mounted

ADDRESS	MODEL NAME	DEVICE NAME
192.168.2.13	BM1	Camera 1_測試
192.168.1.24	DM2	Camera 2
192.168.1.25	DM2	Camera 3
192.168.1.26	DM2	Camera 4
192.168.1.27	DM2	Camera 5
192.168.1.28	DM2	Camera 6

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

DRIVE	MAX SIZE	MOUNT STATUS
E:\	9.94 TB	Mounted

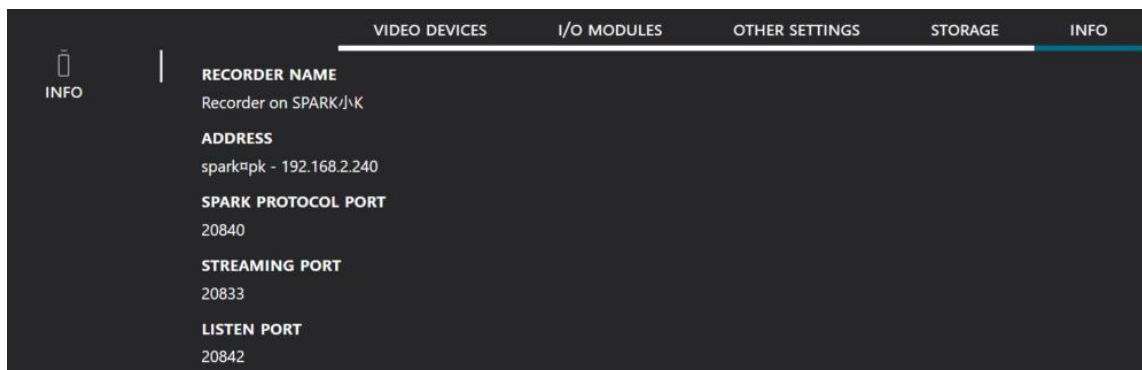
ADDRESS	MODEL NAME	DEVICE NAME
192.168.2.13	BM1	Camera 1_測試
192.168.1.24	DM2	Camera 2
192.168.1.25	DM2	Camera 3
192.168.1.26	DM2	Camera 4
192.168.1.27	DM2	Camera 5
192.168.1.28	DM2	Camera 6

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



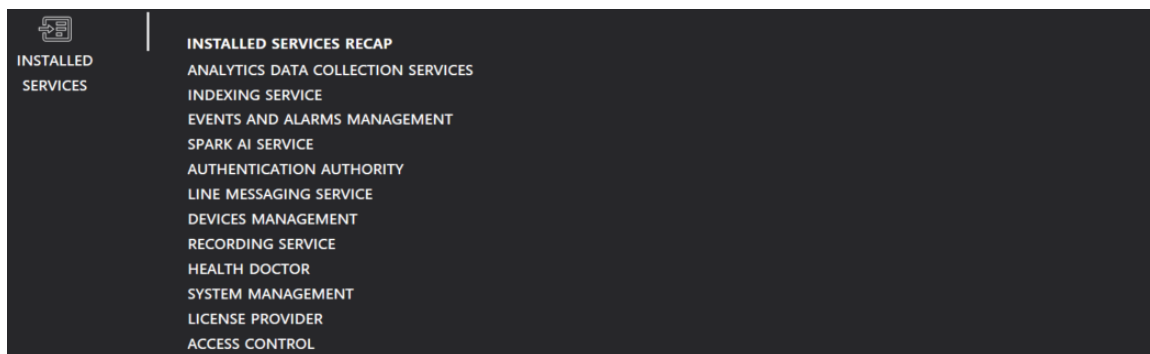
3.8 Information

3.8.1 Information



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

3.8.2 Installed services

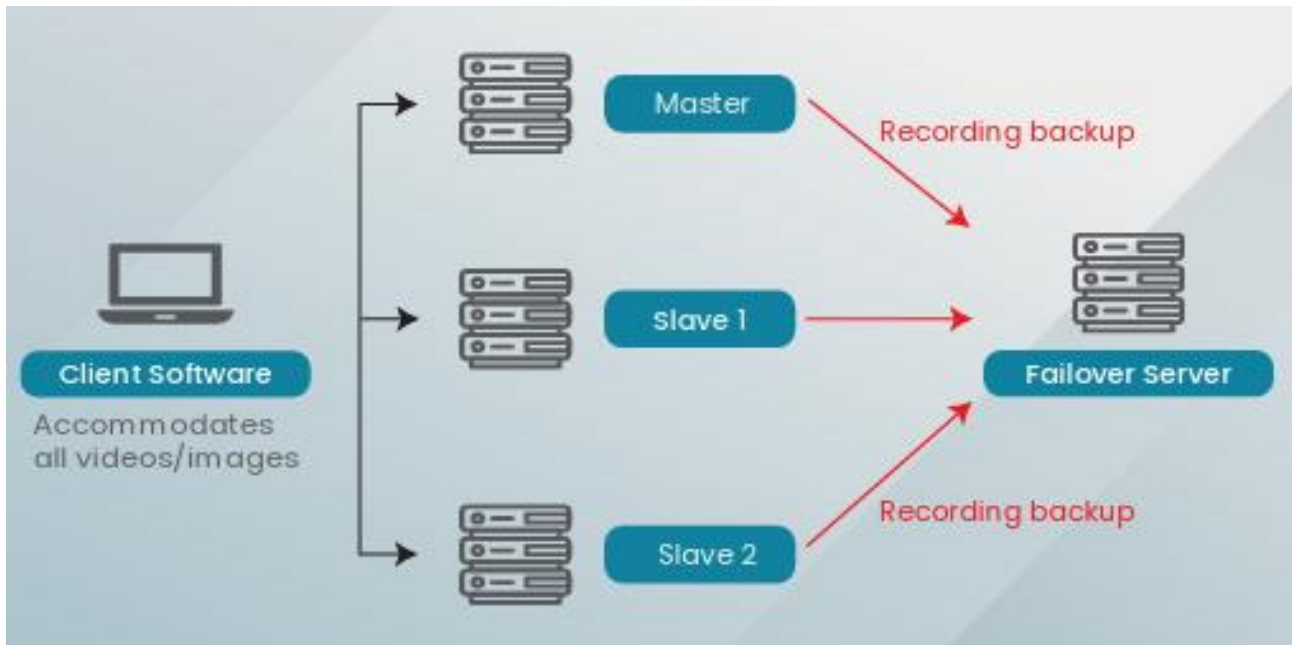


- Installed services content



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

ARGO CONFIG

Devices

Recorder on DESKTOP-119NDSJ
argo-test-pc - 192.168.2.248

Video devices

I/O Modules

Spark AI Service

Add server manually

Host
Connection port

Network password

Node to add profile:
☒ Slave Recorder
☐ FailOver Recorder

DETAILS AUTHENTICATION ADVANCED

☐ Edit server information

☐ Server name

Add Cancel

Add Delete

- Click **[Add]**

Add server manually

Host
Connection port

Network password

Node to add profile:
☒ Slave Recorder
☐ FailOver Recorder



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 window. It has 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 'DETAILS' 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 'AUTHENTICATION' tab. It contains several settings:

- 'Leave authentication authority enabled (if available)': A toggle switch that is turned on. Below it is a note: 'Checking this option the authentication authority on the invited node will be available, resulting in more than one authentication authority available on the network'.
- 'Enable authentication authority mirroring (if supported)': A toggle switch that is turned off. Below it is a note: 'Checking this option an existing authentication authority will be monitored and mirrored making the authentication authority on the invited node a copy of the selected one'.
- 'Selected authentication authority to monitor for mirroring': A dropdown menu showing 'Authentication authority on Recorder on DESKTOP-119NDSJ (argo-test-pc)' with a downward arrow.
- 'Enable authentication authority shadowing (if supported)': A toggle switch that is turned off. Below it is a note: 'Checking this option the mirroring authentication authority on the invited node will be enabled for authentication purposes only when the mirrored authentication authority gets unreachable'.

- 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.

☐

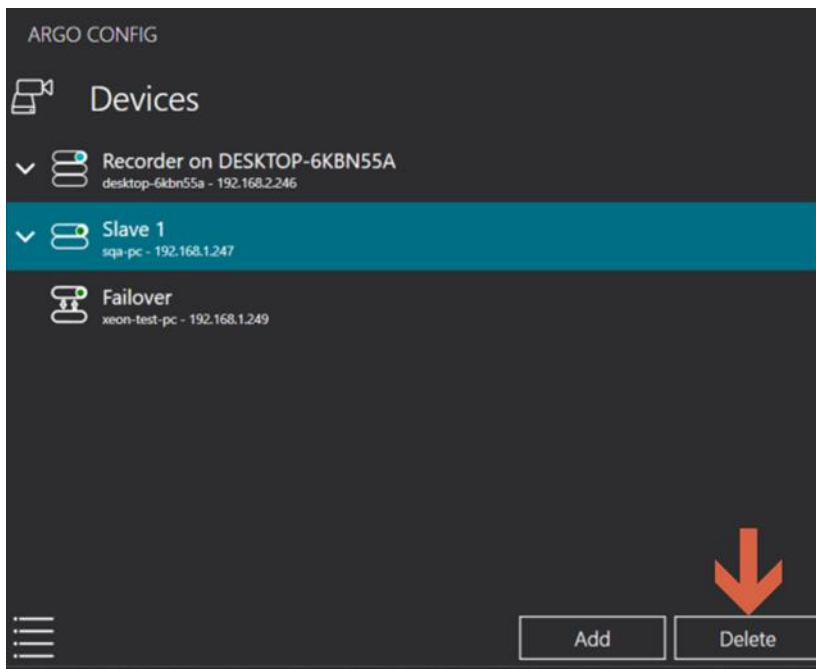
Import directory service config to master

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 left screenshot shows the 'Hierarchy mode' interface. It features a tree view under the 'Recorder on SPARK小K' (192.168.2.240) device. The tree includes 'Video devices' (Camera 1 to 5), 'I/O Modules' (I/O Module 1 and 2), and 'Spark AI Service' (Spark AI Device - Human Detection). The right screenshot shows the 'List mode' interface, displaying a table of devices. The table has columns for ADDRESS, DEVICE TYPE, MODEL NAME, and DEVICE NAME. The 'Recorder' device (192.168.2.240) is highlighted in blue. Below the table, there are 'Add' and 'Delete' buttons.

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

The screenshot shows the 'PASSWORDS' settings page. At the top, there are four tabs: 'SETTINGS', 'GROUPS', 'USERS', and 'CLIENTS SESSIONS'. The 'SETTINGS' tab is selected. Below the tabs, there are three sections: 'Password duration rules:', 'Password length rules:', and 'Password complexity rules:'. Under 'Password duration rules:', there is a toggle switch for 'Maximum number of days of validity' (currently off) and a text input field for 'Number of days before the password expires that a warning message should appear' (currently empty). Under 'Password length rules:', there is a toggle switch for 'Minimum password length' (currently on) and a text input field for 'Minimum password length' (currently set to 5). Under 'Password complexity rules:', there is a toggle switch for 'Enable complex password rules' (currently on). Below this, there is a section for 'Complexity:' with four toggle switches: 'Lower case characters' (on), 'Upper case characters' (off), 'Numeric characters' (off), and 'Special characters' (off).

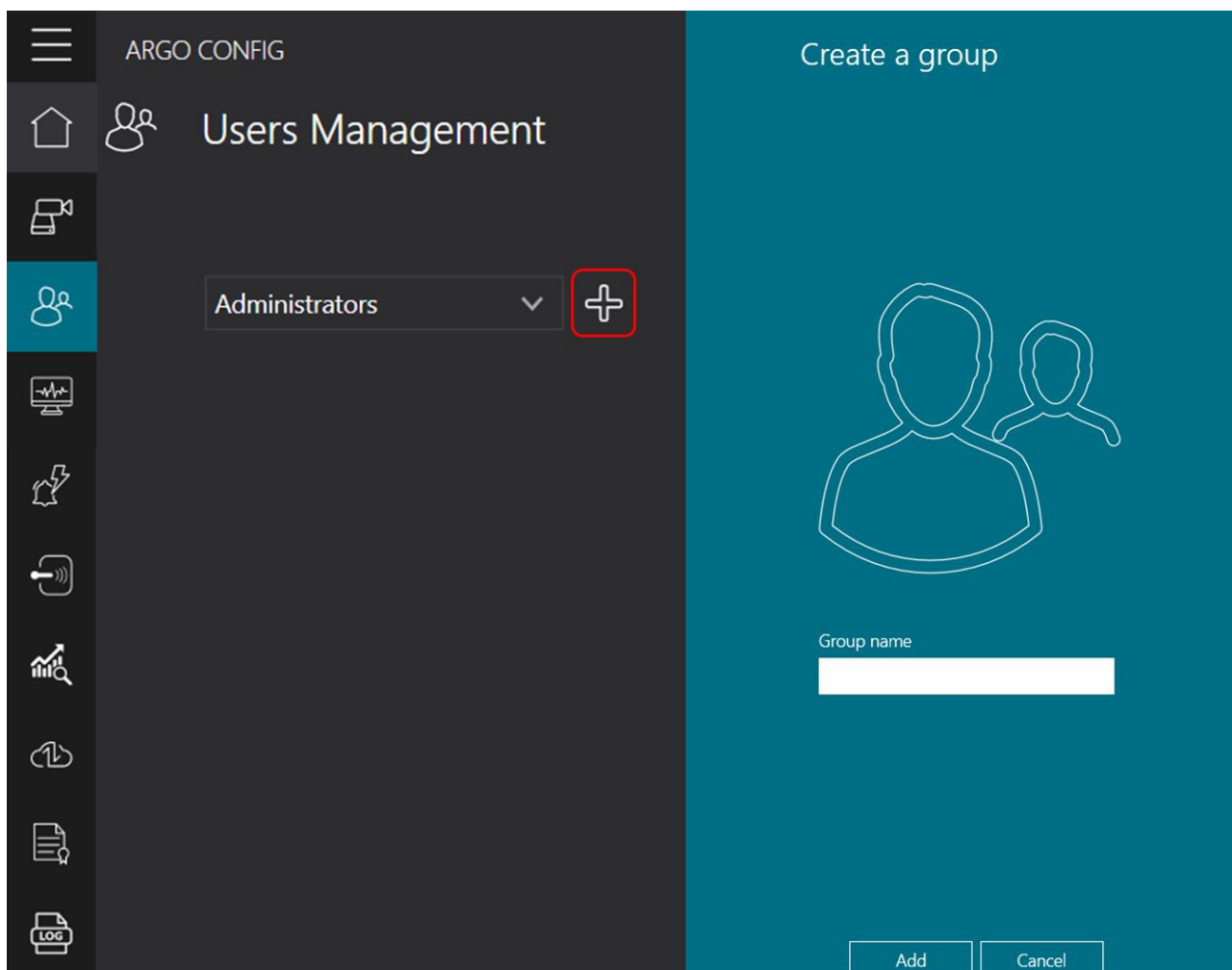
- Password duration rule
Maximum number of days of validity: when the password usage reaches the maximum validity period, it expires and requires resetting. The range of days is from 5 to 100 days.
Reminder message for password expiry: receive a reminder N days before the password expires. The range 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

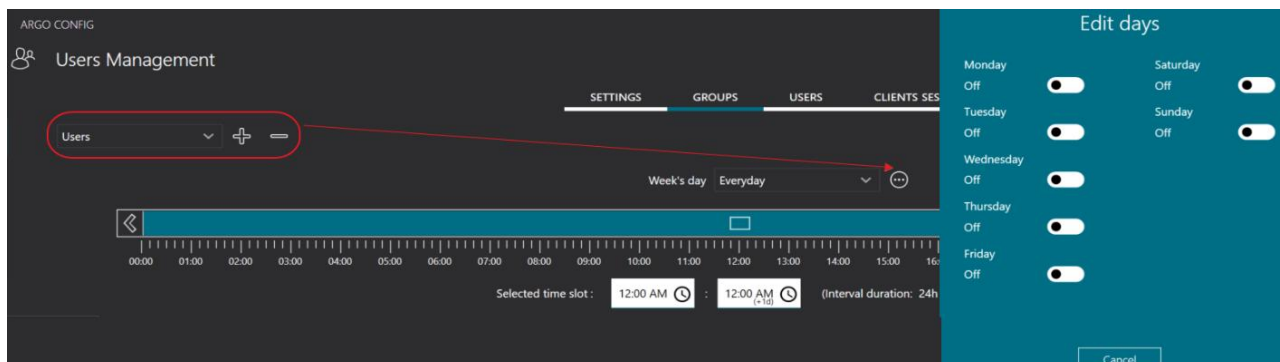
4.2.1 Create groups

- Create groups to classify user access schedules and permissions.



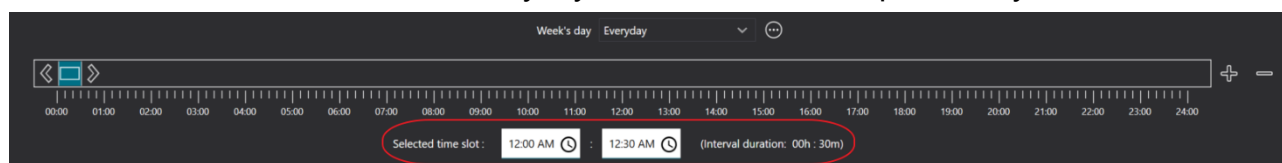
- Click [+]
- Group name: insert name for user group

4.2.2 Set schedules for each group





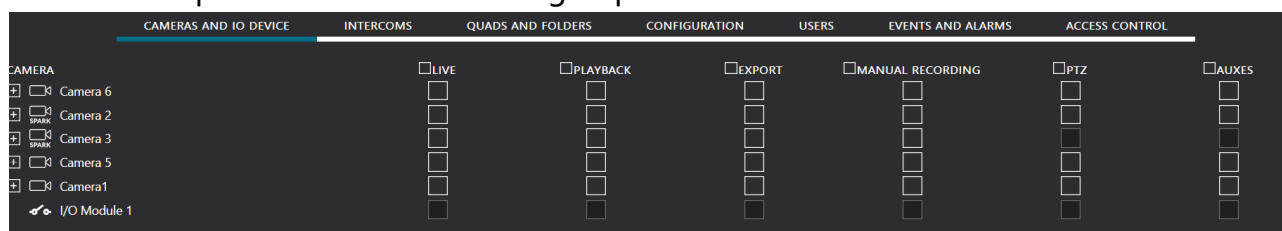
- Edit schedule: default is set everyday. Click [...] to select specific day of the week



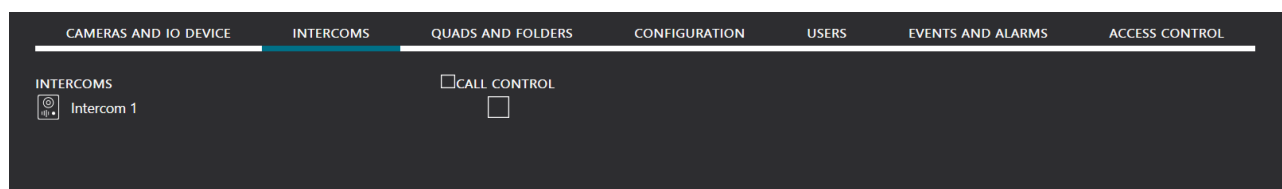
- Add time slot: Click [+] and adjust time slot by dragging left/right or inputting desired time
 - Delete time slot: select the time slot you want to delete and click [-]
 - Edit time slot: adjust the time slot by dragging left/right or inputting desired time
- Note: minimum time interval is 1 hour,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

4.2.3 Set permissions for each group:

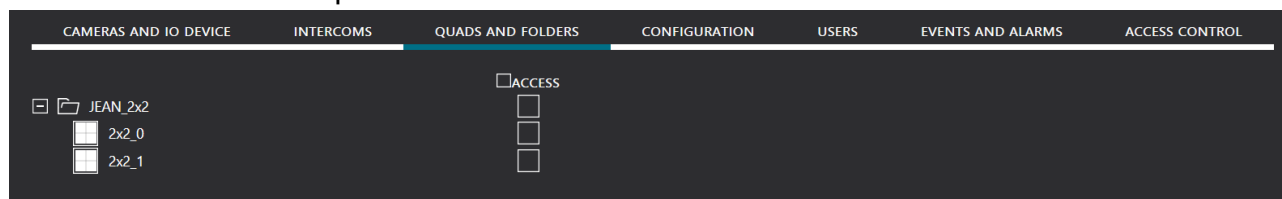
- Allocate permissions for different groups



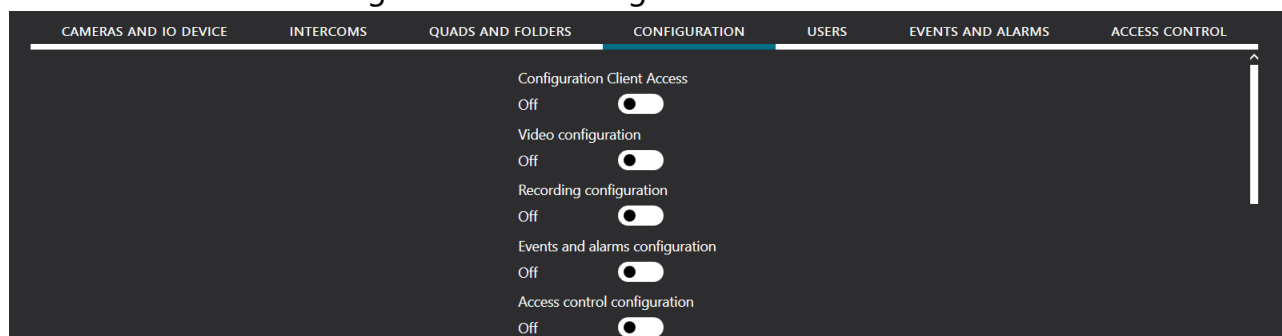
- Cameras: select the camera, I/O modules or devices that the group can manage. Function includes live, playback, export, manual recording, PTZ, Auxes (I/O output).



