



spark
Italian inSight

Argo Config User Manual V1.2



Confidentiality Notice

Copyright© 2024 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.



Installation and system requirements

1. 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, replay, 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.

2. 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 8.1(64-bit); Windows 10(64-bit); 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 8.1(32-bit or 64-bit); Windows 10(32-bit or 64-bit);

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 Server 2012 R2; Windows Server 2016; Windows

7SP1(64bit); Windows 8(64-bit); Windows 8.1(64-bit); Windows 10 (64-bit); Windows

Server 2019; Windows Server 2022; Windows 11(64-bit)



Table of contents

0. START	8
0.1 LOG IN	8
0.2 ARGO CONFIG INTERFACE	11
1. DEVICES	12
1.1 STATISTICS	12
1.2 VIDEO DEVICES.....	12
1.2.1 Add video devices (Automatic scan/ Manual add)	12
1.2.2 Edit video devices.....	14
1.2.3 Delete video device	22
1.2.4 Browse video devices.....	23
1.2.5 Video devices configurations.....	23
1.2.6 Open device web interface	26
1.3 I/O MODULE.....	26
1.3.1 Add I/O module (Auto scan/Manual add).....	26
1.3.2 Edit I/O modules.....	28
1.3.3 Delete I/O modules	28
1.3.4 Browse I/O modules information and status	29
1.4 OTHER SETTINGS	29
1.4.1 Database settings.....	29
1.4.2 External Network Configuration	30
1.4.3 License plate recognition upload settings	36
1.4.4 Web server settings.....	36
1.5 STORAGE	37
1.5.1 Add storage.....	37
1.5.2 Edit storage	38
1.5.3 Delete storage	38
1.6 INFORMATION.....	39
1.6.1 Information.....	39
1.6.2 Installed services.....	39
1.6.3 License overview.....	39
1.7 SPARK AI SERVICES.....	40
1.7.1 Spark AI devices.....	40
1.7.2 Spark AI device camera.....	41
1.7.2.1 Add camera to Spark AI service.....	41
1.7.2.2 Edit camera on Spark AI services.....	42



1.7.2.3 Delete camera on Spark AI	45
1.7.2.4 Information.....	45
1.7.3 AI analytics (fire detection/smoke detection)	45
1.8 SERVER.....	48
1.8.1.1 Primary server and secondary servers.....	48
1.8.1.2 Add server.....	50
1.8.1.3 Delete server	52
1.9 VIEW MODE.....	53
2. USER MANAGEMENT.....	54
2.1 PASSWORD SETTINGS.....	54
2.2 GROUPS.....	54
2.2.1 Create groups	54
2.2.2 Set schedules for each group:	55
2.2.3 Set permissions for each group:	55
2.2.4 Delete group	58
2.3 USER	58
2.3.1 Add user	58
2.3.2 Delete User	59
2.4 CLIENT CONNECTION INFORMATION.....	59
3. HEALTH DOCTOR.....	61
3.1 SYSTEM HEALTH CHECK CONFIGURATION.....	61
3.2 ADD RESPONSE ACTION	62
3.2.1 Send email	63
3.2.2 Line Notify.....	66
3.3 EDIT RESPONSE ACTION.....	68
3.4 DELETE RESPONSE ACTION.....	68
3.5 EXECUTE RESPONSE ACTION	69
4. EVENT AND MANAGEMENT.....	70
4.1 ADD/EDIT/COPY/DELETE EVENT	70
4.2 TRIGGER CONDITIONS.....	72
4.2.1 Add trigger condition	72
4.2.1.1 Advanced Setting for Trigger Conditions	74
4.2.2 Edit trigger condition.....	74
4.2.3 Delete trigger condition	75
4.3 RESPONSE ACTION.....	75
4.3.1 Response action schedule.....	75
4.3.2 Add response action	76



4.3.3 Edit response action	83
4.3.4 Delete response action.....	84
4.3.5 Execute response action	84
4.4 SET THE EVENT AS ALARM	84
4.4.1 Edit alarm setting	84
5. ACCESS CONTROL.....	88
5.1 ADD/EDIT/DELETE LIST.....	88
5.2 ACCESS ID	89
5.2.1 Add access ID.....	89
5.2.2 Edit access ID	90
5.2.3 Deactivate/Delete all access ID	90
5.2.4 Export/Import access ID	91
6. VIDEO ANALYTICS DATA COLLECTION	94
6.1 SENS CAM SETTINGS.....	94
6.1.1 Login settings	94
6.1.2 Image setting.....	95
6.1.3 Analytics settings.....	96
6.2 VIDEO ANALYTICS DATA COLLECTION SETTINGS.....	98
6.2.1 Add video analytics parameters.....	98
6.2.2 Set video analytics parameters.....	98
6.2.3 Delete video analytics parameter	99
7. BACKUP AND RESTORE	100
7.1 BACKUP.....	100
7.2 RESTORE	100
7.3 SCHEDULED BACKUP	101
8. LICENSE.....	102
8.1 INFORMATION.....	102
8.2 MANAGE LICENSE.....	102
8.3 CHANNEL LICENSE KEY	103
8.4 INTEGRATED DEVICES.....	103
9. LOG.....	104
9.1 DATA TRACE	104
9.2 SYSTEM LOG	106
9.3 DETAILED LOG	107
10. ARGO CLIENT.....	109
11. OPTIONS	110
11.1 LANGUAGE	110



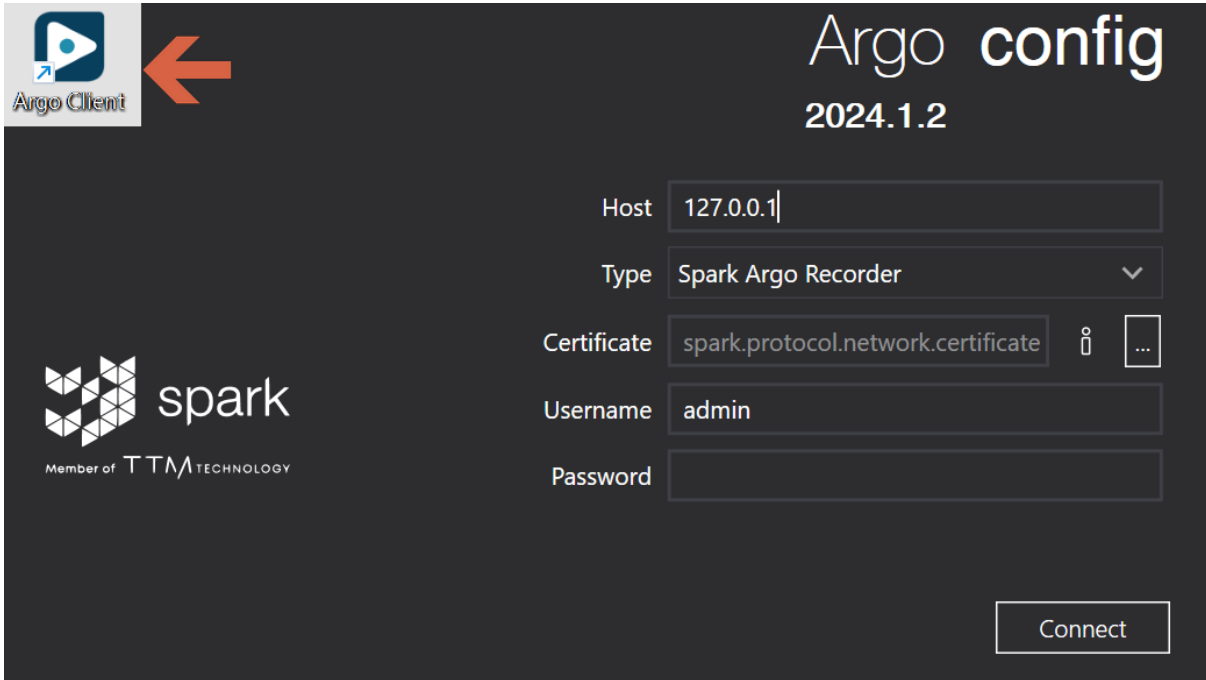
11.2 INTERFACE.....	110
11.3 DRAWING.....	111
11.4 USER INTERACTION MODE	112
11.5 WATERMARK.....	113
11.6 ADVANCED.....	114
12. USER.....	115
12.1 CHANGE PASSWORD	115
12.2 LOGOUT/CLOSE	115
13. ABOUT	116



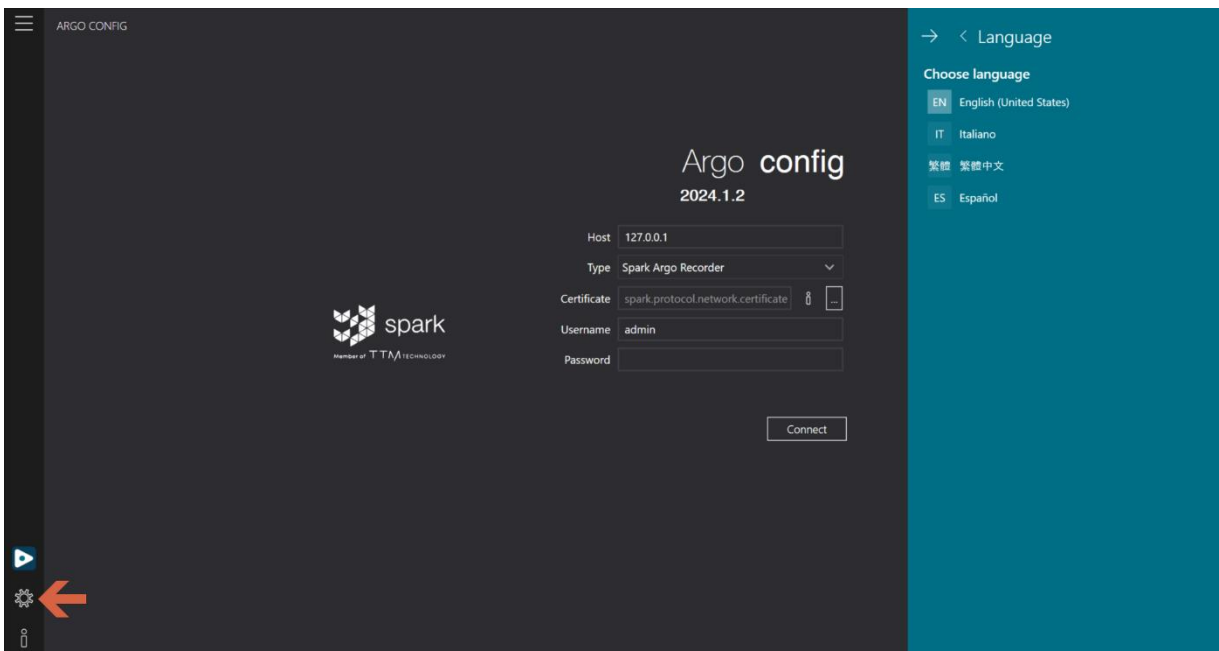
- 0. START

0.1 Log in

Step 1. Double click Argo config to open login window



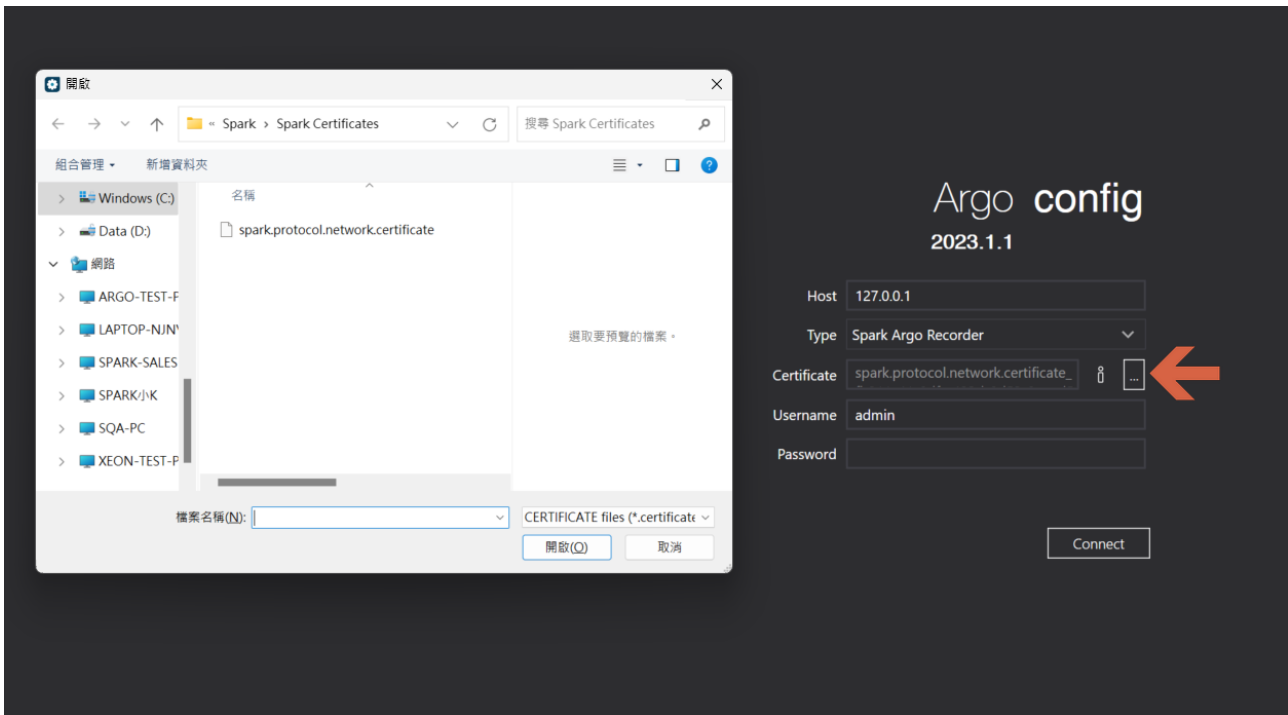
Step 2. Select language



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

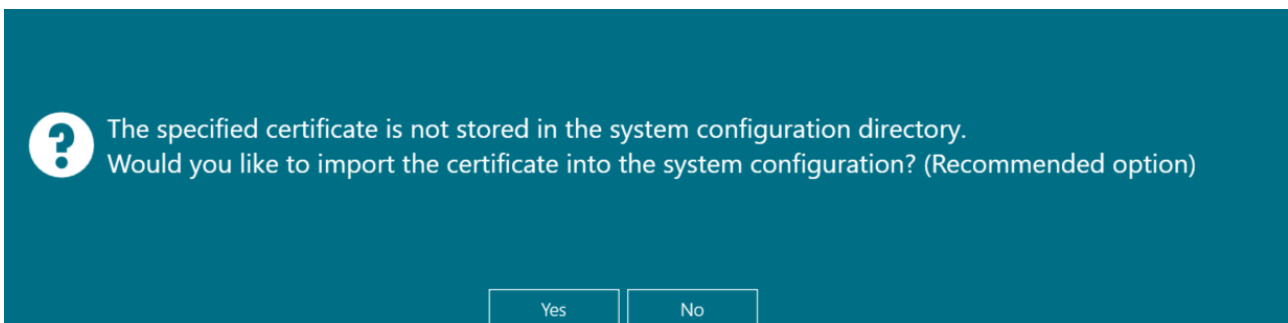


Step 3. Log in Argo config



- 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**]

Step 4. On first login, you will be asked if you want to import the certificate. Click Yes to save the certificate in the system.





Step 5. After logging in, the system will ask to change the password. The new password must contain at least one special character, one upper case letter, one lower case letter and a minimum length of 8 characters.

i Change User Password

Username

Old password

New password

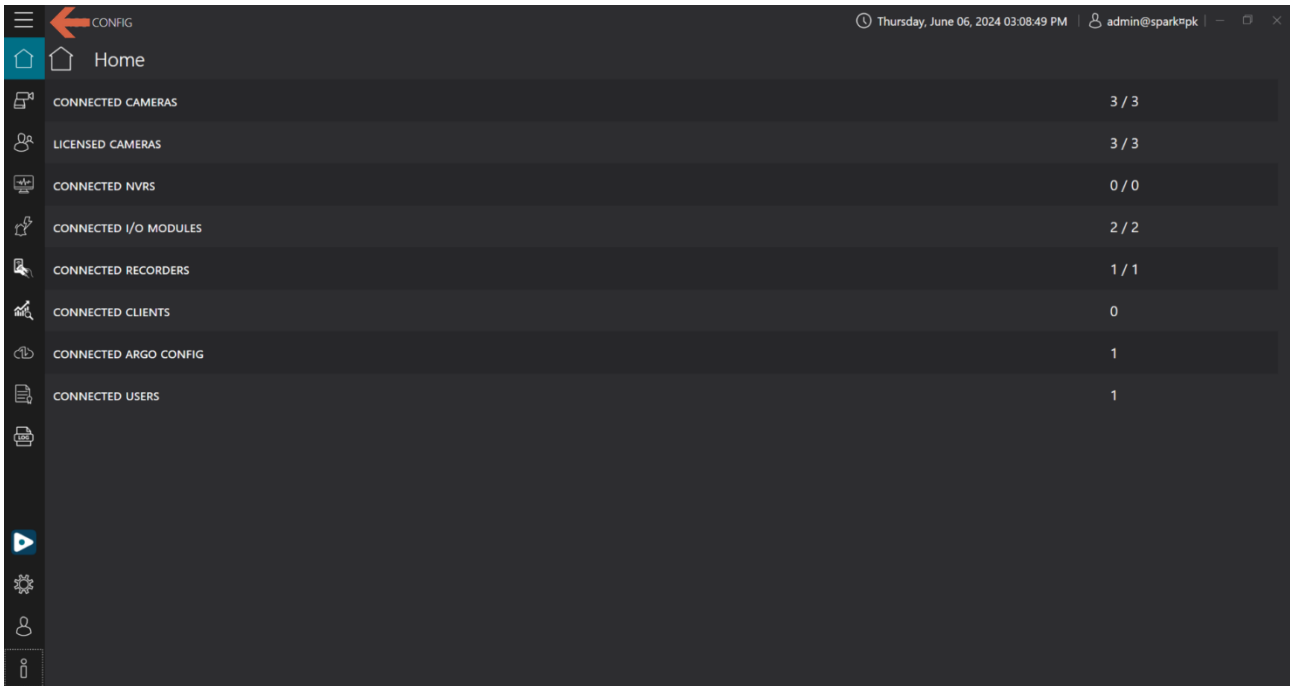
Confirm password

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

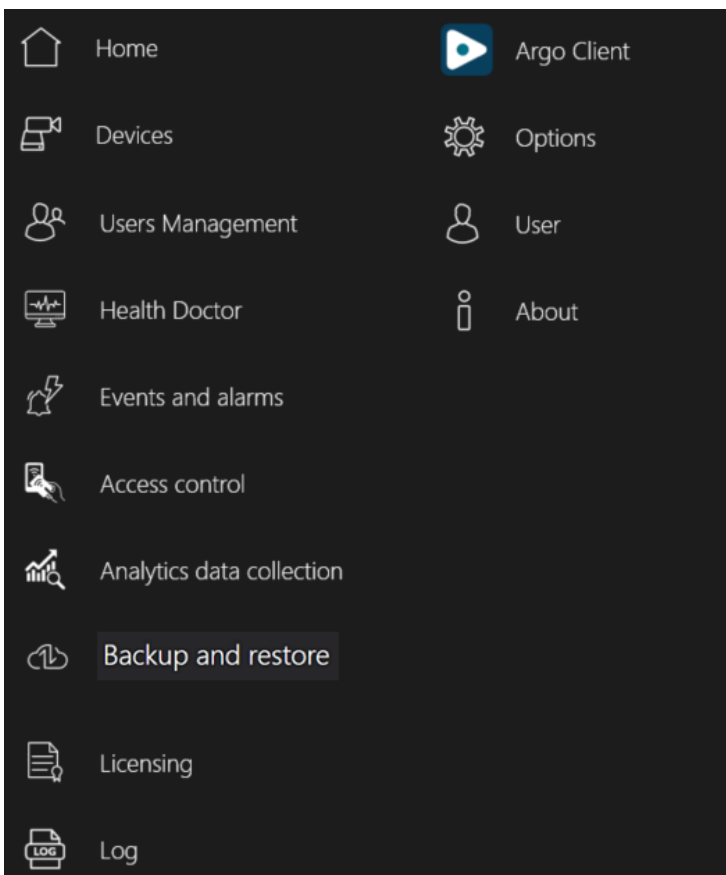
- When using single login interface, users only need to insert the changed password to log in.
- When using quick login interface, users must change the default password to the changed password to log in.



0.2 Argo config interface



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

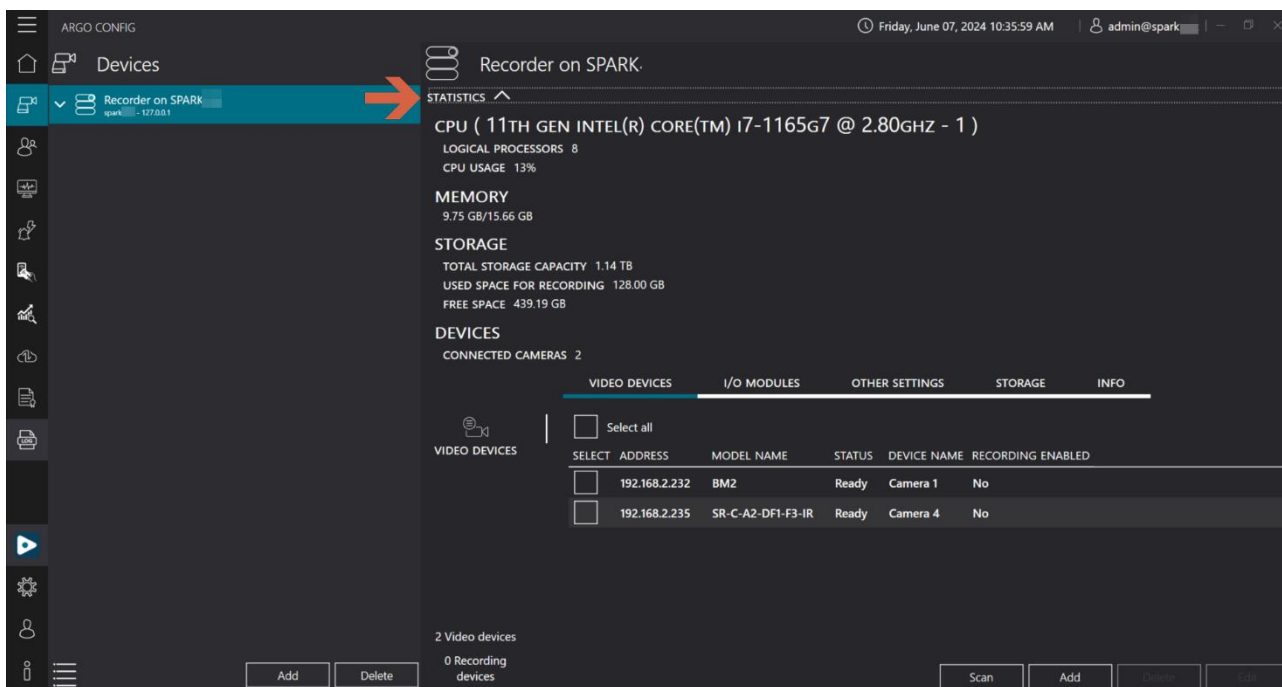


- Menu: Devices/ User management /Health Doctor/Events and alarms/Access Control/ Analytics data collection/Backup and restore/Licensing/Log /Argo client/Options/User/About



1. DEVICES

1.1 Statistics

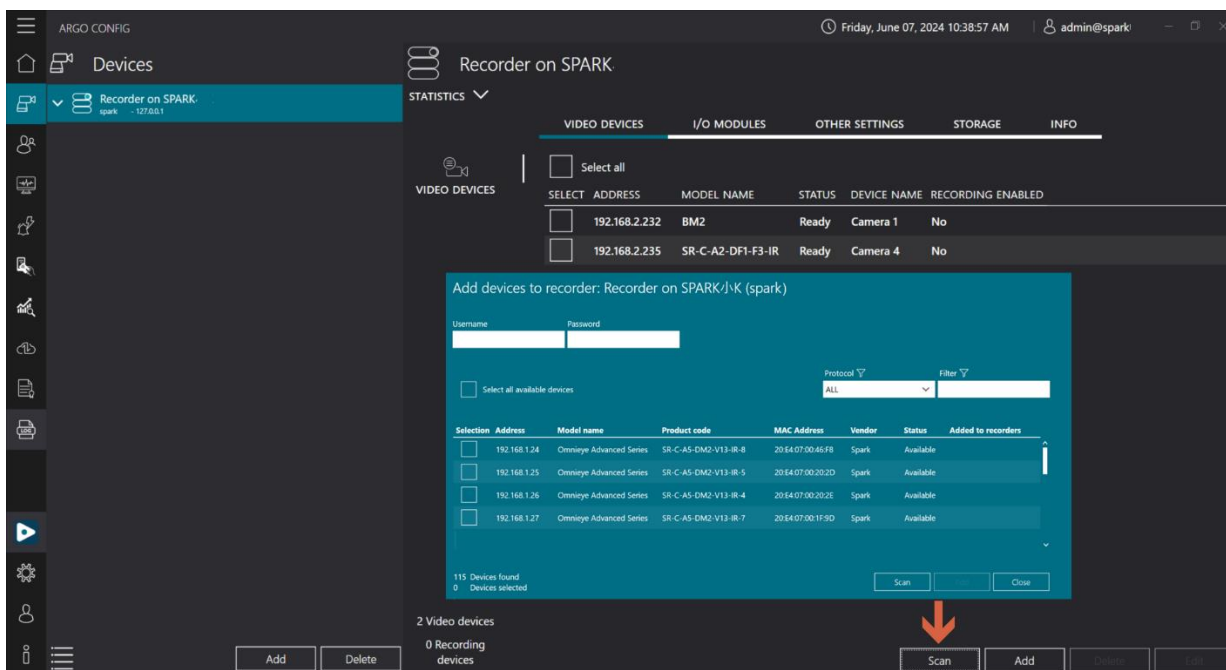


- Click on **[Statistics]**
- Browse device status on Statistics: CPU/memory/Storage/Device

1.2 Video Devices

1.2.1 Add video devices (Scan devices/Add devices to recorder manually)

A. Scan devices

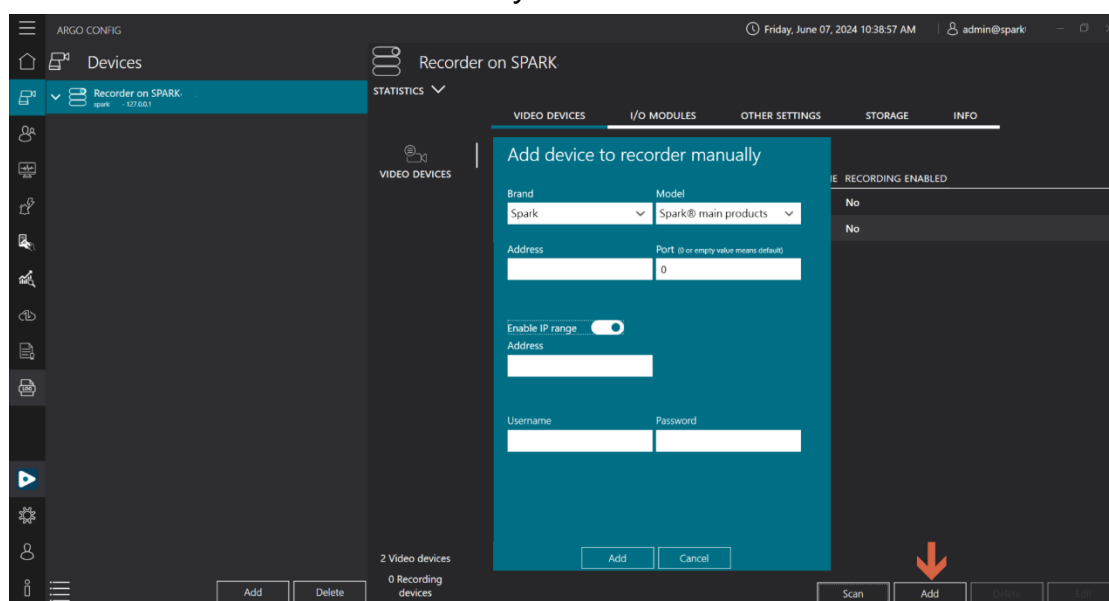




- Click **[Scan]** at the bottom right.
- Select devices and then click **[Add]**
- Username: Insert device username.
- Password: Insert device password.

Note: 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 devices to recorder manually



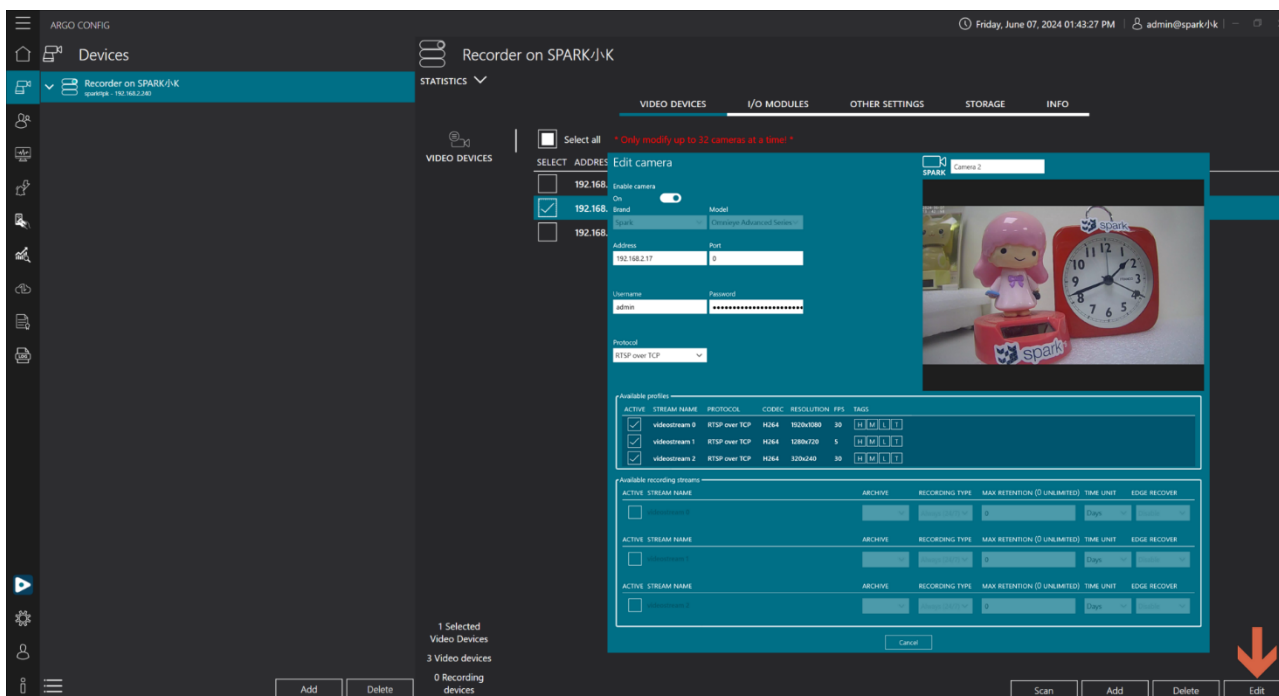
- Click **[Add]** at the bottom right.
- Brand: Select device brand name (below list for reference)
- Address: Insert device IP address
- Port: Insert device port number (default is 0)
- Enable IP range: insert desired IP range
- Username: Insert device username.
- Password: Insert device password.