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



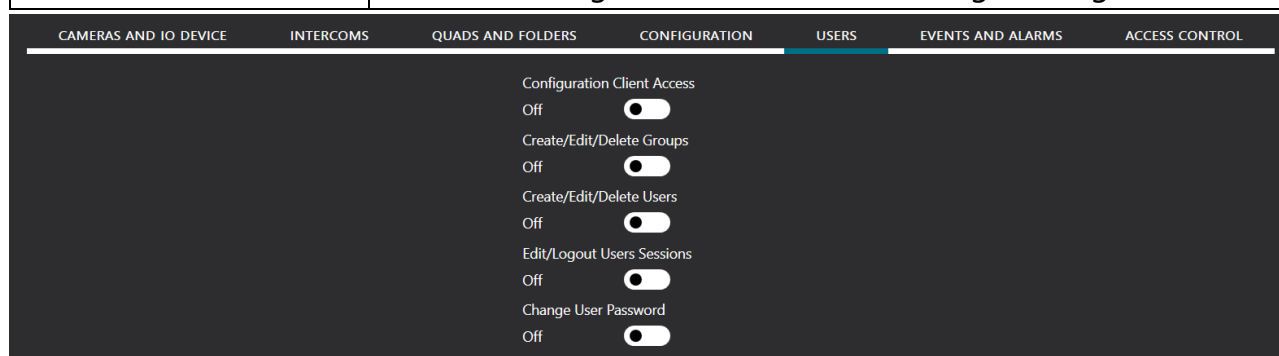
- Quad grants: select the screens that the group can view. Once enabled, the group can view these monitoring screens in the Argo Client.





- 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 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.

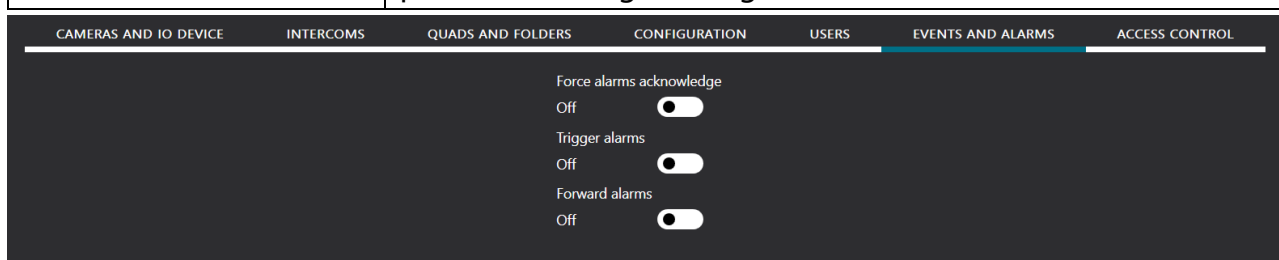


- User grants: set user configuration that the group can manage.

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

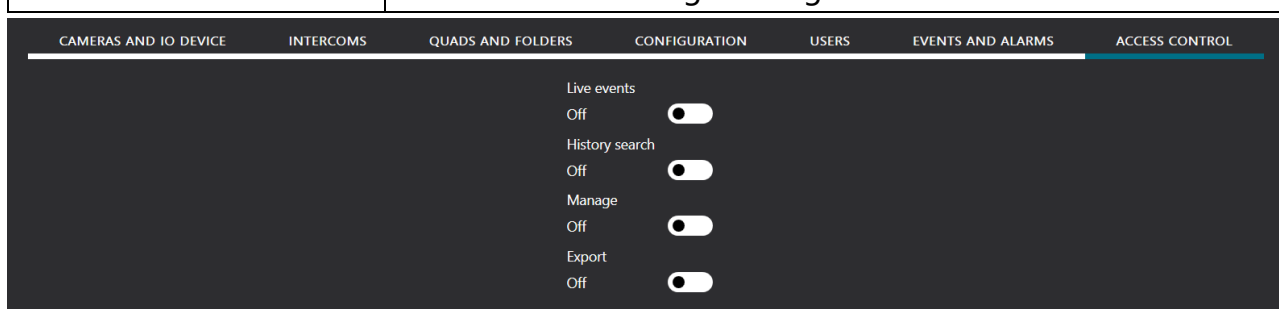


Options	Description
Create/Edit/Delete Groups	When disabled, users of the selected group will not be able to create/edit/delete groups on Argo Config.
Create/Edit/Delete Users	When disabled, users of the selected group will not be able to create/edit/delete users on Argo Config.
Edit/Logout User Sessions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



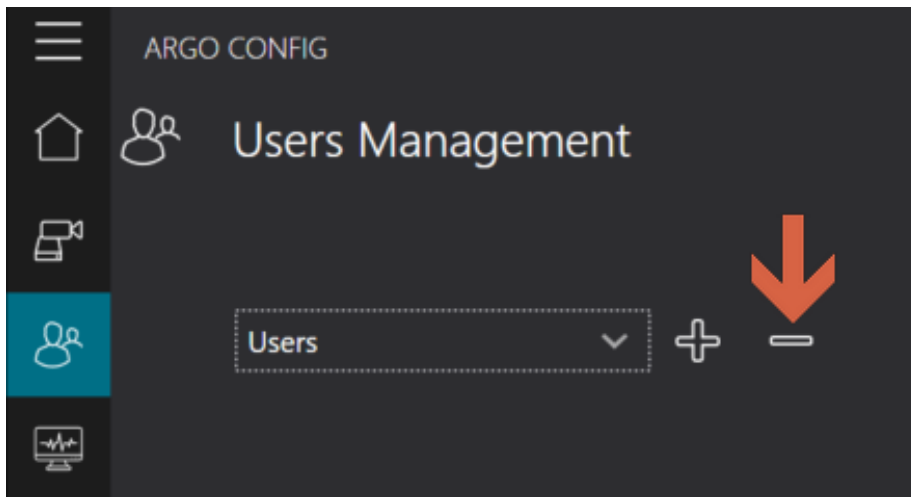
- Access control: set access control configuration that the group can manage.

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

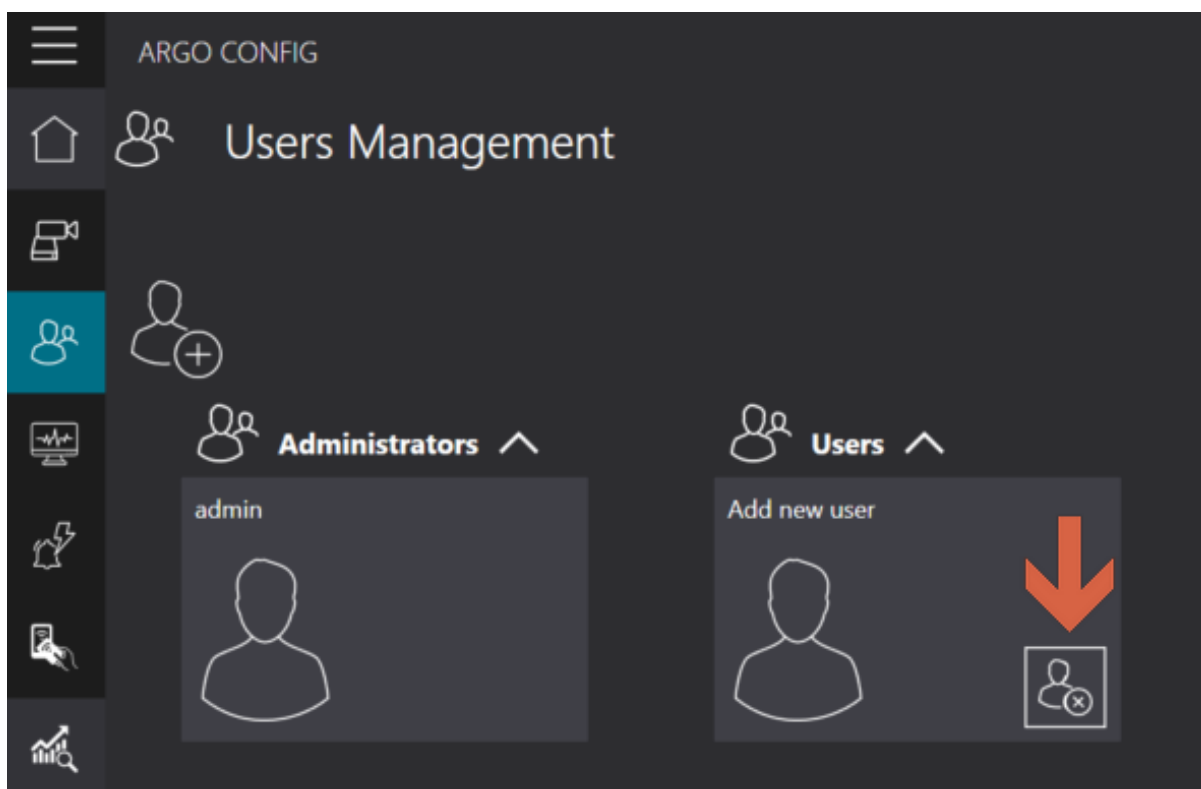
The screenshot displays the 'Users Management' section of the Argo Client interface. On the left, a sidebar contains a menu with icons for home, users, and other functions. The main area is titled 'Users Management' and features a tabbed interface with 'SETTINGS', 'GROUPS', 'USERS', and 'CLIENTS SESSIONS'. The 'USERS' tab is active, showing a list of users under the 'Administrators' group, with an 'admin' user listed. A large orange arrow points to the '+ Add new user' button. To the right, a modal window titled 'Add new user' is open, containing the following fields and options:

- Group:** A dropdown menu with 'Users' selected.
- Username:** A text input field with 'Add new user' entered.
- Password:** A text input field with a toggle icon.
- Confirm password:** A text input field with a toggle icon.
- User password never expires:** A toggle switch (currently off).
- User must change password:** A toggle switch (currently on).
- Cancel:** A button at the bottom right.

- 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

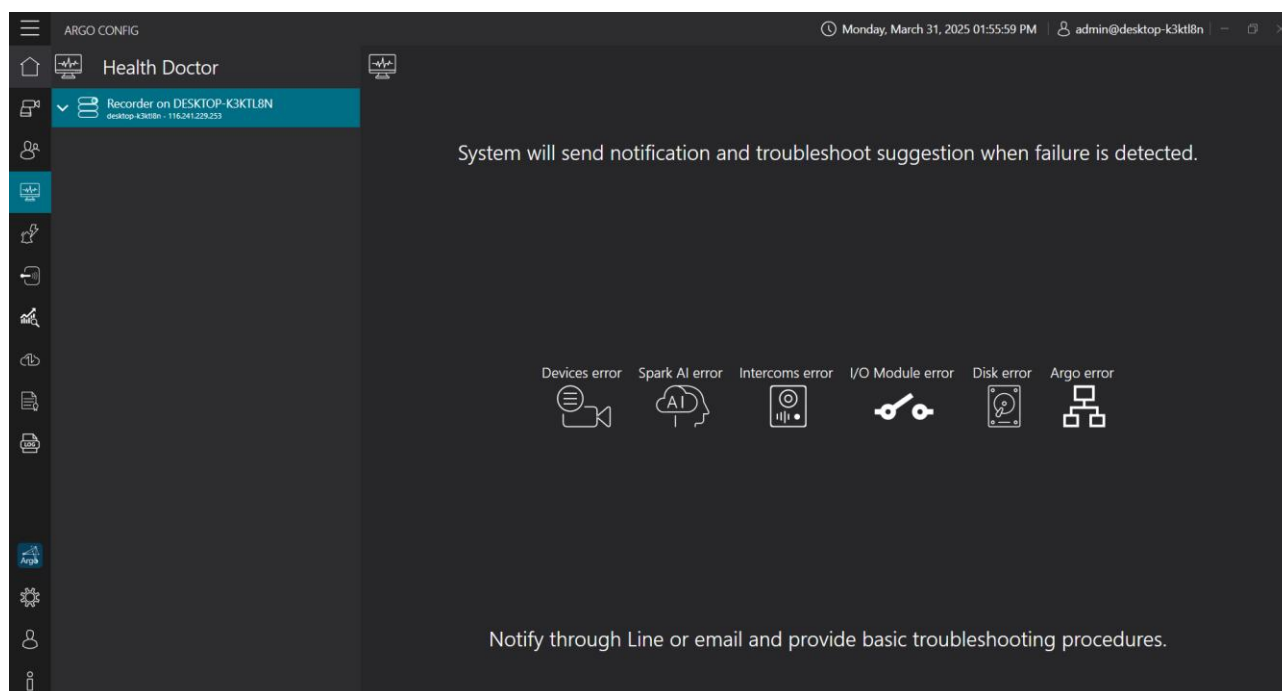
- View and disconnect users connected to Argo Client

ARGO CONFIG						
Users Management						
SETTINGS GROUPS USERS CLIENTS SESSIONS						
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.

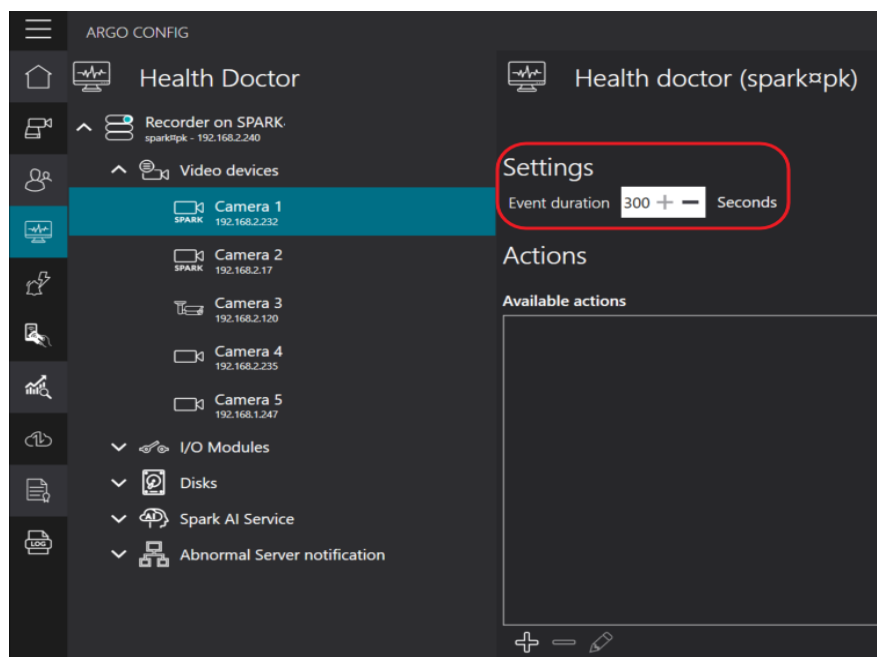


5. HEALTH DOCTOR



- 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 'Actions' panel shows 'Available actions' with a list of actions. An orange arrow points to the '+' icon in the 'Available actions' list. The main dialog box has the following fields:

- Action name:** A text input field.
- Action category:** A dropdown menu with 'Send email' selected.
- Select email account:** A dropdown menu with a search icon and a list of accounts.
- To:** A text input field with 'Cc' and 'Bcc' buttons.
- Subject:** A text input field.