Brand	Description
AMTK	AMTK devices
Generic	If the camera model is displayed as unknown, the system can use the Generic API for addition.
ICE	ICE license plate recognition devices



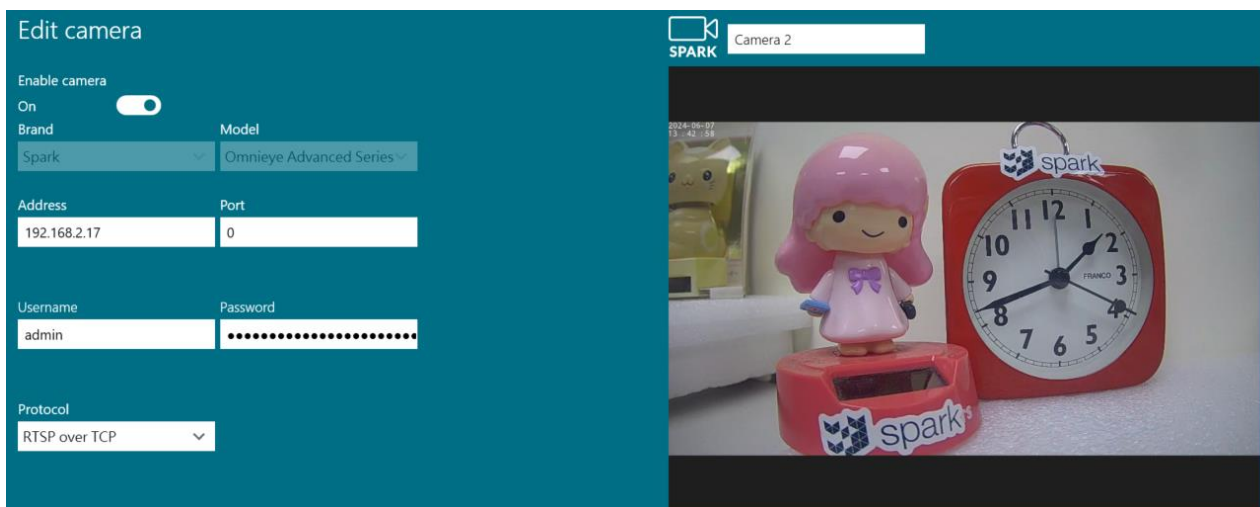
LPR Reader	License plate recognition devices
Milesight	Milesight devices
ONVIF	ONVIF compliant devices
Spark	Spark devices

1.2.2 Edit video devices



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

Step 1. Edit camera



- Enable camera: enable/disable camera
- Brand: selected during camera addition, cannot be modified.



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

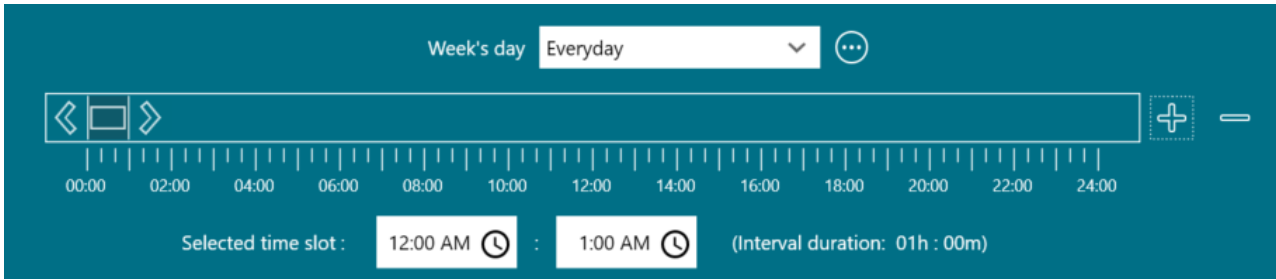
Step 2. Available profiles

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

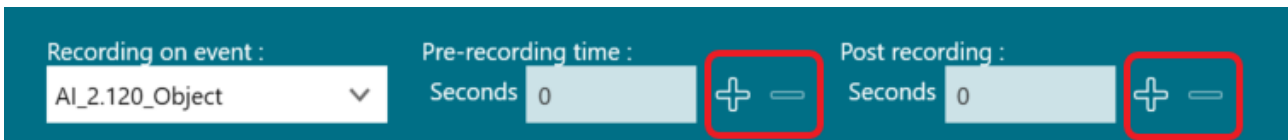
- Select the profile(s) to display (default is all enabled).

Step 3. Available recording streams

- 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.



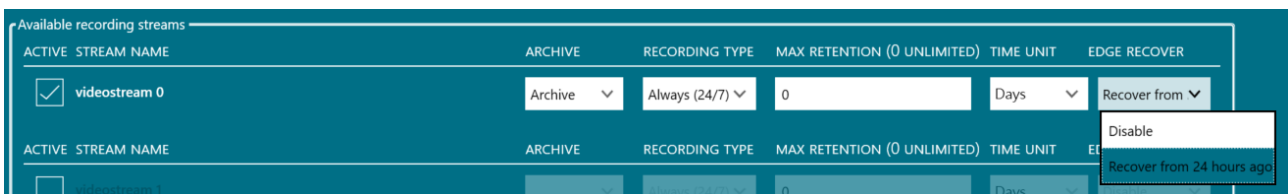
- Add schedule: Click [+] and drag left or right to adjust the time slot, or input the selected time slot.
- Delete schedule: Select the time slot you want to delete and click [-].
- Edit schedule: Select the time slot and drag left or right to adjust it, or input the selected time slot.



- D. Recording on event: 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

- E. 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.

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



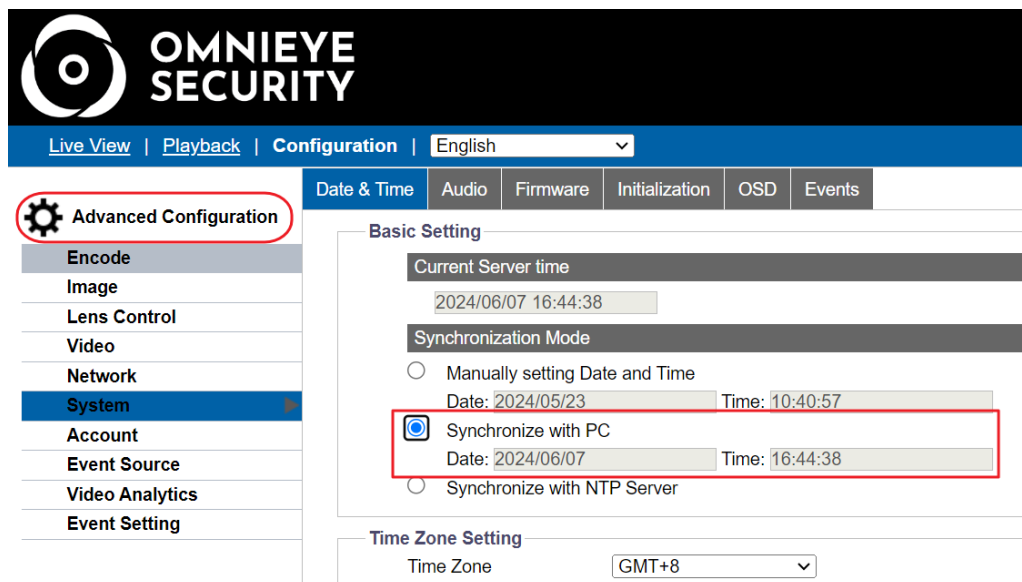
- G. Edge Recover: select Recover from 24 hours ago/Disable, activate/deactivate edge recover.
- Mechanism: prevents expected interruptions in recording caused by improper use of camera cables or deterioration of network cables causing disconnection, leading to the inability to trace past recording records.



- 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



- 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

- 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

- 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

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



Add devices to recorder: Recorder on SPARK (spark)

Username Password

Select all available devices

Protocol Filter

Selection	Address	Model name	Product code	MAC Address	Vendor	Status	Added to recorders
<input type="checkbox"/>	192.168.1.24	Omnieye Advanced Series	SR-C-A5-DM2-V13-IR-8	20:E4:████████	Spark	Available	
<input type="checkbox"/>	192.168.1.25	Omnieye Advanced Series	SR-C-A5-DM2-V13-IR-5	20:E4:████████	Spark	Available	
<input type="checkbox"/>	192.168.1.26	Omnieye Advanced Series	SR-C-A5-DM2-V13-IR-4	20:E4:████████	Spark	Available	
<input type="checkbox"/>	192.168.1.27	Omnieye Advanced Series	SR-C-A5-DM2-V13-IR-7	20:E4:████████	Spark	Available	
<input type="checkbox"/>	192.168.1.28	Omnieye Advanced Series	SR-C-A5-DM2-V13-IR-11	20:E4:████████	Spark	Available	
<input type="checkbox"/>	192.168.1.29	Omnieye Advanced Series	SR-C-A5-DM2-V13-IR-6	20:E4:████████	Spark	Available	

114 Devices found
0 Devices selected

- Please refer to 1.2.1

Step 7. Edit device - video devices

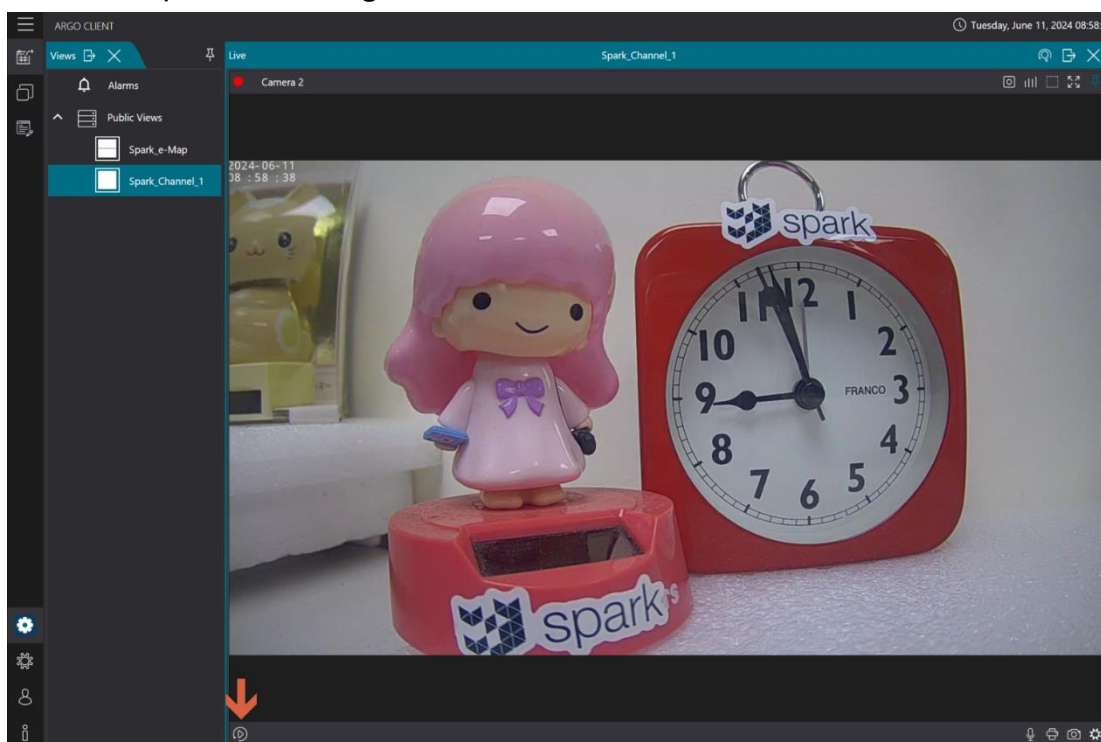
The screenshot shows the 'Recorder on SPARK' configuration page. On the left, a list of video devices is shown with the device at 192.168.2.17 selected. The 'Edit camera' dialog is open, showing fields for Brand (Spark), Model (Omnieye Advanced Series), Address (192.168.2.17), Port (8), Username (admin), and Password (*****). Below these fields, there are sections for 'Available profiles' and 'Available recording streams'. The 'Available profiles' section shows three profiles: 'VideoStream0', 'VideoStream1', and 'VideoStream2', all with 'RTSP over TCP' protocol and 'H264' codec. The 'Available recording streams' section shows three streams, with 'VideoStream0' selected. The 'Recover from' setting is set to 'Recover from 24 hours ago'. At the bottom right of the dialog, there is a red arrow pointing down.

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

c. Argo Client system configuration

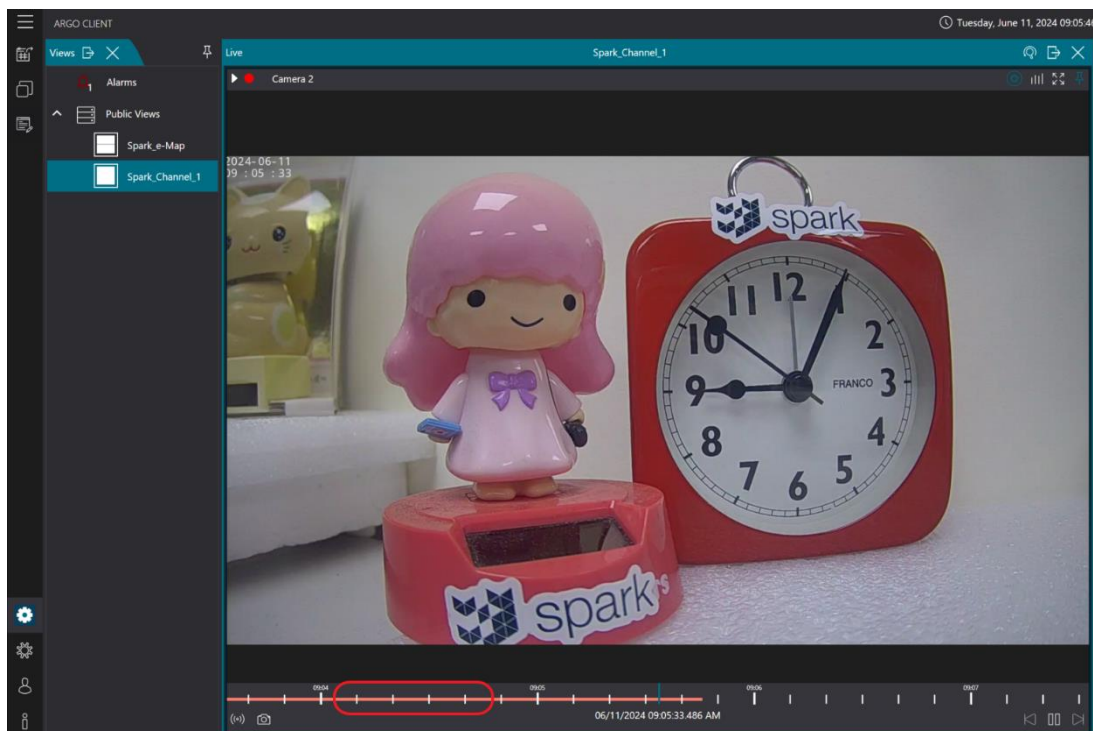


Step 8. monitoring interface



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

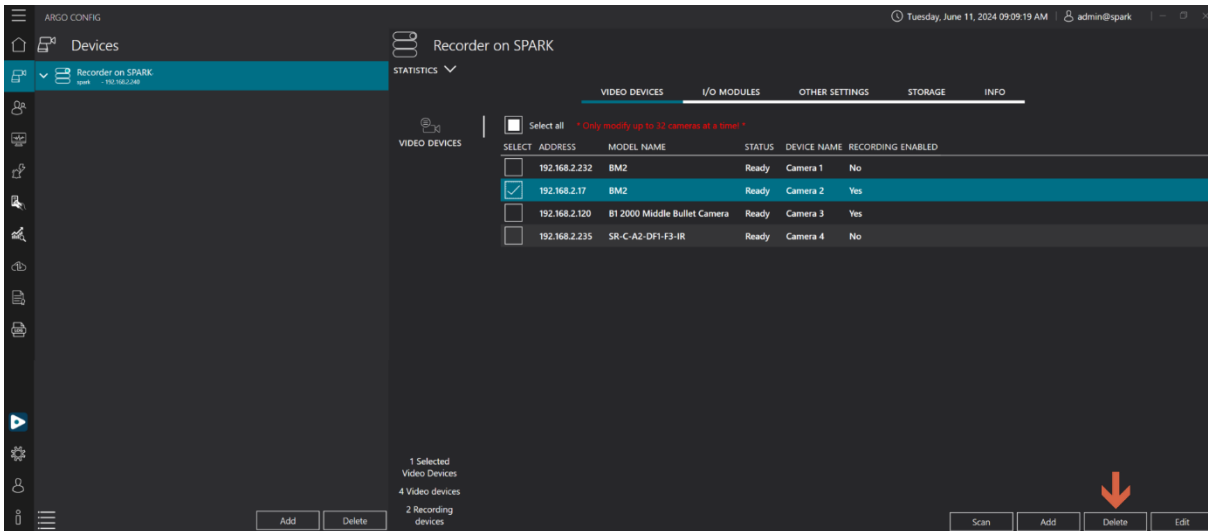
Step 9. Replay



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

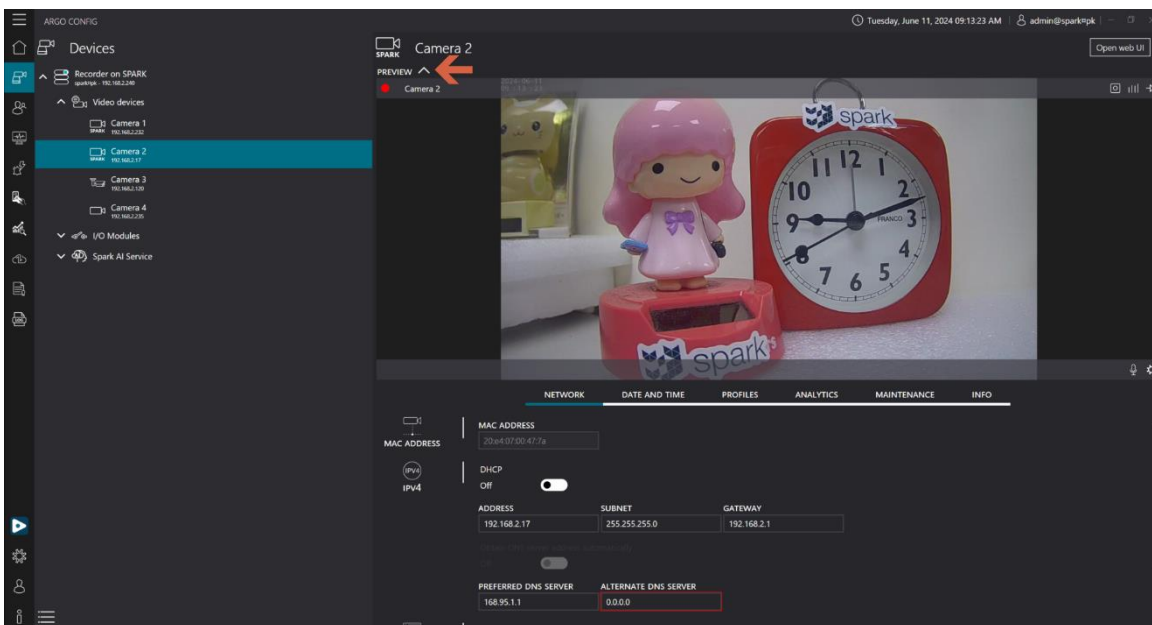


1.2.3 Delete video device



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

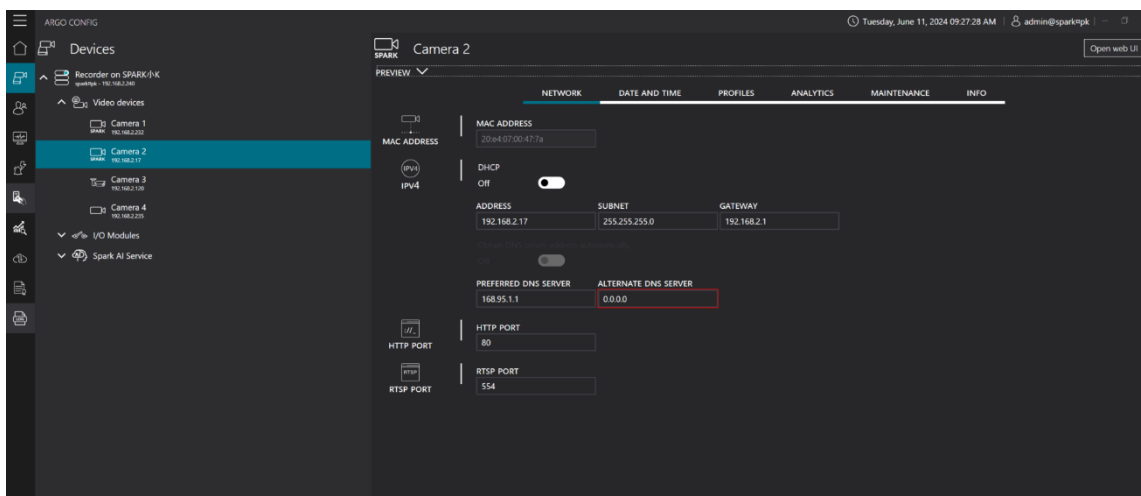
1.2.4 Preview video devices



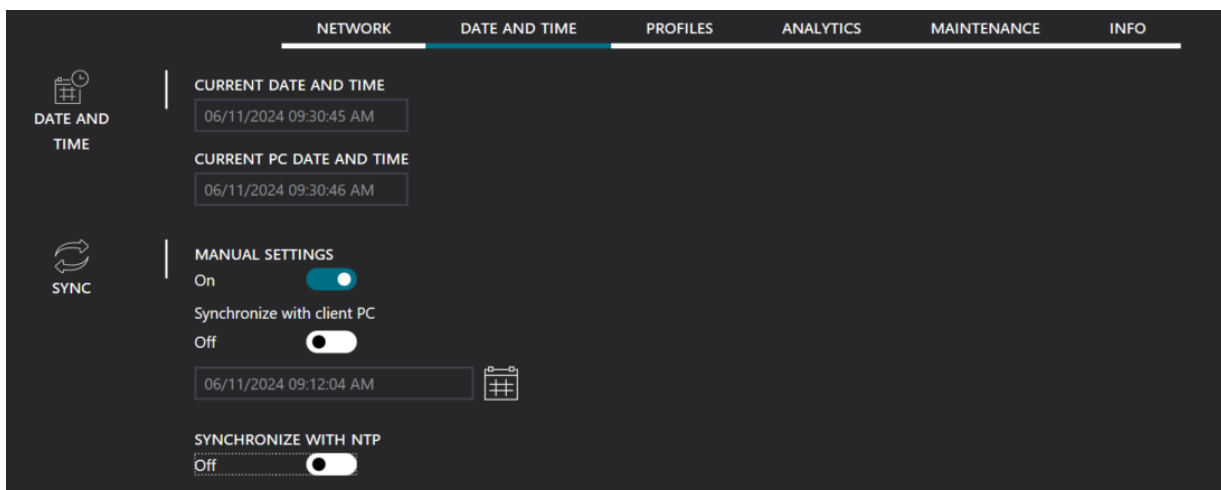
- Click **[Preview]**



1.2.5 Video devices configurations



- Network: edit device network settings
 - MAC address: unable to edit.
 - IPV4: When DHCP is enabled, 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.



- Date and time: Edit device date and time settings.
 - Date and Time: Browse current date and time, and computer date and time.



NETWORK DATE AND TIME PROFILES ANALYTICS MAINTENANCE INFO

DATE AND TIME

CURRENT DATE AND TIME
06/11/2024 09:29:05 AM

CURRENT PC DATE AND TIME
06/11/2024 09:29:06 AM

SYNC

MANUAL SETTINGS
Off

SYNCHRONIZE WITH NTP
On

Server 1
pool.ntp.org

* The NTP server test is performed locally through the host PC network connection: this means that if the device network configuration is not done properly the device will not be able to reach the NTP server correctly. Please check gateway and DNS server network settings.

- Sync: Enable manual settings to turn on/off synchronization with the client and NTP synchronization.
- Server 1~3 Dialogs input NTP server address and click test to check NTP status.

NETWORK DATE AND TIME PROFILES ANALYTICS MAINTENANCE INFO

PROFILES

SELECT	STREAM NAME	PROTOCOL	CODEC	RESOLUTION	FPS	ENABLED
<input type="checkbox"/>	videostream 0	RTSP over TCP	H264	1920x1080	30	Yes
<input type="checkbox"/>	videostream 1	RTSP over TCP	H264	1280x720	5	Yes
<input type="checkbox"/>	videostream 2	RTSP over TCP	H264	320x240	30	Yes

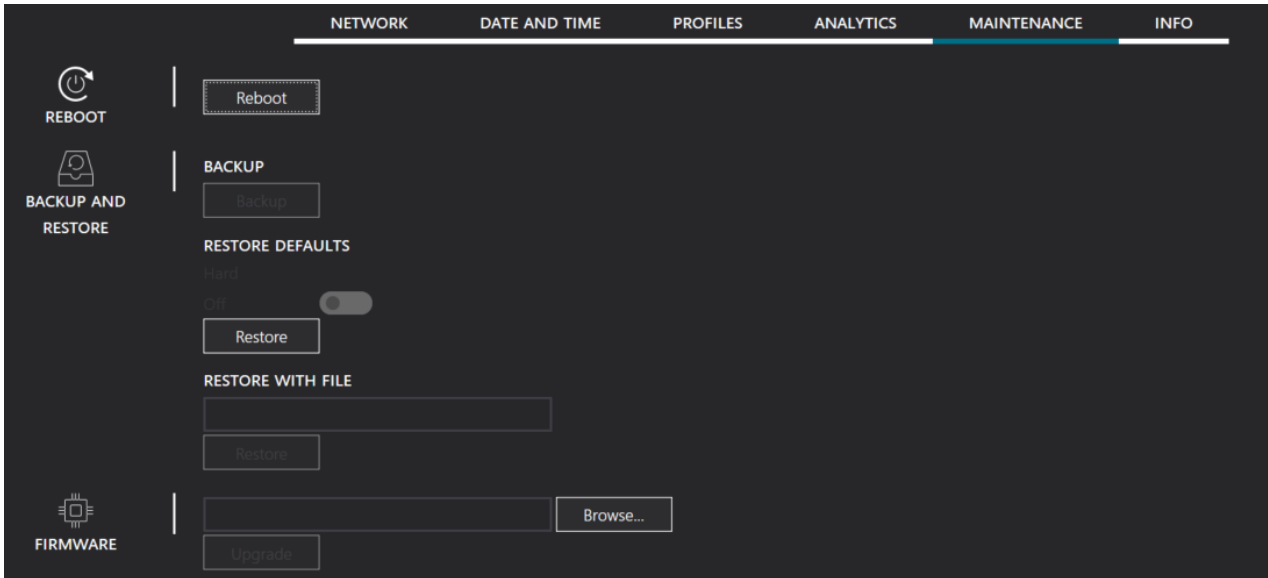
- Profiles: select the stream you want to edit for advanced settings.

NETWORK DATE AND TIME PROFILES ANALYTICS MAINTENANCE INFO

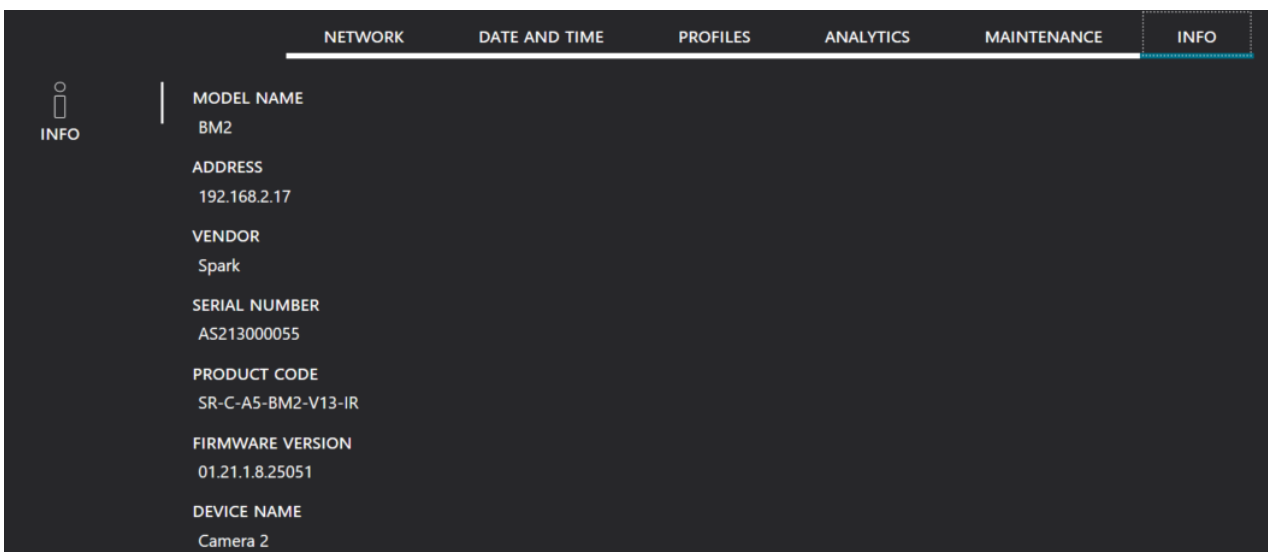
ANALYTICS

Motion	Tampering	Audio
Trip wire	Intrusion	Loitering
Departure	Withdrawn	Adverseway
Abandon		

- Analytics: preview device video analytics status.



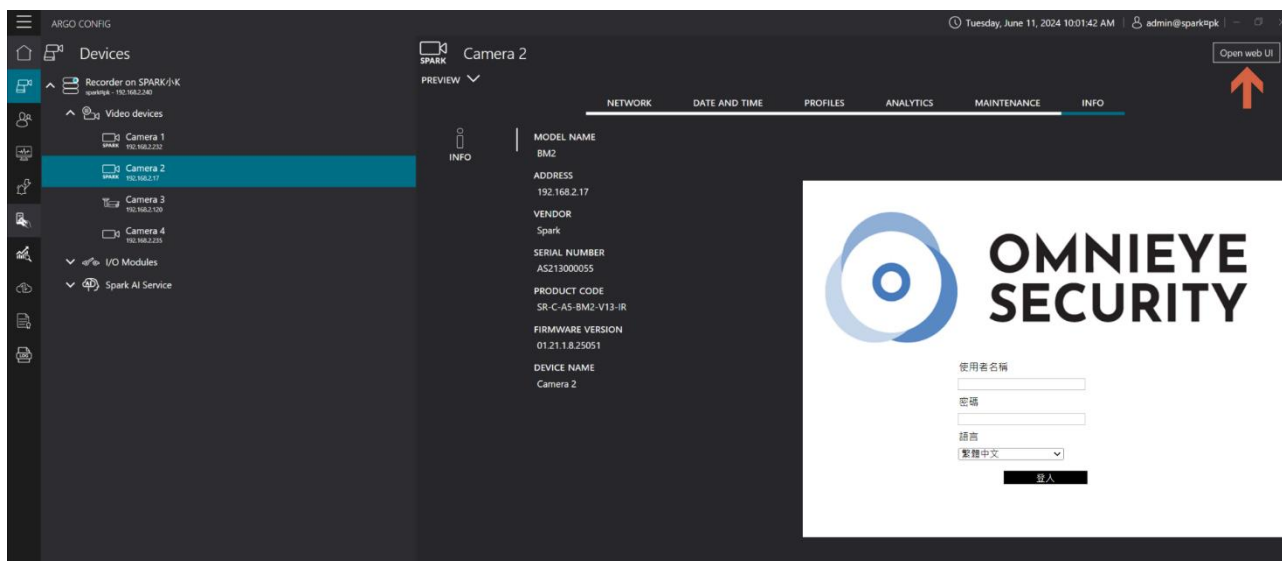
- Maintenance: edit device maintenance settings.
 - Reboot: Restart device.
 - Backup: Backup device settings.
 - Restore: Restore device settings.
 - Firmware: Update firmware version of the camera.



- Info: browse device information



1.2.6 Open device web interface

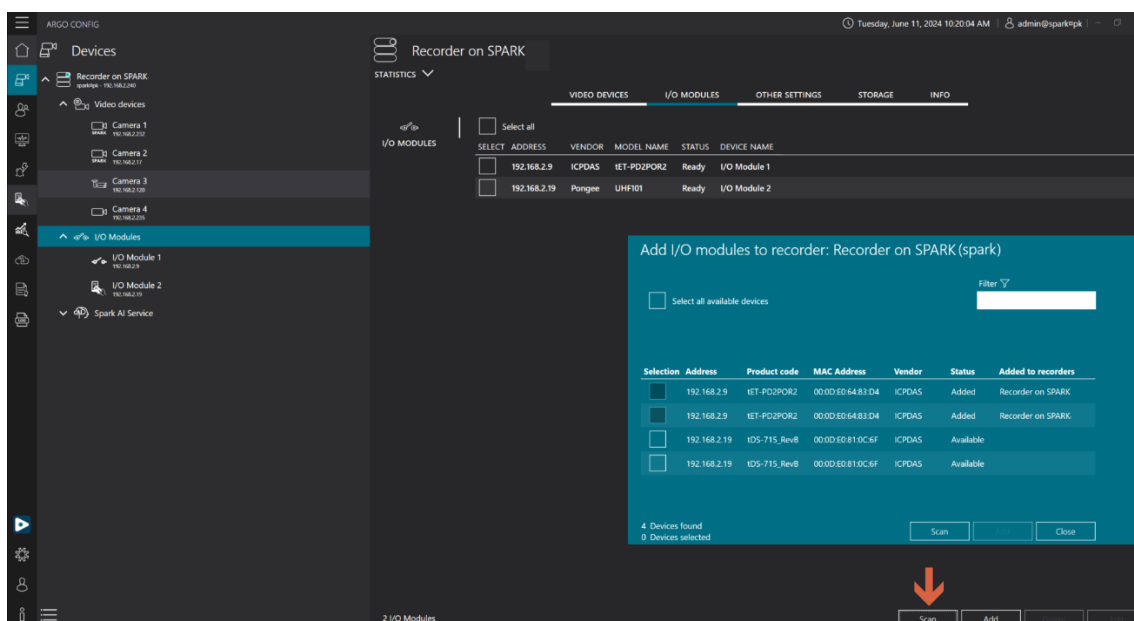


- Click on **[Open Web UI]**
- Username: insert username
- Password: insert password
- Language: select language

1.3 I/O Module

1.3.1 Add I/O module (Scan devices/Add device to recorder manually)

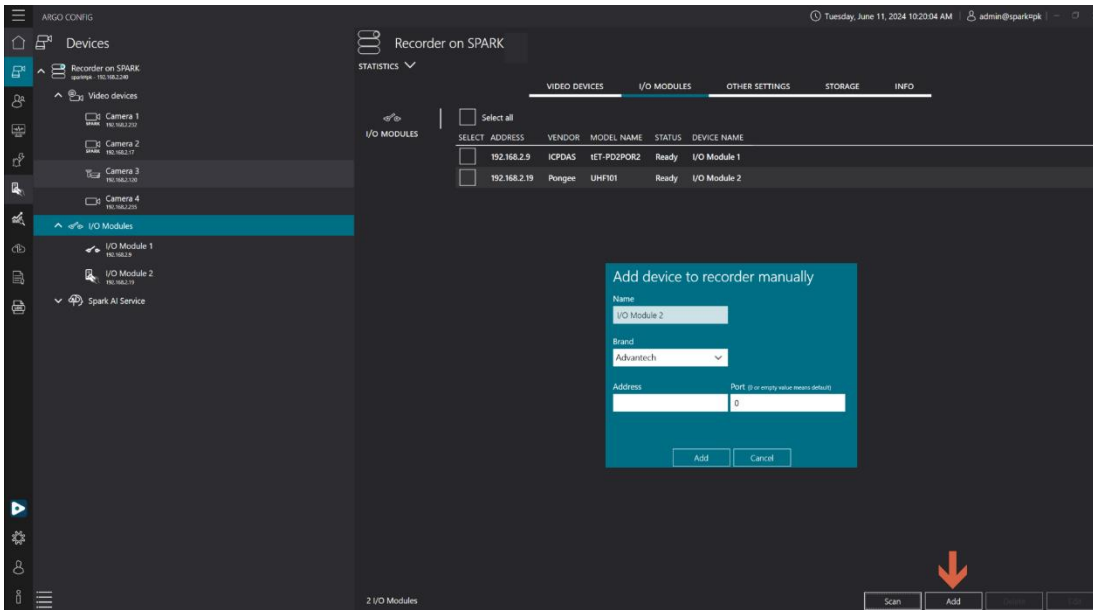
A. Scan device



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



B. Add devices to recorder manually I/O modules



- 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



1.3.2 Edit I/O modules

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

I/O MODULES

Select all

SELECT	ADDRESS	VENDOR	MODEL NAME	STATUS	DEVICE NAME
<input checked="" type="checkbox"/>	192.168.2.9	ICPDAS	tET-PD2POR2	Ready	I/O Module 1
<input type="checkbox"/>	192.168.2.19	Pongee	UHF101	Ready	I/O Module 2

Edit I/O module

Enabled On

Name: I/O Module 1

Brand: ICPDAS

Address: 192.168.2.9 Port #: 0 (or empty value means default)

2 I/O Modules

Scan Add Delete Edit

- 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).

1.3.3 Delete I/O modules

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

I/O MODULES

Select all

SELECT	ADDRESS	VENDOR	MODEL NAME	STATUS	DEVICE NAME
<input checked="" type="checkbox"/>	192.168.2.9	ICPDAS	tET-PD2POR2	Ready	I/O Module 1
<input type="checkbox"/>	192.168.2.19	Pongee	UHF101	Ready	I/O Module 2

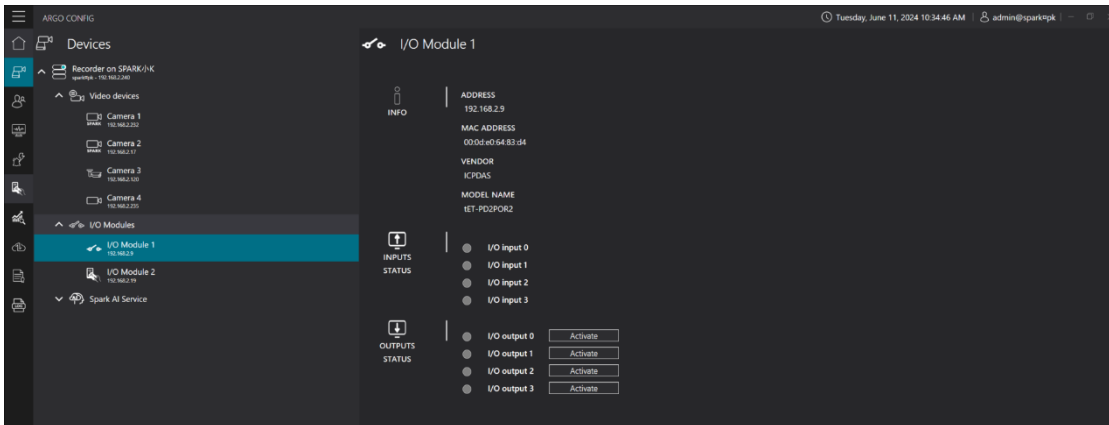
2 I/O Modules

Scan Add Delete Edit

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



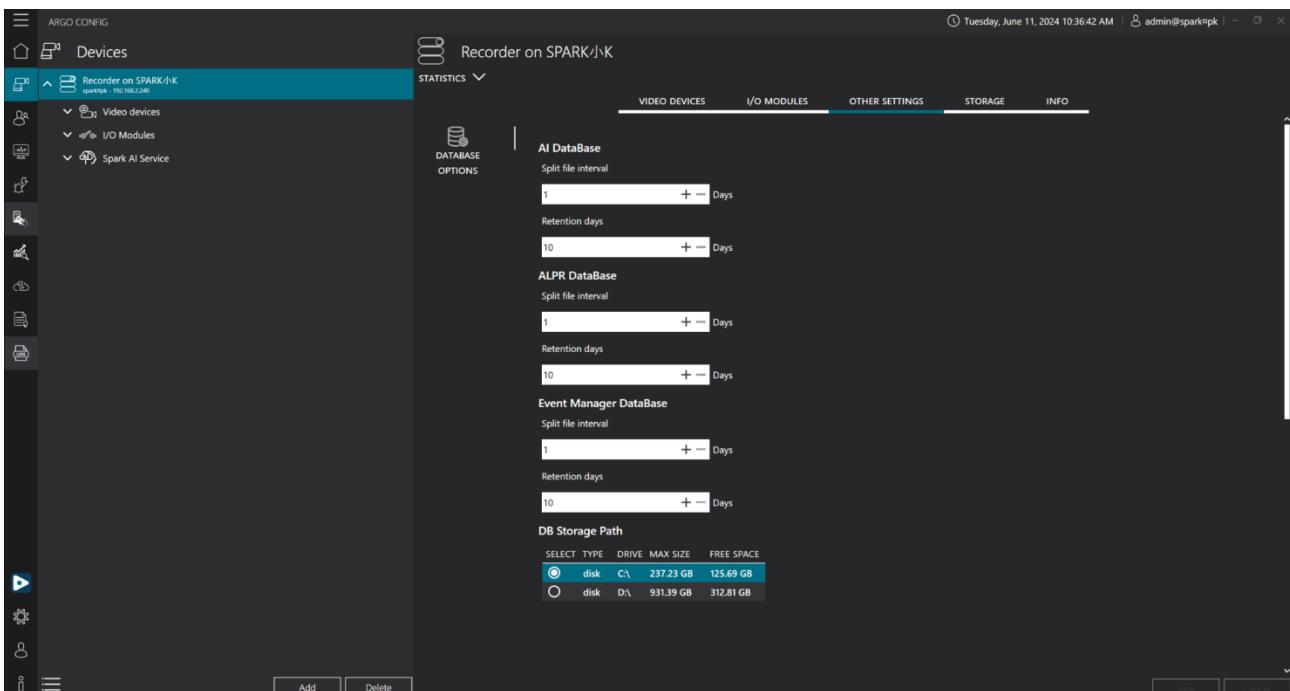
1.3.4 Browse I/O modules information and status



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

1.4 Other settings

1.4.1 Database options



- A. AI Database: Records usage data related to AI functions in Spark Recorder.
- B. AI License Plate Recognition 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.



- 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 10 to 1000 days.

- D. Database Storage Directory: Directory on the hard drive where the database can be stored in Spark Recorder.

1.4.2 External Network Settings

EXTERNAL NETWORK SETTINGS

Public ip address and port

External IP
0.0.0.0

Port Forwarding
0 (0 ~ 65535)

Listen port
20842 (0 ~ 65535)

- External address: the local WAN (Wide Area Network) IP address used for external communication. This function supports switching to sending short links via Line Notify.
- 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:

- Short links can replace sending photos via LINE Notify, avoiding reaching the limit of sending photos via LINE.
- The WAN IP address can be checked using <https://www.whatismyip.com.tw/tw/>
- The router must support Port Forwarding functionality to set up port forwarding.



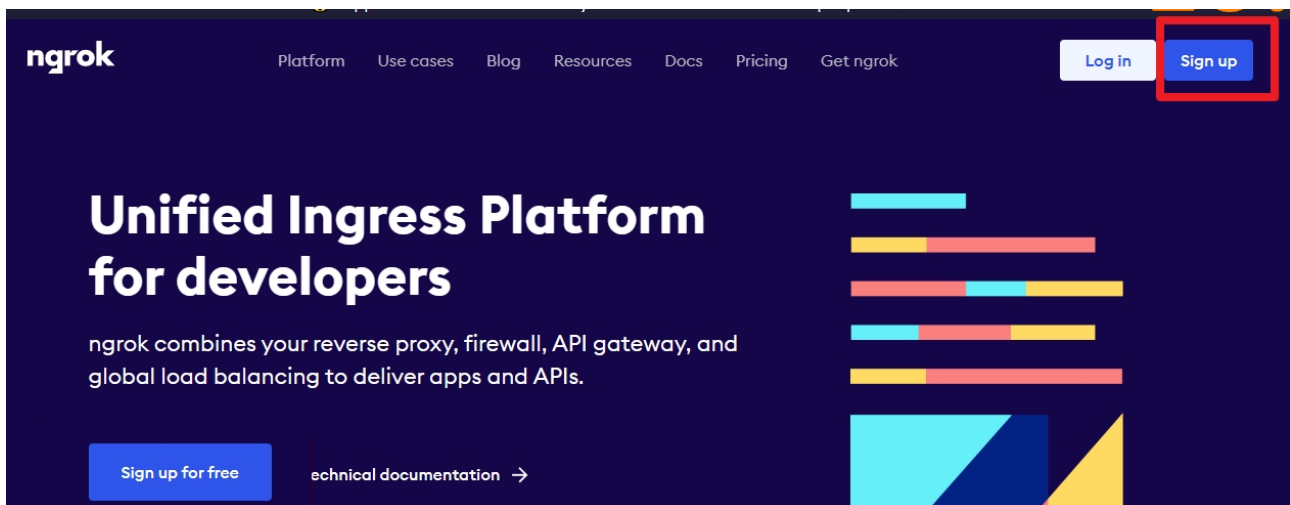
d. It is recommended to disable the computer firewall to ensure this function operates correctly.

e. Use NGROK forwarding service for communication port redirection settings.

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.

ngrok

Verify Email

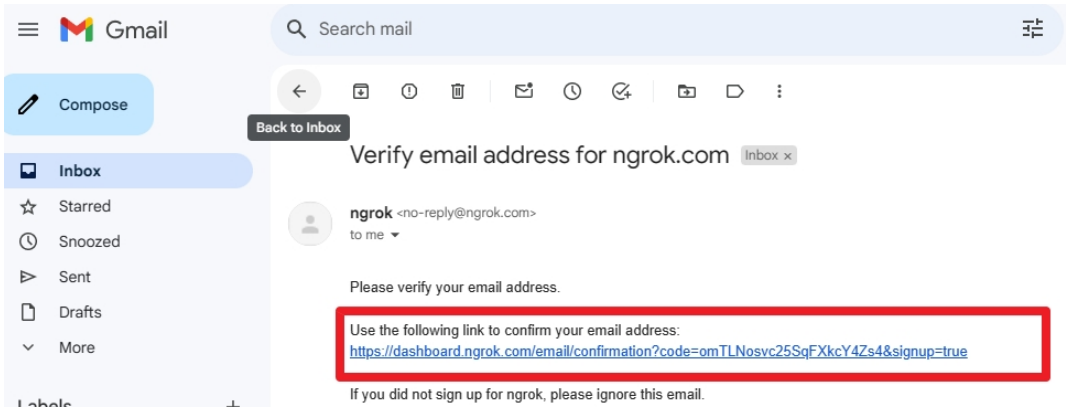


A verification email has been sent to .

Click the link in the email to verify your account

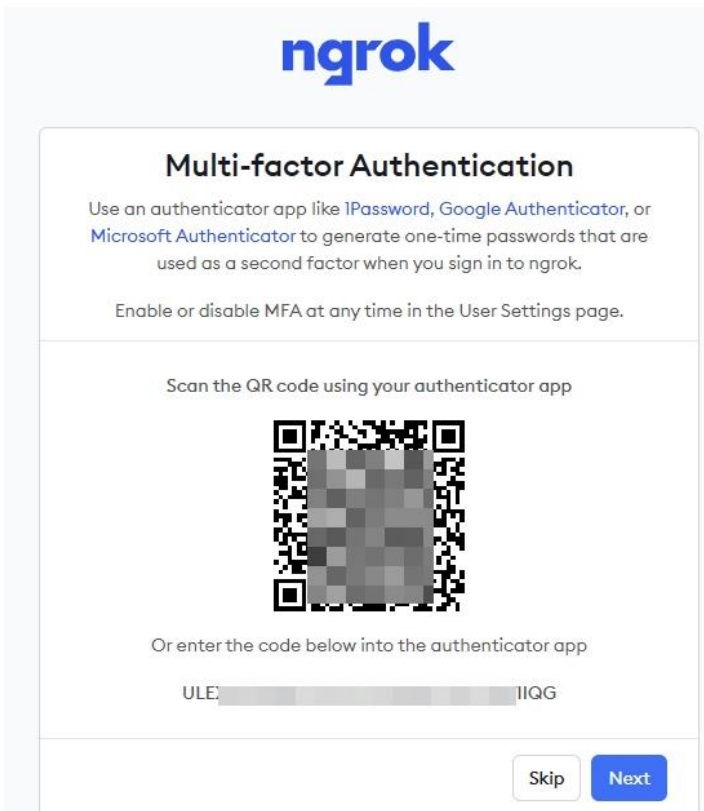
[Cancel](#) [Resend email](#) [Go to Gmail](#)

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

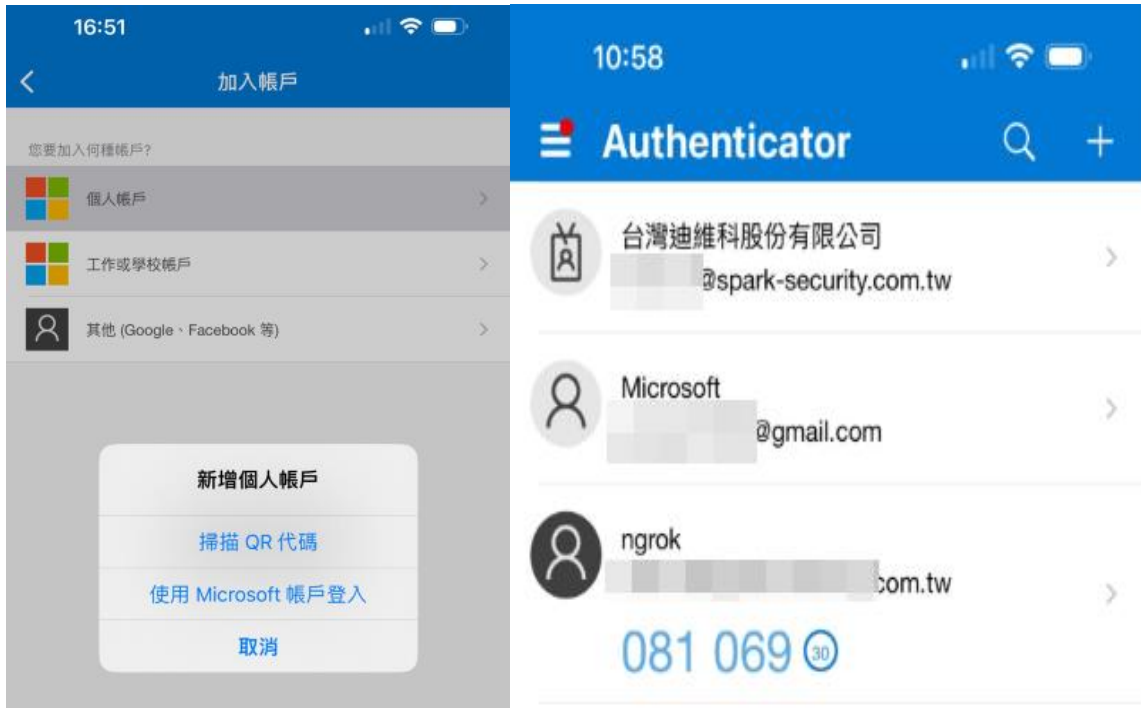


Step 6. Ngrok will display a QR code and authentication code. It is recommended to use a smartphone to scan the QR code for authentication. Click "Next" to proceed.

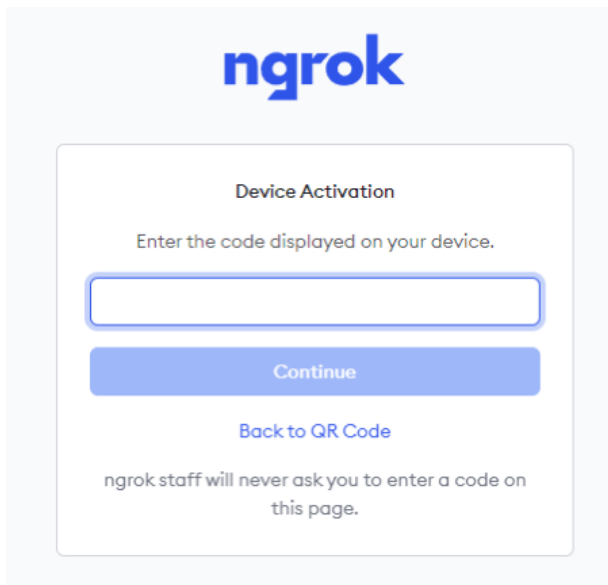
Note: Please complete Step 6 before clicking "Next". You can use the Microsoft Authenticator app or Google Authenticator app to scan for authentication.



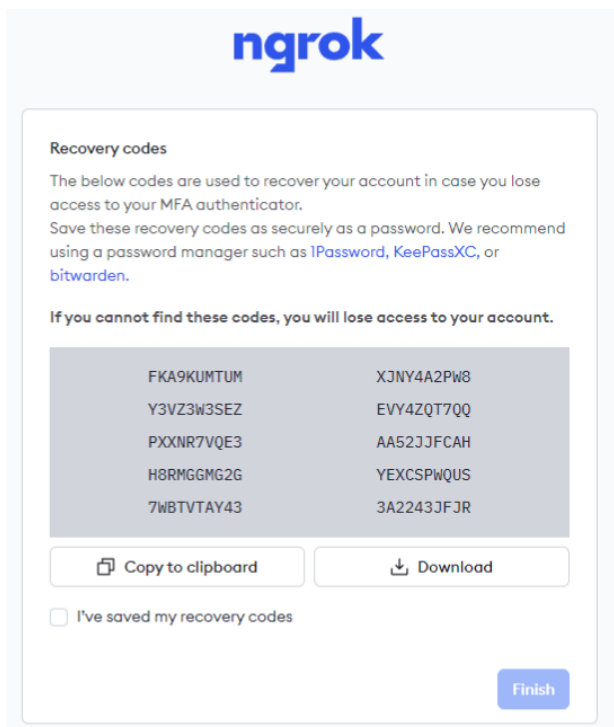
Step 7. Open the Authenticator app and scan the QR code to obtain a six-digit authentication code.



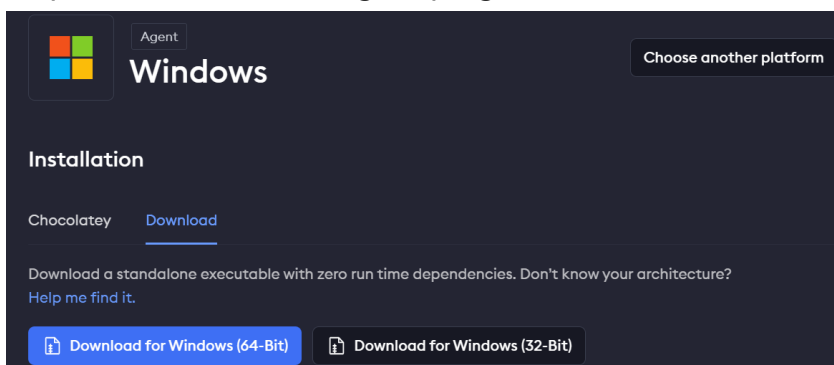
Step 8. Enter the six-digit code generated by the Authenticator app and click "Continue".



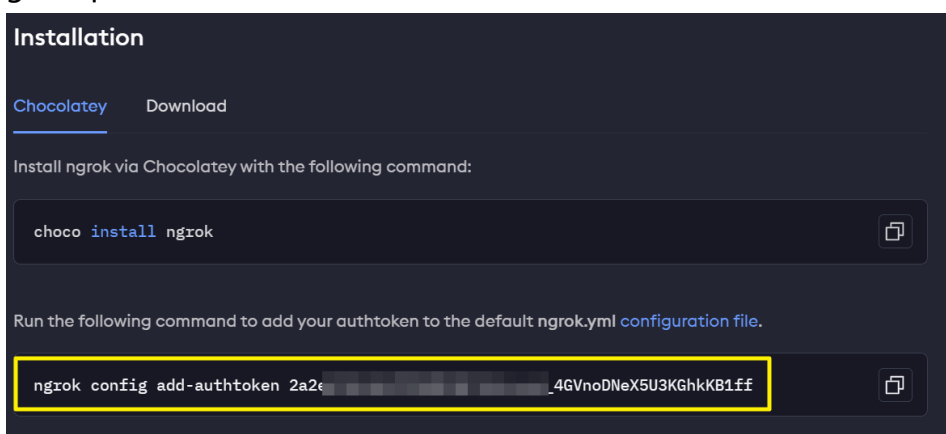
Step 9. Backup and store the recovery code for future account management.



Step 10. Download the Ngrok program file.



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



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



```
D:\Download\nngrok-v3-stable-windows-amd64>ngrok config add-authtoken 2a2[REDACTED]1ff
```

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

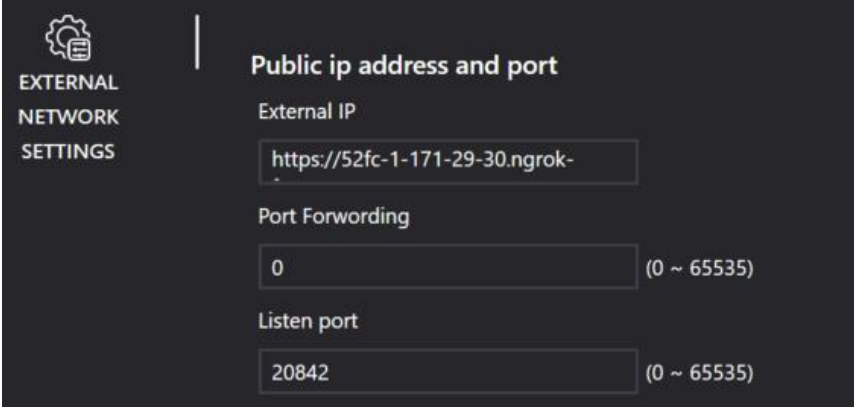
```
ngrok is a command line application, try typing 'ngrok.exe http 80'
at this terminal prompt to expose port 80.
D:\Download\nngrok-v3-stable-windows-amd64>ngrok.exe http 20842
```

```
ngrok (Ctrl+C to quit)
Try our new Traffic Inspector Dev Preview: https://ngrok.com/r/ti

Session Status      online
Account             [REDACTED]@gmail.com (Plan: Free)
Version             3.10.0
Region              Japan (jp)
Latency             35ms
Web Interface       http://127.0.0.1:4040
Forwarding           https://7c37-1-171-31-44.ngrok-free.app -> http://localhost:20842

Connections
  ttl   opn   rt1   rt5   p50   p90
   0    0    0.00 0.00 0.00 0.00
```

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





1.4.3 LPR upload setting

LPR UPLOAD SETTING

LPR FTP uploading

Enable

Path

ftp://192.168.2.22 (ftp://ip address)

Username

spark

Password

spark

Temporary Folder

C:\ProgramData\Spark\jpeg_tmp

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

1.4.4 Web server settings

WEB SERVER SETTINGS

Web Server

Enable

Port

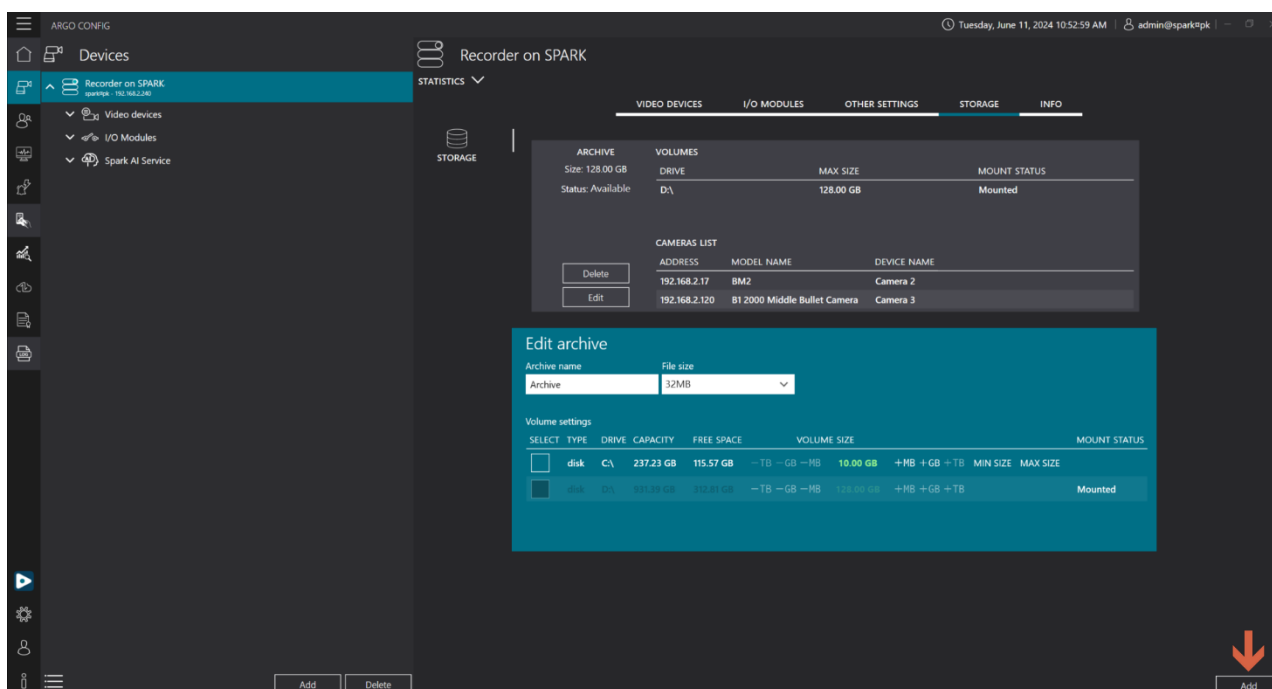
8080 (80, 1025 ~ 65535)

- Once enabled, you can use web server to monitor
- Port: insert port number
Range: 80, 1025~65535



1.5 Storage

1.5.1 Add Archive



- 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

Volume settings										
SELECT	TYPE	DRIVE	CAPACITY	FREE SPACE	VOLUME SIZE			MOUNT STATUS		
<input type="checkbox"/>	disk	C:\	237.23 GB	115.54 GB	-TB	-GB	-MB	10.00 GB	+MB +GB +TB	MIN SIZE MAX SIZE
<input checked="" type="checkbox"/>	disk	D:\	931.39 GB	312.81 GB	-TB	-GB	-MB	128.00 GB	+MB +GB +TB	Mounted

- 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.