At the bottom of the dialog box 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

- 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

Add

Cancel

- 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

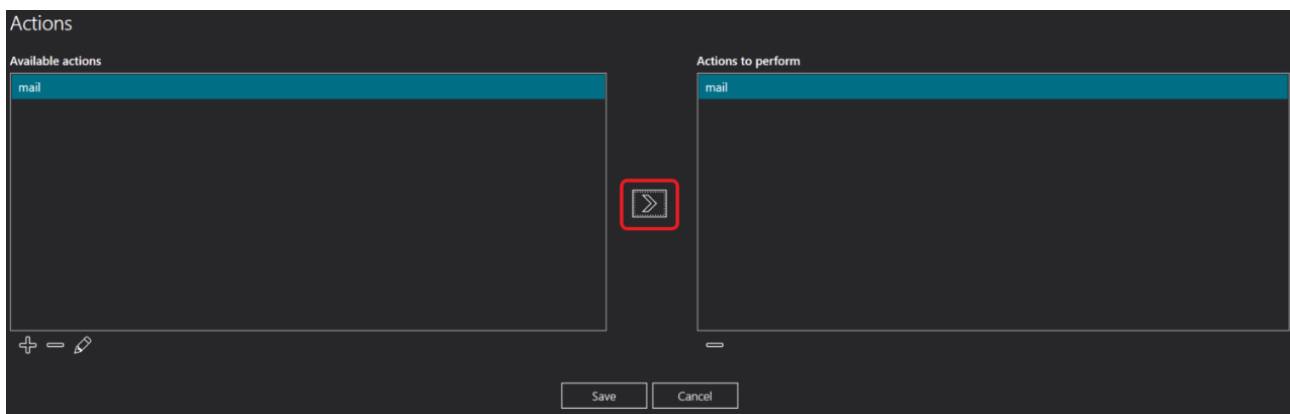
Available actions

mail

- Select the response action and then click [-]



5.5 Execute response action



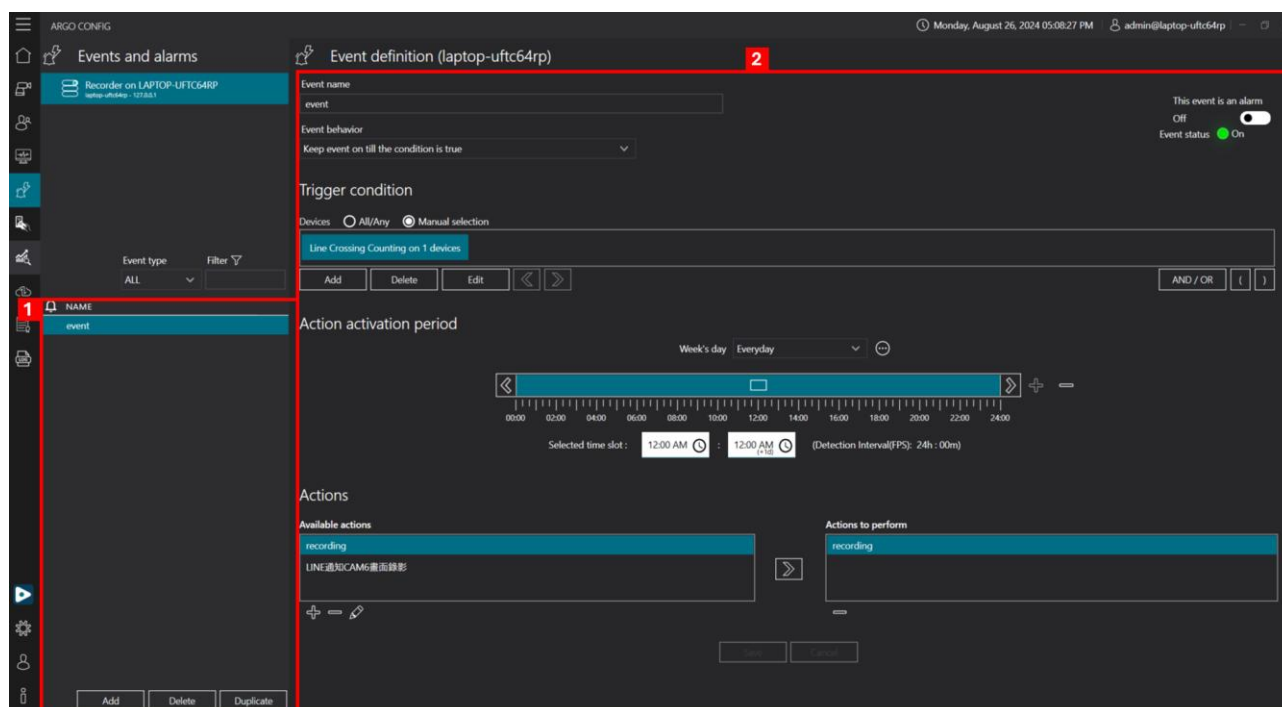
- Apply the executed response behavior: select the response behavior you want to apply, and click [>]
- Delete the executed response behavior: select the executed response behavior you want to delete and click [-]



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

The screenshot displays the 'Event definition (sparkpk)' window in the Argo Config application. The 'Create new event' modal is open, showing the following configuration:

- Event name:** AI_2.120_Object
- Event behavior:** Keep event on till the condition is true
- Trigger condition:** Manual selection
- Action activation period:** Week's day: Everyday, Selected time slot: 12:00 AM to 12:00 AM (Interval duration: 24h: 00m)
- Actions:** AI_2.120_Object

A red arrow points to the 'Add' button at the bottom left of the modal.

- 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

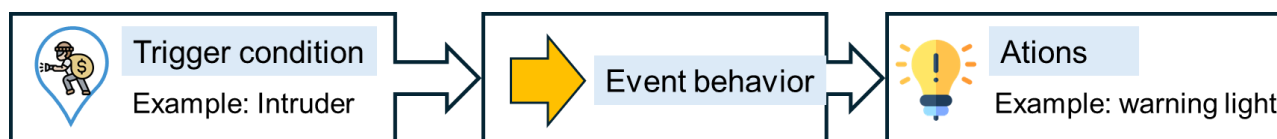
- Select the event you want to edit, proceed with the editing and click **[Save]**

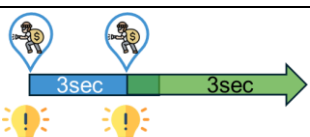
C. Copy/Delete Event

- 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	 Each trigger is recorded as a single event.	Intruder enters the area, the warning light activates immediately.
Keep event active for X seconds from the condition trigger	 After the trigger ends, the event continues for 5 seconds before concluding.	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	 If no additional triggers occur within the 5-second continuation period, the event concludes.	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	 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	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

Trigger condition

Devices ☐ All/Any ☒ Manual selection

Object Detection on 1 devices

Add Delete Edit < >

Add condition

Event Category
System events

Events
Connected to device

Negate event
Off

Filter

Sources

SELECT	NAME
☐	Camera 1 (192.168.2.232) - on Recorder on SPARK小K (192.168.2.240)
☐	Camera 2 (192.168.2.17) - on Recorder on SPARK小K (192.168.2.240)
☐	Camera 3 (192.168.2.120) - on Recorder on SPARK小K (192.168.2.240)
☐	Camera 4 (192.168.2.235) - on Recorder on SPARK小K (192.168.2.240)
☐	Camera 5 (192.168.1.247) - on Recorder on SPARK小K (192.168.2.240)
☐	I/O Module 1 (192.168.2.9) - on Recorder on SPARK小K (192.168.2.240)

Operator across sources

☒ AND ☐ OR

Add Cancel

- 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
Dual Verification	Select any two access control devices for access verification. For example, the event is triggered when both Face Recognition and RFID verification are successful.
Category signaled for Face Detection	Triggers an event when a face is detected.
Category signaled for Plate Detection	Triggers an event when a license plate is detected.
Category signaled for RFID	Triggers an event when an RFID credential (eTag or card) is detected.



Event	Description
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.

- Dual Authentication Settings

The Dual Authentication function combines two types of detection devices, such as an RFID card reader and Face Recognition (FACE), for identity verification. Before using this function, create the RFID and FACE access records and ensure that the User Name is identical in both records. Dual authentication is successful when both RFID and face verification are completed successfully.

(1) Confirm that the **User Name** is identical for both the FACE and RFID records.

ALL Allow Deny Expired						
List	Filter	ID type				
ALL		ALL	Add list Edit			
NO	USER NAME	ACCESS ID	ID TYPE	START DATE	EXPIRE DATE	TIME VALIDITY
1	Dennis	0660219963	RFID	Thursday, September 17, 2026	Tuesday, January 1, 2030	00:00:00 - 24:00:00
2	Dennis	0909776	FACE	Wednesday, July 22, 2026	Tuesday, January 1, 2030	00:00:00 - 24:00:00

(2) Under **Source**, select the two` detection devices used for dual authentication.

Event Category: Access control

Events: Dual Verification

Filter

Sources

SELECT	NAME	IP ADDRESS	NODE
☐	1F室外大門口 - AnalyticsStreamPerimeter4	192.168.1.132	Recorder on DESKTOP-FUTS800 (192.168.1.111)
☒	Soyal - Soyal Node	192.168.1.151	Recorder on DESKTOP-FUTS800 (192.168.1.111)
☐	一樓大廳人臉辨識 - AnalyticsStreamPerimeter2	192.168.1.135	Recorder on DESKTOP-FUTS800 (192.168.1.111)
☒	會議室PM1 - AnalyticsStreamPerimeter5	192.168.1.123	Recorder on DESKTOP-FUTS800 (192.168.1.111)



- 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
VLM detection	Triggers an event when the device detects a matching VLM event.



VLM detection

- Scenario: To trigger an event when a person is detected without a hat or without clothing, configure the conditions as follows.

Edit condition

Event Category
Spark AI Service

Events
VLM detection

Filter
Prompt

Detection Type
Person Appearance

Filter

Sources ☒ All ☐ Any

SELECT	NAME	IP ADDRESS	NODE
☒	大門 - AnalyticsStreamPerimeter7 (VLM3)	192.168.1.132	Recorder on DESKTOP-FUTS8O0 (192.168.1.111)
☐	會議室DM2 - AnalyticsStreamPerimeter7 (VLM3)	192.168.1.129	Recorder on DESKTOP-FUTS8O0 (192.168.1.111)

Detection Source ☐ All ☒ Any

SELECT	NAME	STATUS
☒	Hat	Exclude
☒	Clothes	Exclude
☐	Pants	Include
☐	Glasses	Include

OK Cancel

- Filter: Select the detection source, including Prompt and Match database.
- Detection Type: Select the detection type.
- Source: Select the detection devices.
 - **All:** The event is triggered only when all selected devices detect the event.
 - **Any:** The event is triggered when any selected device detects the event.
- **Detection Source:** Select the detection items.
 - **All:** The condition is met only when all selected items are triggered.
 - **Any:** The condition is met when any selected item is triggered.
- Status:
 - **Include:** The specified object must be detected.
 - **Exclude:** The specified object must not be detected.



– Camera video analytics

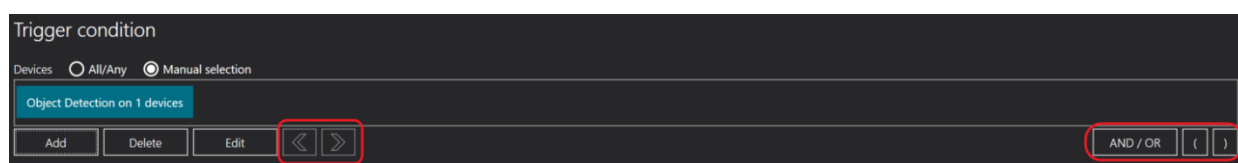
Event	Description
Tampering	Triggers when tampering is detected
Motion	Triggers when motion is detected
Audio	Triggers when audio is detected
Tripwire	Triggers when line crossing behavior is detected.
People density	Triggers when crowd gathering is detected.
Perimeter	Triggers when an intruder is detected.
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	– 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 [**([])**] 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

Event definition (sparkpk)

Event name
AI_2.120_Object 1

Event behavior
Keep event on till the condition is true

Trigger condition

Devices ☐ All/Any ☒ Manual selection

Object Detection on 1 devices

Add Delete Edit

Event Category
Spark AI Service

Events
Object Detection

Filter

Sources

SELECT	NAME
☒	Camera 3 - AI_2.120_Object (192.168.2.120) - on Recorder on SPARK (192.168.2.240)
☐	Camera 5 - AnalyticsStreamPerimeter2 (192.168.1.247) - on Recorder on SPARK (192.168.2.240)

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

6.3.4 Delete trigger condition

Event definition (sparkpk)

Event name
AI_2.120_Object 1

Event behavior
Keep event on till the condition is true

Trigger condition

Devices ☐ All/Any ☒ Manual selection

Object Detection on 1 devices

Add Delete Edit

- 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 



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:  :  (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

Add action

Action name

Action category

Start recording

Select a camera

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

Add action

Action name

Action category

Aux output

Action duration

0 + -

Actions delay time

0 + -

Select an aux output

Camera 1 - I/O output 0 (172.21.5.10) - Recorder on LAPTOP-UFTC64RP (laptop-uftc64rp)

Set aux output new status

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

Add action

Action name
Test

Action category
Send email

Actions delay time
0

Select email account
NewEmailAccount

To

Subject

Body

Email accounts

Configured email accounts
Gmail

Name
Gmail

SMTP server name
smtp.gmail.com:587

Username
test

Password
.....

Email displayed name
Spark_Alarm_gmail

Email address
sparksq888@gmail.com

- 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
LED Display

Actions delay time
0 + - Sec

IP Address

Content [Detail Settings ...](#)

- Action Delay Time: Set the delay time before the action is executed after the event is triggered.
- IP Address: Enter the IP address of the LED display.
- Content: Click [Detail Settings] to configure the display content.

LED Detail Settings

Insert Content

Recognition Text
[Access ID](#) [User name](#)

Color
Red [Insert Color](#)

Effect
No Effect [Insert Effect](#)

Display Timeout(ms) 5000 [Text After Clear](#) Please present your ID [Insert Clear](#)

Idle Content
No tailgating [Insert Text](#) [Line Break](#)

Stream
video stream 1(192.168.1.111)-Recorder on DESKTOP-FUTS800~ [Insert Stream](#)

Content

Example

Format
{lpr(licenseplate)}
{lpr(username)}
{RGB(0,255,0)}
{CLEAR(5000)}
{CLEAR(5000)}(LicensePlate}
{EFFECT(0)}
{STREAMUUID(uid)}
Text

Single-line Example [Apply](#)
{lpr(licenseplate)}(RGB(0,255,0)){CLEAR(10000)}(PleaseExchangeID)){EFFECT(0)}{STREAMUUID(xxxxxxxx-xxxx-xxxx-xxxx-xxxx)}

Preview
ABC-1234

Two-line example [Apply](#)
{lpr(licenseplate)}(RGB(0,255,0)){CLEAR(5000)}
No tailgating(RGB(255,0,0)){EFFECT(0)}{CLEAR(5000)}(LPR)){STREAMUUID(xxxxxxxx-xxxx-xxxx-xxxx-xxxx)}

Preview
ABC-1234
No tailgating

- Recognition Text: Display the Access ID or User Name on the LED panel.
- Access ID Format: {lpr(licenseplate)}



- User Name Format: {lpr(username)}
- Color: Set the text color displayed on the LED panel. Format: {RGB(0, 255, 0)}
- Effect: Set the text display effect.
 - No Effect: Disable the display effect. Format: {EFFECT(6)}
 - Scrolling Effect: Display the text scrolling from left to right. Format: {EFFECT(0)}
- Display Timeout (ms): Set how long the recognition information remains on the LED panel before it is cleared. If no clear time is specified, the recognition information remains displayed until the next recognition event. Format: {CLEAR(5000)} indicates that the information will be cleared after 5 seconds.
- Text After Clear: Specify the text to be displayed after the recognition information is cleared. For example, {CLEAR(5000)}(Please Replace Your Pass)} displays the recognition information for 5 seconds, then clears it and displays "Please Replace Your Pass."
- Idle Content: Set the default text displayed on the LED panel when no event is detected.
- Stream: Select the camera recognition stream source associated with the LED display.



H. HTTPS Event Sending

Add action

Action name

Action category

HTTPS Event Action

Actions delay time

0 + - Sec

Type

POST

Username

Password

URL

Content

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

Add

Cancel

- **Action Delay Time:** Set the delay time before the action is executed after the event is triggered.
- **Type:** Select **POST** or **GET**.
- **Username:** Enter the account used for login or authentication when sending the HTTP event.
- **Password:** Enter the password used for login or authentication when sending the HTTP event.
- **URL (Uniform Resource Locator):** Enter the URL to be accessed or executed, for example: <https://192.168.X.X:8080/> or <https://www.xxxx.com>.



- **Content:**

- Enter {time} to display the event trigger time.
- Enter {Event Name} to display the name of the triggered event.

6.4.3 Edit response action

The screenshot shows the 'Edit action' interface. On the left, under 'Available actions', 'LINE MESSAGE' is selected. The main area contains the following fields:

- Action name:** LINE MESSAGE
- Action category:** Line message
- Actions delay time:** 0
- Token:** 69z8Usj3gVSV/MUaDIPf4leze/9d8Q0c85F5X43HggYkkHMFu7LC2Fd7v8L6H3tB4trZFVupwWFn/
- Body:** test

- Select response action and click

6.4.4 Delete response action

The screenshot shows the 'Actions' panel with 'AI_2.120_Object' in the 'Available actions' list. A red arrow points to the minus icon at the bottom left of the list.

- Select response action and click [-]

6.4.5 Execute response action

The screenshot shows the 'Actions' panel with 'AI_2.120_Object' in both the 'Available actions' and 'Actions to perform' lists. A red box highlights the greater-than icon between the two lists. 'Save' and 'Cancel' buttons are at the bottom.

- 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 a web interface for creating and editing events. The left screenshot is titled 'Create new event' and the right is 'Edit alarm configuration'. A red arrow points from the left to the right.

Create new event

Event name: [Text input field]

Event behavior: [Dropdown menu: Keep event on till the condition is true]

Trigger condition: [Form with 'Devices' section (All/Any, Manual selection) and 'AND / OR' logic]

Action activation period: [Time range selector with 'Week's day' dropdown (Everyday) and 'Selected time slot' (12:00 AM to 12:00 AM, Interval duration: 24h : 00m)]

Actions: [Available actions: LINE MESSAGE, Actions to perform: [Text input field]]

Edit alarm configuration

1. This event is an alarm: [Toggle switch: On]

2. Edit alarm configuration: [Text input field]

Event status: [Green circle icon: Off]

Alarm status: [Red circle icon: Unknown]

- 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

1

100

Lowest

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

60

+

-

 seconds since alarm has been triggered

☒

 Can be triggered manually

☐

 Play a sound on client machine when an alarm occurs

☐

 Use event scheduler

Cancel

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

Related devices

ADDRESS	DEVICE NAME	MODEL NAME	STATUS	NODE

Edit devices

Filter

SELECT	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

Save Cancel

- 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:
 - On: The alarm recipient in Argo Client must enter a note in the User Note field before closing or forwarding the alarm.
 - Off: The alarm can be closed without entering a user note.
 - If Auto-Close Alarm is enabled, this requirement does not apply. The system will automatically close the alarm.
- Auto-acknowledge alarm:
 - On: The alarm is automatically closed after the specified time. Range: 1–300 seconds.
 - Off: The alarm must be closed manually by the user. If the same event continues to be triggered while the alarm remains open, no additional alarm records will be generated.



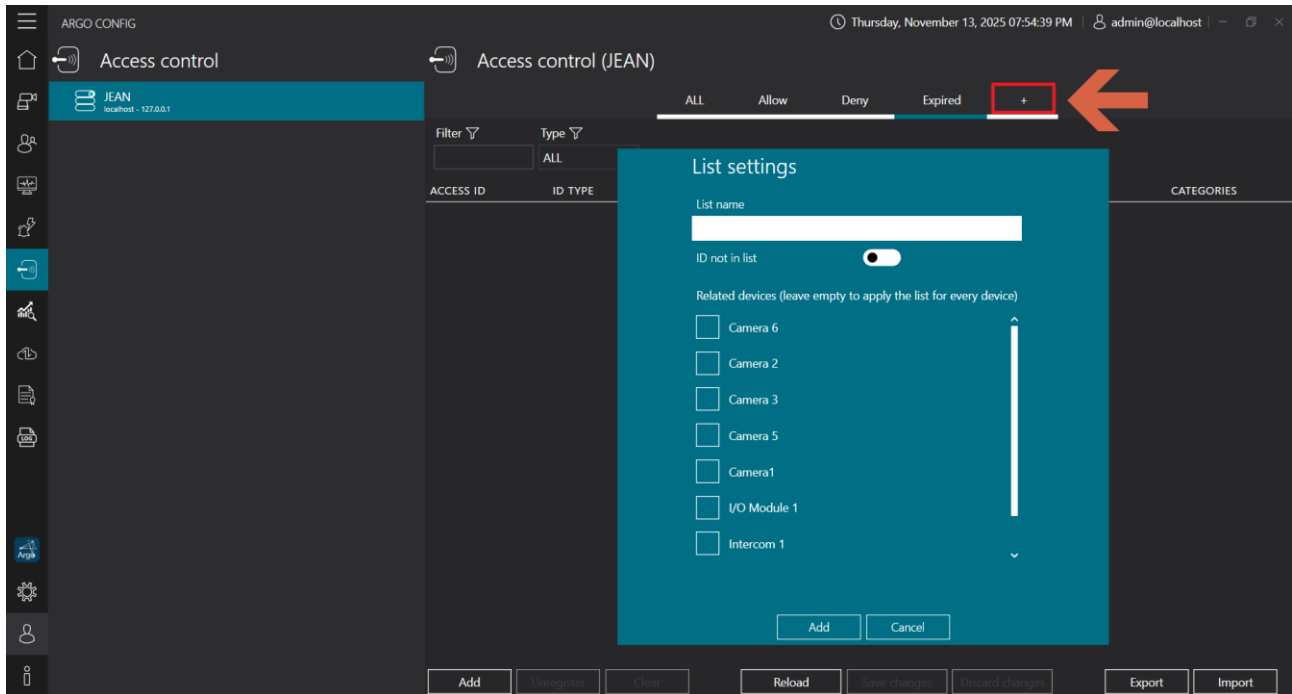
- Manually Triggerable: When enabled, you can click **[Manually Trigger Alarm]** to test the Argo Client's alarm sending functionality.
- Sound Alert on Alarm Trigger: When enabled, a sound will be emitted from the Argo Client host when an alarm is triggered.