1.5.2 Edit storage

The screenshot shows the 'STORAGE' tab in a software interface. At the top, there are navigation tabs: VIDEO DEVICES, I/O MODULES, OTHER SETTINGS, STORAGE (selected), and INFO. On the left, there is a 'STORAGE' icon. The main area displays an 'ARCHIVE' section with 'Size: 128.00 GB' and 'Status: Available'. Below it is a 'VOLUMES' table with columns 'DRIVE', 'MAX SIZE', and 'MOUNT STATUS'. The table contains one row: 'D:\', '128.00 GB', and 'Mounted'. Below the volumes is a 'CAMERAS LIST' table with columns 'ADDRESS', 'MODEL NAME', and 'DEVICE NAME'. It contains two rows: '192.168.2.17', 'BM2', 'Camera 2' and '192.168.2.120', 'B1 2000 Middle Bullet Camera', 'Camera 3'. To the left of the cameras list are 'Delete' and 'Edit' buttons, with an orange arrow pointing to the 'Edit' button. Below this is an 'Edit archive' dialog box with an 'Archive name' field containing 'Archive'. At the bottom of the dialog is a 'Volume settings' table with columns 'SELECT', 'TYPE', 'DRIVE', 'CAPACITY', 'FREE SPACE', 'VOLUME SIZE', and 'MOUNT STATUS'. It contains two rows: one for 'C:\' (237.23 GB capacity, 115.54 GB free space, 10.00 GB volume size) and one for 'D:\' (931.39 GB capacity, 312.81 GB free space, 128.00 GB volume size, 'Mounted' status). The 'D:\' row has a checked checkbox in the 'SELECT' column.

Click on the storage space you want to edit and then click on **[Edit]** on the left.

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

1.5.3 Delete storage

The screenshot shows the same 'STORAGE' tab as in the previous image. The 'ARCHIVE' section shows 'Size: 128.00 GB' and 'Status: Available'. The 'VOLUMES' table is the same. The 'CAMERAS LIST' table is the same. In this view, an orange arrow points down to the 'Delete' button, which is highlighted with a white border. The 'Edit' button is also visible below it.

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



1.6 Information

1.6.1 Information

VIDEO DEVICES | I/O MODULES | OTHER SETTINGS | STORAGE | **INFO**

INFO

RECORDER NAME
Recorder on SPARK小K

ADDRESS
sparkpk - 192.168.2.240

SPARK PROTOCOL PORT
20840

STREAMING PORT
20833

LISTEN PORT
20842

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

1.6.2 Installed services

INSTALLED SERVICES

INSTALLED SERVICES RECAP

ANALYTICS DATA COLLECTION SERVICES
INDEXING SERVICE
EVENTS AND ALARMS MANAGEMENT
SPARK AI SERVICE
AUTHENTICATION AUTHORITY
LINE MESSAGING SERVICE
DEVICES MANAGEMENT
RECORDING SERVICE
HEALTH DOCTOR
SYSTEM MANAGEMENT
LICENSE PROVIDER
ACCESS CONTROL

- Installed services content

1.6.3 License summary

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
AI Service Human Detection Integration License(28062C4C)	Trial				9/15/2024	OK
Argo integration license	Trial				9/30/2024	OK
I/O Modules activation license	Trial				9/30/2024	OK

- Browse license overview and status

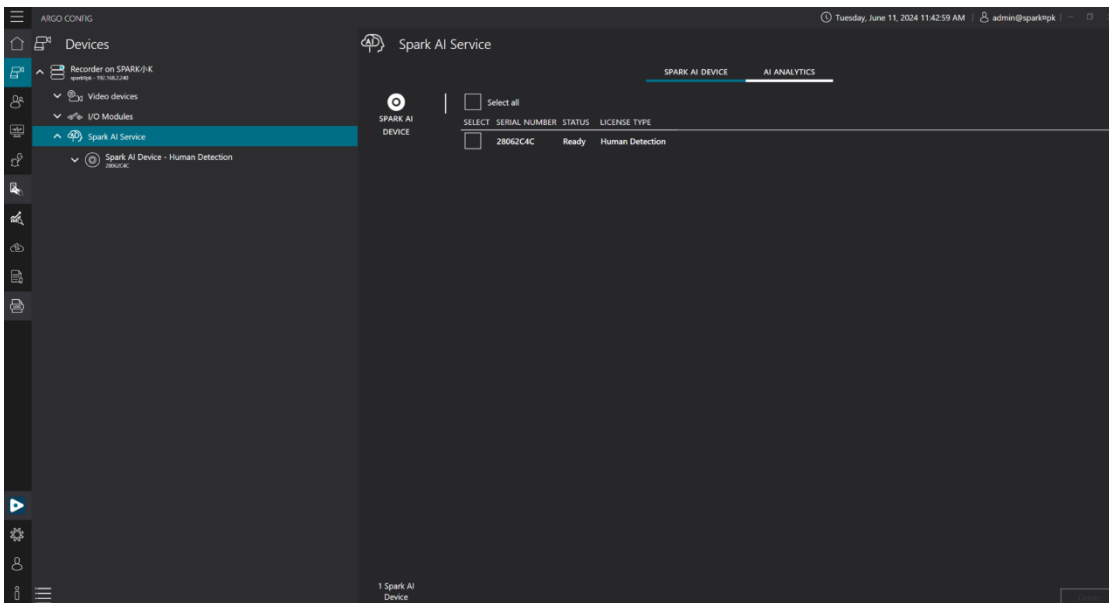
1.7 Spark AI services

1.7.1 Spark AI devices

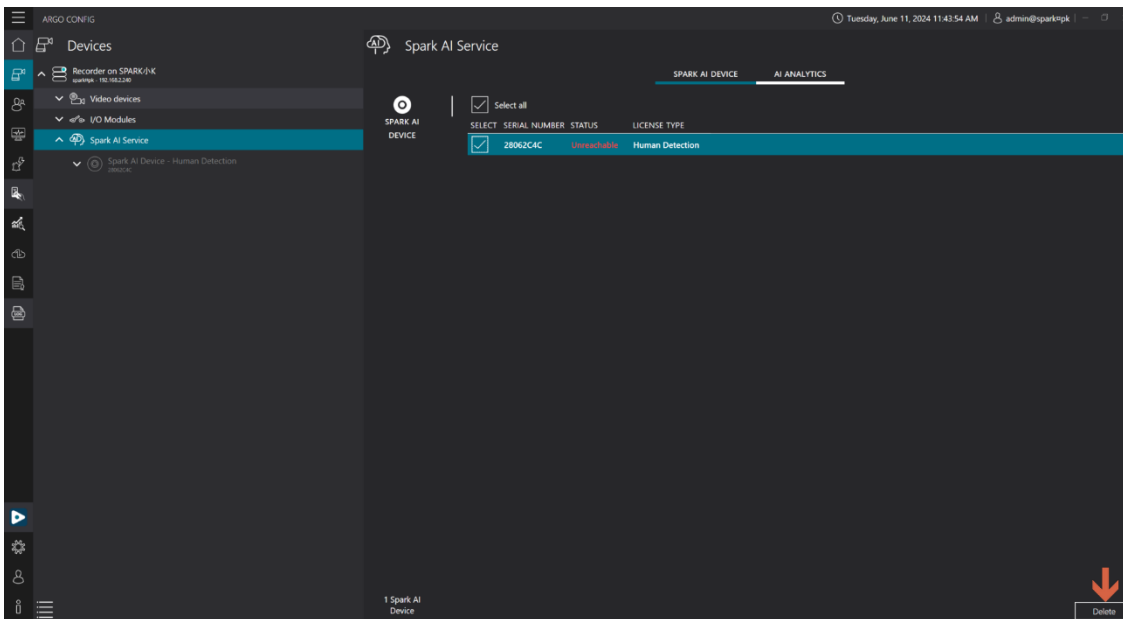
A. Overview of Spark AI devices



- Spark AI device serial number / status / license type (Human detection / vehicle detection / LPR)



B. Delete Spark AI devices



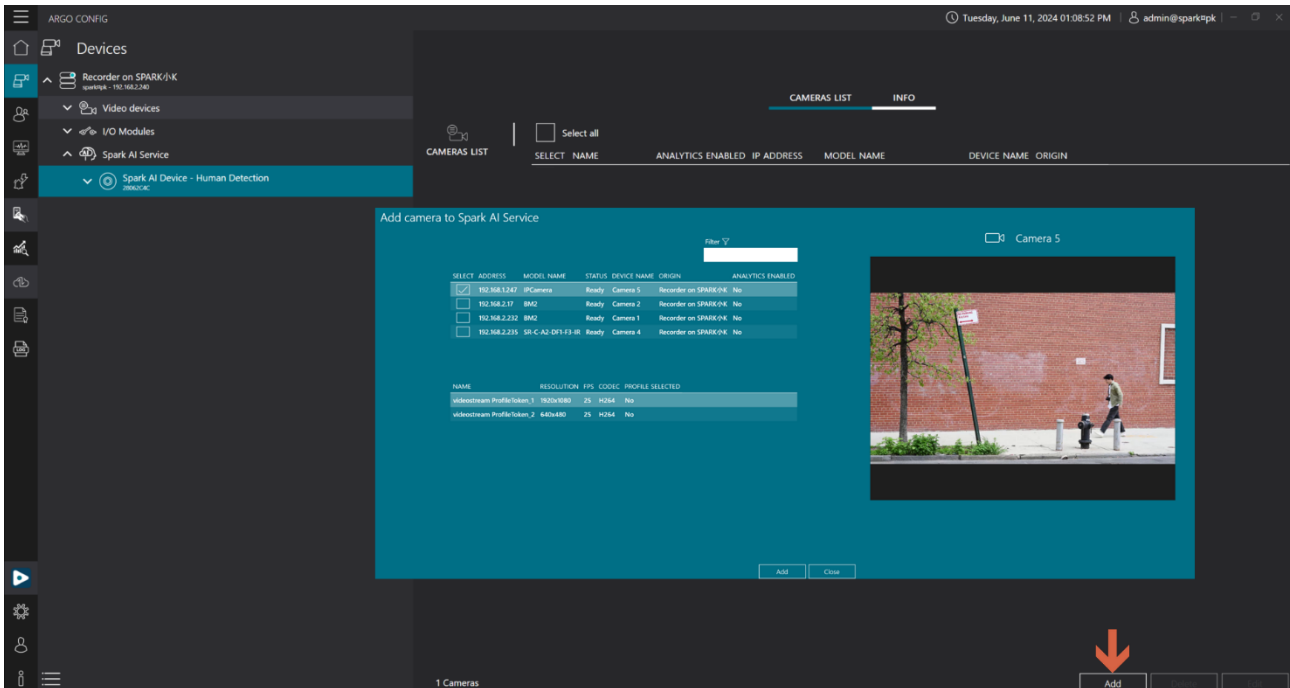
- Select Spark AI device you want to delete and click **[Delete]**

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



1.7.2 Spark AI device camera

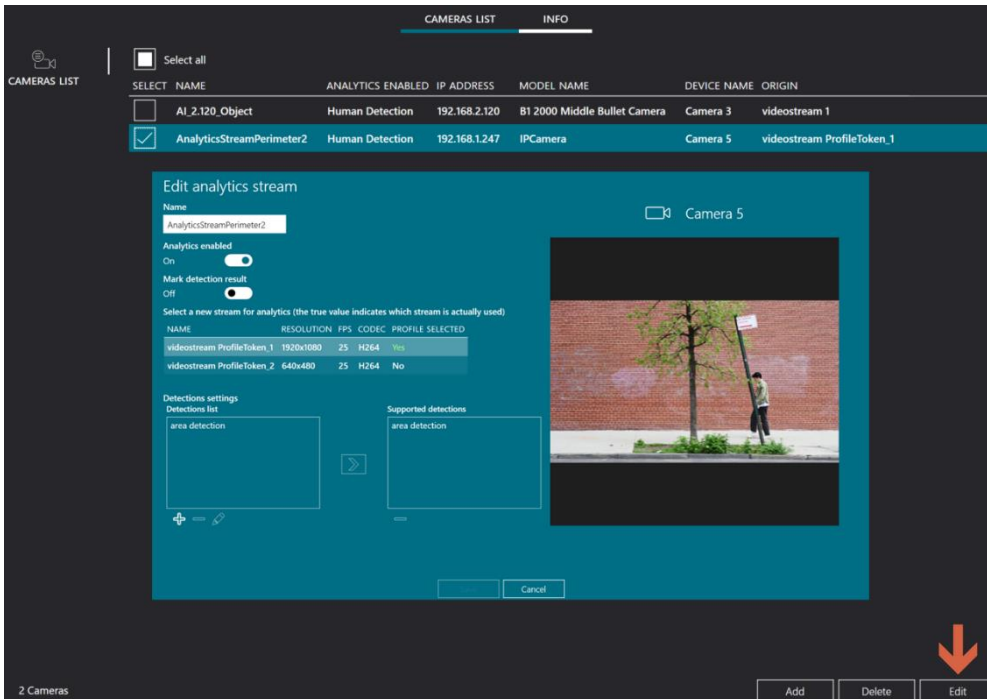
1.7.2.1 Add camera to Spark AI service



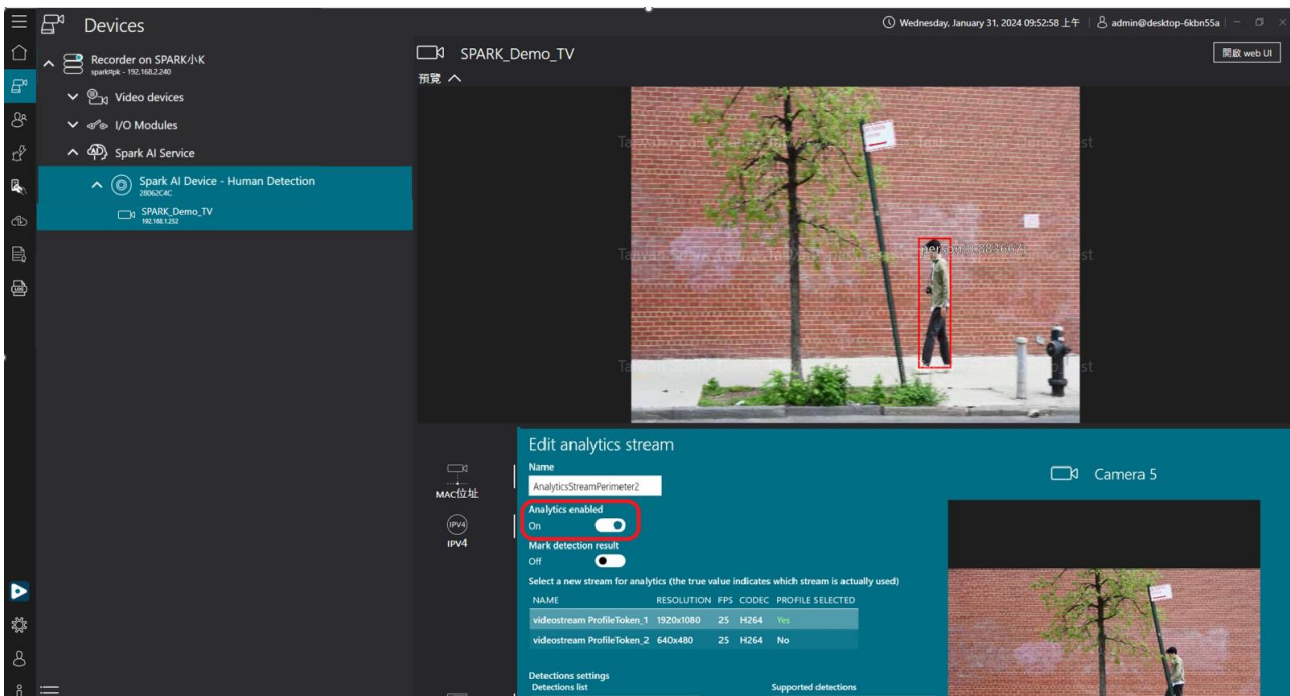
- Click on the bottom right **[Add]**
- Select the cameras you want to add to the Spark AI service
- Select camera profile



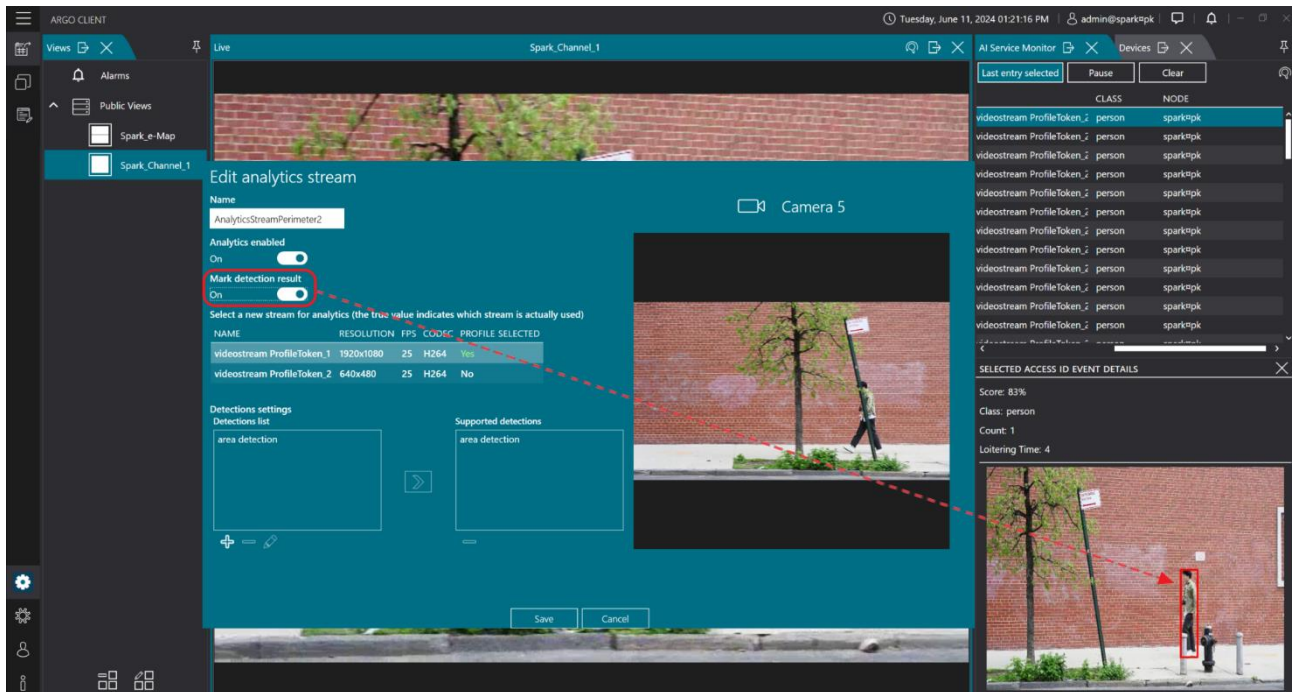
1.7.2.2 Edit camera on Spark AI services



- Select the Spark AI service camera you want to edit and click on the bottom right [Edit]

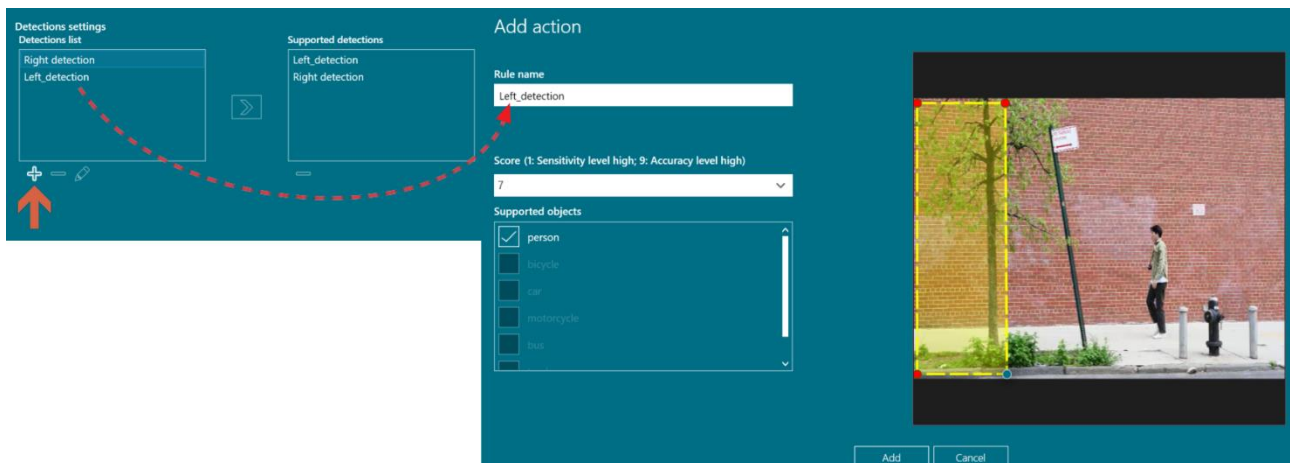


- Enable video analytics: once enabled, you can see detected objects outlined in red.



- Marked detection results: When enabled, images of detected objects will be surrounded by red boxes and displayed in the AI service client monitoring window.
- Detection area settings: Edit detection area for the Spark AI service camera.

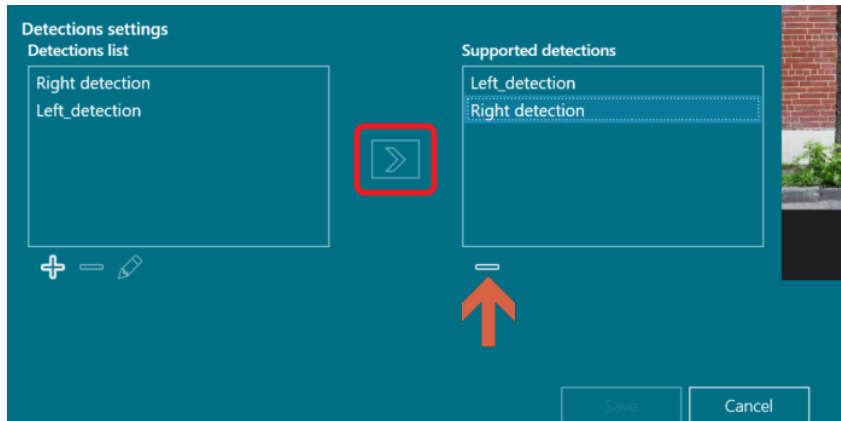
a. Add detection area list



- Click on the bottom left [+]
- Rule name: insert a name for the detection area
- Score: select the sensitivity and accuracy of the detection area. The lower the score, the easier it is to detect objects, and the higher the score, the higher the accuracy. Range: 1-9
- Supported objects : select object type
 - Person detection - detect human (default)
 - Vehicle detection - bicycle, car, motorcycle, bus, trucks
- Right screen: Drag to adjust the detection area

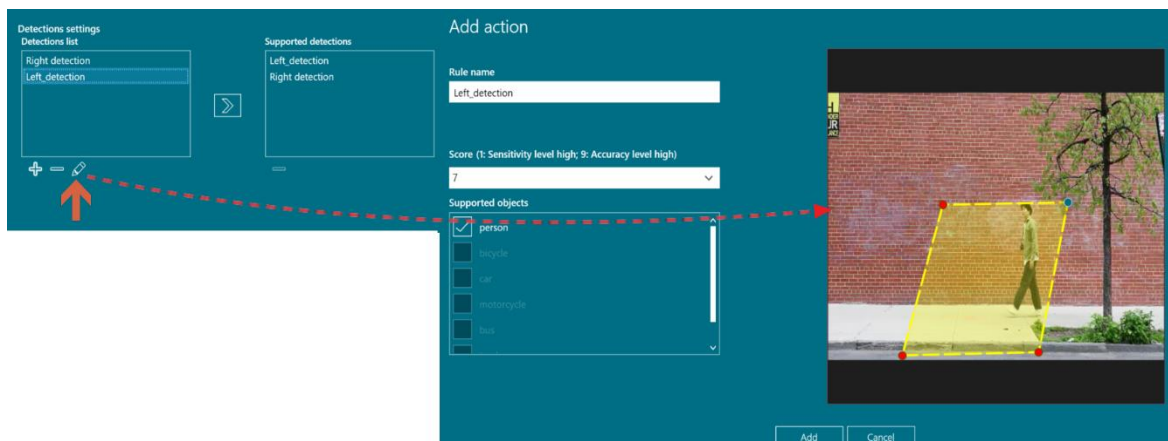


b. Execute detection area



- Apply to Execute Area Detection: Select the area list for detection and click [>]
- Delete Executing Area Detection: Select the area detection you want to delete and click on the bottom left [-]

c. Edit the List of Selectable Areas



- Select the selectable area detection you want to edit and click on

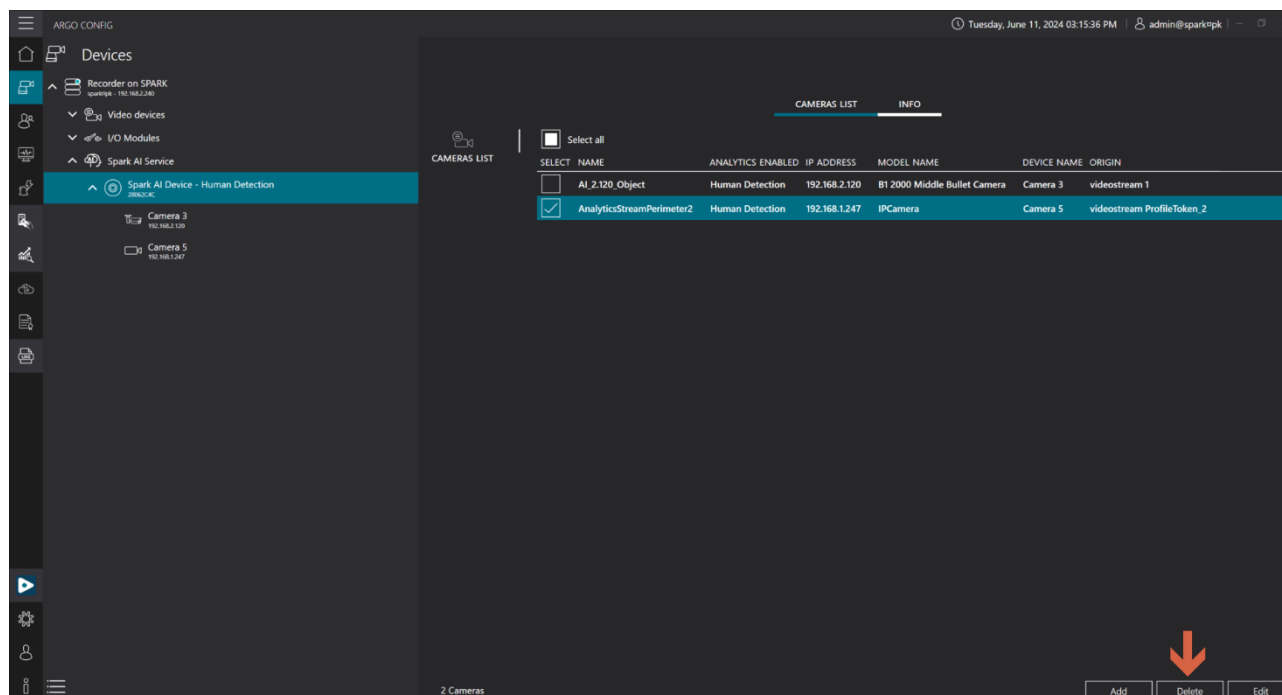
d. Delete selectable area list



- Select the selectable area list you want to delete and click on the bottom left [-]

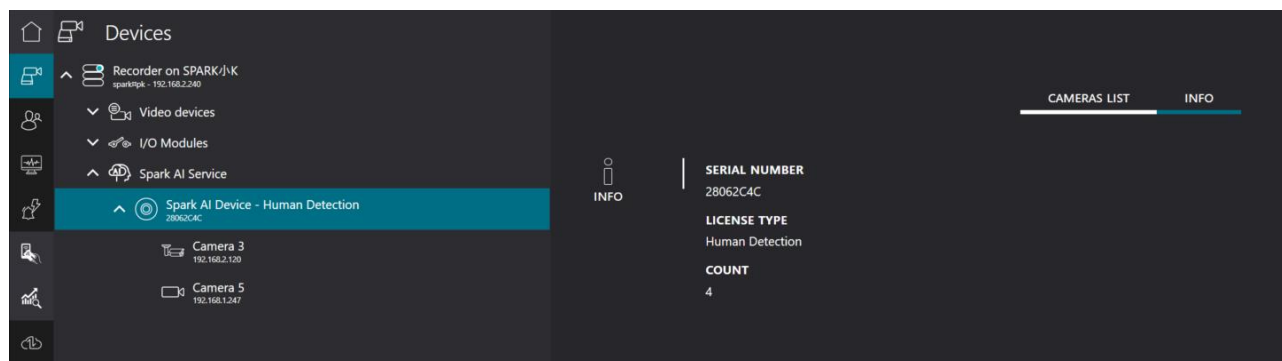


1.7.2.3 Delete camera on Spark AI



- Select the cameras you want to delete from the Spark AI service and click on the bottom right [**Delete**]

1.7.2.4 Information

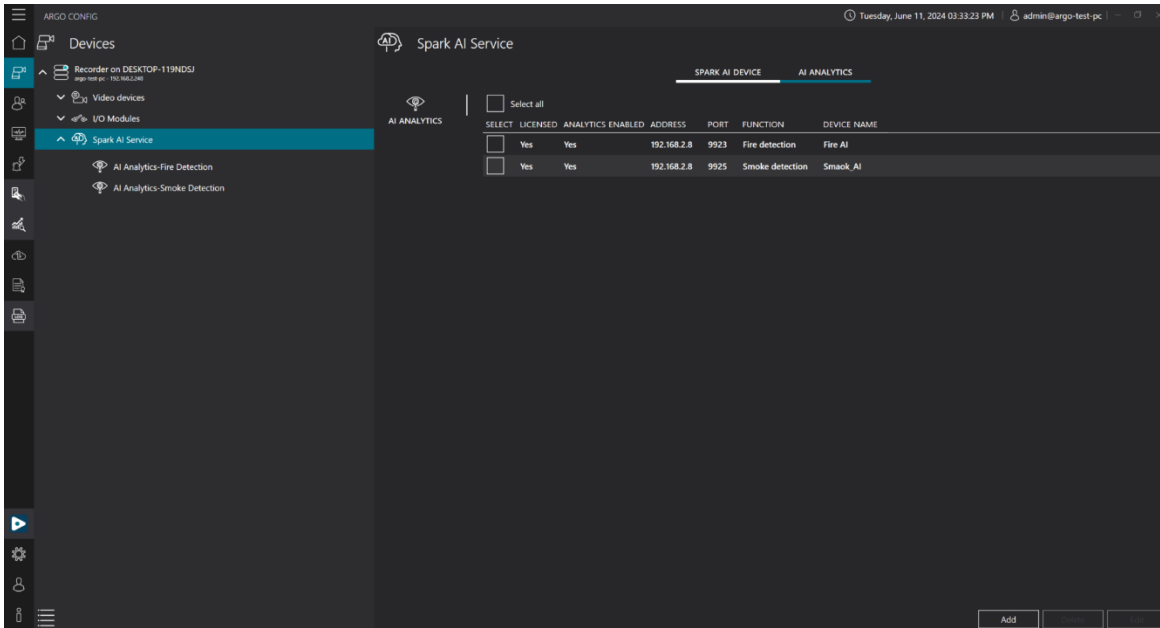


- Browse Spark AI detection device information (Serial number/ License type/ Count).

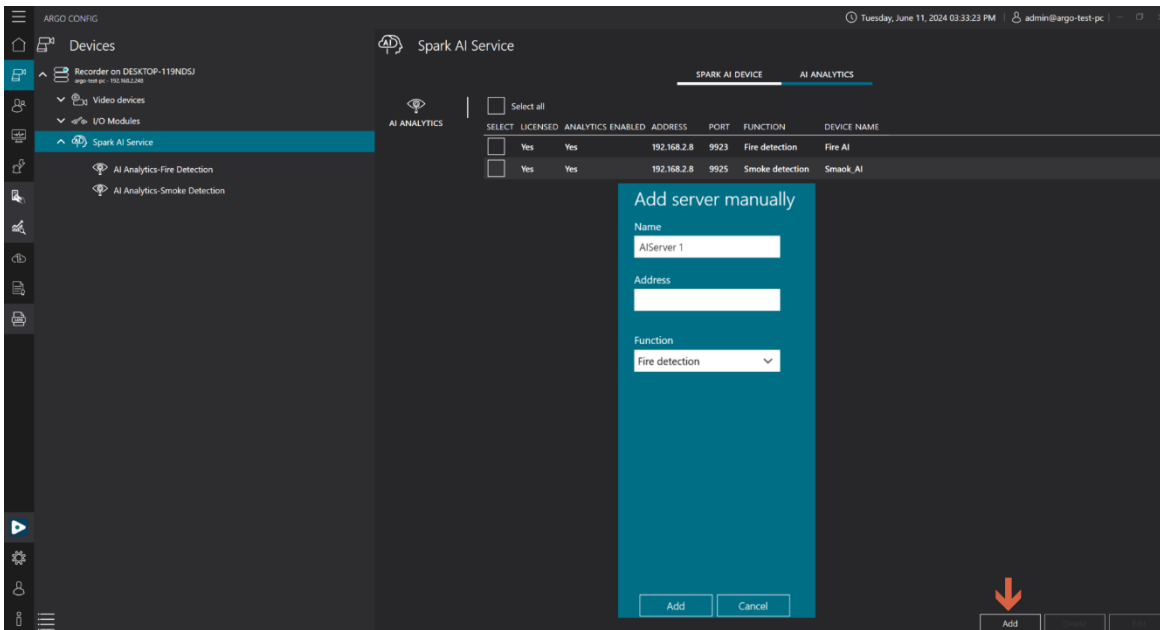
1.7.3 AI analytics (fire detection/smoke detection)

A. Overview AI analytics

- AI analytics license status / enable AI analytics / IP address / port / function / device name
- Functions: Fire detection/Smoke detection

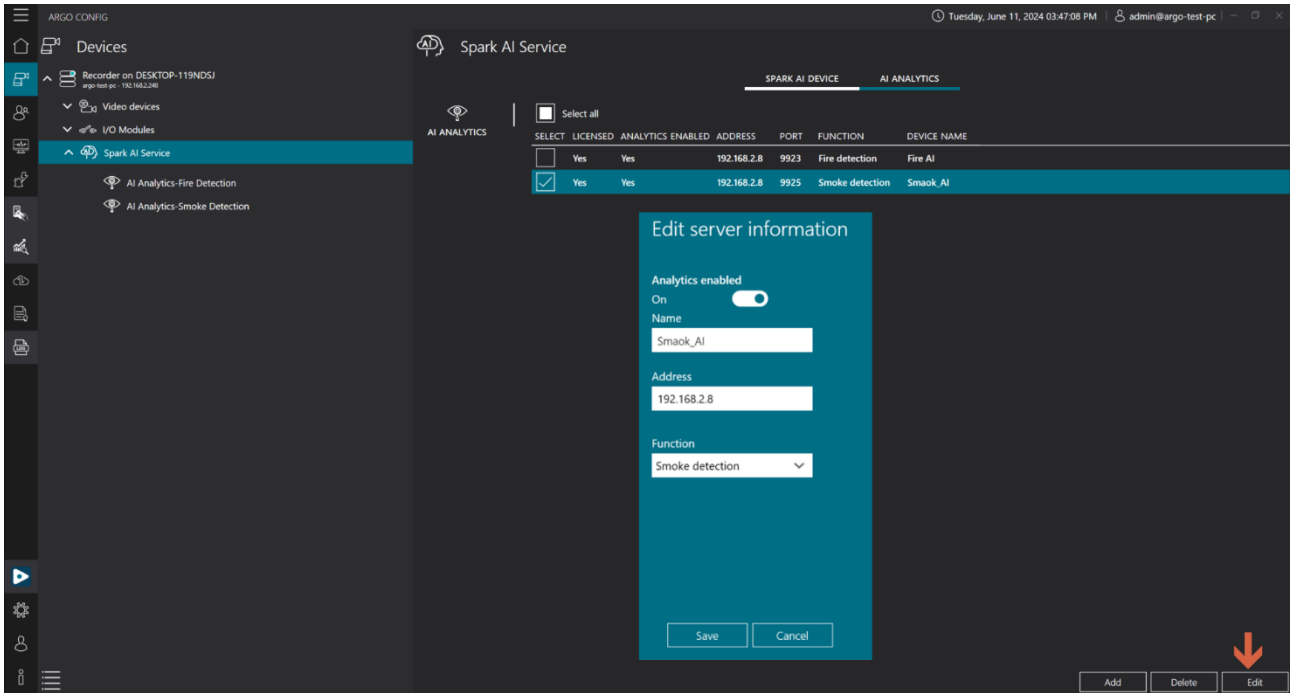


B. Manual add server



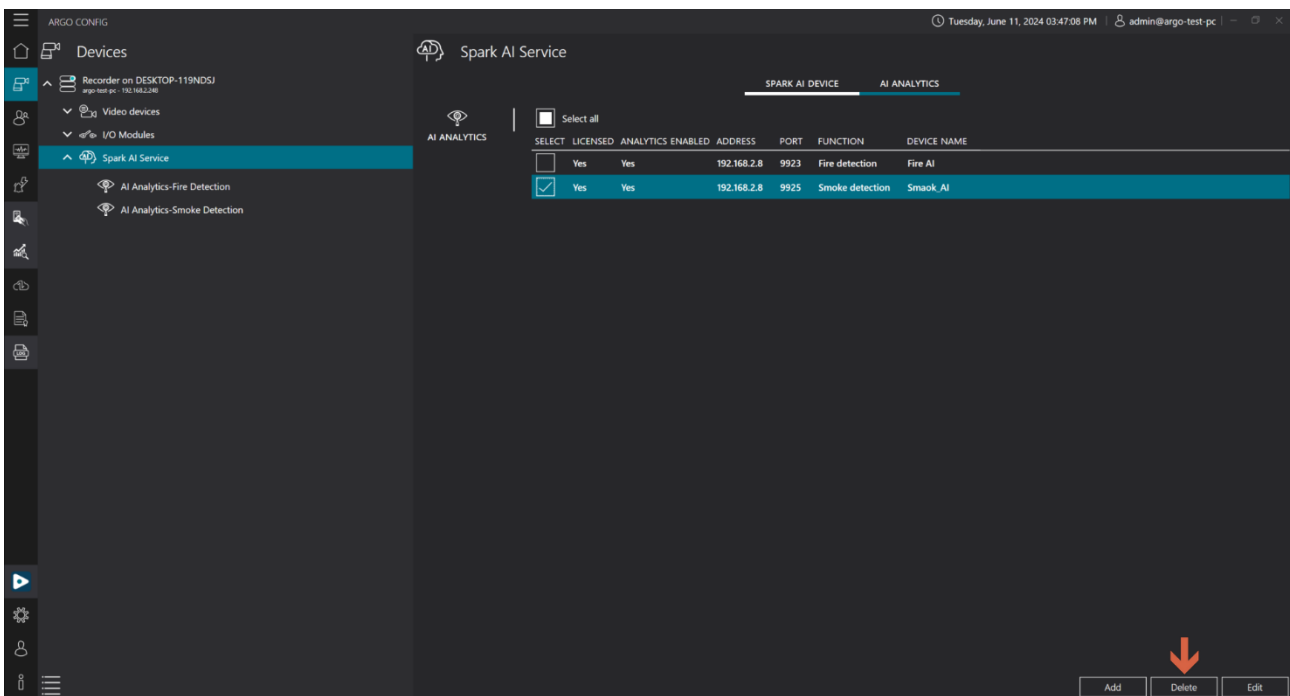
- Click on the bottom right **[Add]**
- Name: The name of the server you want to add
- IP Address: The IP address you want to add
- Function: Fire detection / Smoke detection

C. Edit server information



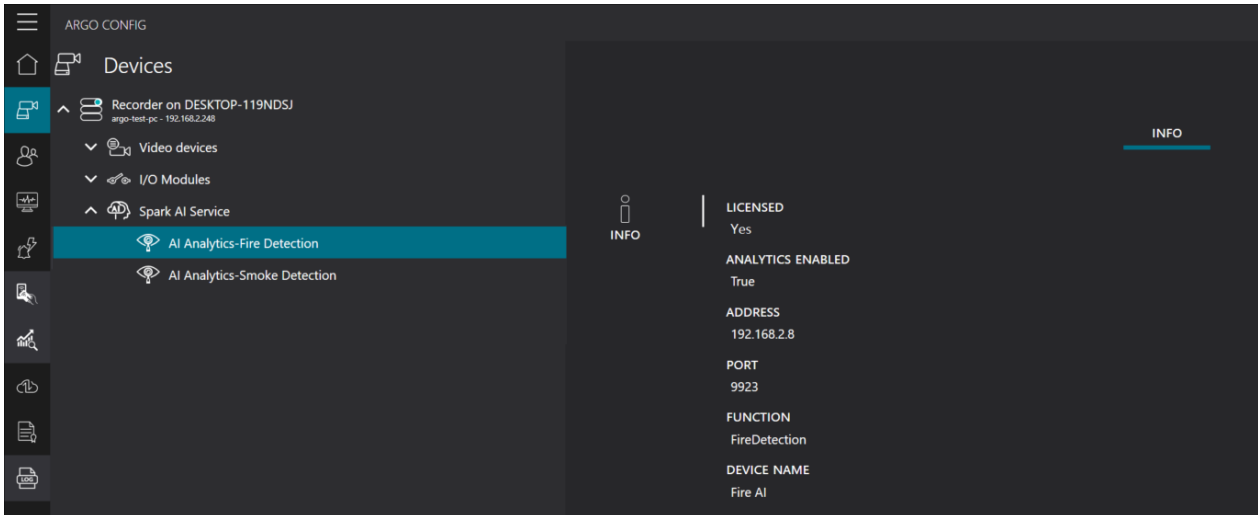
- Select device you want to edit and click **[Edit]**

D. Delete server



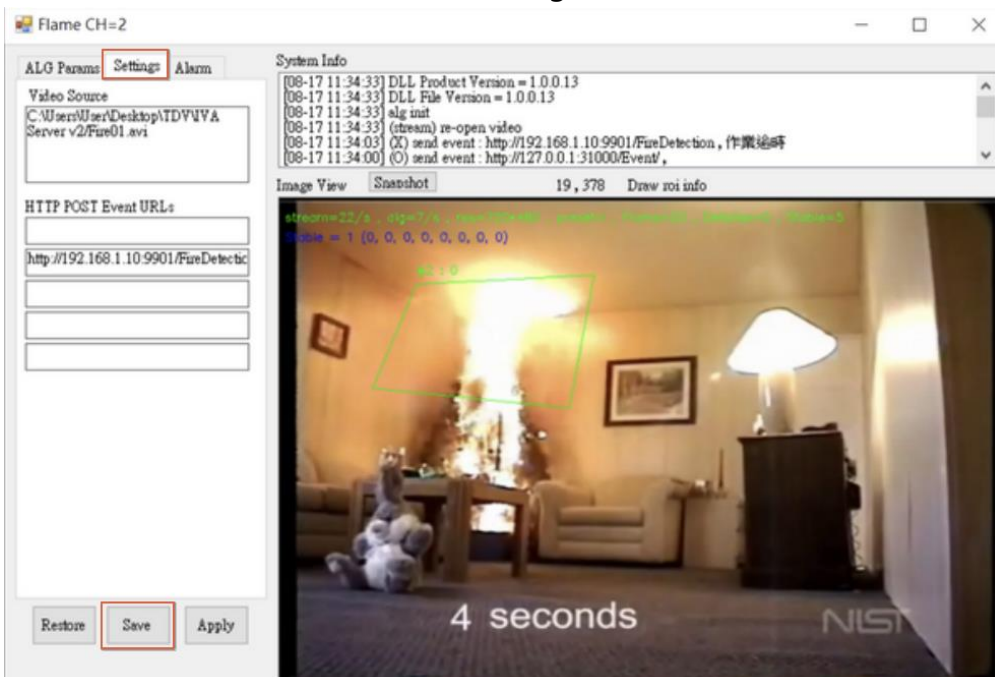
- Select device you want to delete and click **[Delete]**

E. Information



- Browse AI video analytics - fire detection/smoke detection device information
Information: license status / video analytics status / IP address / port / functions / device name

F. IVA(RTSP/IP address) execute settings



- Click **[Settings]**
- Insert RTSP and IP address then click **[Save]**

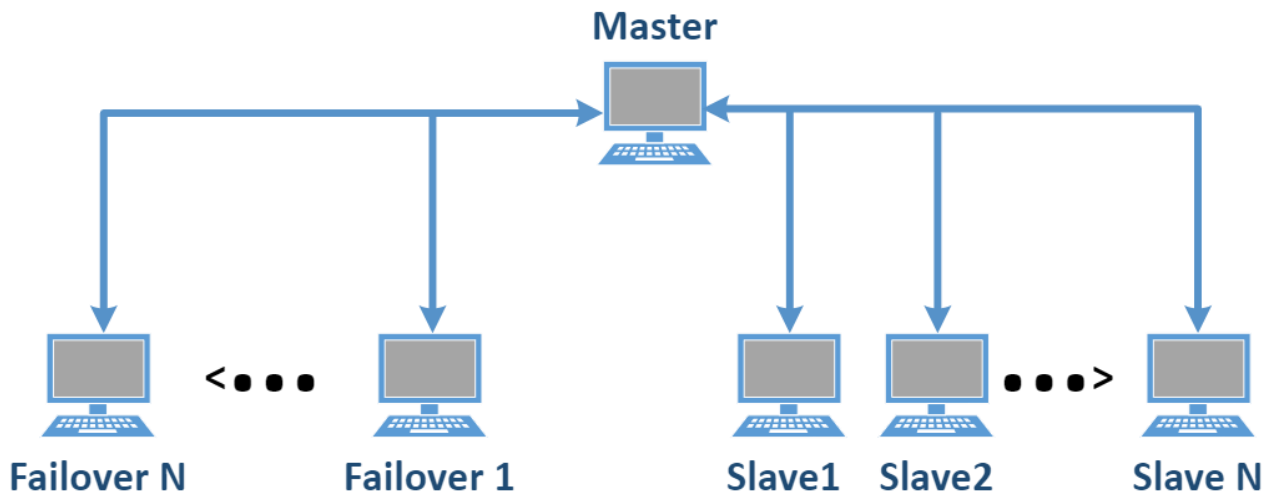
1.8 Server

1.8.1.1 Primary server and secondary servers

- Mechanism: having primary server and secondary servers allows unified remote monitoring of multiple servers through the primary server.

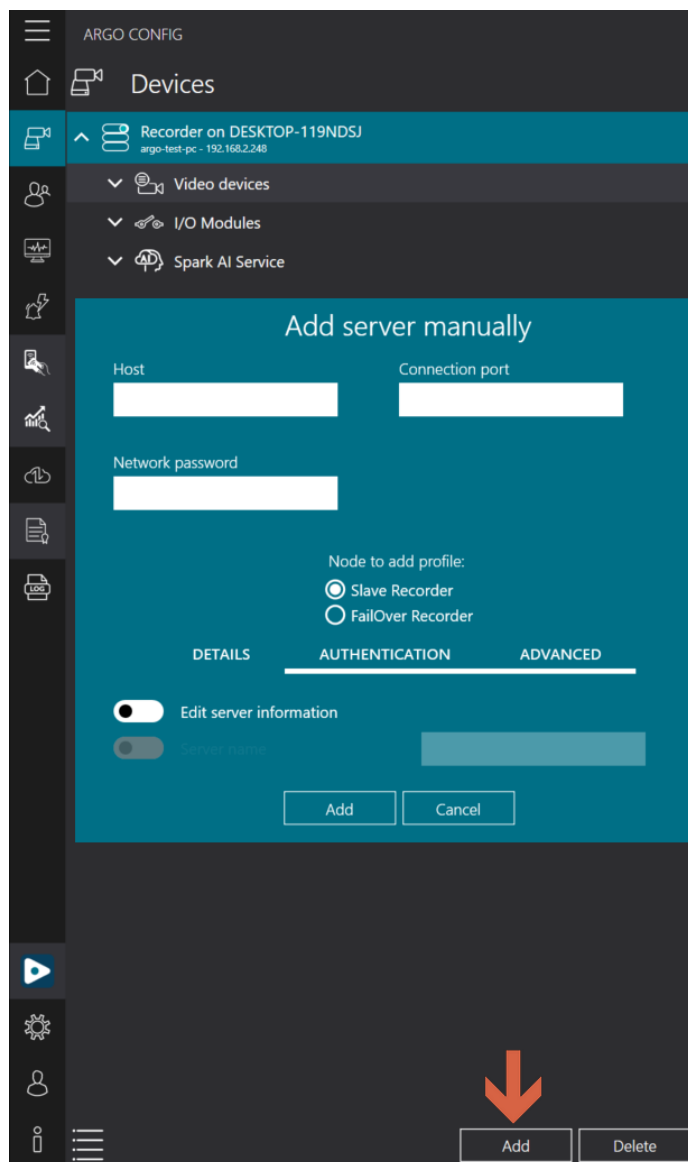


- Add secondary servers/failover server or delete server, follow below steps:

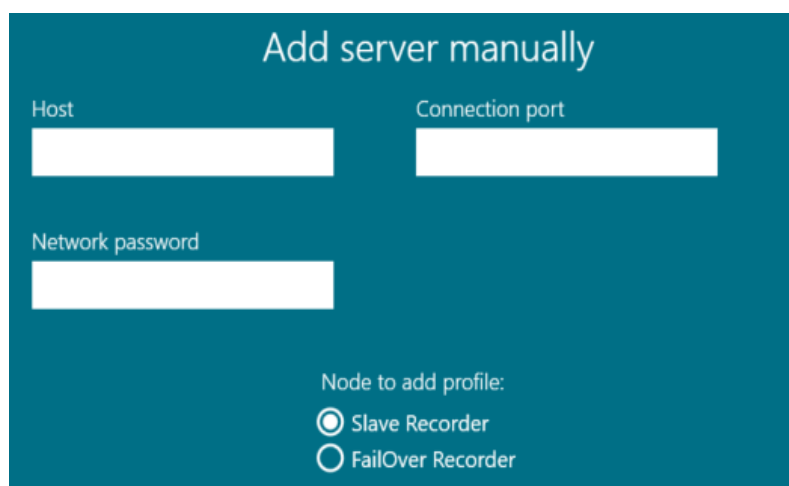




1.8.1.2 Add server



- Click **[Add]**





Step 1. Insert server information

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

Step 2. Select server type

- Server type: Slave Recorder / Failover Recorder
- Slave Recorder: add other servers to the device list for unified management.
- Failover Recorder: 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 features three tabs: 'DETAILS', 'AUTHENTICATION', and 'ADVANCED'. Under the 'DETAILS' tab, there is a toggle switch for 'Edit server information' which is currently turned on. Below this is a 'Server name' field with a text input box. At the bottom of the panel are two buttons: 'Add' and 'Cancel'.

- Edit server information: enable to edit server name.

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

b. Permissions

The screenshot shows the 'Permissions' section of the server configuration window. It features three toggle switches: 'Leave authentication authority enabled (if available)' which is turned on, 'Enable authentication authority mirroring (if supported)' which is turned off, and 'Enable authentication authority shadowing (if supported)' which is turned off. Below the toggles is a dropdown menu labeled 'Selected authentication authority to monitor for mirroring' with the selected option 'Authentication authority on Recorder on DESKTOP-119NDSJ (argo-test-pc)'.



- Leave authentication authority enabled: 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

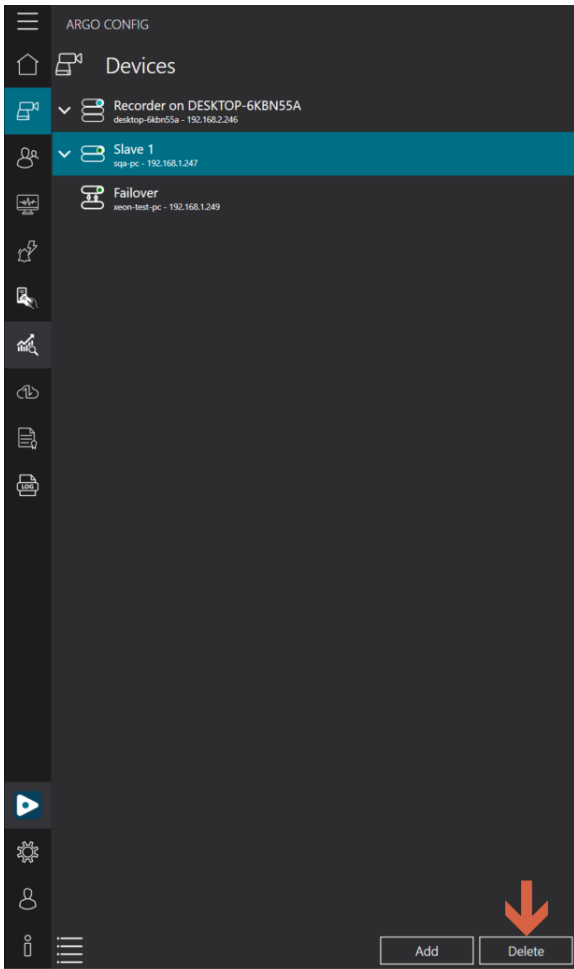
The master server is behind a NAT network and use this following address as its public address.

Add Cancel

- No direct connection to the 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 master: enable to input the external WAN IP address to allow devices outside the local network to connect to this server's network address.



1.8.1.3 Delete server



- Click **[Delete]**



1.9 View mode

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

Left Screenshot: Hierarchy mode

The interface shows a hierarchical tree structure under the heading "Hierarchy mode". The root node is "Recorder on SPARK小K" (192.168.2.240). It contains several sub-nodes:

- Video devices
 - Camera 1 (192.168.2.232)
 - Camera 2 (192.168.2.17)
 - Camera 3 (192.168.2.120)
 - Camera 4 (192.168.2.235)
 - Camera 5 (192.168.1.247)
- I/O Modules
 - I/O Module 1 (192.168.2.9)
 - I/O Module 2 (192.168.2.19)
- Spark AI Service
 - Spark AI Device - Human Detection (28062C4C)
 - Camera 3 (192.168.2.120)
 - Camera 5 (192.168.1.247)

Right Screenshot: List mode

The interface shows a table view under the heading "List mode". It includes a "Device type" dropdown menu set to "All" and a "Filter" input field. The table lists the following devices:

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 Key2

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



2. USER MANAGEMENT

2.1 Password settings

1. Configure users password

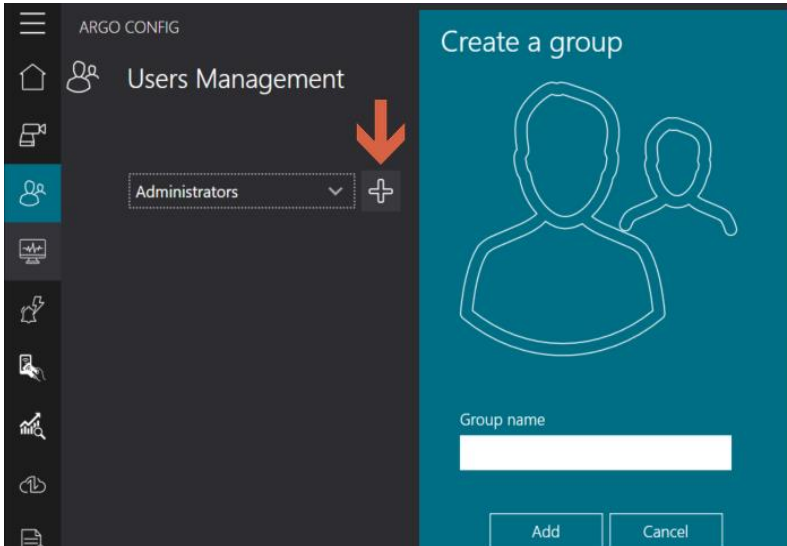
- Password duration rules
Maximum number of days of validity: when the password usage reaches the maximum validity period, it expires and requires resetting. The range of days is from 5 to 100 days.
Number of days before the password expires that a warning message should appear: receive a reminder N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



2.2 Groups

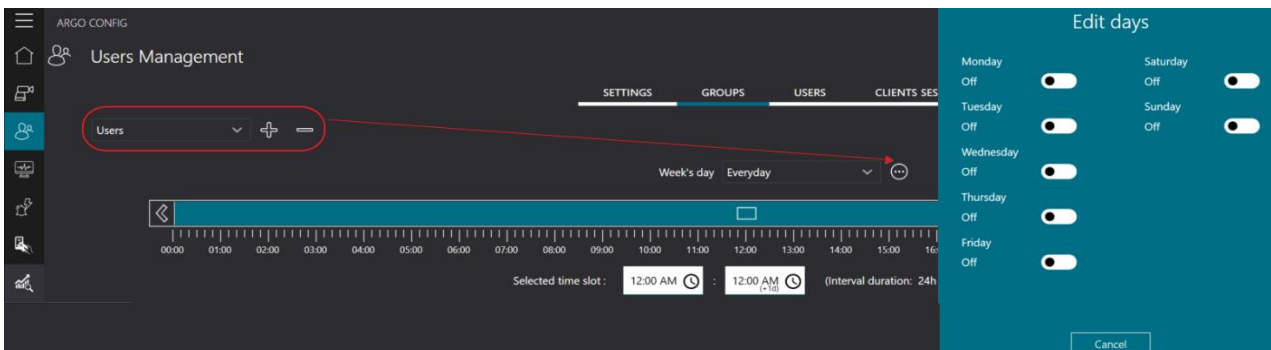
2.2.1 Create groups

- Create groups to classify user access schedules and permissions.

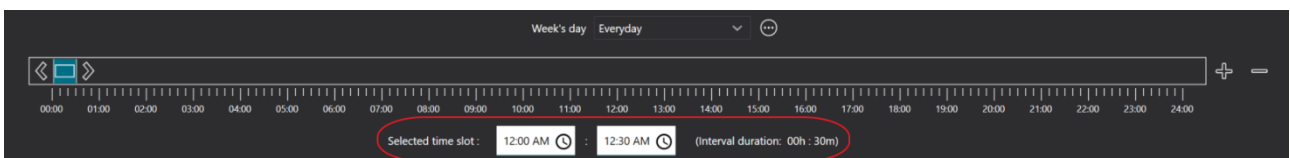


- Click [+]
- Group name: insert name for user group

2.2.2 Set schedules for each group



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

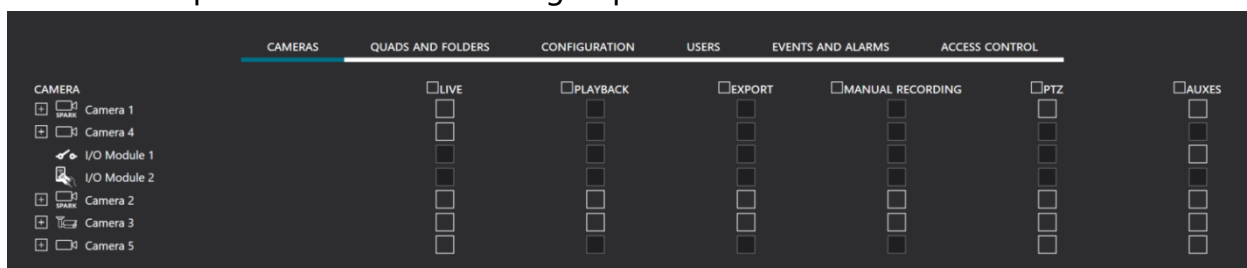


- Add time slot: Click [+] and adjust time slot by dragging left/right or inputting desired time
 - Delete time slot: select the time slot you want to delete and click [-]
 - Edit time slot: adjust the time slot by dragging left/right or inputting desired time
- Note: minimum time interval is 1 hour,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

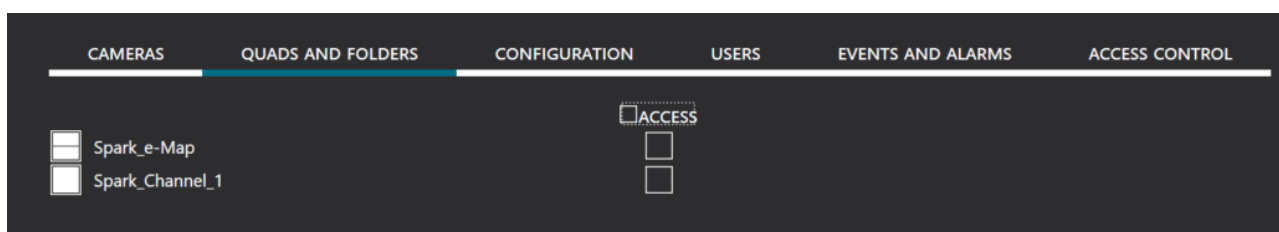


2.2.3 Set permissions for each group:

- Allocate permissions for different groups



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



- Quads and folders: select the screens that the group can view. Once enabled, the group can view these monitoring screens in the Argos Client.
- Configuration: 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 Argos Config.
Video configuration	When disabled, users of the selected group will not be able to access video configuration on Argos Config.
Recording configuration	When disabled, users of the selected group will not be able to access recording configuration on Argos Config.
Events and alarms configuration	When disabled, users of the selected group will not be able to access events and alarms configuration on Argos Config.
Access control configuration	When disabled, users of the selected group will not be able to access access control configuration on Argos Config.
Video analytics configuration	When disabled, users of the selected group will not be able to access video analytics configuration on Argos 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 formaton 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.
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.