7. ACCESS CONTROL

7.1 Add/Edit/Delete list

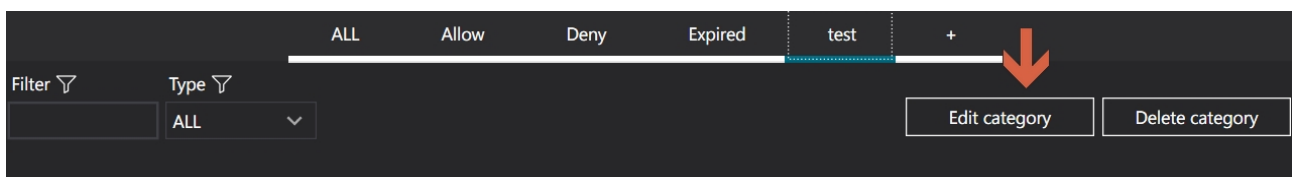
A. Add list



- 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

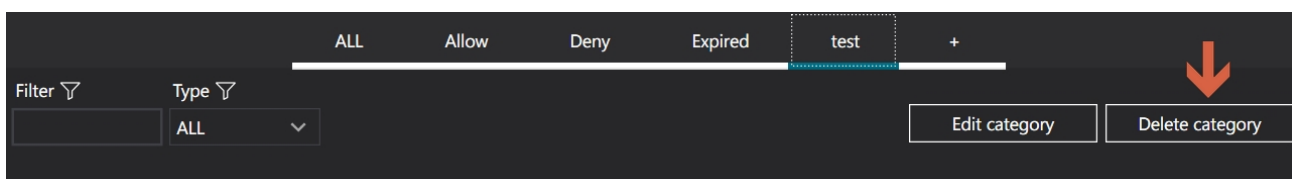
Note: leave empty to apply the list for every device

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

- Click [Add] in the bottom-left corner.
- User Name: Enter the user name.
- ID Type: Select LPR (License Plate Recognition), RFID, or FACE (Face Recognition). Multiple access records can be added under the same user name. Enter an alphanumeric ID without hyphens (-), for example, ABC1234. Each Access ID must be unique.
- LPR: Used for license plate recognition.
 - Access ID: The system uses this ID to identify vehicle entry and exit. Enter the license plate number in this field.
- RFID: Used for high-frequency RFID (e-Tag).
 - Access ID: The system uses this ID to identify entry and exit. Enter the RFID number in this field.
- FACE: Used for face recognition.
 - Access ID: Enter an identification number, such as an employee ID or other unique ID.
 - Image File Path: Upload a reference image for face recognition. Only JPG files with a clear, visible face are supported (as shown below).



- Note: Before uploading an image, make sure Face Detection has been added under [Spark AI Device].



- Begin of overall validity (Start): Set the start date of the Access ID validity period.
- End of overall validity (End): Set the end date of the Access ID validity period.
- Begin of Daily validity (Start): Set the daily start time during which the Access ID is valid for entry and exit.
- End of Daily validity (End): Set the daily end time during which the Access ID is valid for entry and exit.
- List: Select the status of the record: Whitelist, Blacklist, or Expired, and select the custom list to which the record belongs.
- Note: Enter an optional note for the Access ID.

7.2.2 Edit access ID

ARGO CONFIG Tuesday, June 11, 2024 08:30:04 PM admin@master

Access control Access control (master)

Recorder on DESKTOP-9C43ST0 master - 192.168.1.250

台灣油維科 Slave 1 slave1 - 192.168.2.251

台灣油維科 Slave 2 slave2 - 192.168.1.252

Filter Type ALL

ARQ-2991	LPR	Tuesday, June 11, 202	Thursday, July 11, 202	00:00:00 - 24:00:00	Deny
FHC8637	LPR	Tuesday, June 11, 202	Wednesday, June 12, .	00:00:00 - 24:00:00	Allow

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

Categories: All Deny

Add Unregister Clear Reload Save changes Discard changes Export Import

- Select the access ID you want to edit, proceed to edit and then 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

ARGO CONFIG Tuesday, June 11, 2024 08:28:15 PM admin@master

Access control (master)

ALL Allow Deny Expired +

Filter Type ALL

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

Access id: ARQ-2991

Id type: LPR

Begin of overall validity: 6/11/2024 12:00:00 AM

End of overall validity: 7/11/2024 12:00:00 AM

Begin of daily validity: 12:00 AM

End of daily validity: 12:00 AM (+1d)

Notes:

Categories: Allow Deny

Add Unregister Clear Reload Save changes Discard changes Export Import

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

B. Clear

ARGO CONFIG Tuesday, June 11, 2024 08:27:34 PM admin@master

Access control (master)

ALL Allow Deny Expired +

Filter Type ALL

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

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:

Categories: Allow Deny

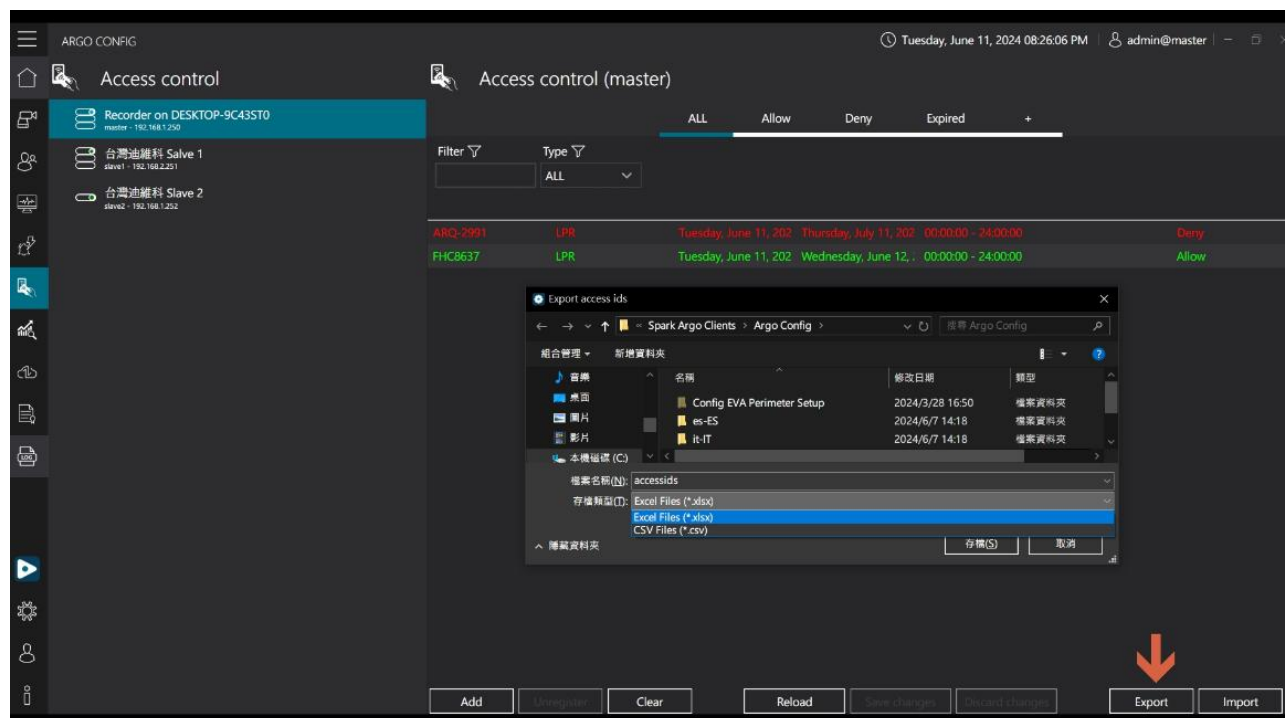
Add Unregister Clear Reload Save changes Discard changes Export Import

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

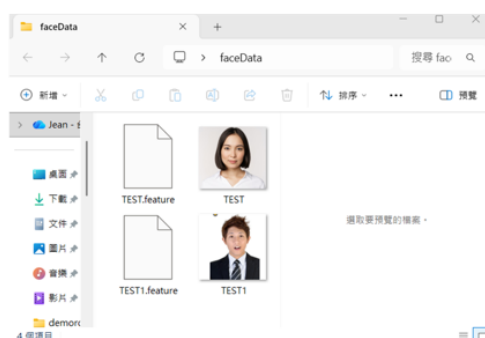
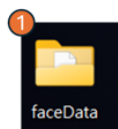


7.2.4 Export/Import access ID

A. Export



- 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.



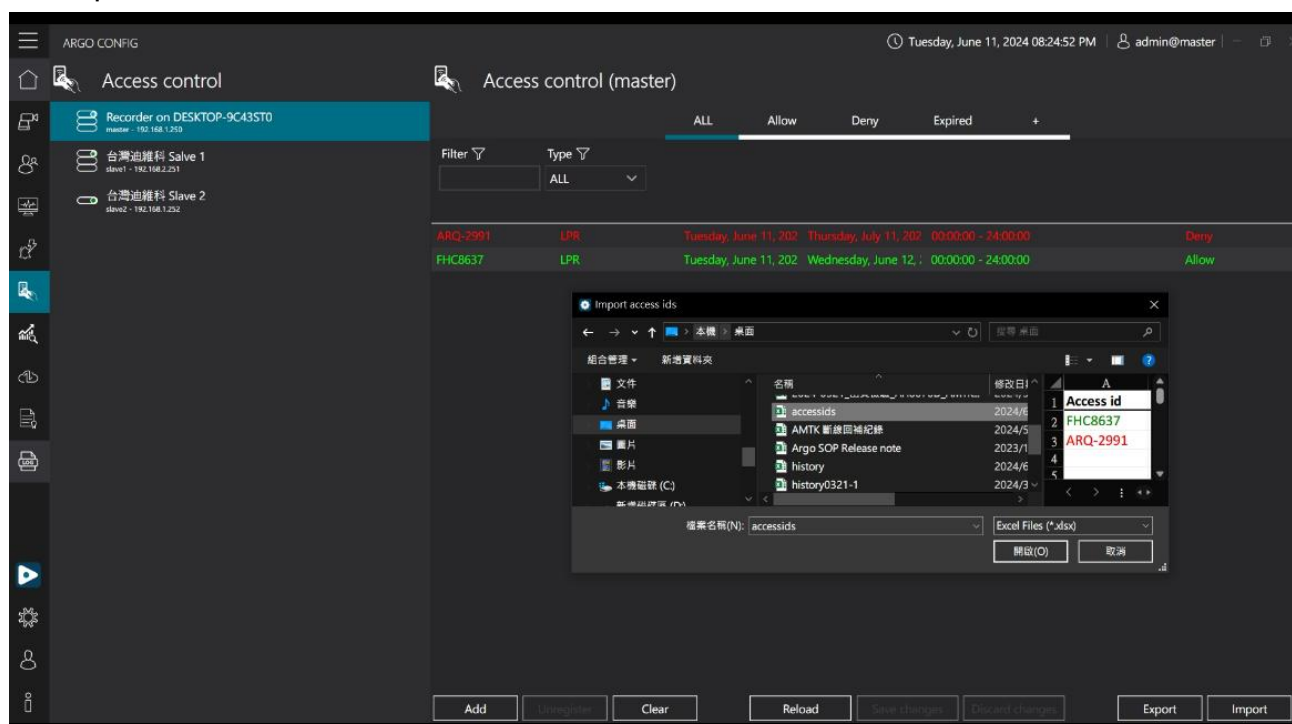
	A	B	C	D	E	F	G	H	I
1	Access ID	ID type	Begin of overall validity	End of overall validity	Begin of daily validity	End of daily validity	Notes	Status and list	User name
2	TEST1	FACE	2026/09/20 00:00:00	2026/10/29 00:00:00	00:00:00	24:00:00		Allowed	Test2
3	TEST	FACE	2026/09/29 00:00:00	2026/10/29 00:00:00	00:00:00	24:00:00		Allowed	Test
4	AAA456	LPR	2026/09/30 00:00:00	2026/10/30 00:00:00	00:00:00	24:00:00		Denied	TEST3

Note:

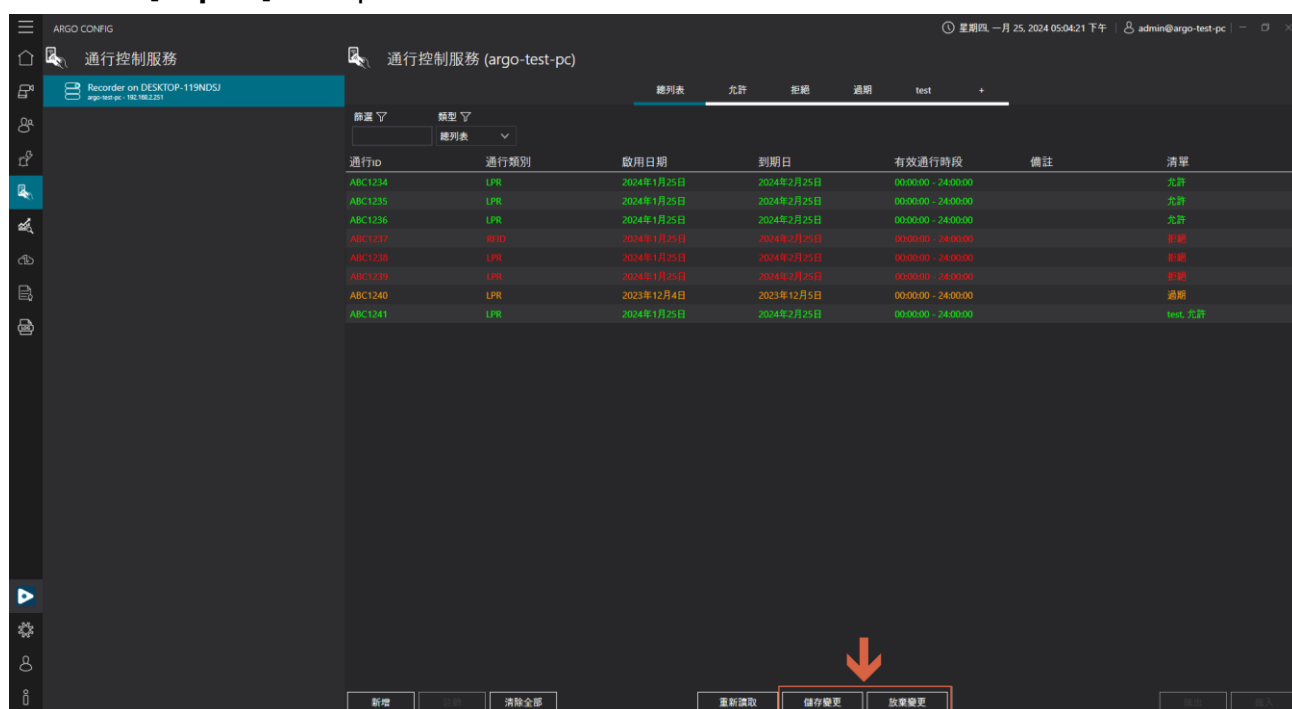
1. When importing exported files (**XLSX or CSV**) that include a **FaceData** folder, place the **FaceData** folder in the same directory as the exported file.
2. If a face image exported from Argo is replaced, the corresponding **feature data file** must also be deleted before importing the data.



B. Import



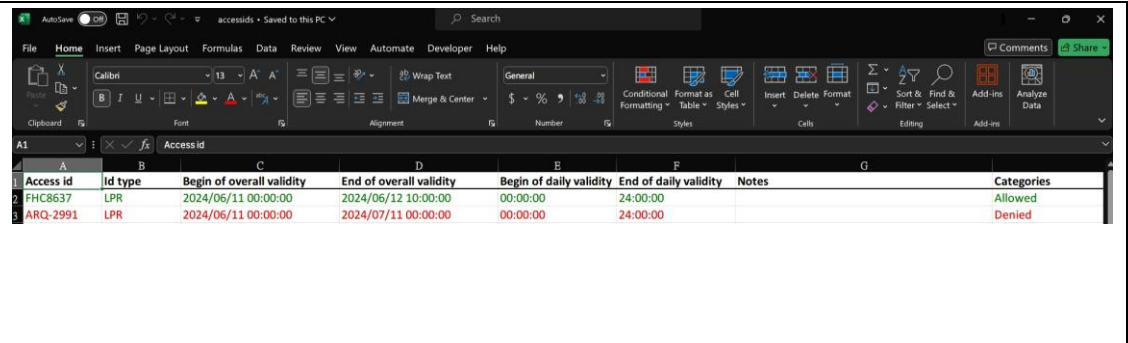
- Click **[Import]** to Import access ID file.



- 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	
csv file	accessids - 記事本 檔案(F) 編輯(E) 格式(O) 檢視(V) 說明 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



8. VIDEO ANALYTICS DATA COLLECTION

8.1 Sens Cam settings

8.1.1 Login settings

The screenshot displays the 'First Access Configuration' page for the 'SENS-CAM AI' device. The page includes the following fields and options:

- User Name:** admin
- Password:** [masked]
- Re-type Password:** [masked]
- Password rules:**
 - 1. Minimum 8 characters
 - 2. Use uppercase characters [A-Z], lowercase characters [a-z] and numbers [0-9]
 - 3. No more than 3 identical consecutive characters
 - Allowed blank and 15%&()*+,-.;<=>?@{}^_~
- DHCP server:** ☐ Obtain an IP address and DNS server automatically
- NTP server:** [empty field]
- Time Zone:** (GMT+08:00)Taipei
- Daylight Saving Time:** ☒ On ☐ Off
- Product Code:** SR-C-12-SENS-F6-IW_WHITE
- MAC Address:** 20:E4:07:00:1D:88

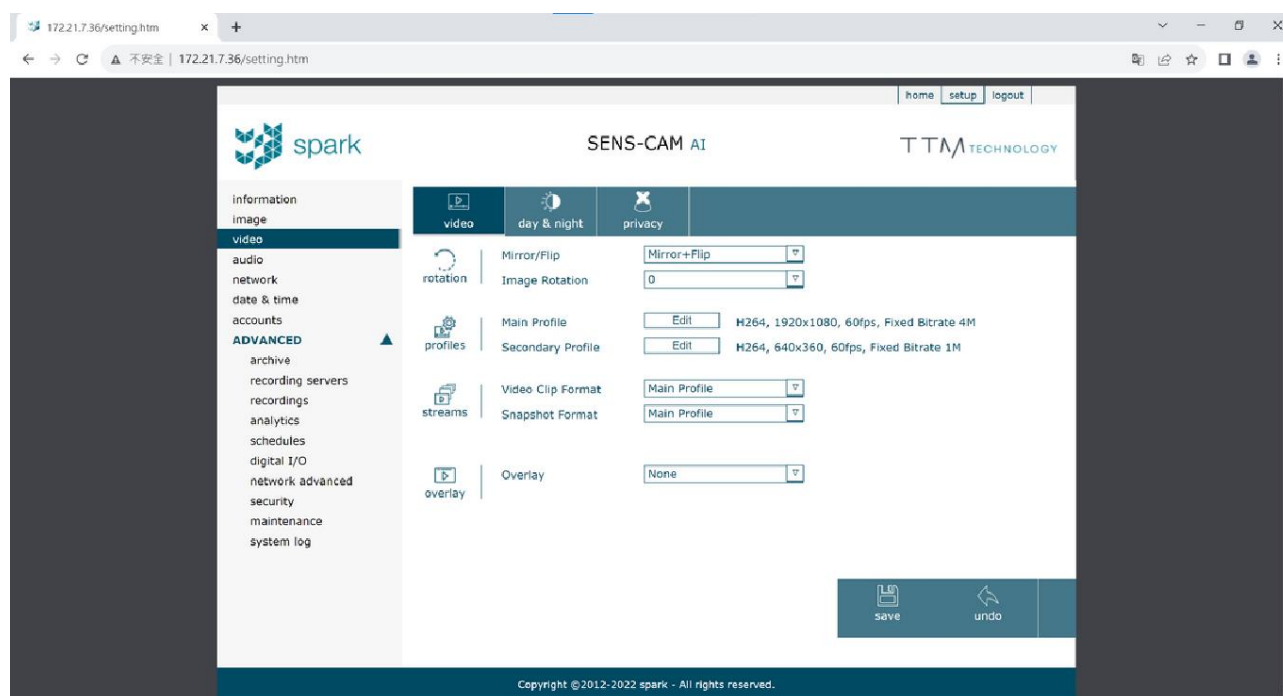
At the bottom right, there are 'save' and 'undo' buttons. The footer indicates 'Copyright ©2012-2022 spark - All rights reserved.'