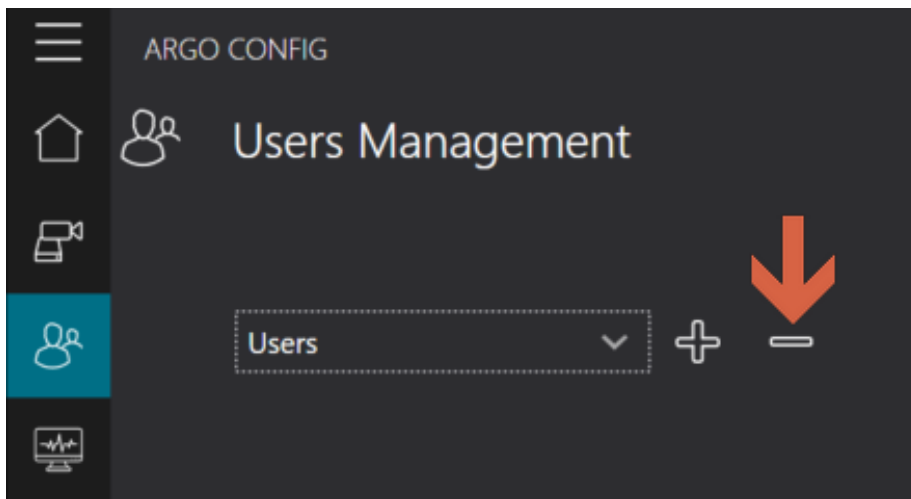
Options	Description
Force alarms acknowledge	When disabled, users of the selected group will not be able to force alarm acknowledgment on Argo Config.
Trigger alarms	When disabled, users of the selected group will not be able to manually trigger alarm on Argo Config.
Forward alarms	When disabled, users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

2.2.4 Delete group

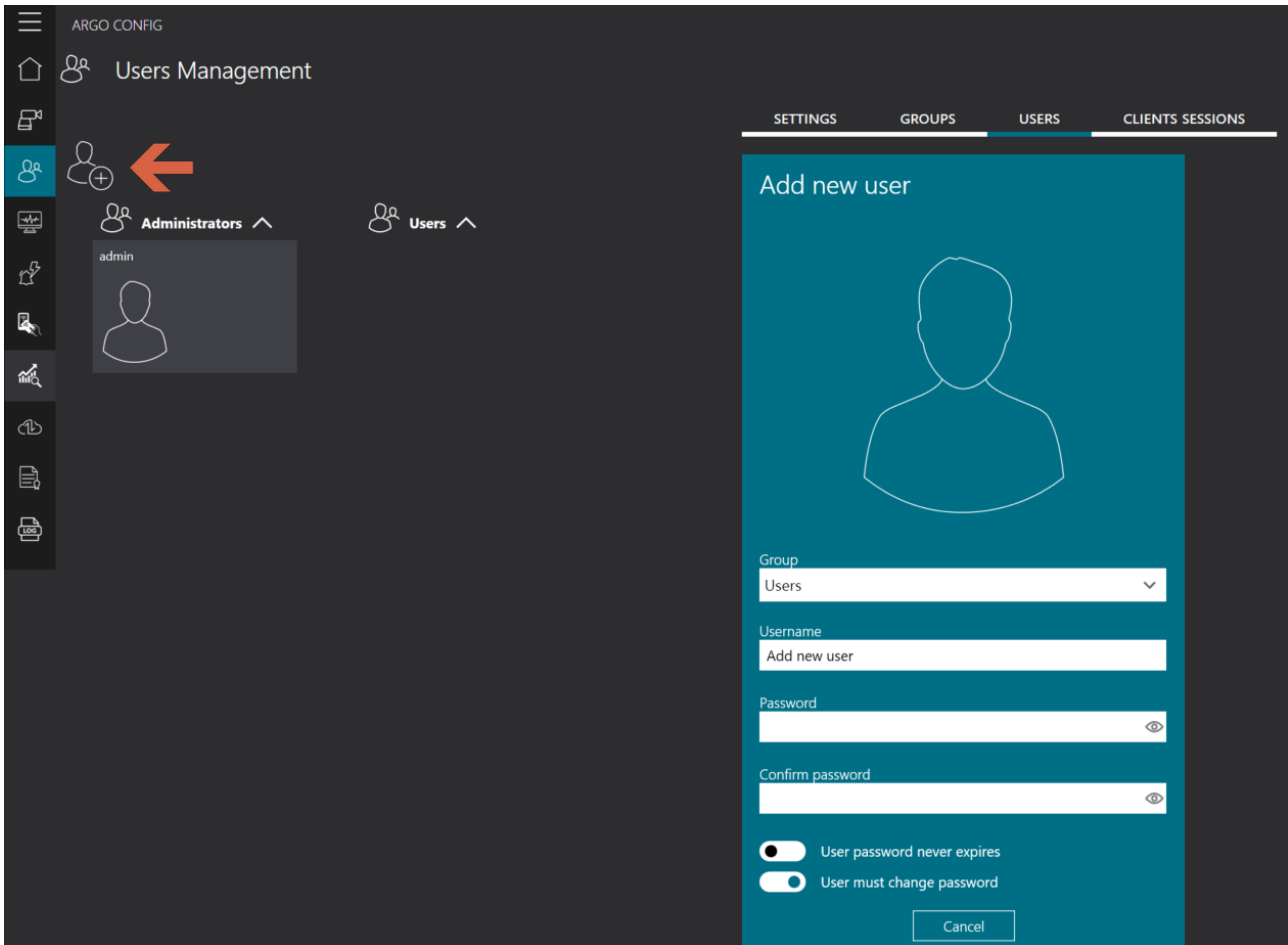


- Select group and click [-]



2.3 User

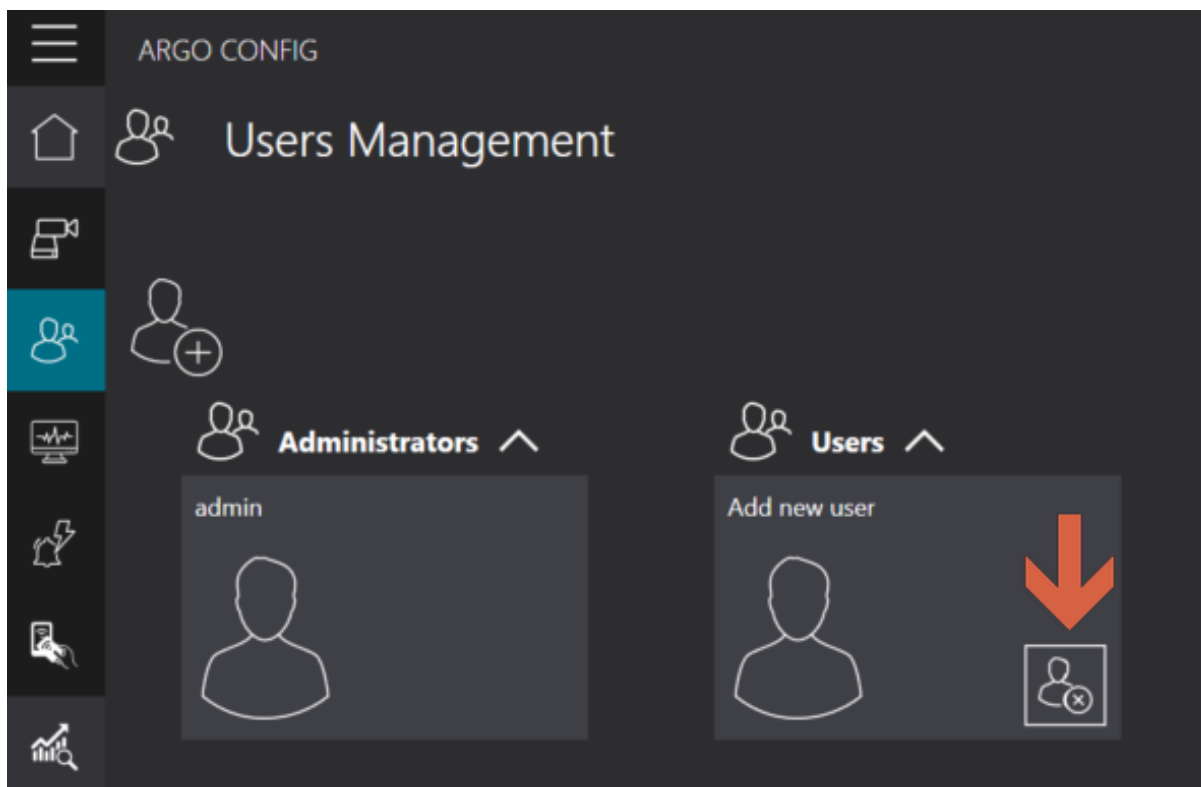
2.3.1 Add user



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



2.3.2 Delete User



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

2.4 Client connection information

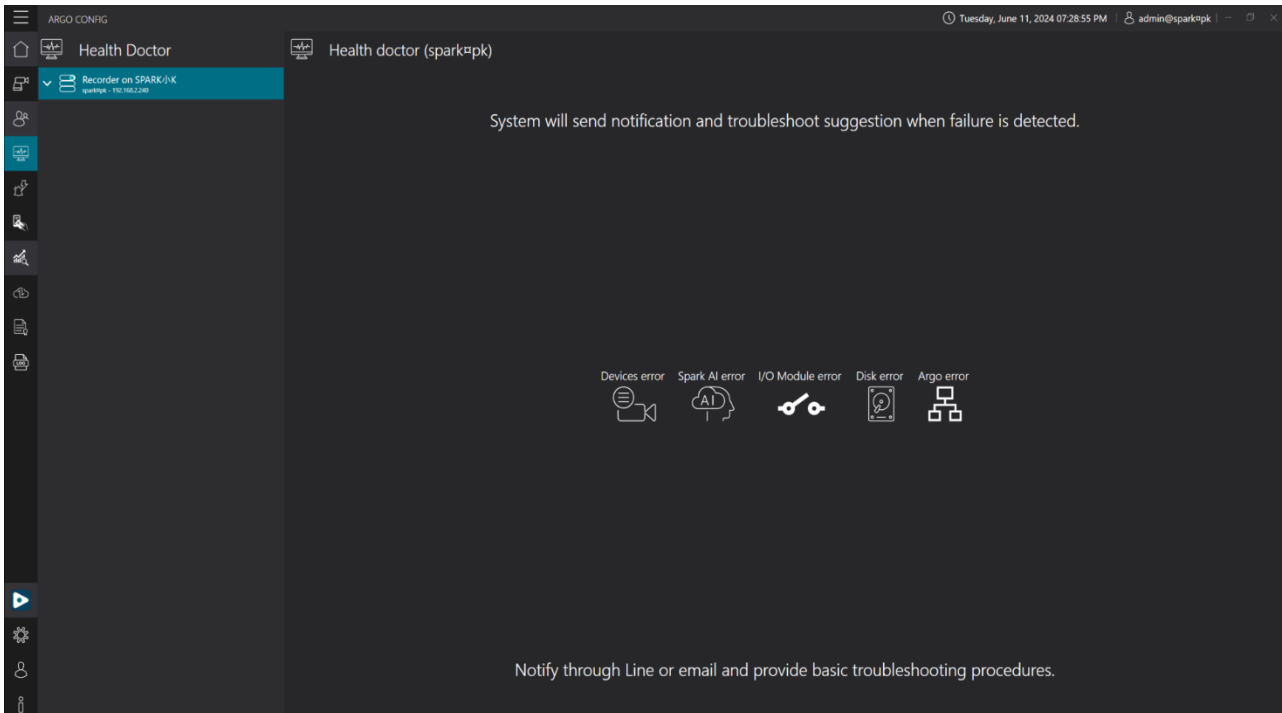
- View and disconnect users connected to Argo Client

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

- Username: users currently logged into Argo client
 - Group: group to which the user currently logged into the Argo Client system belongs.
 - Client machine: hostname connected to Argo Config for using the Argo Client system.
 - IP address: IP address of the server
 - Type: login type
 - Connecting timestamp: 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.

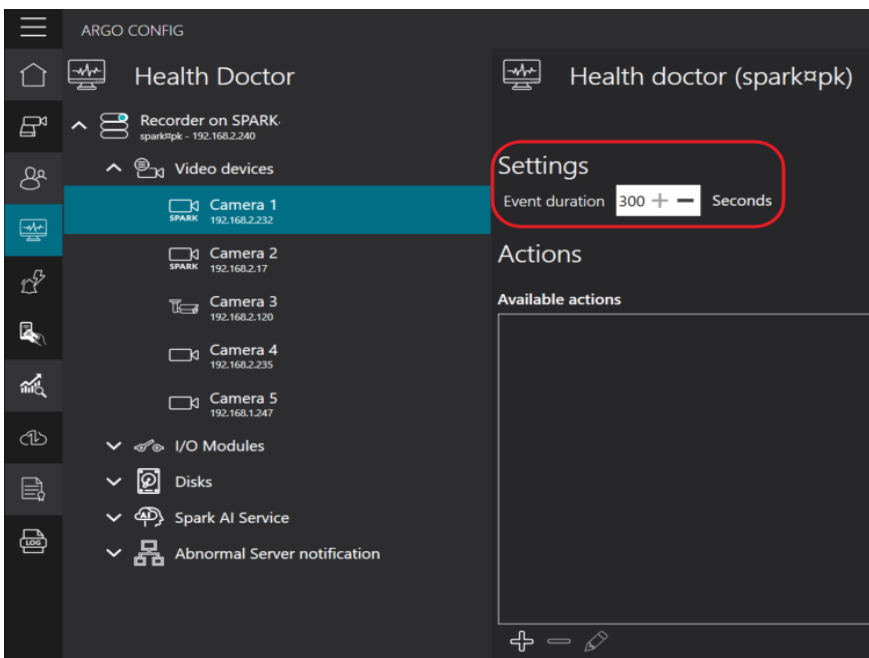


3. HEALTH DOCTOR



- 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

3.1 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.

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

Notification Sequence:

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

3.2 Add available action

- Click [+]
- Action name: insert response action name
- 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.

- 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.

- Action category



3.2.1 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)
- Username: 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 [-]



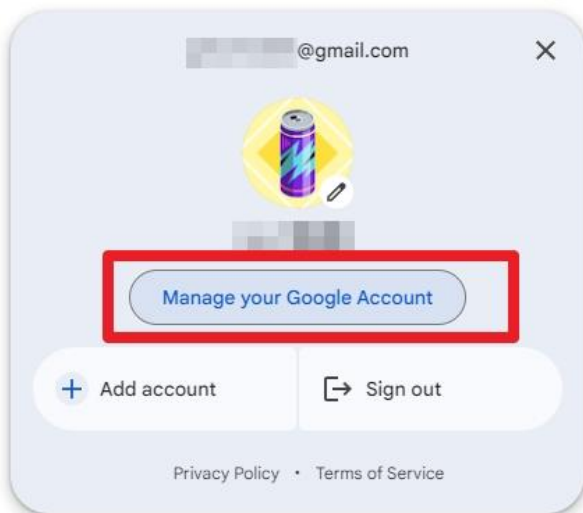
c. SMTP server name: SMTP server corresponding to each email service

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".

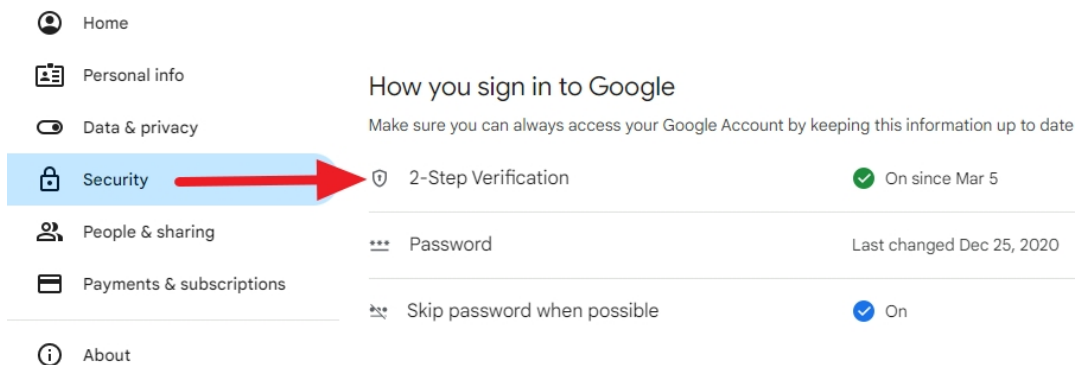
Setting up two-step verification for Gmail to obtain an application-specific password:

Step 1. Go to the Gmail homepage, click on "Manage your Google Account."

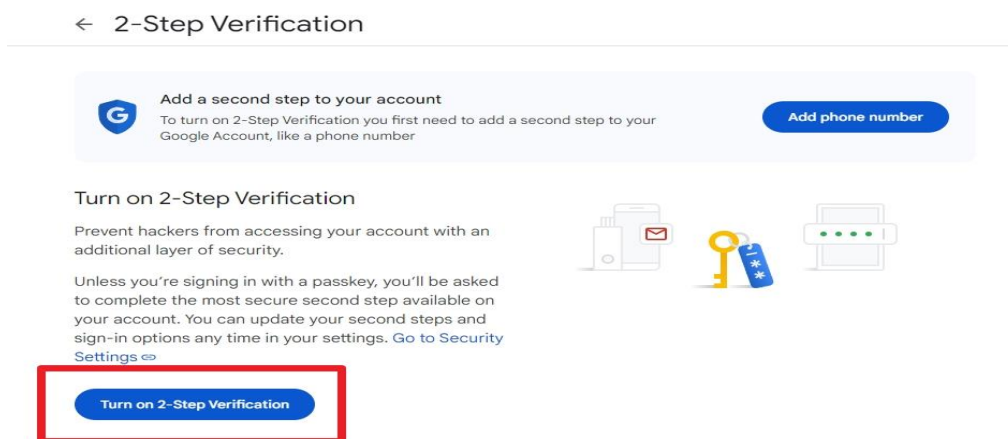




Step 2. Click on "Security" to enter two-step verification, then enter your account password.



Step 3. On the two-step verification page, click on application password



If the application password does not display correctly, change the URL from <https://myaccount.google.com/u/1/signinoptions/twosv?pli=1&rapt=> to

<https://myaccount.google.com/apppasswords?pli=1&rapt=> and press Enter to open this page.

Note: Due to Google's continuous security updates, this method may not always open the application password page. It depends on the settings of your Google account management and the interface operation at the time.

Step 4. Create an application name.



← App passwords

App passwords help you sign into your Google Account on older apps and services that don't support modern security standards.

App passwords are less secure than using up-to-date apps and services that use modern security standards. Before you create an app password, you should check to see if your app needs this in order to sign in.
[Learn more](#)

You don't have any app passwords.

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

Create

Step 5. Backup the generated password, then click Finish to complete the setup process. **Note: This password serves as the email password.**

Generated app password

Your app password for your device

How to use it

Go to the settings for your Google Account in the application or device you are trying to set up. Replace your password with the 16-character password shown above.

Just like your normal password, this app password grants complete access to your Google Account. You won't need to remember it, so don't write it down or share it with anyone.

Done



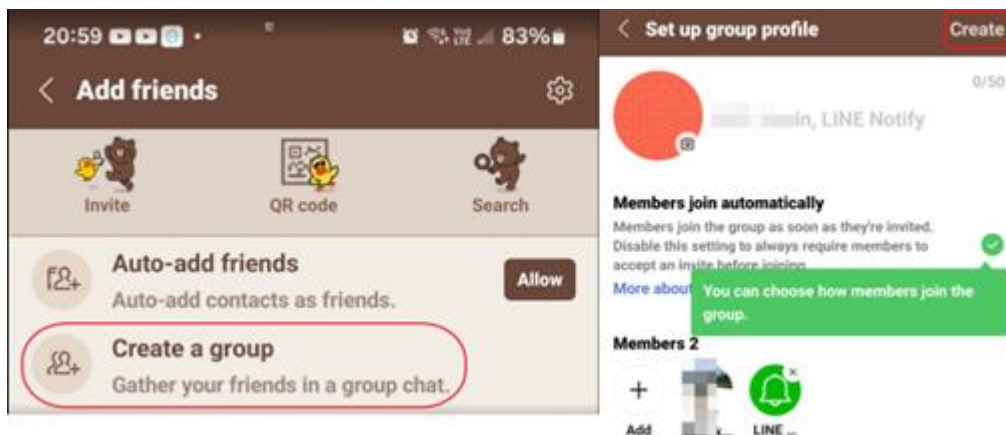
3.2.2 Line Notify

- 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.

Apply for Line Notify token (Please use LINE desktop version)

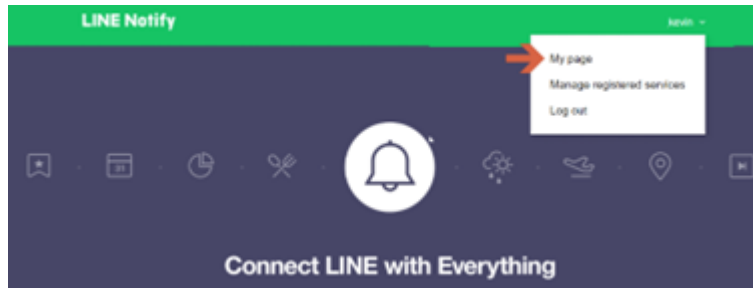
Step 1. Create a group with Line Notify in the Line app on your phone. If you don't have LINE Notify, please search and add it to your friends list first



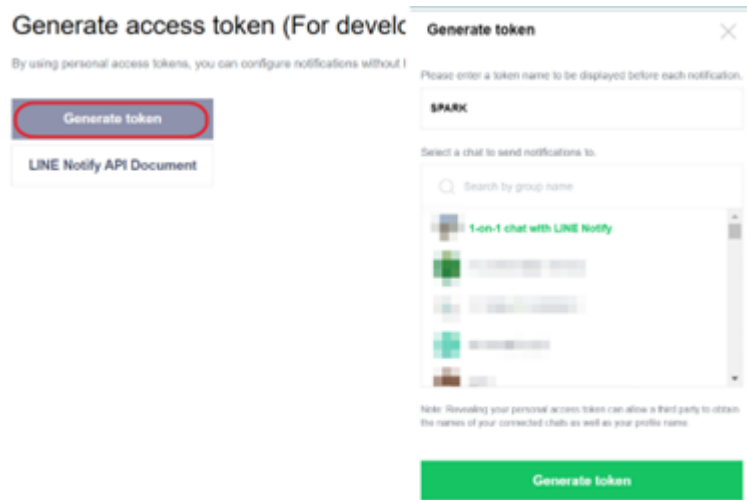
Step 2. Go to Line Notify official website <https://notify-bot.line.me/zh TW/>



Step 3. Log in and open My Page.



Step 4. Click **[Issue Token]** and select the group to receive the response behavior
Note: The group must include Line Notify members.



Step 5. Click to copy and save the token to Notepad/File

Note: If you leave this page, new tokens will not be displayed again. Before leaving the page, please copy the token first





3.3 Edit response action

Actions

Available actions

mail

Action name
mail

Action category
Send email

Action duration
0 + -

Actions delay time
0 + -

Select email account
Gmail

To
spark@spark-security.com.yw

Subject
spark_notify

Body

Duplicate OK Cancel

- Select the response action and then click

3.4 Delete response action

Actions

Available actions

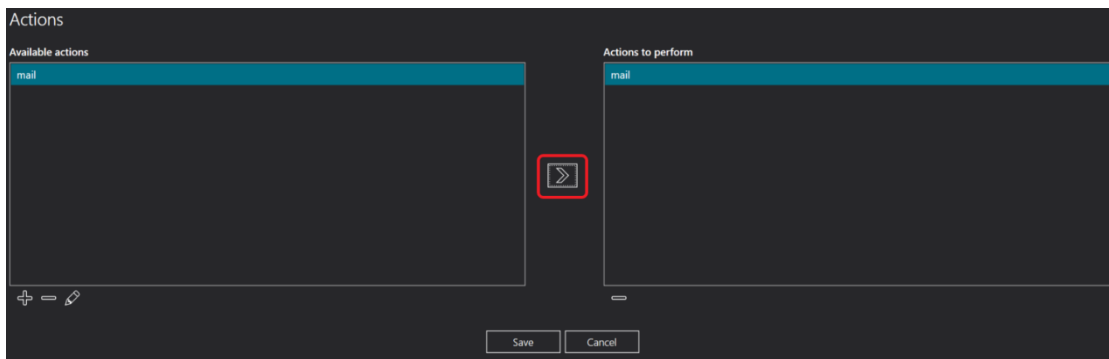
mail

+ -

- Select the response action and then click [-]



3.5 Execute response action



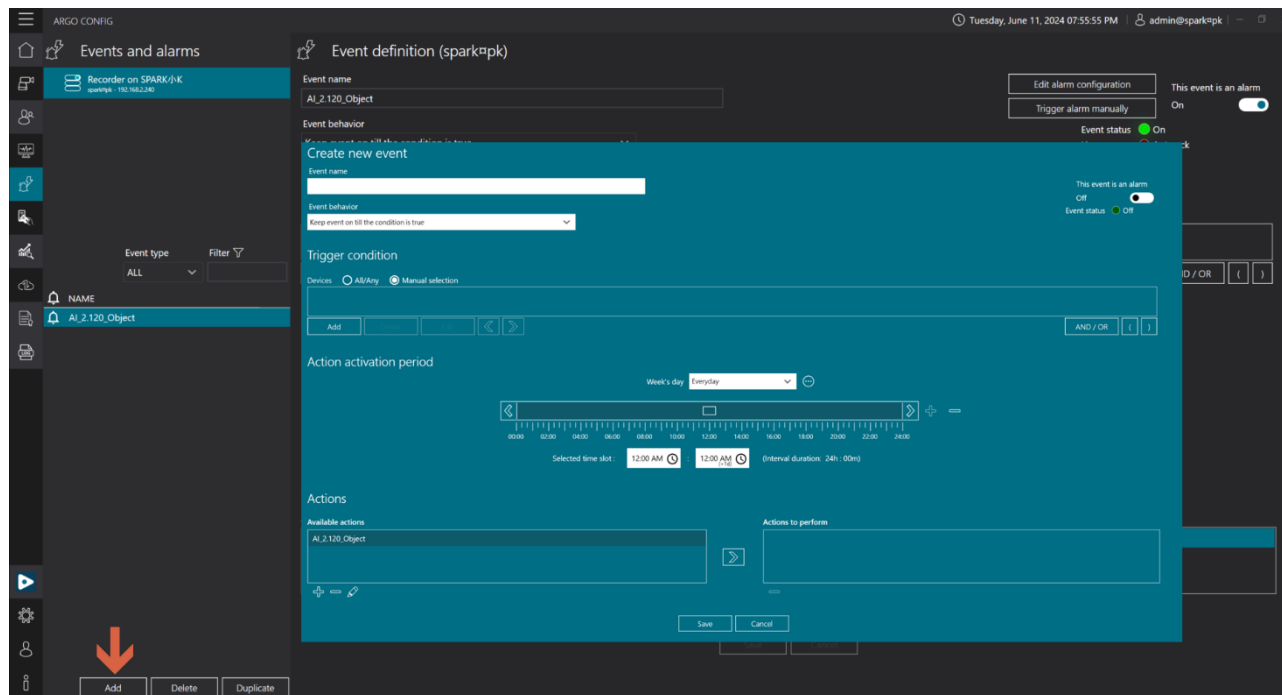
- Apply the executed response behavior: select the response behavior you want to apply, and click [>]
- Delete the executed response behavior: select the executed response behavior you want to delete and click [-]



4. EVENT AND MANAGEMENT

4.1 Add/Edit/Copy/Delete Event

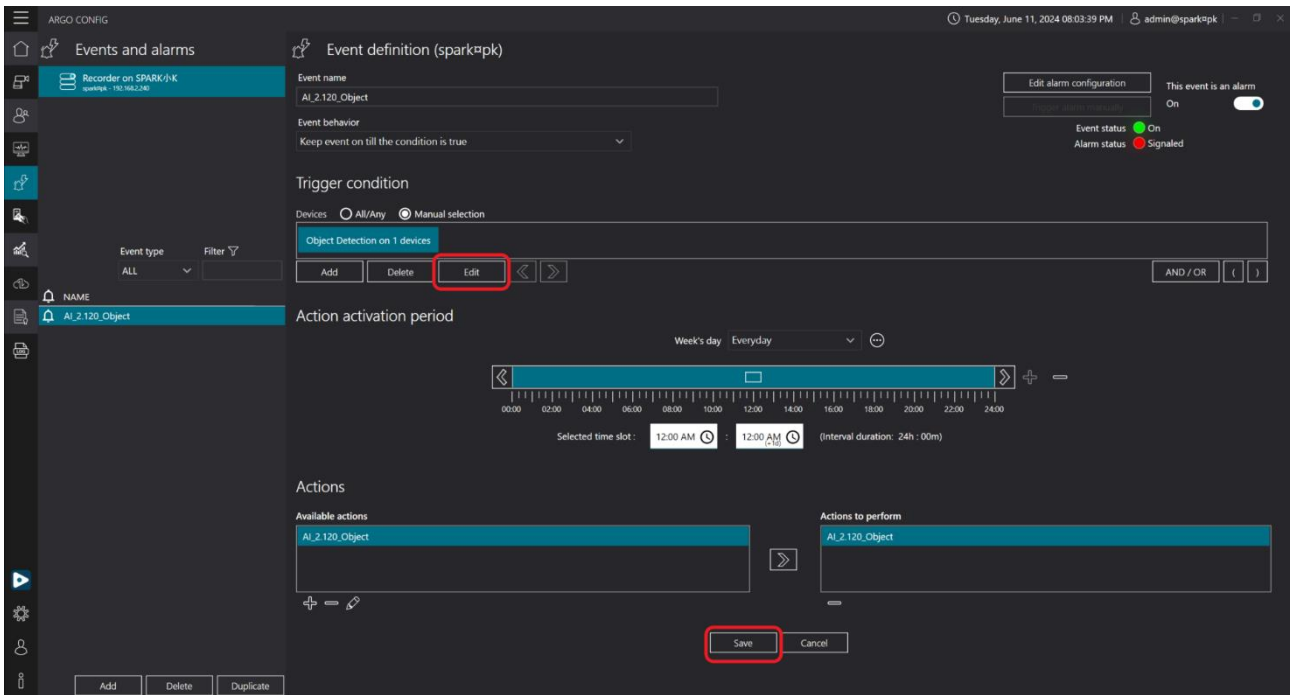
A. Add event



- Click **[Add]**
- Event name: insert name of the event
- Event behavior: select event behavior
 - Keep event on till the condition is true: The event is established at the moment when the triggering condition is met.
 - Keep the event active for X seconds from the condition trigger: When the triggering condition is met, keep the event for X seconds (range: 1-100 seconds).
 - Keep event for X seconds after the trigger condition ends: After the triggering condition ends, maintain the event for X seconds (range: 1-100 seconds).
 - Keep the event active for X seconds and raise event again if condition still trigger: Keep the event for X seconds when the triggering condition is met. If the triggering condition continues to occur, restart the event (range: 1-100 seconds).