- 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.

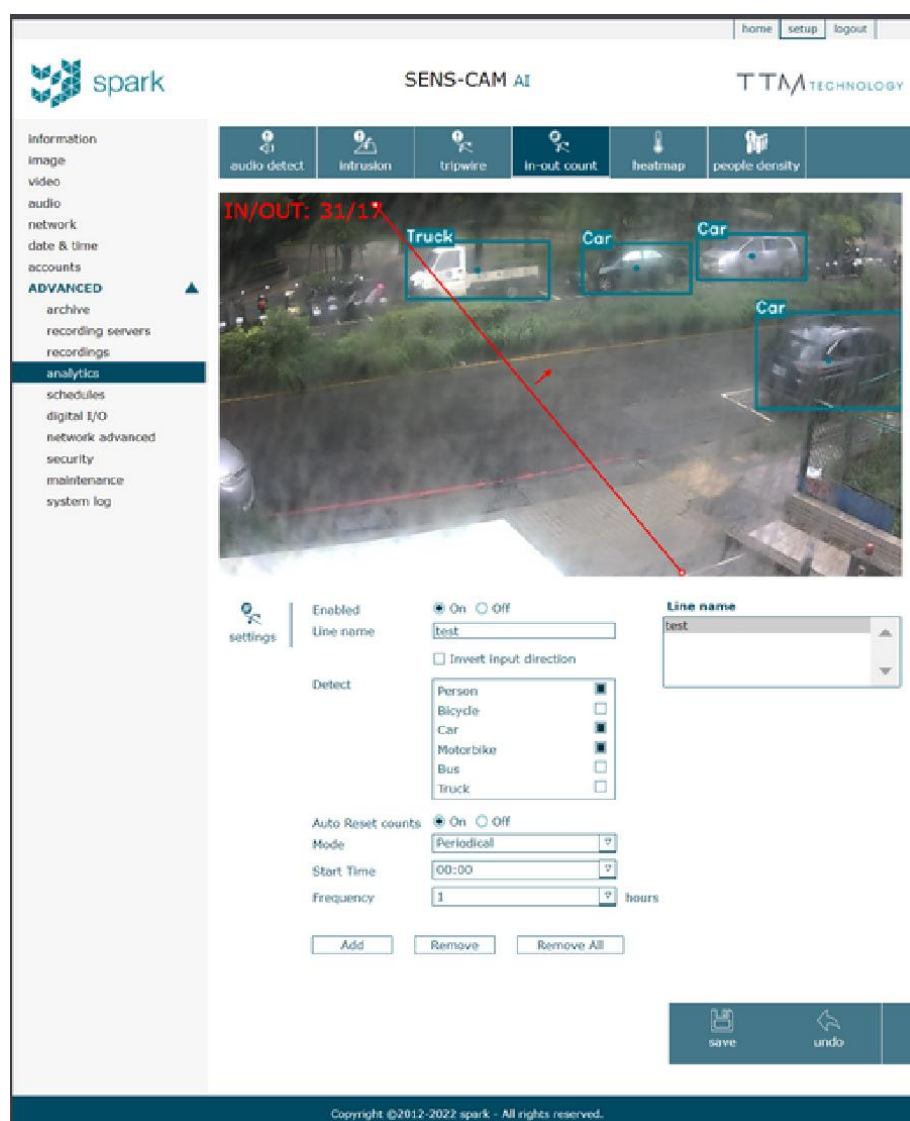
8.1.2 Image setting



- 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.



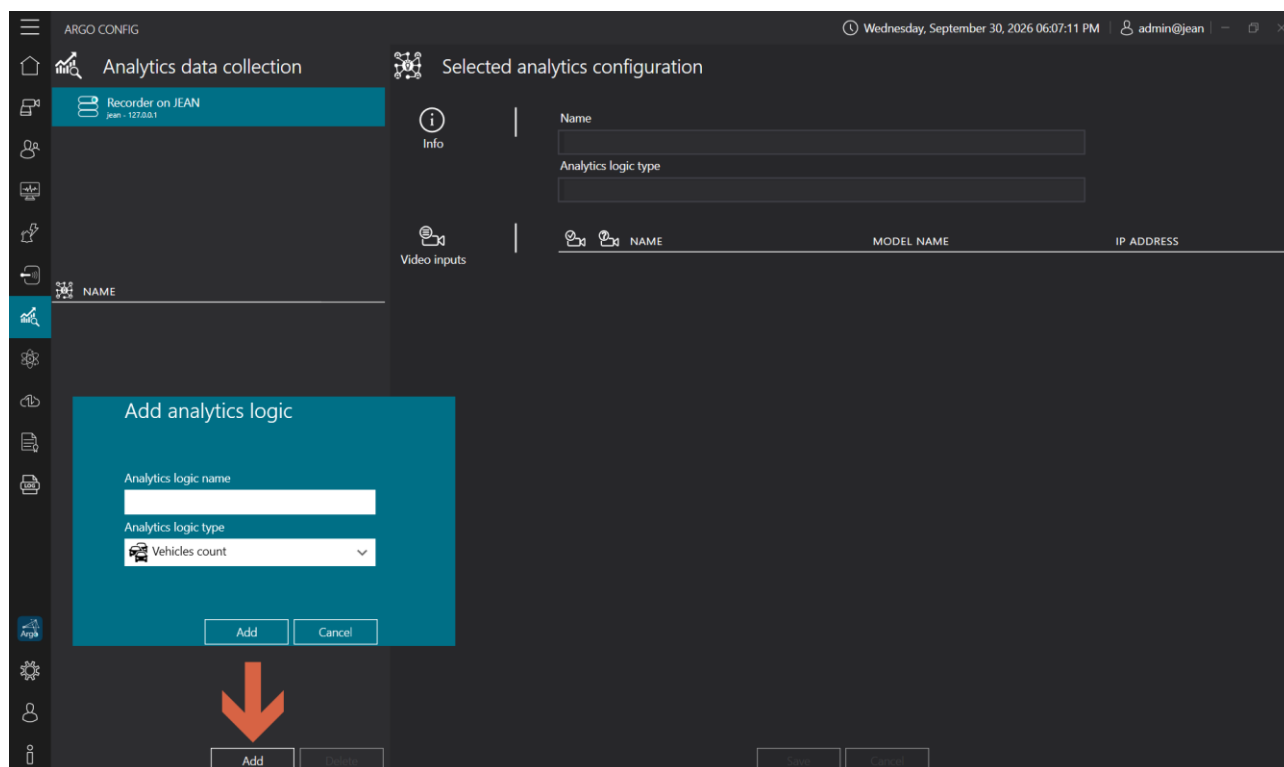
B. Delete analytics

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



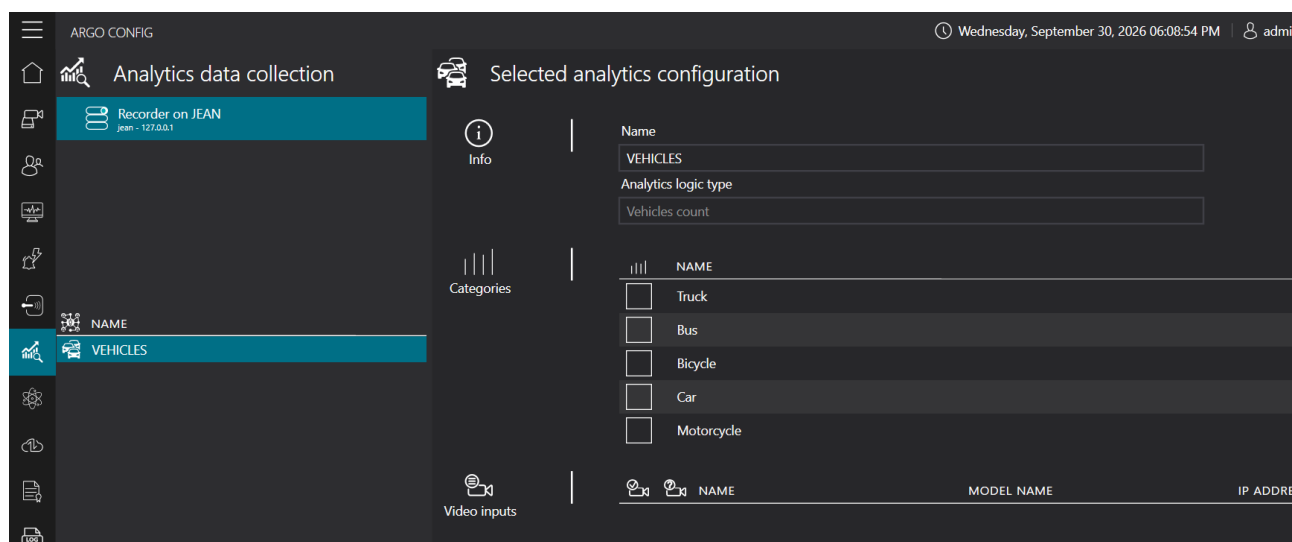
8.2 Video analytics data collection settings

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

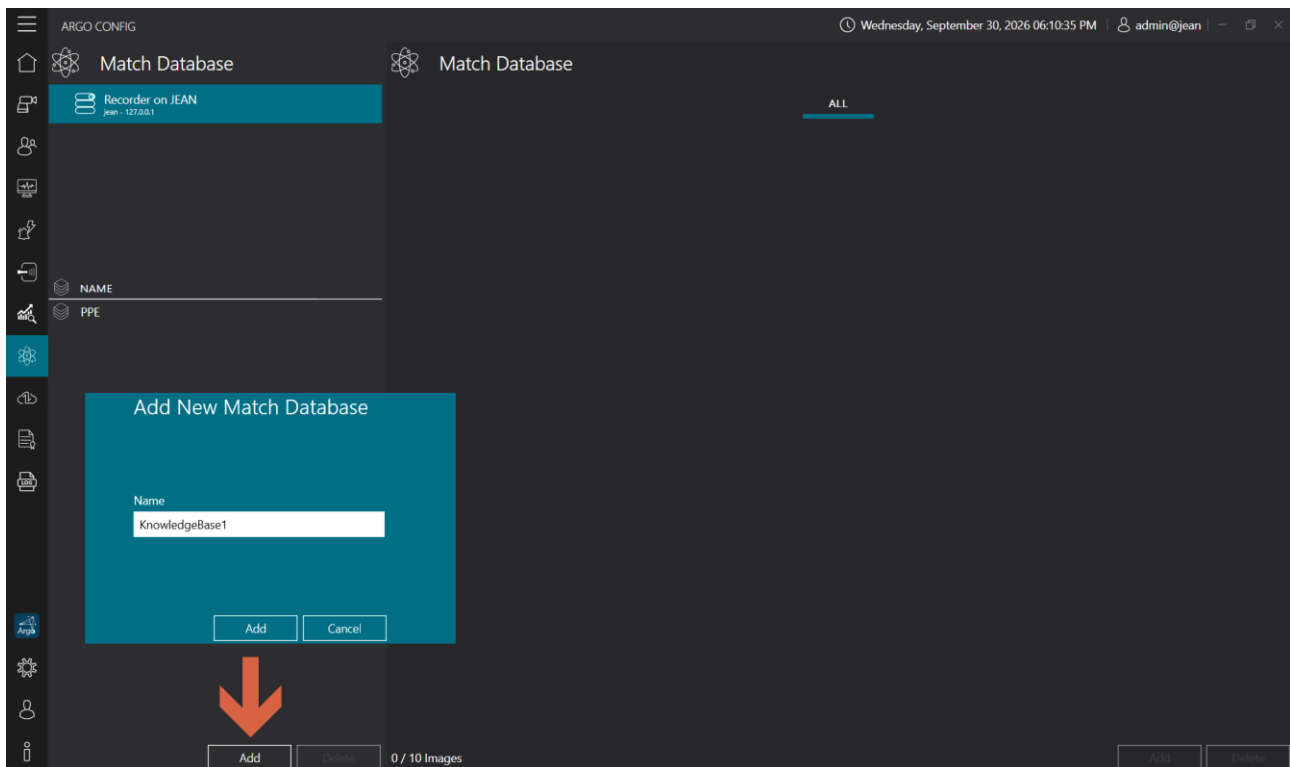
8.2.3 Delete video analytics parameter

The screenshot shows the ARGO CONFIG web interface. The top bar displays the title 'ARGO CONFIG' and the date/time 'Tuesday, June 11, 2024 08:06:40 PM' along with the user 'admin@desktop-6kbn55a'. The left sidebar contains a list of icons, with the 'Analytics data collection' icon highlighted. The main panel is titled 'Selected analytics configuration' and is divided into three sections: 'Info', 'Categories', and 'Video inputs'. The 'Info' section shows the 'Name' as 'CAR'. The 'Categories' section shows a list of categories with checkboxes: 'truck', 'bus', 'bicycle', 'car' (checked), and 'motorcycle'. The 'Video inputs' section shows a table with columns 'NAME', 'MODEL NAME', and 'IP ADDRESS'. At the bottom left, there are 'Add' and 'Delete' buttons. An orange arrow points to the 'Delete' button.

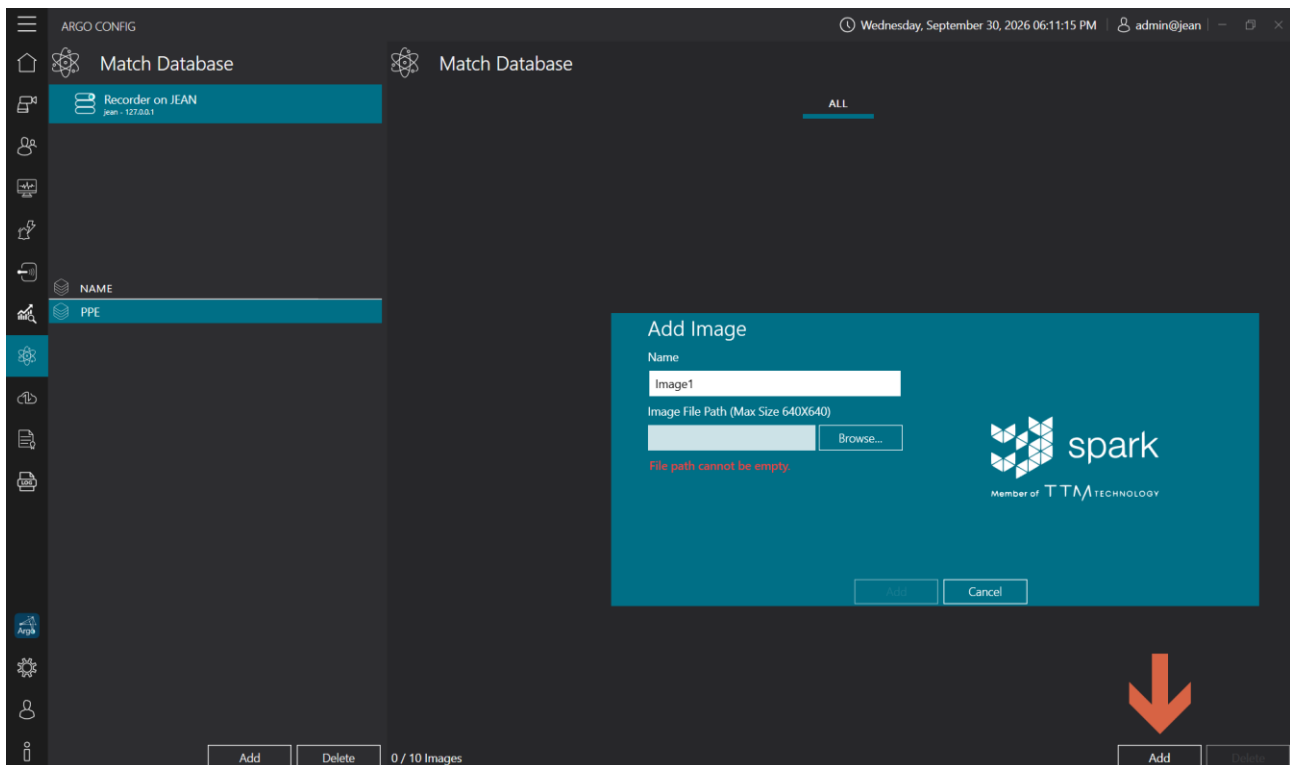
- Select the parameter you want to delete and click **[Delete]**



9. MATCH DATABASE



- Click [Add] to create a new Reference Image Library category.
- Name: Enter the category name



- Click [Add] to add a new image for analysis and matching.
- Name: Enter the image name.
- Image Path: Select the image to be used for recognition. (640 × 640 pixels)



10. BACKUP AND RESTORE

10.1 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
☐		Slave 1	Recorder	Slave 1	☐ Events database	Ready
☒	192.168.1.246	Recorder on DESKTOP-6KBN55A	Recorder	Recorder on DESKTOP-6KBN55A	☒ Events database ☒ Licenses	Ready
☐	192.168.1.249	Failover	Recorder	Failover	☐ 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**]

10.2 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\0611Test.abkp

Browse...

Backup file details:

Date and time: 6/11/2024 7:59:57 PM

Description:

Backup file content:

Select all available devices

Device type: All Filter

SELECTION	IP ADDRESS	DEVICE NAME	DEVICE TYPE	MODEL NAME	OPTIONS	DESTINATION	STATUS
☒	desktop-6kbn55a	Recorder on DESKTOP-6KBN55A	Recorder	Recorder on DESKTOP-6KBN55A	☒ Events database ☒ Licenses	Recorder on DESKTOP-6KBN55A	Connected

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]**

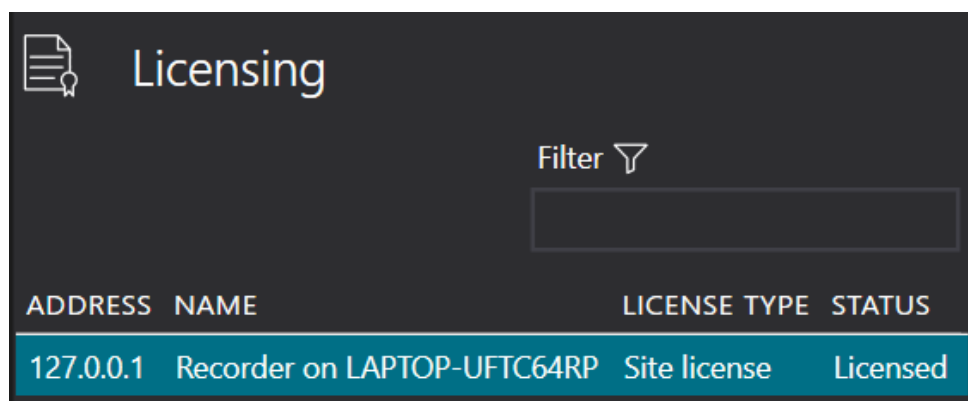
10.3 Scheduled backup

IP ADDRESS	DEVICE NAME	OPTIONS	KEEP TIME	SCHEDULE TIME	PATH	STATUS
192.168.1.246	Recorder on DESKTOP-6KBN55A	☐ Events database ☐ ALPM DB ☐ Record videos	Month	12:00 AM	Browse...	Disable
			Month	12:00 AM	Browse...	Disable
			Month	12:00 AM	Browse...	Disable
	Slave 1	☐ Events database ☐ ALPM DB ☒ Record videos	Month	3:14 PM	Browse...	Disable
			Month	12:00 AM	Browse...	Disable
			Month	12:00 AM	Browse...	Disable
192.168.1.249	Failover	☐ Events database ☐ Record videos	Month	12:00 AM	Browse...	Disable
			Month	12:00 AM	Browse...	Disable
			Month	12:00 AM	Browse...	Disable

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



11. LICENSE



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

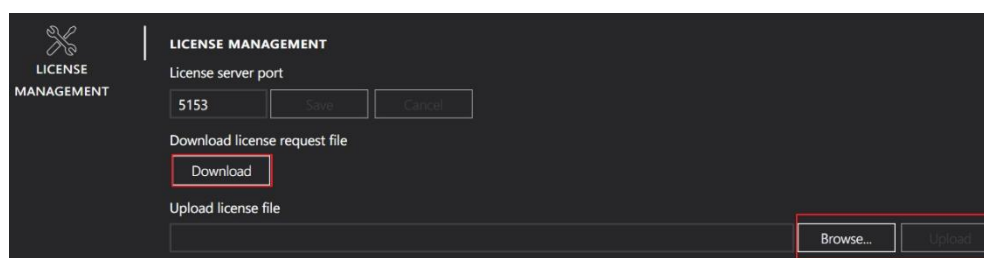
- IP address: current IP address
- Name: server name
- License key type: multiple channel license
- Status: license status

11.1 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.

11.2 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]**.



11.3 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.

11.4 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.



12.LOG

12.1 Data trace

ARGO CONFIG Tuesday, June 11, 2024 07:49:15 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
☒	Recorder on DESKTOP-6KBN55A	desktop-6kbn55a	Online
☒	Slave 1	localhost	Online
☒	Failover	xeon-test-pc	Online

Search Delete

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 to CSV

A. Search data trace

Log

AUDIT LOG June 2024 ED 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
☒	Recorder on DESKTOP-6KBN55A	desktop-6kbn55a	Online
☒	Slave 1	localhost	Online
☒	Failover	xeon-test-pc	Online

Search

- 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

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
☒	Recorder on DESKTOP-6KBN55A	desktop-6kbn55a	Online
☒	Slave 1	localhost	Online
☒	Fallover	xeon-test-pc	Online

Search [] Delete []

- 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

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 to CSV []

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



12.2 System log

ARGO CONFIG Tuesday, June 11, 2024 07:34:02 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
☐	Recorder on DESKTOP-6KBN55A	desktop-6kbn55a	Online
☐	Slave 1	localhost	Online
☐	Failover	xeon-test-pc	Online

Search

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 00:00:04.890	INFO	Status of event "systemevent_69d74598-a248-46e0-942a-b2934d65dc36" is now "inactive".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)

Export to CSV

A. Search system log

ARGO CONFIG

Log

June 2024

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

Please choose at least a node from the list below:

SELECT	NODE	ADDRESS	STATUS
☒	Recorder on DESKTOP-6KBN55A	desktop-6kbn55a	Online
☒	Slave 1	localhost	Online
☒	Failover	xeon-test-pc	Online

Search

- 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

- 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

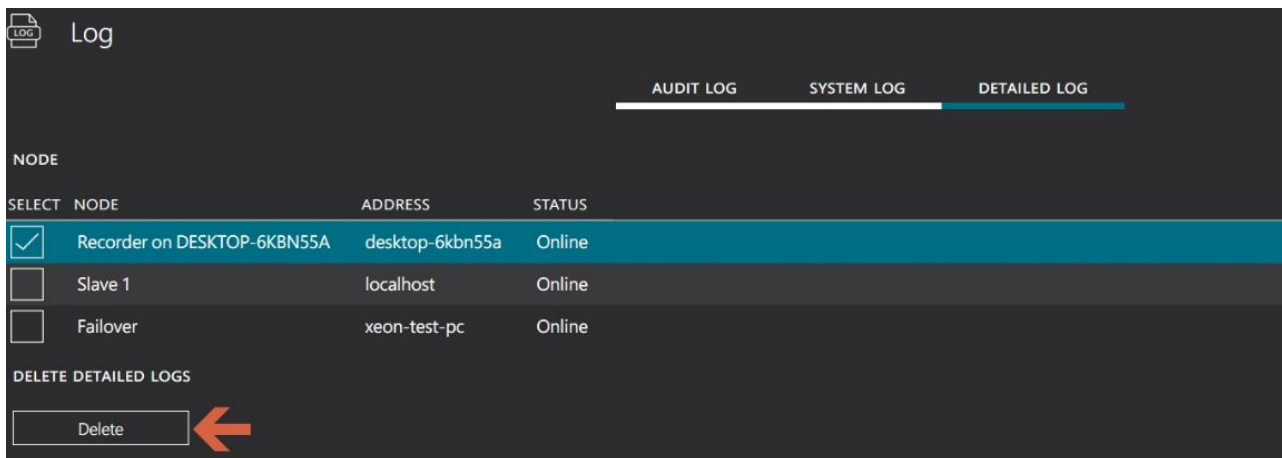
DATE	LEVEL	MESSAGE	NODE
2024-06-11 00:00:00.351	INFO	Status of event "systemevent_69d74598-a248-46e0-942a-b2934d65dc36" is now "inactive".	Recorder on DESKTOP-6KBN55A (desktop-6kbn55a)
2024-06-11 00:00:00.353	INFO	Status of event "systemevent_69d74598-a248-46e0-942a-b2934d65dc36" is now "active".	Recorder 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 the search results of the system log.
- Click **[Export CSV]**



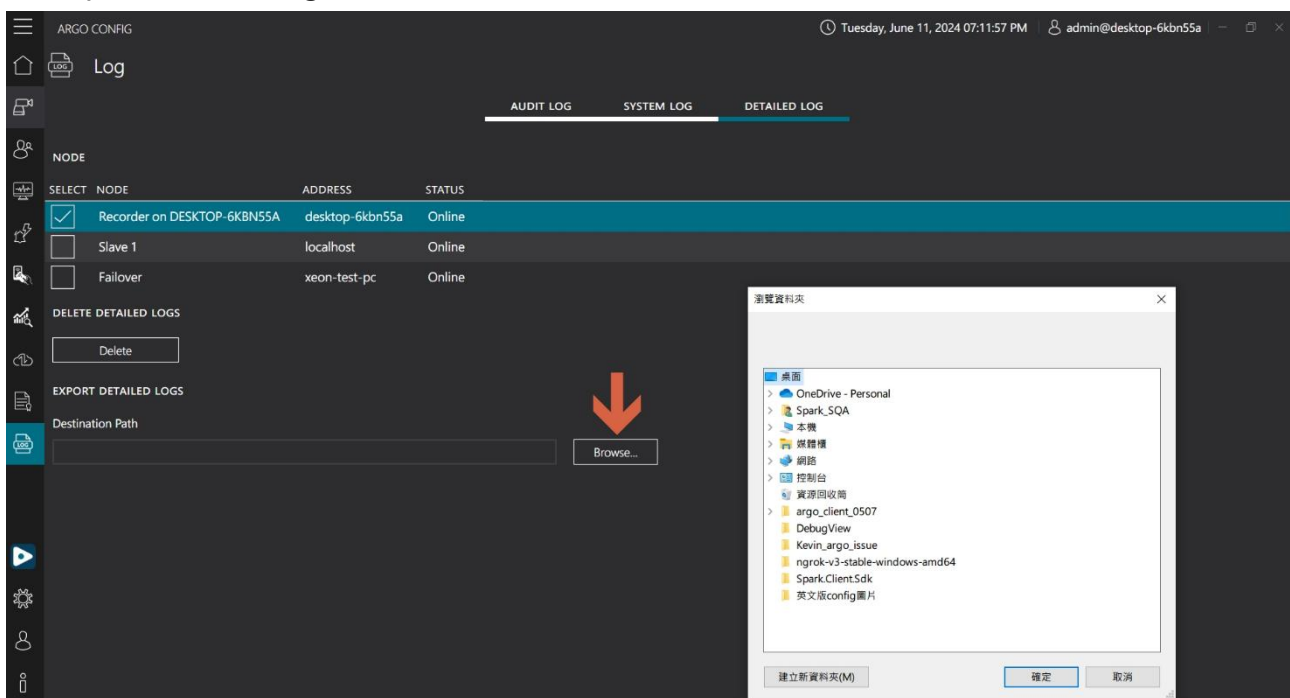
12.3 Detailed log

A. Delete detailed log



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

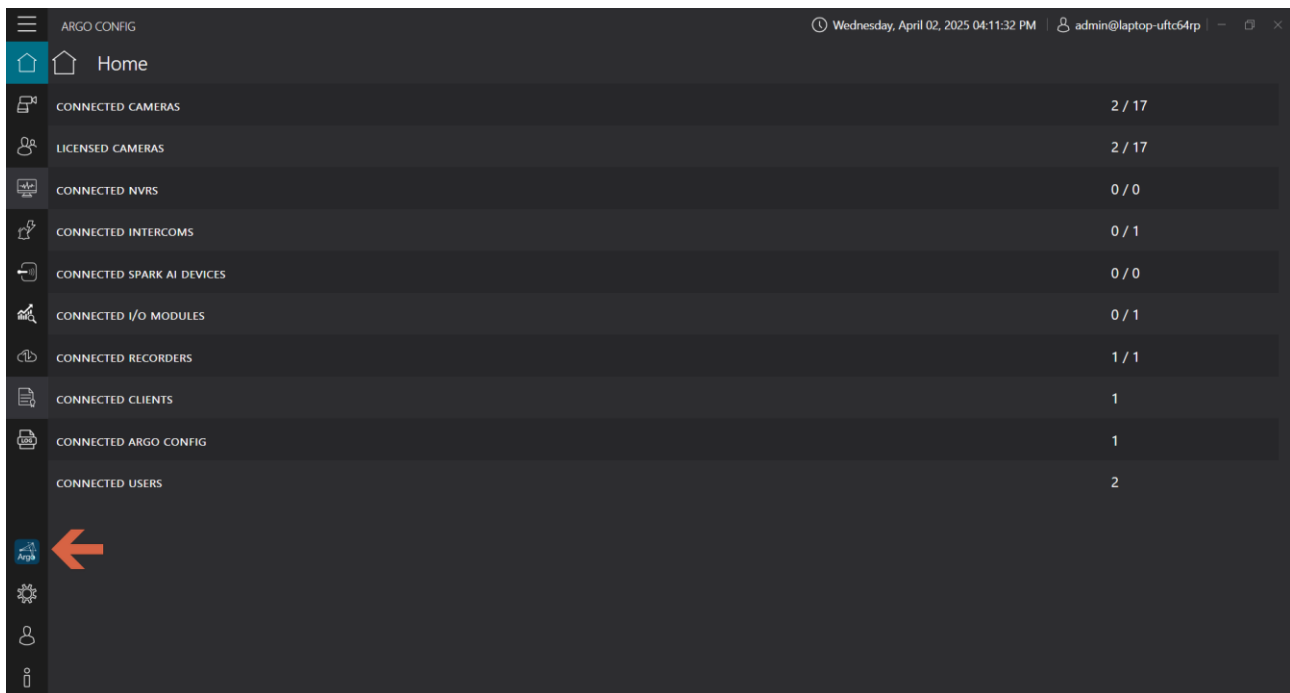
B. Export detailed log



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



13. ARGO CLIENT

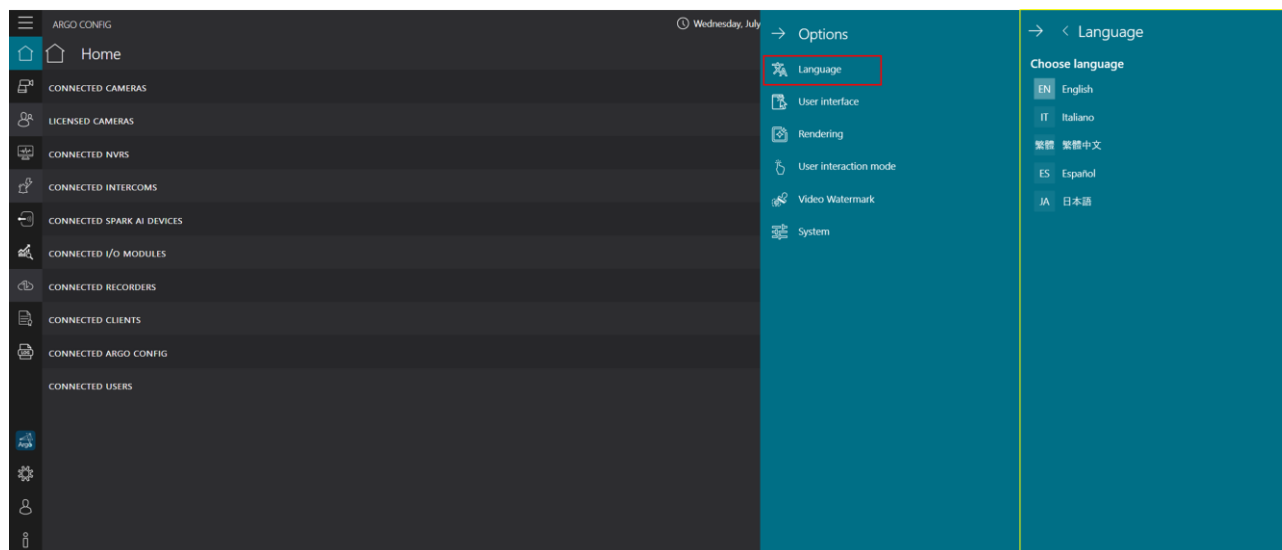


- Click the **[Argo Client icon]** on the bottom left
- Link from Argo Config to Argo Client



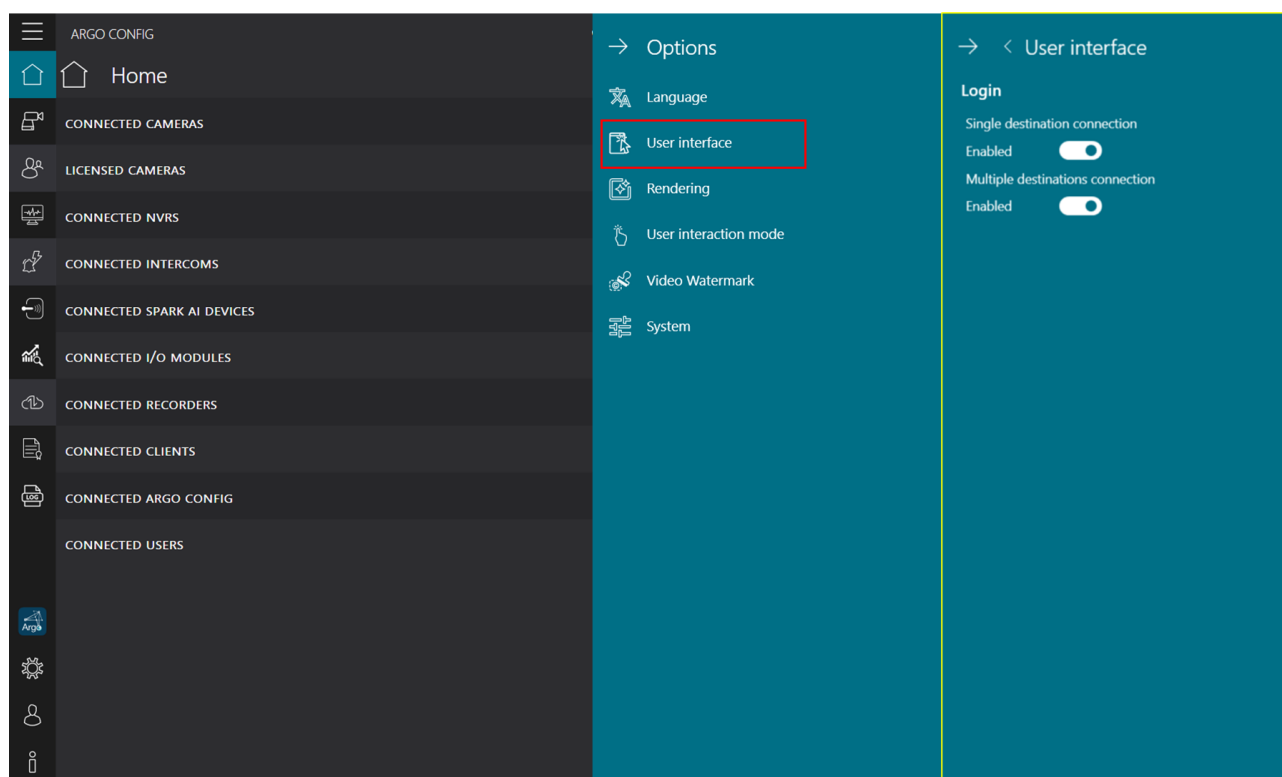
14.OPTIONS

14.1 Language



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

14.2 Interface



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



Single login page

Host: localhost
Type: Spark Argo Recorder
Certificate: spark.protocol.network.certificate
Username: admin
Password:
Connect

Quick login page

CONFIGURED DESTINATIONS

Name	Address	Username
localhost	localhost:20847	admin

Add Edit Delete Connect

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

14.3 Rendering

ARGO CONFIG

Home

CONNECTED CAMERAS

LICENSED CAMERAS

CONNECTED NVRS

CONNECTED INTERCOMS

CONNECTED SPARK AI DEVICES

CONNECTED I/O MODULES

CONNECTED RECORDERS

CONNECTED CLIENTS

CONNECTED ARGO CONFIG

CONNECTED USERS

Options

Language

User interface

Rendering

User interaction mode

Video Watermark

System

Rendering

Live streams behaviour

Specify the behaviour to use when handling live video stre

Auto

Analytics

Display analytic metadata streams.