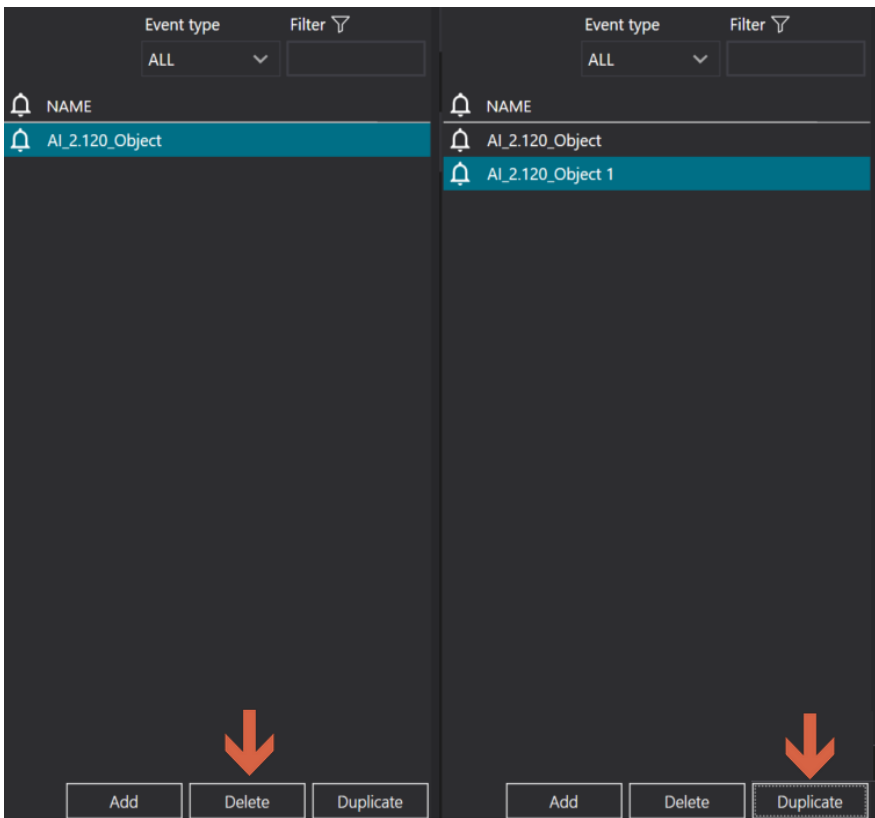


B. Edit event



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



4.2 Trigger conditions

4.2.1 Add trigger condition

- Click **[Add]**
- Event Category: system event, event and alarms, I/O events, on edge analytics events, 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 %.



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

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

- Access Control

Event	Description
Category signaled	Triggers when an ID present in category is detected.
Category signaled for allowed id is detected	Triggers when an ID present in category and allow list is detected.
Category signaled for denied id is detected	Triggers when an ID present in category and deny list is detected.
Category signaled for expired id is detected	Triggers when an ID present in category and expired list is detected.

- Spark AI Services

Event	Description
Fire detection	Triggers when fire is detected



License status	Triggers when Spark AI service license status is abnormal
Smoke detection	Triggers when smoke is detected
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).

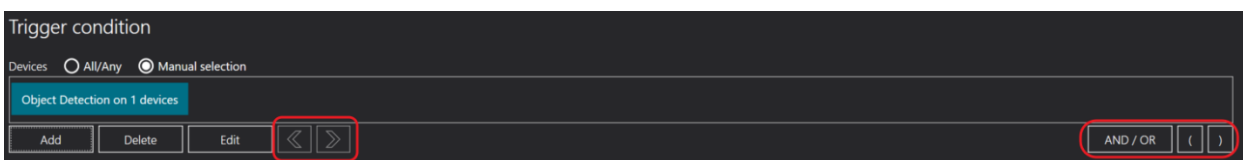
- Camera video analytics

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.

Note:

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

4.2.1.1 Advanced Setting for Trigger Conditions



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

Examples:

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



4.2.2 Edit trigger condition

Event definition (sparkapk)

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 < >

Edit condition

Event Category
Spark AI Service

Events
Object Detection

Filter

Sources

SELECT	NAME
<input checked="" type="checkbox"/>	Camera 3 - AI_2.120_Object (192.168.2.120) - on Recorder on SPARK (192.168.2.240)
<input type="checkbox"/>	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]**

4.2.3 Delete trigger condition

Event definition (sparkapk)

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

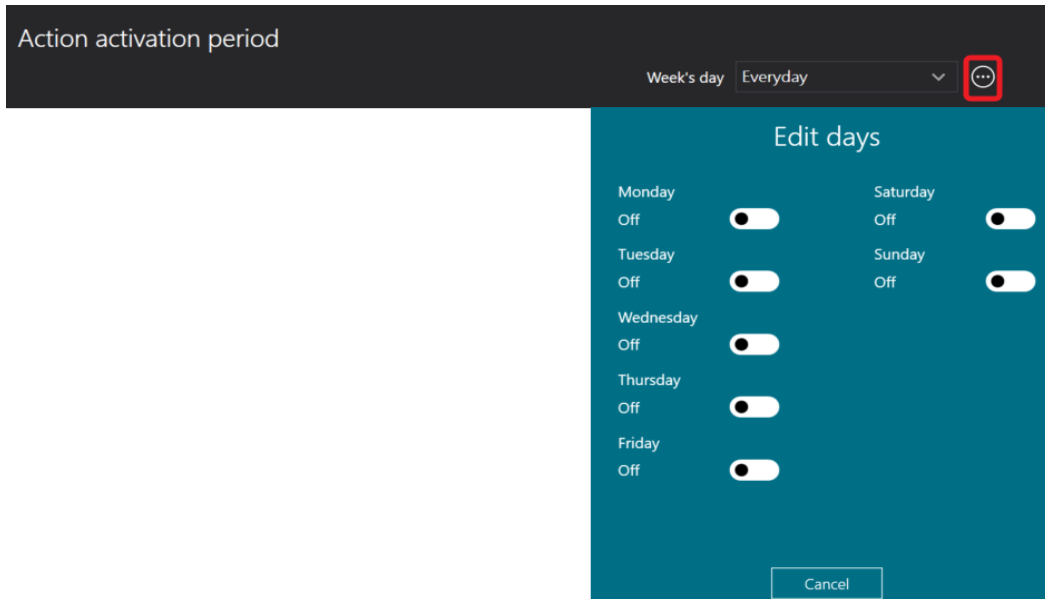
Add Delete Edit < >

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



4.3 Response action

4.3.1 Response action schedule



- Edit time slot: 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



4.3.2 Add response action

- Click [+]
- Action name: insert response action name
- Action duration: set the duration for which the response action should last, ranging from 0 to 300 seconds.
- Actions delay time: After the trigger condition is met, the response action occurs after a delay of N seconds, ranging from 0 to 300 seconds.
- Action category

A. Start recording

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

Note:



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

B. I/O output

The screenshot shows a configuration form titled 'Add action' with a teal background. It includes the following fields and controls:

- Action name:** A text input field.
- Action category:** A dropdown menu with 'Aux output' selected.
- Action duration:** A numeric input field with '0' and '+' '-' buttons.
- Actions delay time:** A numeric input field with '0' and '+' '-' buttons.
- Select an aux output:** A dropdown menu with 'Camera 1 - I/O output 0 (192.168.2.232) - Recorder on SPARK' selected.
- Set aux output new status:** A toggle switch currently set to '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

The screenshot shows a configuration form titled 'Add action' with a teal background. It includes the following fields and controls:

- Action name:** A text input field.
- Action category:** A dropdown menu with 'Go to preset' selected.
- Action duration:** A numeric input field with '0' and '+' '-' buttons.
- Actions delay time:** A numeric input field with '0' and '+' '-' buttons.
- Select a PTZ camera:** A dropdown menu with 'Camera 1 - PTZ controller 0 (192.168.2.232) - Recorder on SPARK' selected.
- Select preset:** A dropdown menu.

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



D. Start tour

The 'Add action' dialog for 'Start tour' includes the following fields:

- Action name:** A text input field.
- Action category:** A dropdown menu set to 'Start tour'.
- Action duration:** A numeric input field set to 0 with '+' and '-' buttons.
- Actions delay time:** A numeric input field set to 0 with '+' and '-' buttons.
- Select a PTZ camera:** A dropdown menu showing 'Camera 1 - PTZ controller 0 (192.168.2.232) - Recorder on SPARK (spark9pk)'.
- Select tour to start:** A dropdown menu.

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

E. Send email

The 'Add action' dialog for 'Send email' includes the following fields:

- Action name:** A text input field.
- Action category:** A dropdown menu set to 'Send email'.
- Action duration:** A numeric input field set to 0 with '+' and '-' buttons.
- Actions delay time:** A numeric input field set to 0 with '+' and '-' buttons.
- Select email account:** A dropdown menu with a red arrow pointing to the '...' button.
- To:** A text input field with 'Cc' and 'Bcc' buttons.
- Subject:** A text input field.
- Body:** A text input field.

The 'Email accounts' configuration panel includes the following fields:

- Configured email accounts:** A list box showing 'Gmail'.
- Name:** A text input field set to 'Gmail'.
- SMTP server name:** A text input field set to 'smtp.gmail.com:587'.
- Username:** A text input field set to 'test'.
- Password:** A password input field with a visibility toggle.
- Email displayed name:** A text input field set to 'Spark_Alarm_gmail'.
- Email address:** A text input field set to 'sparksqa888@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)
- User name: insert the email account
- Password: insert the email password
- Email Displayed 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.

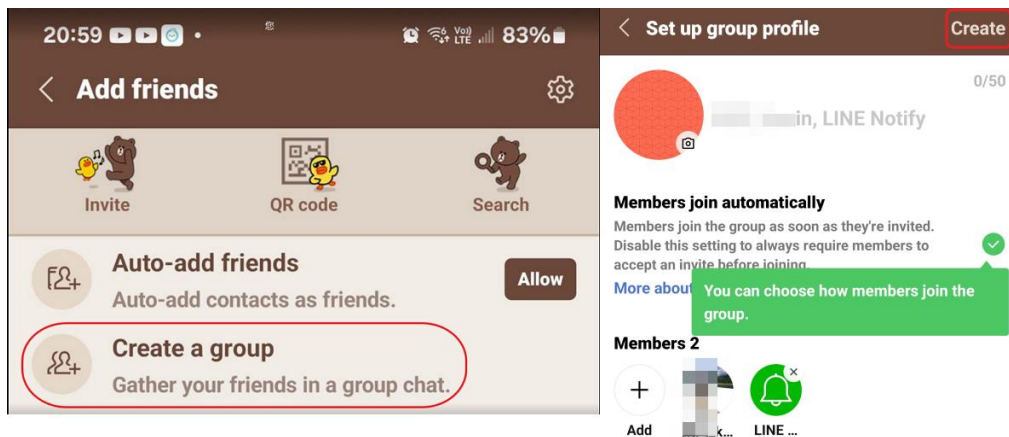


F. Line Notify

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

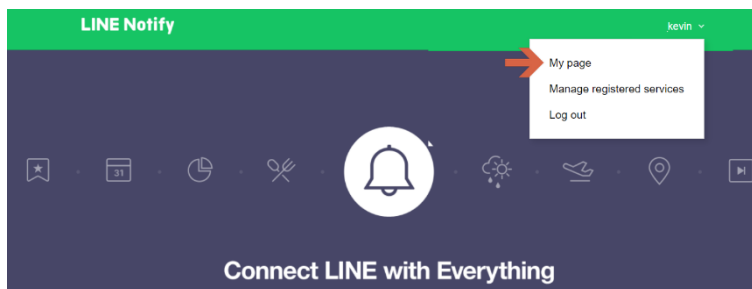
Apply for Line Notify token (Please use LINE desktop version)

Step 1. create a group with Line Notify in the Line app on your phone.



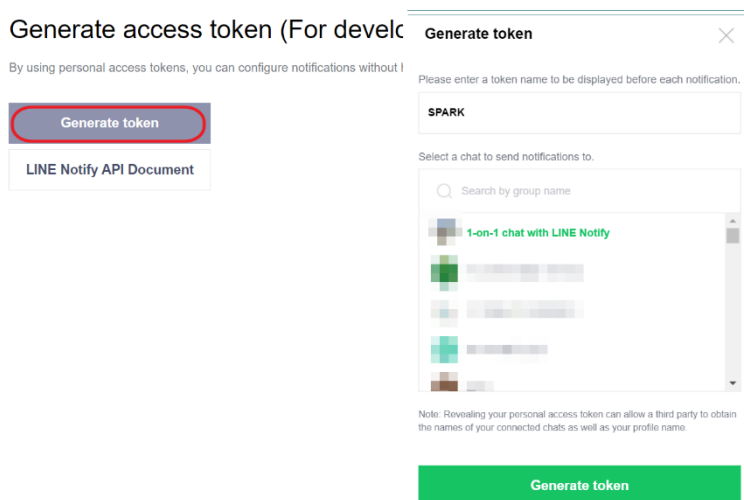
Step 2. Go to Line Notify official website https://notify-bot.line.me/zh_TW/

Step 3. Log in and open My Page



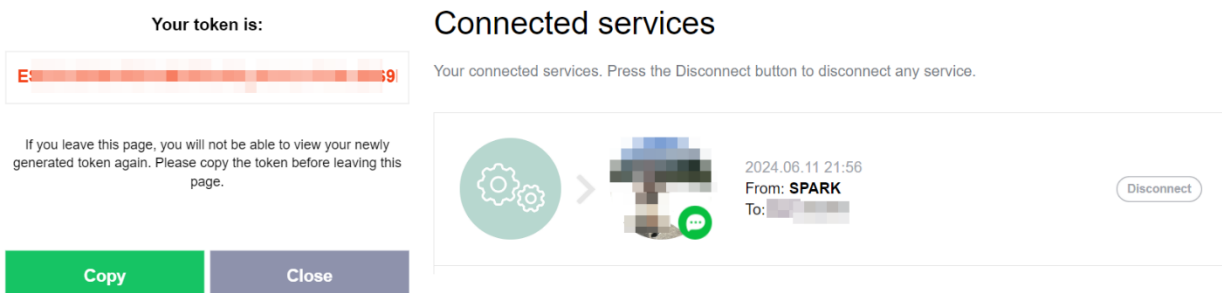
Step 4. Click [**Generate Token**] and select the group to receive the response behavior

Note: The group must include Line Notify members.



Step 5. Click to copy and save the token to Notepad/File

Note: If you leave this page, new tokens will not be displayed again. Before leaving the page, please copy the token first





G. LED display

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

Please refer to the syntax explanation below

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

`{lpr(licenseplate)}` => Replaced with the detected license plate.

`{RGB(Red,Green,Blue)}` => Specifies the corresponding text color.

If not specified, default is RGB(255,0,0) red. Refer to the "color code chart."

`{CLEAR(10000)}` => displays the text for 10000 milliseconds

If not specified, the text will not be cleared.

`{EFFECT(0)}` => Specifies the display effect of the string.

H. HTTPS Event Sending

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

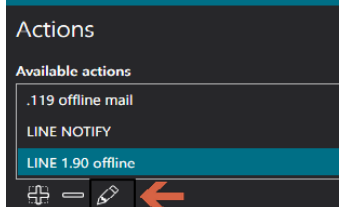
E.g.: <https://192.168.X.X:8080/> or <https://www.xxxx.com>




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

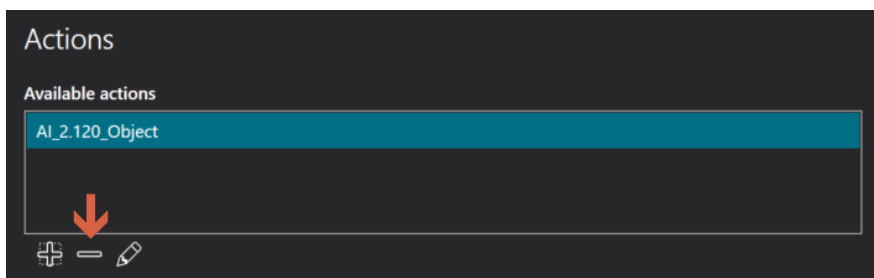
insert {Event Name} to print the name of the event triggered.

4.3.3 Edit response action



- Select response action and click 

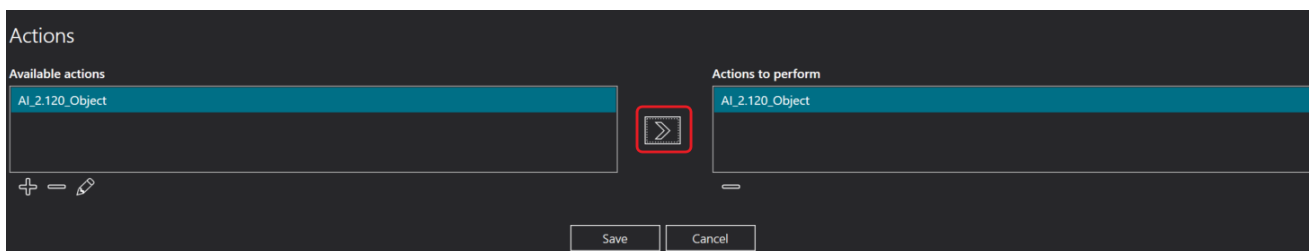
4.3.4 Delete response action



- Select response action and click [-]

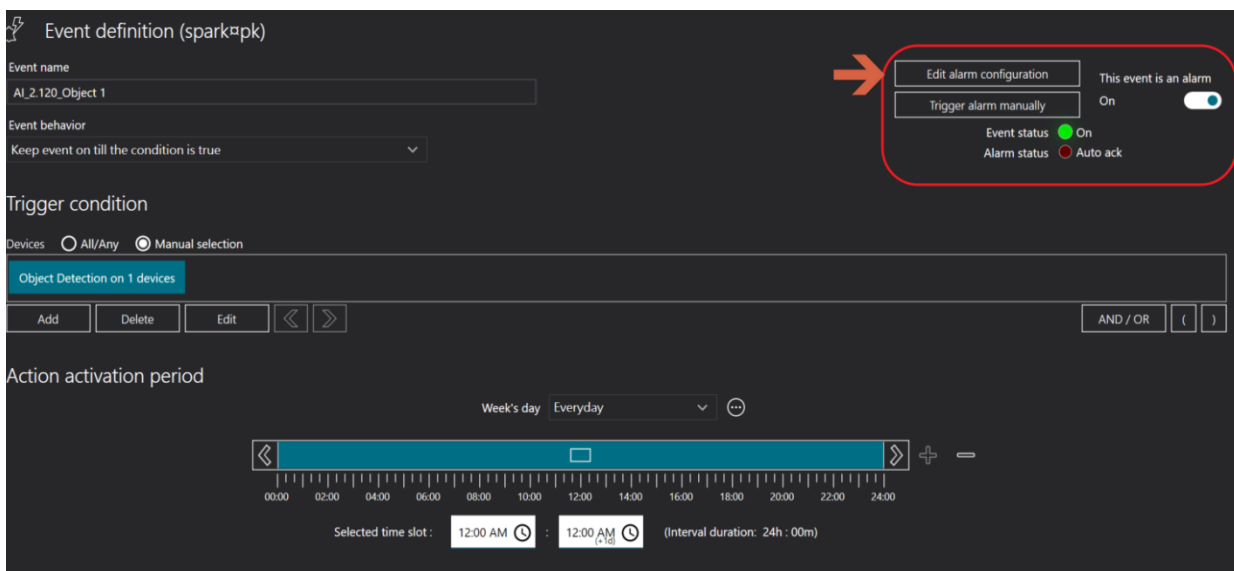


4.3.5 Execute response action



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

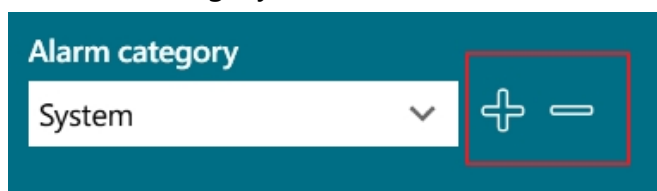
4.4 Set the event as alarm



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

4.4.1 Edit alarm setting

A. Alarm category



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

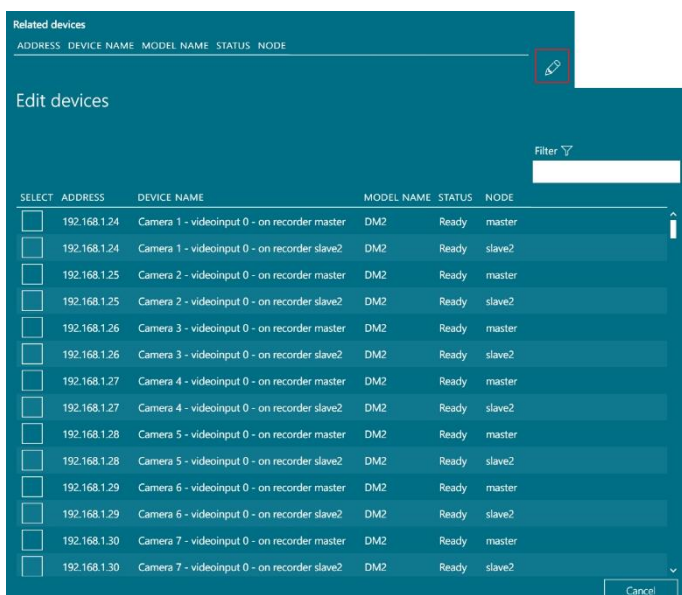


B. Alarm priority



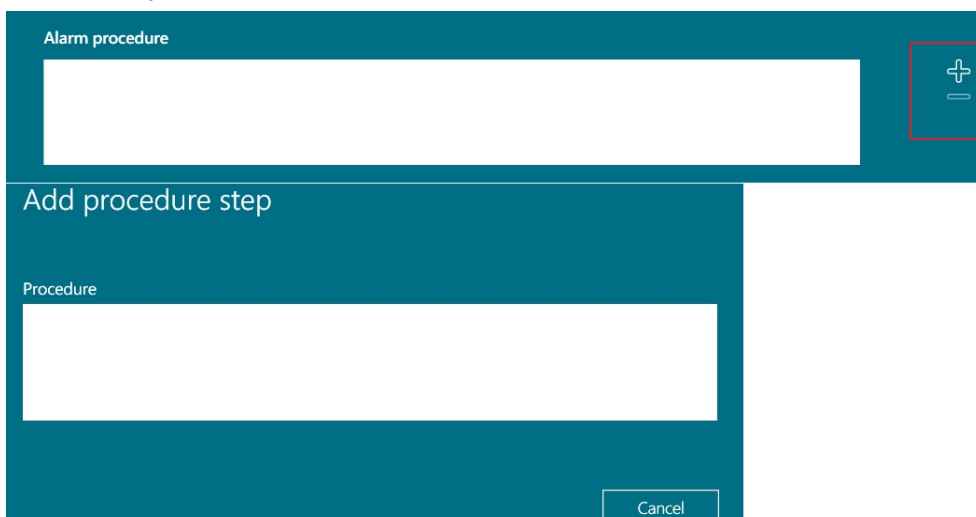
- Drag to adjust alarm priority level

C. Related devices



- Click  and select related devices

D. Alarm procedure





- Customize Alarm Handling Procedure
- Click [+/-] to add/delete processing procedure steps.

E. Alarm recipients

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

Add recipients

Groups

Filter ▾

SELECT	NAME
<input type="checkbox"/>	Administrators
<input type="checkbox"/>	Users

Add recipients

Users

Filter ▾

SELECT	USER	GROUP
<input type="checkbox"/>	admin	Administrators
<input type="checkbox"/>	admin1	Users
<input type="checkbox"/>	admin2	Users
<input type="checkbox"/>	admin3	Users
<input type="checkbox"/>	spark	Administrators

- 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

Alarm options

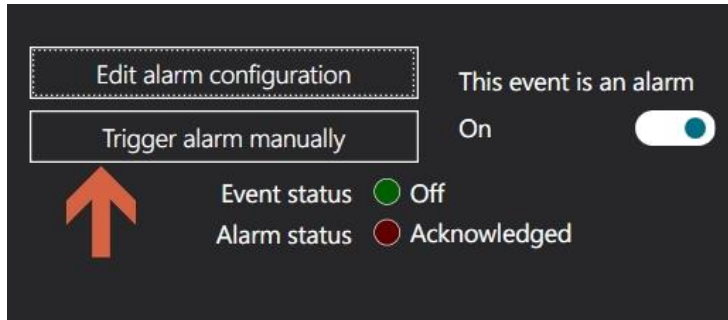
User note is mandatory

Auto-acknowledge alarm after 5 + - seconds since alarm has been triggered

Can be triggered manually

Play a sound on client machine when an alarm occurs

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



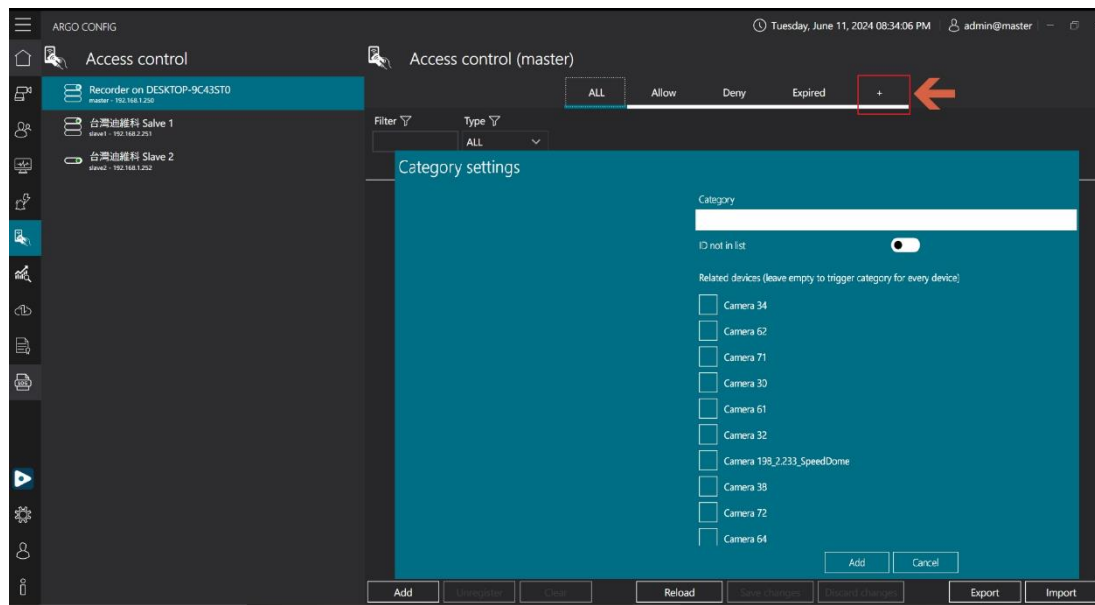
- Can be triggered manually: When enabled, you can click **[Manually Trigger Alarm]** to test the Argo Client's alarm sending functionality.
- Play a sound on client machine when alarm occurs: When enabled, a sound will be emitted from the Argo Client host when an alarm is triggered.



5. ACCESS CONTROL

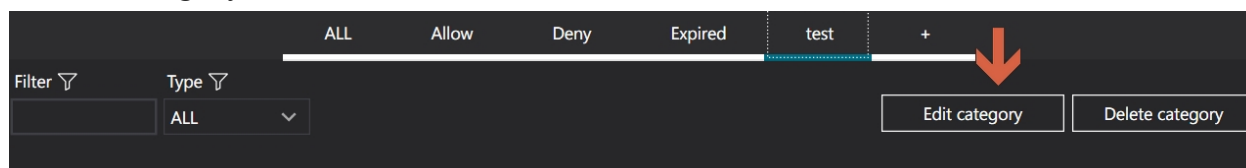
■ Add/Edit/Delete category

1. Add category



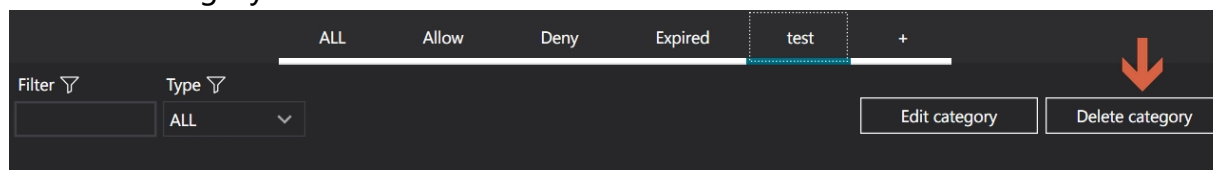
- Click [+] to add a new category to the access service list.
 - Category: name the category of the access service list
 - ID not in list: IDs not in this list are the access standards
 - Related devices: select the devices to be used for this access service list
- Note: if left blank, all devices are linked devices

2. Edit category



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

3. Delete category



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



5.1 Access ID

5.1.1 Add access ID

The screenshot shows the 'Access control (master)' configuration window. On the left, there is a sidebar with a list of devices: 'Recorder on DESKTOP-9C43ST0' (master), '台灣油維科 Salve 1' (slave1), and '台灣油維科 Slave 2' (slave2). The main area displays a table with columns for 'ALL', 'Allow', 'Deny', and 'Expired'. A modal form for adding a new access ID is open, featuring the following fields: 'Access id' (text input), 'Id type' (dropdown menu), 'Begin of overall validity' (date-time picker), 'End of overall validity' (date-time picker), 'Begin of daily validity' (time picker), and 'End of daily validity' (time picker). There is also a 'Notes' text area and 'Categories' (Allow/Deny) radio buttons. At the bottom of the form are 'Add' and 'Cancel' buttons. An orange arrow points to the 'Add' button.