On

Show analytic metadata configuration areas

On

Audio

Auto enable audio stream

On

Live stream presentation buffering

Minimum buffering (ms.) - [0 ~ 10000]

150

Maximum buffering (ms.) - [100 ~ 15000]

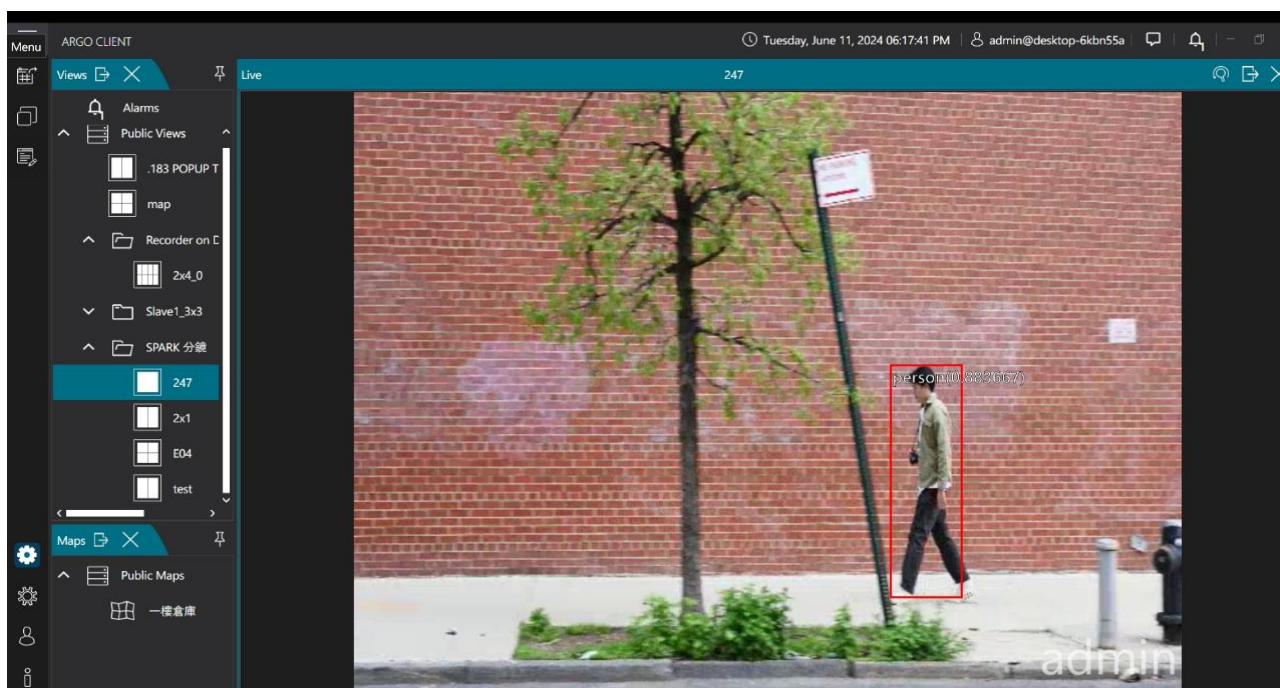
400

- 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.

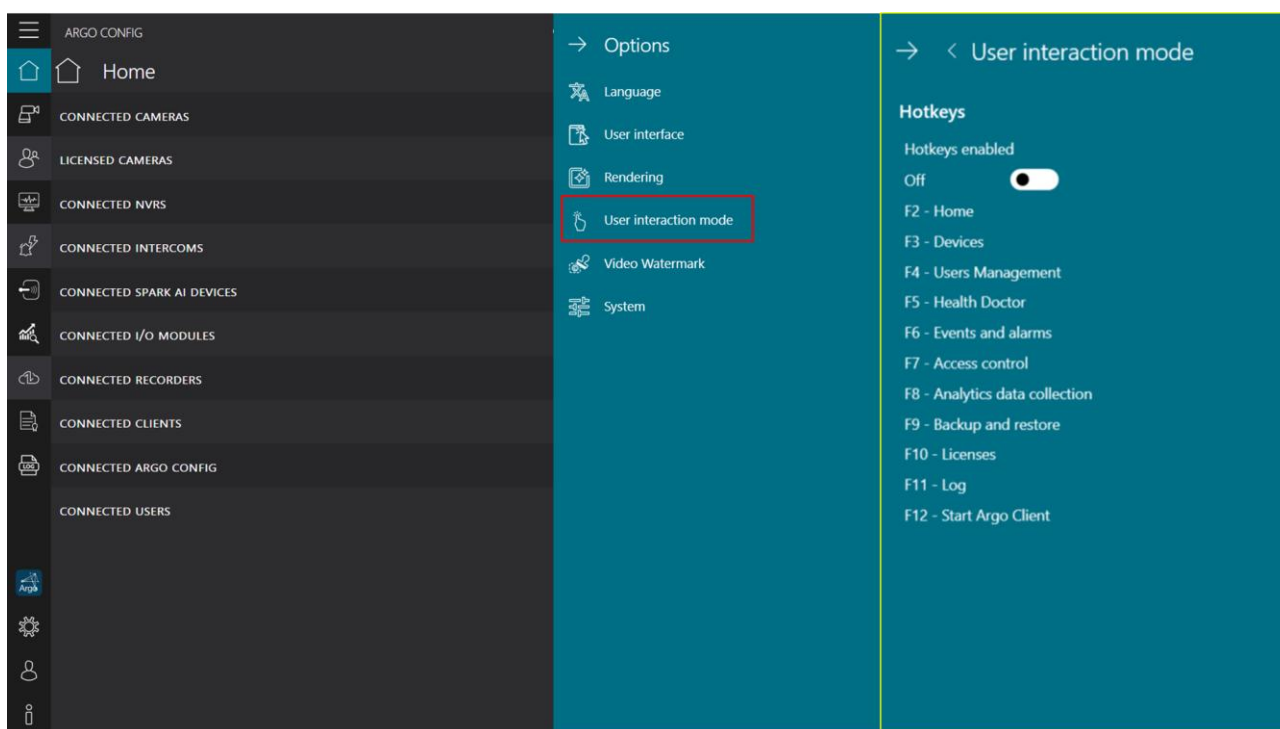
Note: Specifying real-time streaming behavior to Auto typically results in a lower resolution to reduce computer power consumption.



- 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.



14.4 User interaction mode

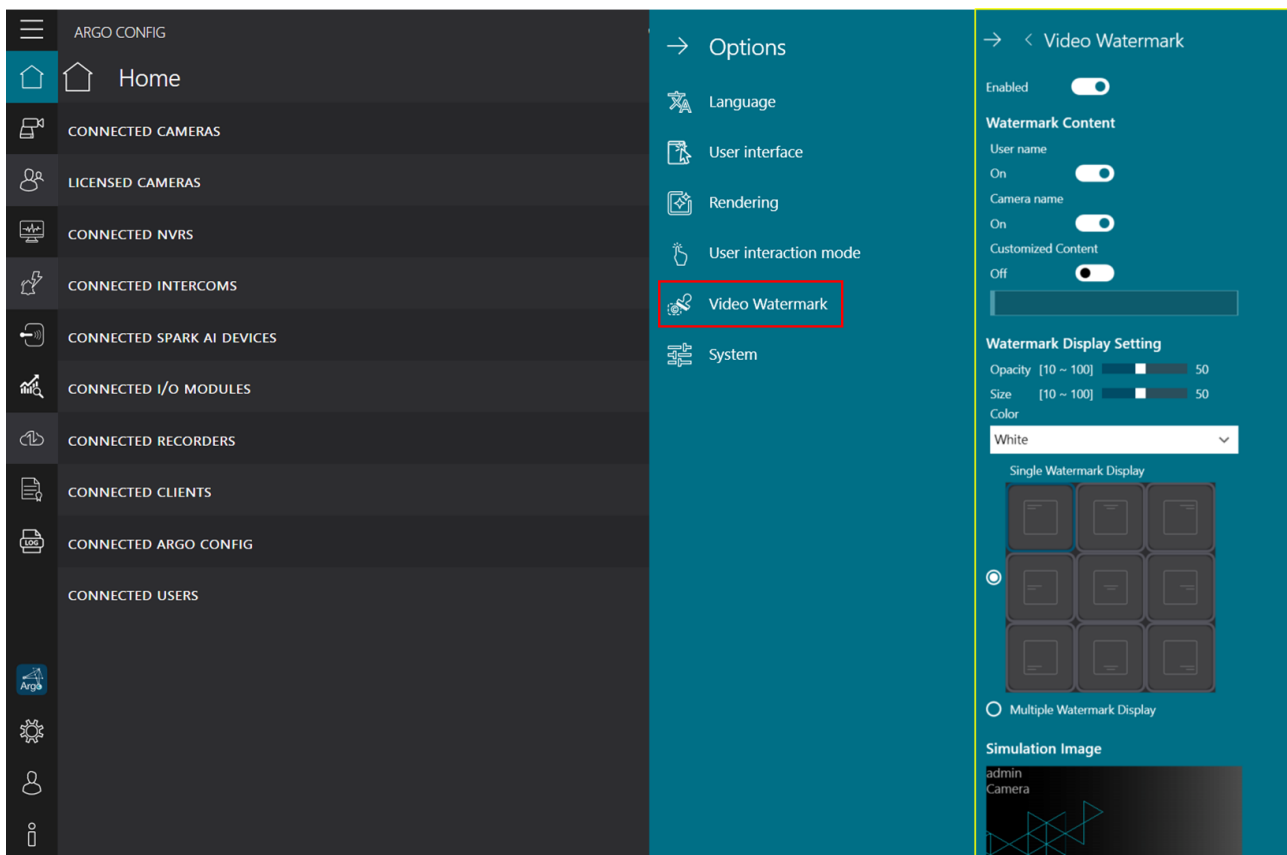


- Click the bottom left **[Gear Icon]** and select **[user interaction mode]**.
- Shortcuts: when enabled, users can use below shortcuts.

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		



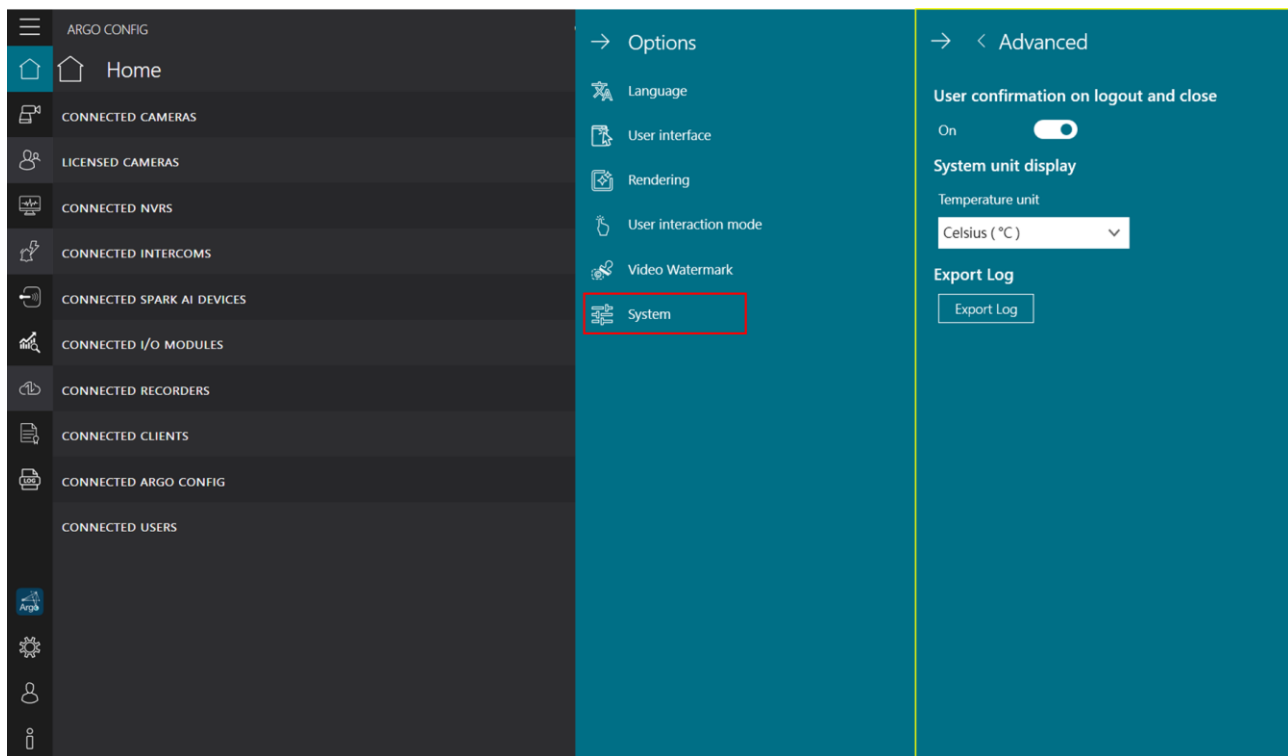
14.5 Watermark



- 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.



14.6 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



15. USER

15.1 Change password

Change User Password

Username: admin

Old password: [input field]

New password: [input field]

Confirm password: [input field]

WARNING: CAPS LOCK is active

Change password Cancel

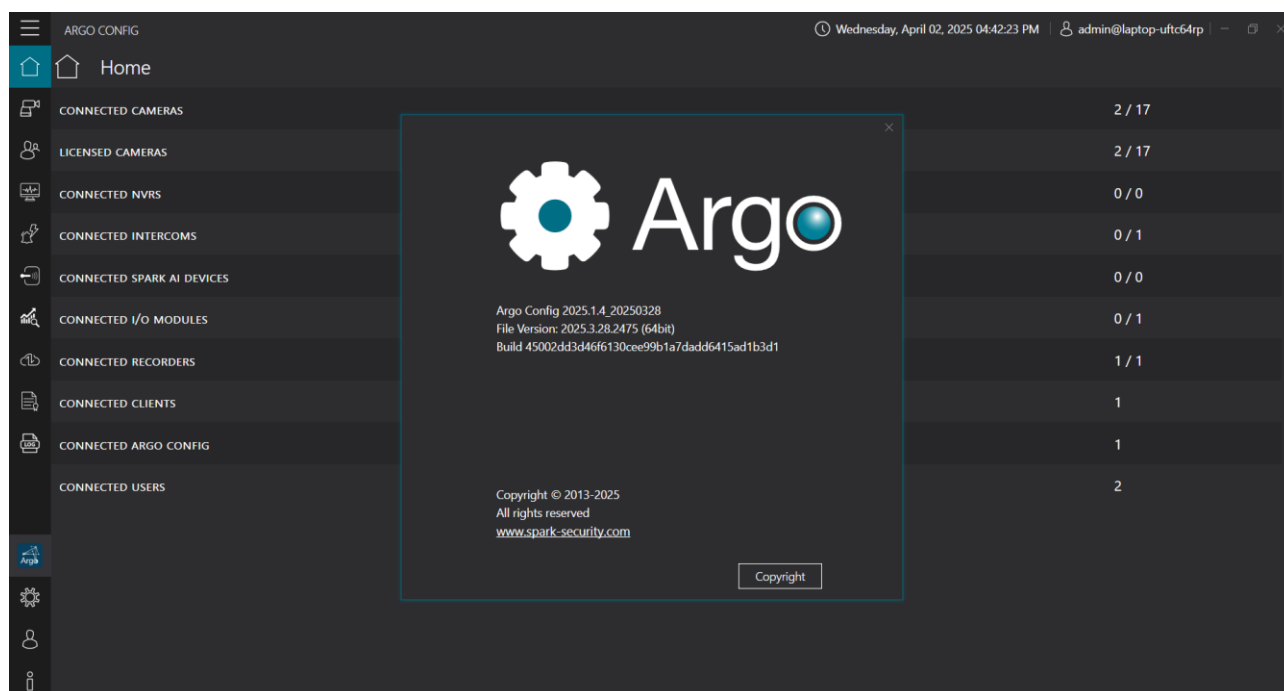
- Click on **[User]** then click **[change password]**. After changing password, click **[change password]** to confirm.
- Username: usernames cannot be modified.
- Old password: insert username old password
- New password: insert new password
- Retype password: retype the password

15.2 Logout/Close

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



16.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.



17. OTHER

17.1 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

1 2 3

Enter company info Check application Application complete

Create a LINE official account Required

Login info

Username Sample [Log out](#)

Service region Zambia

Account info

Account name Ex: BROWN Cafe 0/20
This name will appear on the LINE friend list and chat screen.

Email address user@example.com 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 Main industry Subindustry



Step4: Check your LINE Official Account

LINE Official Account Manager

Accounts Groups

Accounts

Create new

Accounts (1)

Account name Friends Role Plan

Sample channel	0	Administrator	コミュニケーション
----------------	---	---------------	-----------

Hide menu labels

© 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.

LINE Developers About News Products Documentation FAQ Glossary More

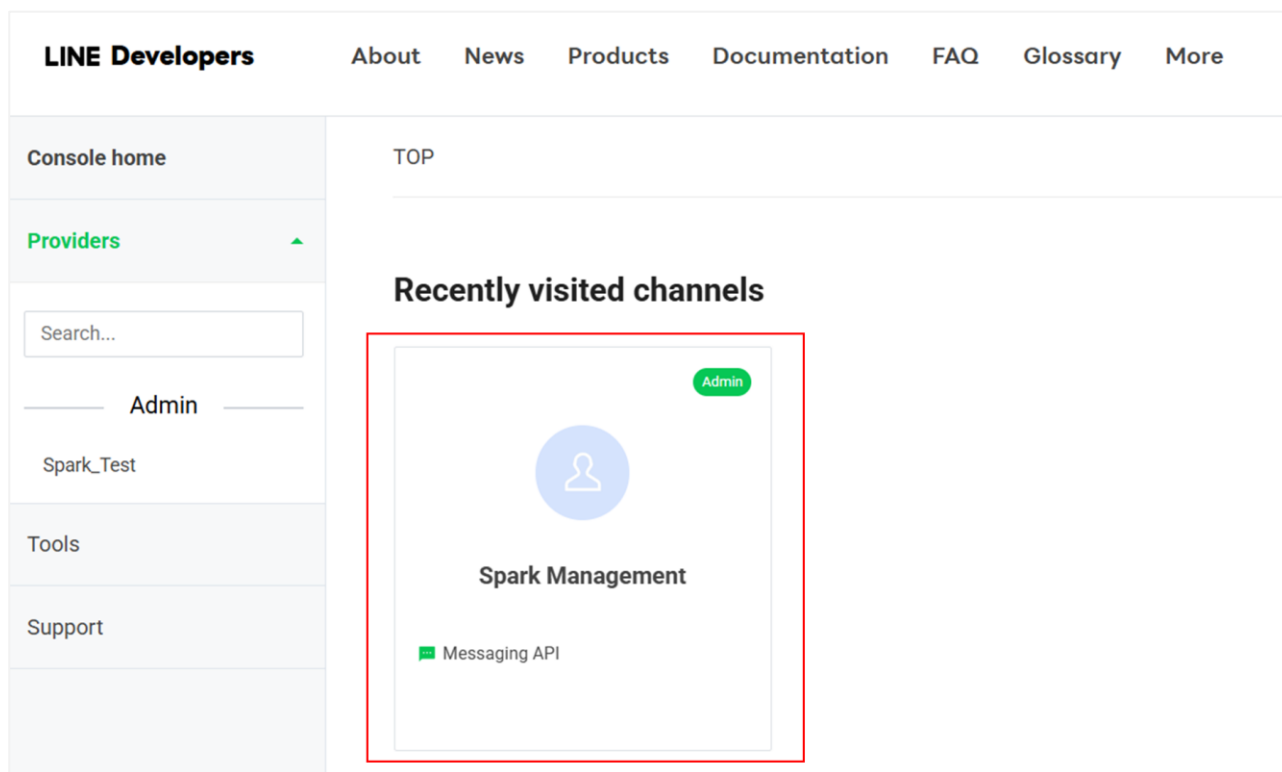
Console

Connect with {/LINE Developers}

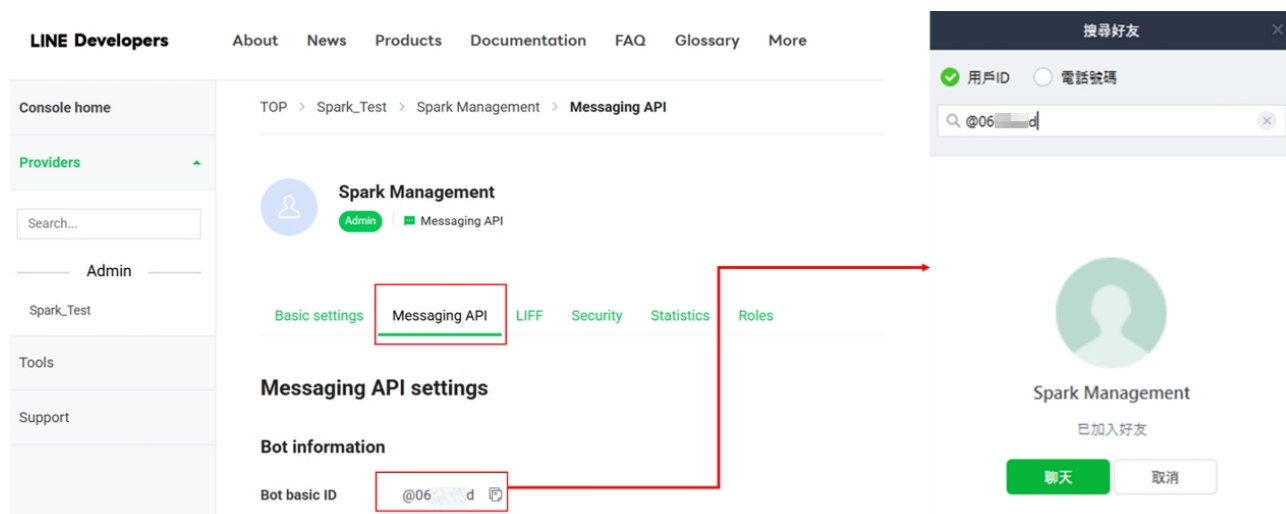
/ Start Console >



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=



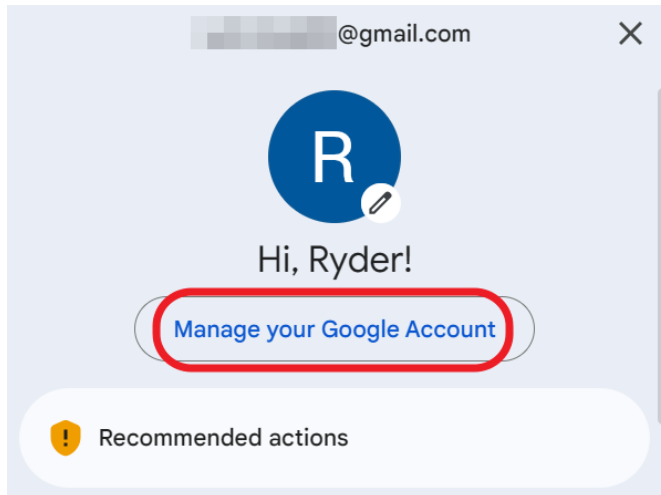
Reissue

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

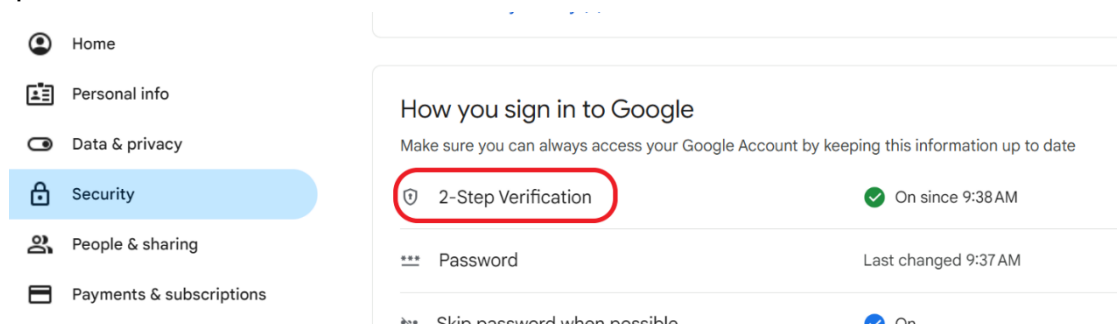


17.2 Applying for Gmail Two-Step Verification for App Password

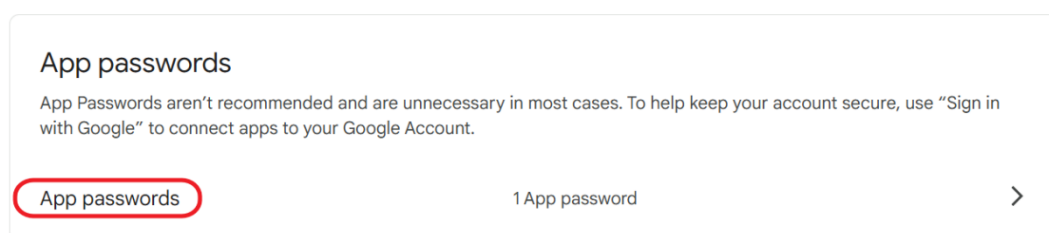
Step1: Go to the Gmail homepage, click on "Manage your Google Account."



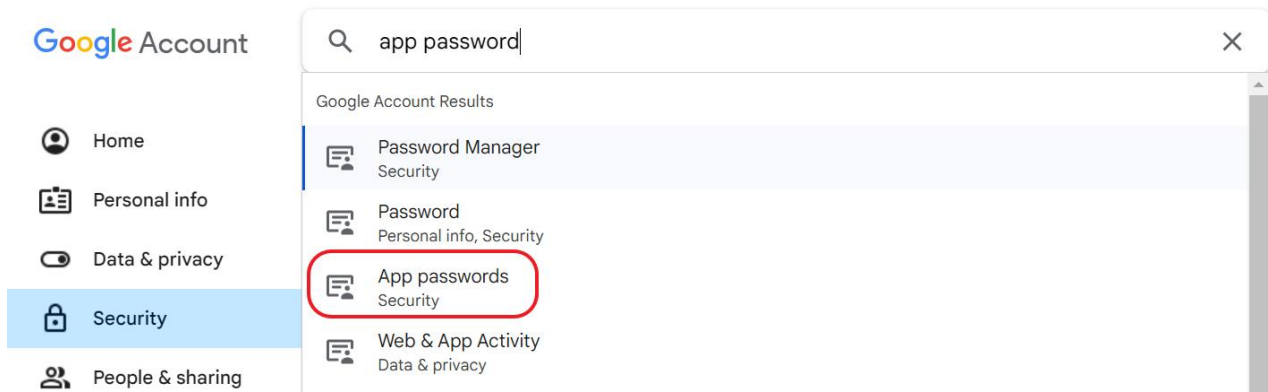
Step2: Click on "Security" to enter two-step verification, then enter your account password.



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.

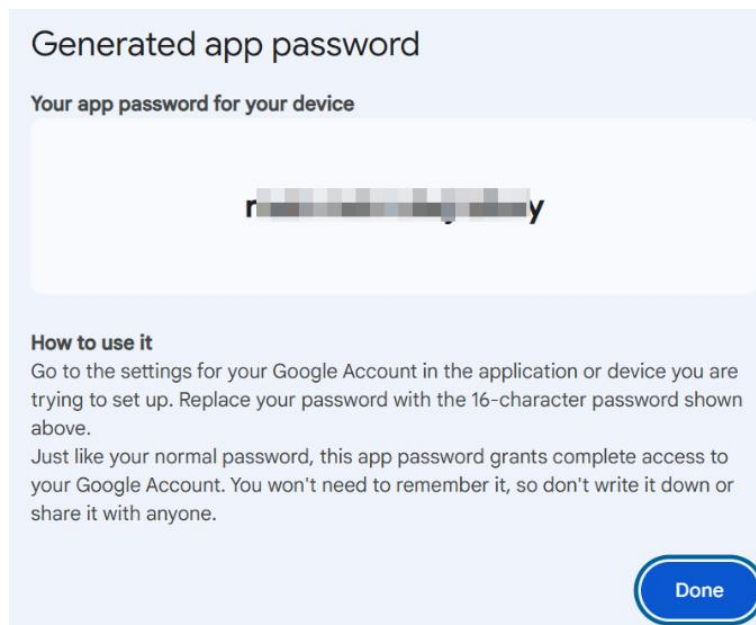
Your app passwords

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.

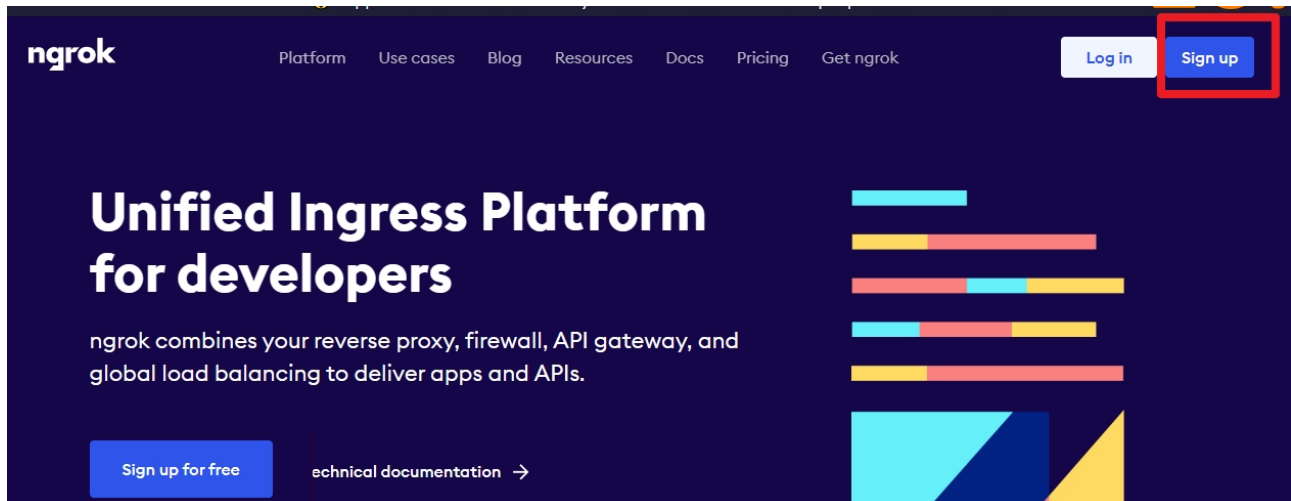


17.3 Applying for Ngrok Account Tutorial

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

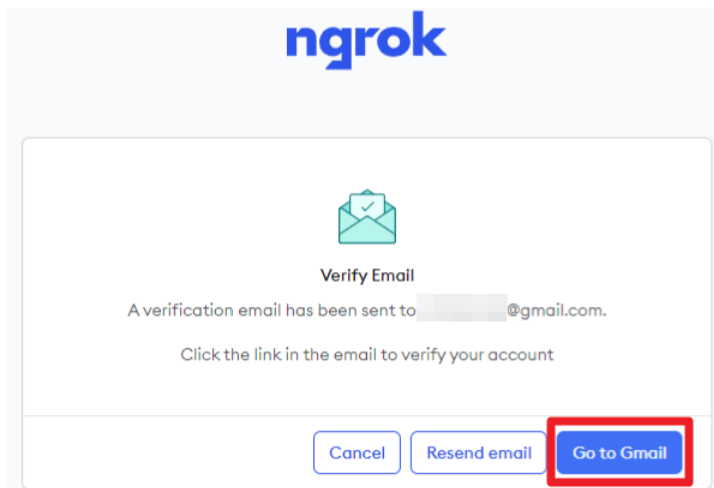
☐ 我不是機器人  reCAPTCHA
隱私權 - 條款

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

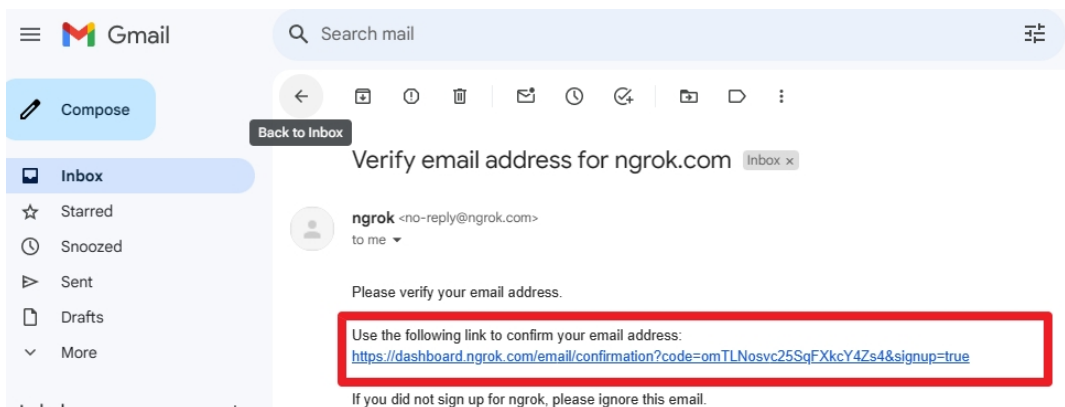
Sign up



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

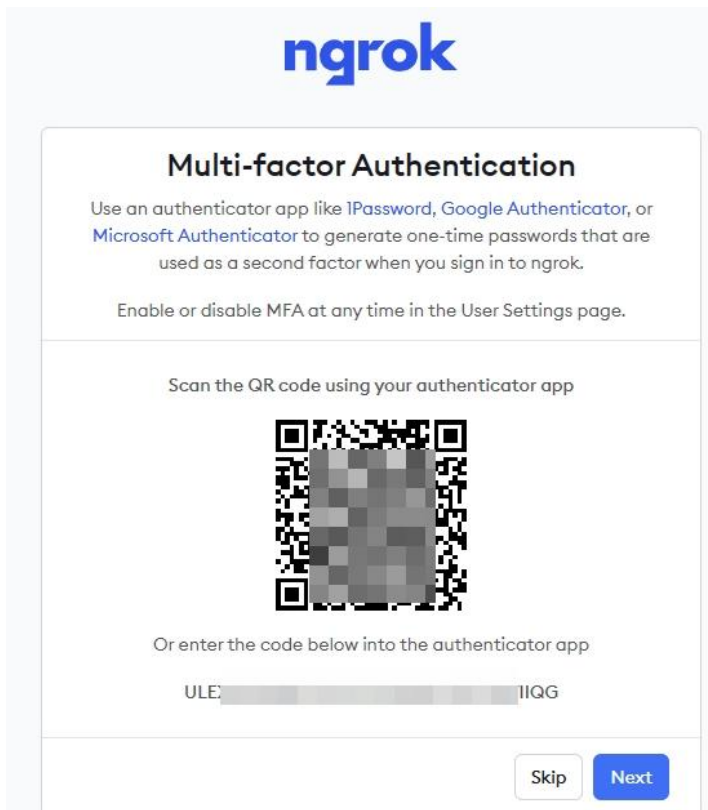


Step 5. Click the link in the email to confirm the account.

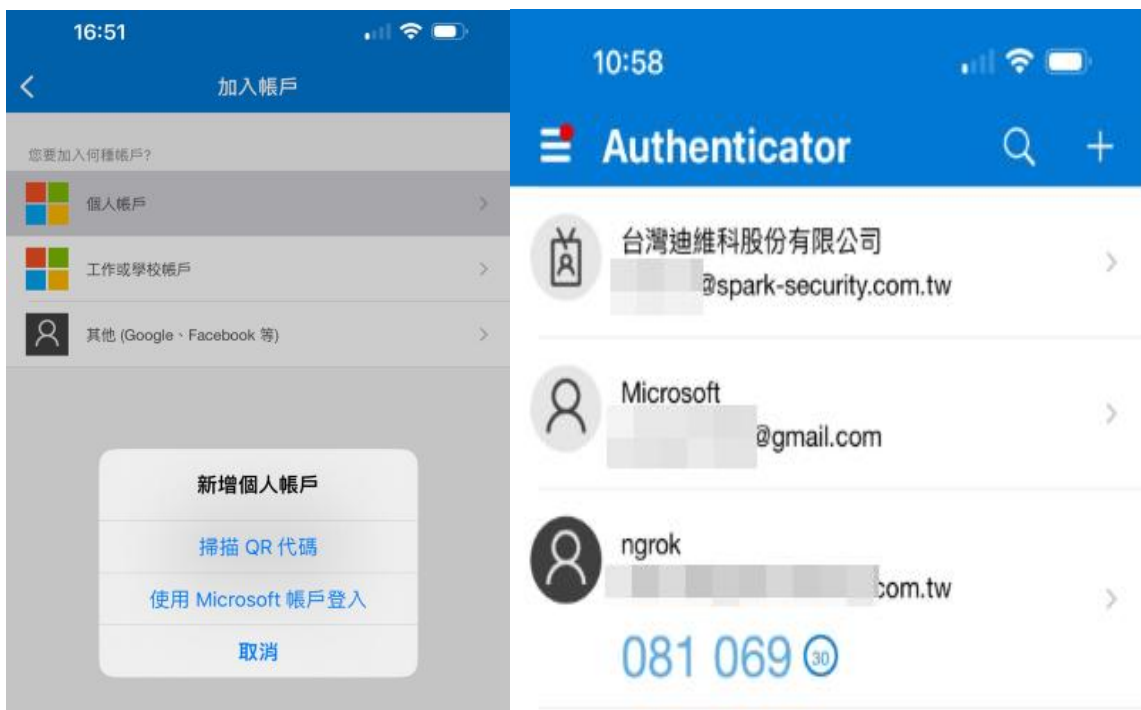


Step 6. Ngrok will display a QR code and authentication code. It is recommended to use a smartphone to scan the QR code for authentication. Click "Next" to proceed.

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".



The screenshot shows the 'Device Activation' page on the Ngrok website. At the top is the Ngrok logo. Below it, the heading 'Device Activation' is centered. The instruction 'Enter the code displayed on your device.' is followed by a text input field. Below the input field is a blue 'Continue' button. Underneath the button is a link 'Back to QR Code'. At the bottom, a note states 'ngrok staff will never ask you to enter a code on this page.'

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

The screenshot shows the 'Recovery codes' page on the Ngrok website. It features the Ngrok logo at the top. The heading 'Recovery codes' is followed by explanatory text about using these codes to recover the account. Below this, a table displays ten recovery codes arranged in two columns. At the bottom of the table are two buttons: 'Copy to clipboard' and 'Download'. Below these buttons is a checkbox labeled 'I've saved my recovery codes' and a blue 'Finish' button.

FKA9KUMTUM	XJNY4A2PW8
Y3VZ3W3SEZ	EVY4ZQT7QQ
PXXNR7VQE3	AA52JJFCAH
H8RMGGMG2G	YEXCSPWQUS
7WBTVTAY43	3A2243JFJR

Step 10. Download the Ngrok program file.

The screenshot shows the Windows Chocolatey download page for Ngrok. It features the Windows logo and the word 'Windows' at the top. A button 'Choose another platform' is in the top right. Below the header, the 'Installation' section has tabs for 'Chocolatey' and 'Download'. The 'Download' tab is active, showing instructions to download a standalone executable. At the bottom, there are two buttons: 'Download for Windows (64-Bit)' and 'Download for Windows (32-Bit)'.

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..._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..._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
Try our new Traffic Inspector Dev Preview: https://ngrok.com/r/ti

Session Status      online
Account             @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

https://52fc-1-171-29-30.ngrok-

Port Forwarding

0 (0 ~ 65535)

Listen port

20842 (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