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



5.1.2 Edit access ID

The screenshot displays the ARGO CONFIG interface for editing access control. The main window is titled 'Access control (master)' and shows a table of access IDs. The table has columns for ID, Type, Validity, and Status. Two entries are visible: 'ARGO-2991' (LPR, Deny) and 'FHC8637' (LPR, Allow). A sidebar on the left shows the configuration form for the selected 'Access id' (FHC8637). The form includes fields for '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), and 'End of daily validity' (12:00 AM). A red box highlights the form, and a red arrow points from the 'Begin of overall validity' field in the form to the corresponding field in the table.

Filter	Type	ALL	Allow	Deny	Expired	+
ARGO-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	

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



5.1.3 Deactivate/Clear access ID

A. Deactivate

Access control (master)

Access id	Type	Validity	Category
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

Buttons: Add, Unregister, Clear, Reload, Save changes, Discard changes, Export, Import

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

B. Clear

Access control (master)

Access id	Type	Validity	Category
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

Buttons: Add, Unregister, Clear, Reload, Save changes, Discard changes, Export, Import

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



5.1.4 Export/Import access ID

A. Export

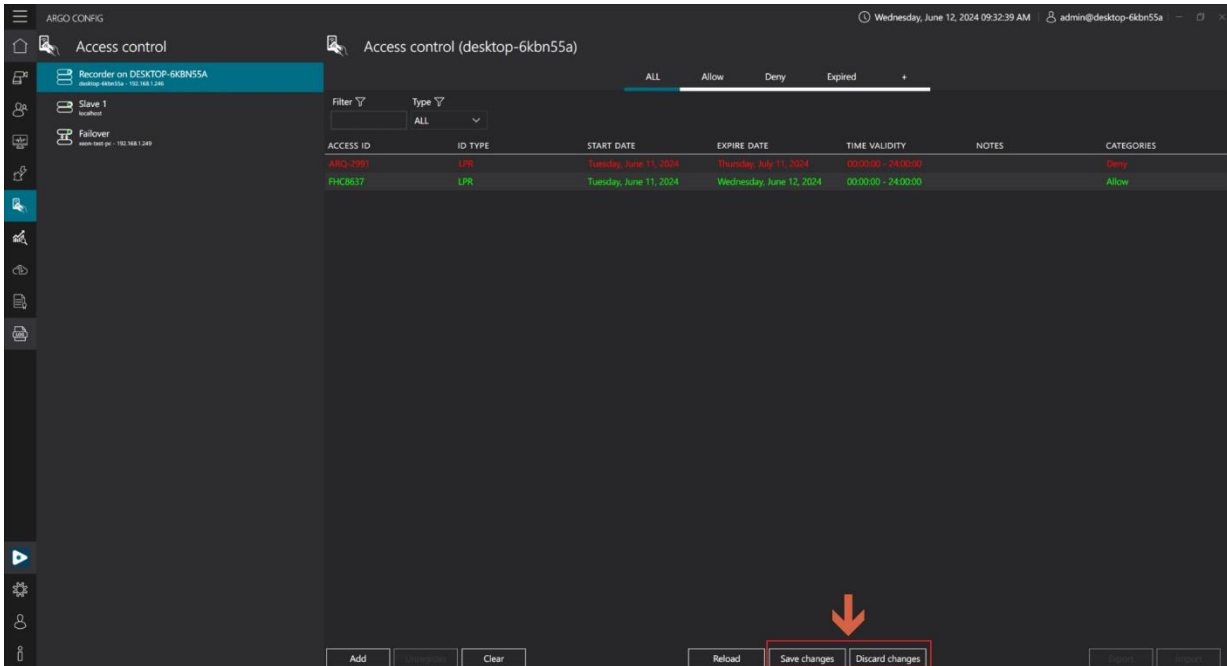
Access id	Id type	Begin of overall validity	End of overall validity	Begin of daily validity	End of daily validity	Notes	Categories
FHC8637	LPR	2024/06/11 00:00:00	2024/06/12 10:00:00	00:00:00	24:00:00		Allowed
ARQ-2991	LPR	2024/06/11 00:00:00	2024/07/11 00:00:00	00:00:00	24:00:00		Denied

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

B. Import

Access id	Id type	Begin of overall validity	End of overall validity	Begin of daily validity	End of daily validity	Notes	Categories
ARQ-2991	LPR	Tuesday, June 11, 2024	Thursday, July 11, 2024	00:00:00	24:00:00		Deny
FHC8637	LPR	Tuesday, June 11, 2024	Wednesday, June 12, 2024	00:00:00	24:00:00		Allow

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



- After importing, click **[Save changes]** 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

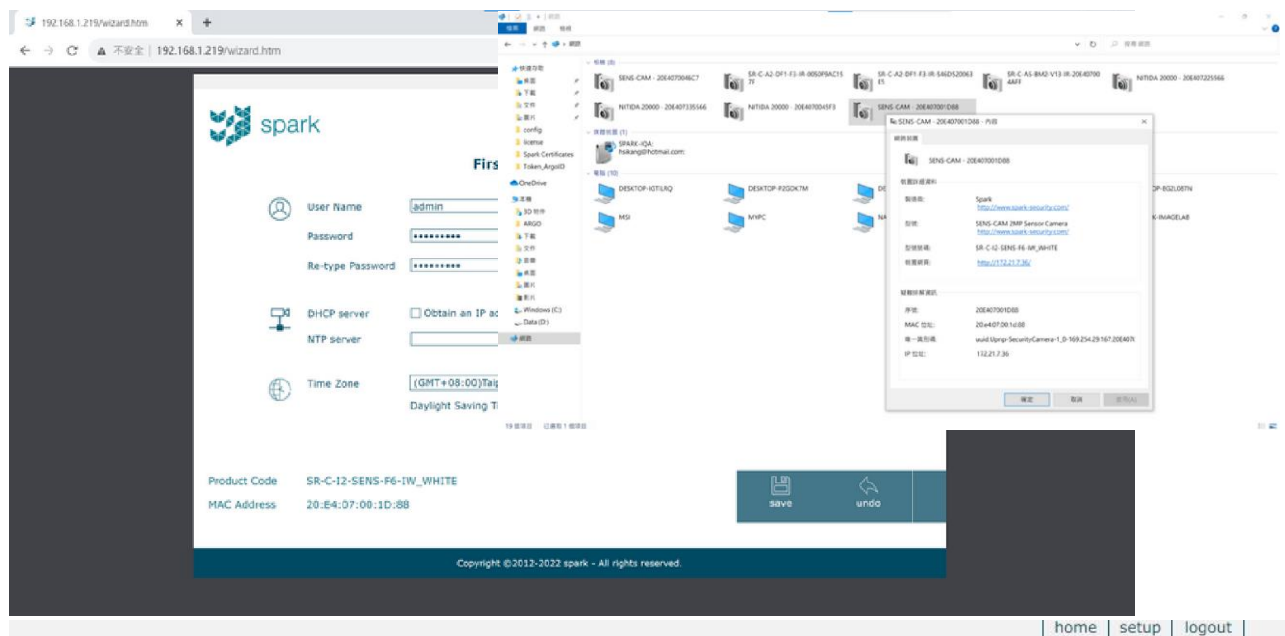
<p>xlsx file</p>	
<p>csv file</p>	<pre>accessids - 記事本 檔案(F) 編輯(E) 格式(O) 檢視(V) 說明 ACCESS ID; ID TYPE; BEGIN OF OVERALL VALIDITY; END OF OVERALL VALIDITY; BEGIN OF DAILY VALIDITY; END OF DAILY VALIDITY; NOTES; CATEGORIES FHC8637; LPR; 2024-06-11T00:00:00.000Z; 2024-06-12T10:00:00.000Z; 00:00:00; 24:00:00; ; Allowed ARQ-2991; LPR; 2024-06-11T00:00:00.000Z; 2024-07-11T00:00:00.000Z; 00:00:00; 24:00:00; ; Denied</pre>



6. VIDEO ANALYTICS DATA COLLECTION

6.1 Sens Cam settings

6.1.1 Login settings



SENS-CAM AI

TTM TECHNOLOGY



- 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.

6.1.2 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.



6.1.3 Analytics settings

home | setup | logout

spark SENS-CAM AI TTM TECHNOLOGY

audio detect intrusion tripwire in-out count heatmap people density

IN/OUT: 97/1

Car

Bus

settings

Enabled On Off

Line name ALL

Invert input direction

Detect

Person	<input checked="" type="checkbox"/>
Bicycle	<input type="checkbox"/>
Car	<input checked="" type="checkbox"/>
Motorbike	<input type="checkbox"/>
Bus	<input type="checkbox"/>
Truck	<input checked="" type="checkbox"/>

Auto Reset counts On Off

Mode Threshold

Threshold 2000 (1~65535)

Add Remove Remove All

Line name

PersonIn

ALL

PersonoOut

save undo

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

home setup logout

spark SENS-CAM AI TTM TECHNOLOGY

audio detect intrusion tripwire in-out count heatmap people density

information
image
video
audio
network
date & time
accounts
ADVANCED
archive
recording servers
recordings
analytics
schedules
digital I/O
network advanced
security
maintenance
system log

Car IN/OUT Car Car Car

settings

Enabled On Off

Line name

Invert input direction

Detect

Person	<input checked="" type="checkbox"/>
Bicycle	<input type="checkbox"/>
Car	<input checked="" type="checkbox"/>
Motorbike	<input type="checkbox"/>
Bus	<input type="checkbox"/>
Truck	<input checked="" type="checkbox"/>

Auto Reset counts On Off

Mode

Threshold (1~65535)

Line name

PersonIn
ALL
PersonoOut

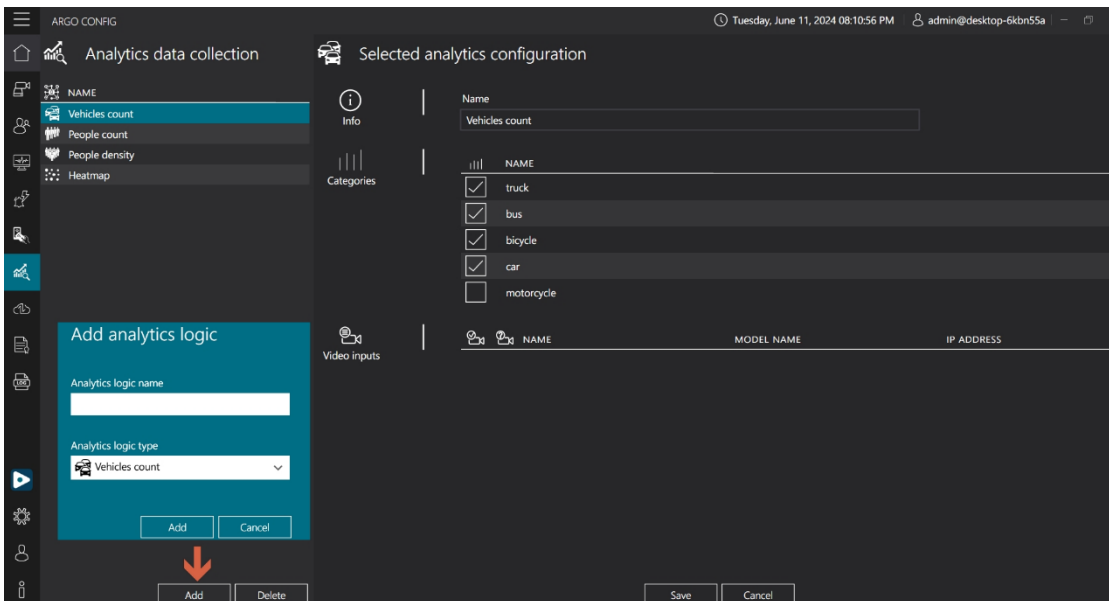
save undo

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



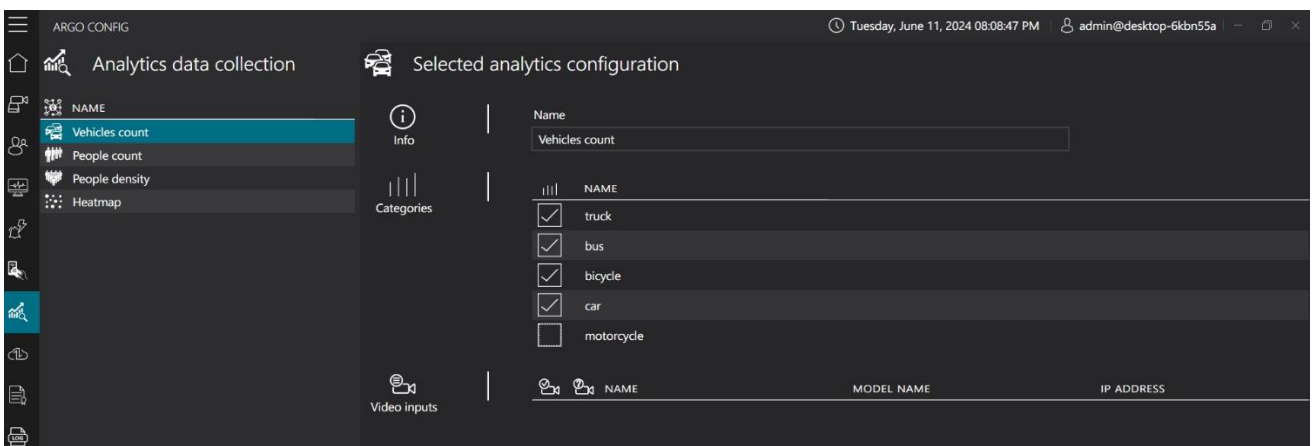
6.2 Video analytics data collection settings

6.2.1 Add video analytics parameters



- Click [Add] to add new parameters
- Analytics logic name: name the parameter
- Analytics logic type: select type (vehicle counting / people counting / people density / heatmap)

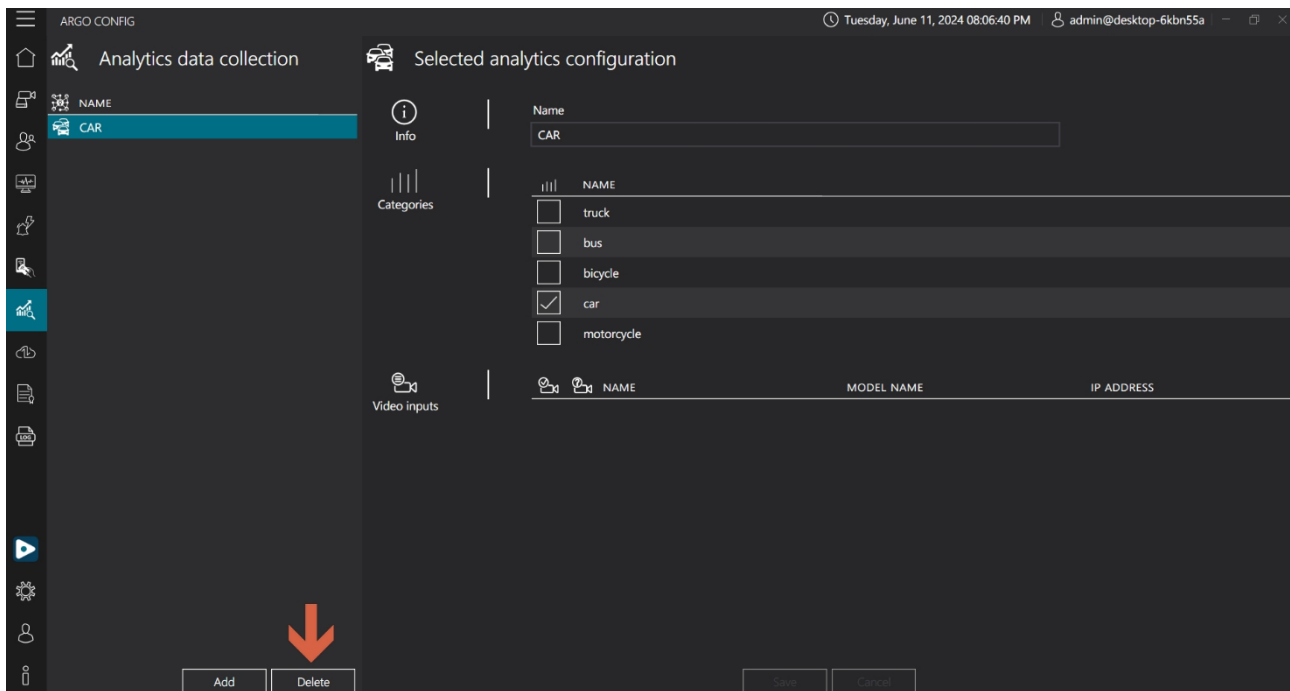
6.2.2 Set video analytics parameters



- Info: displays name of the parameter
- Categories: select the detection object
- Video inputs: select Sens cam device



6.2.3 Delete video analytics parameter

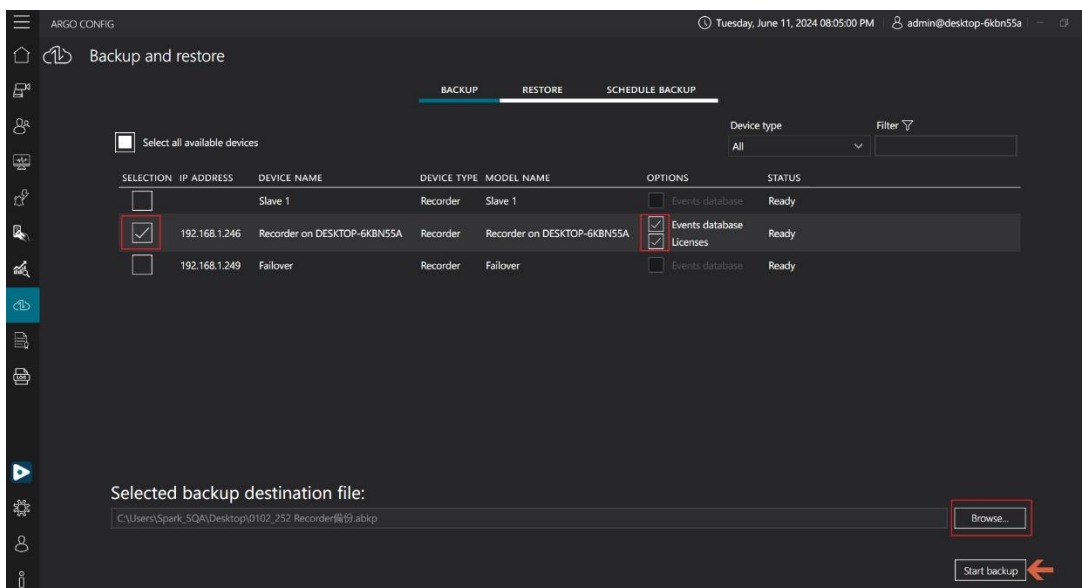


- Select the parameter you want to delete and click **[Delete]**



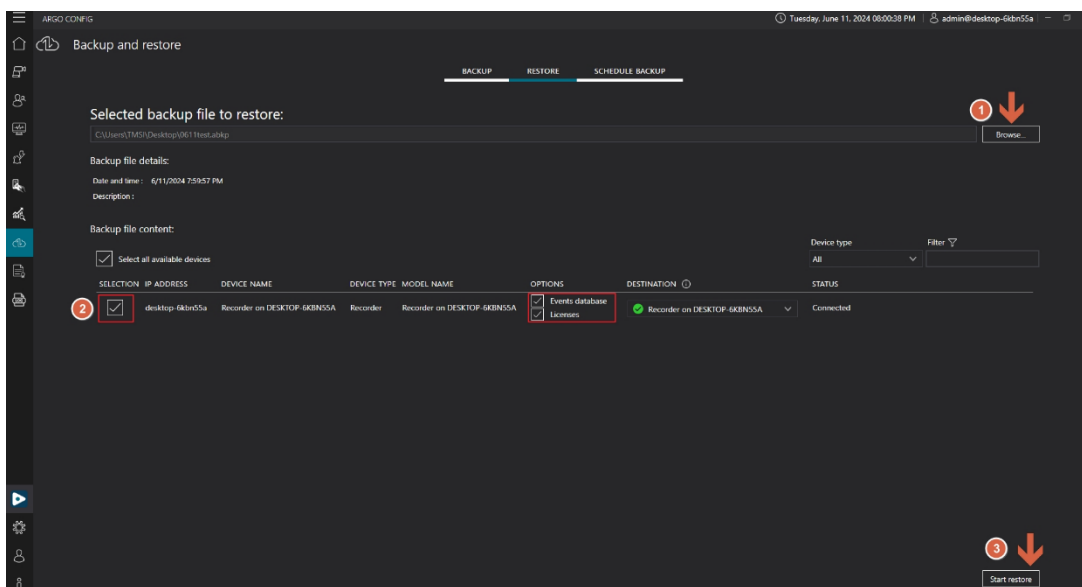
7. BACKUP AND RESTORE

7.1 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**]

7.2 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**]



7.3 Scheduled backup

The screenshot shows the 'Backup and restore' configuration page in ARGO CONFIG. The 'SCHEDULE BACKUP' tab is active. The table below summarizes the backup configurations for each device.

IP ADDRESS	DEVICE NAME	OPTIONS	KEEP TIME	SCHEDULE TIME	PATH	STATUS
192.168.1.246	Recorder on DESKTOP-6KBN55A	<input type="checkbox"/> Events database <input type="checkbox"/> ALPR DB <input type="checkbox"/> Record videos	Month	12:00 AM		Disable
			Month	12:00 AM		Disable
			Month	12:00 AM	\\XEON-TEST-PC\Backup_space\backup2	Disable
	Slave 1	<input type="checkbox"/> Events database <input type="checkbox"/> ALPR DB <input checked="" type="checkbox"/> Record videos	Month	12:00 AM		Disable
			Month	12:00 AM		Disable
			1 + Month	3:14 PM	\\XEON-TEST-PC\Backup_space\backup2	Disable
192.168.1.249	Failover	<input type="checkbox"/> Events database <input type="checkbox"/> Record videos	Month	12:00 AM		Disable
			Month	12:00 AM		Disable
			Month	12:00 AM	\\XEON-TEST-PC\Backup_space\backup2	Disable

A modal dialog box is open, prompting for 'Username' and 'Password'.

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

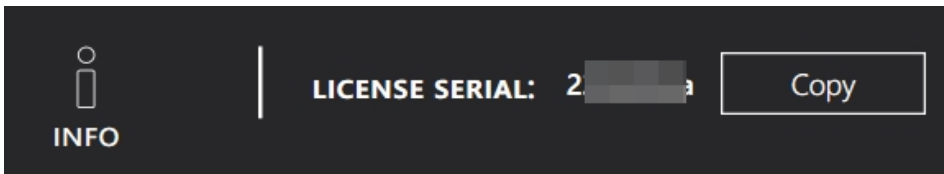


8. LICENSE

ADDRESS	NAME	LICENSE TYPE	STATUS
desktop-6kbn55a	Recorder on DESKTOP-6KBN55A	Site license	Licensed

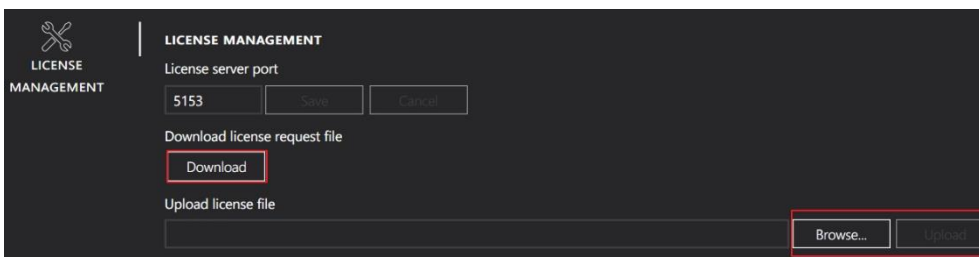
- Address: current IP address
- Name: server name
- License type: multiple channel license
- Status: license status

■ Info



- License Serial: 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.

■ License management



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



■ Channel license

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 / used / available / total / expiration date / status

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

■ Integration licenses

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 / expiration date / status

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



9. LOG

Audit log

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

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)

A. Search Audit log

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

- Level: select the level of 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
- Node: select the nodes where the data trace is located
Note: select at least one node from the list
- Click [Search]



B. Delete Audit log

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

- Buttons for 'AUDIT LOG', 'SYSTEM LOG', and 'DETAILED LOG'.
- Filters: 'LEVEL' set to 'ALL', 'FROM' and 'TO' dates set to '6/11/2024' with calendar icons.
- Text: 'Please choose at least a node from the list below.'
- Table with columns: SELECT, NODE, ADDRESS, STATUS.
- Table rows: Recorder on DESKTOP-6KBN55A (desktop-6kbn55a) Online, Slave 1 (localhost) Online, Failover (xeon-test-pc) Online.
- Buttons: 'Search' and '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
- Node: select the nodes where the data trace is located
Note: select at least one node from the list
- Click **[Delete]**

C. Export Audit log

The screenshot shows the Audit log export interface with the following elements:

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)

Buttons: 'Export to CSV'

Export the search results of the Audit log.

- Click **[Export CSV]**



9.1 System log

The screenshot shows the 'Log' section of the Argo Config interface. It features three tabs: 'AUDIT LOG', 'SYSTEM LOG' (selected), and 'DETAILED LOG'. Below the tabs, there are filters for 'LEVEL' (set to 'ALL'), 'FROM' (6/11/2024), and 'TO' (6/11/2024). A message prompts the user to 'Please choose at least a node from the list below:'. A table lists nodes: Recorder on DESKTOP-6KBN55A, Slave 1, and Failover. Below this is a search bar and a 'Delete' button. The main area displays a list of log entries with columns for DATE, LEVEL, MESSAGE, and NODE. The entries show status changes for various system events. An 'Export to CSV' button is located at the bottom right.

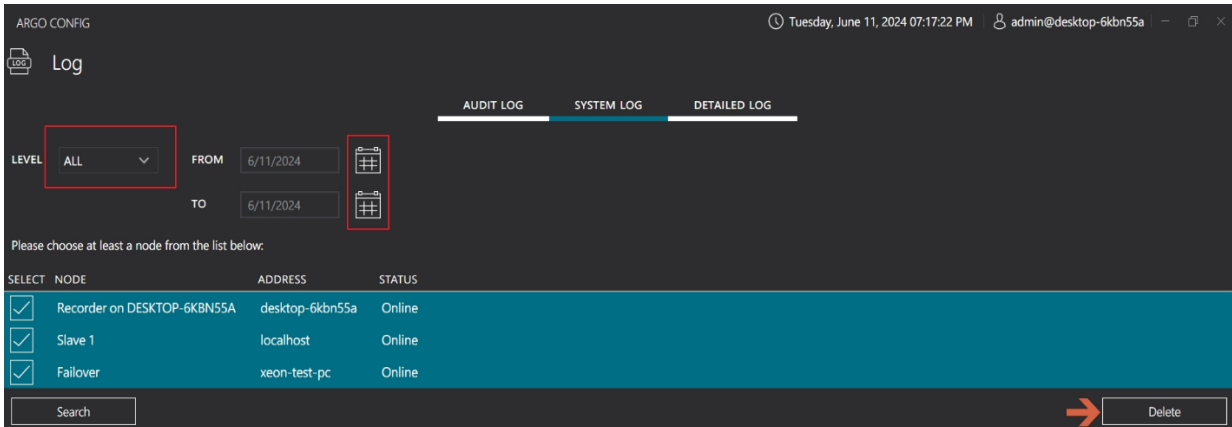
A. Search system log

This screenshot highlights the search filters in the 'Log' interface. A red box around the 'LEVEL' dropdown menu shows it is set to 'ALL'. Another red box around the 'FROM' and 'TO' date pickers shows the date '6/11/2024' selected. A calendar icon is also highlighted. To the right, a calendar for June 2024 is visible, with the 11th circled. Below the filters, the same node selection table is shown with all three nodes checked. A search bar with a red arrow pointing to it is at the bottom left.

- 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
- Node: select the nodes where the system log is located
Note: select at least one node from the list
- Click **[Search]**

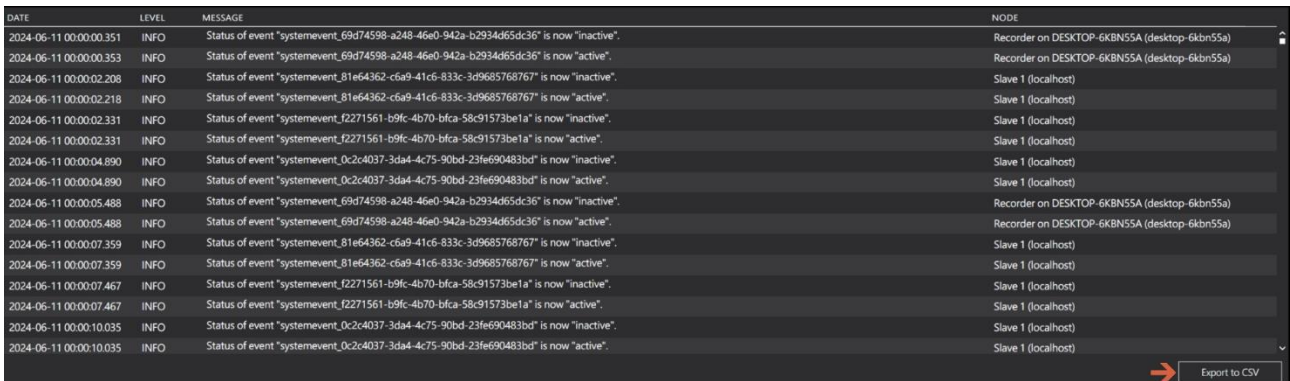


B. Delete system log



- 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

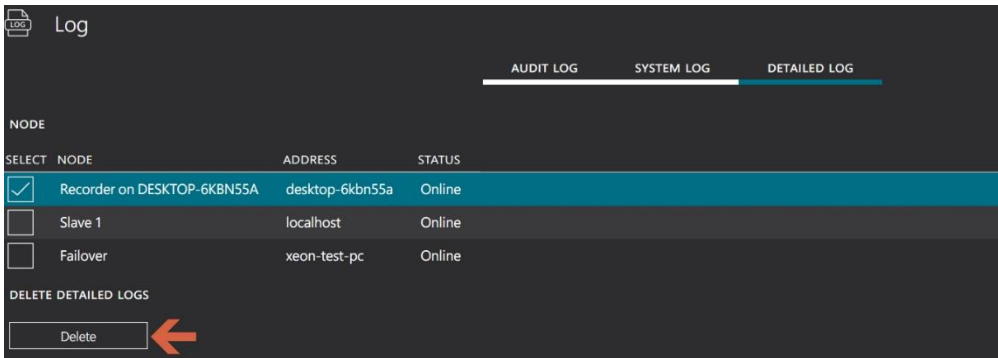


- Export the search results of the system log.
- Click **[Export to CSV]**



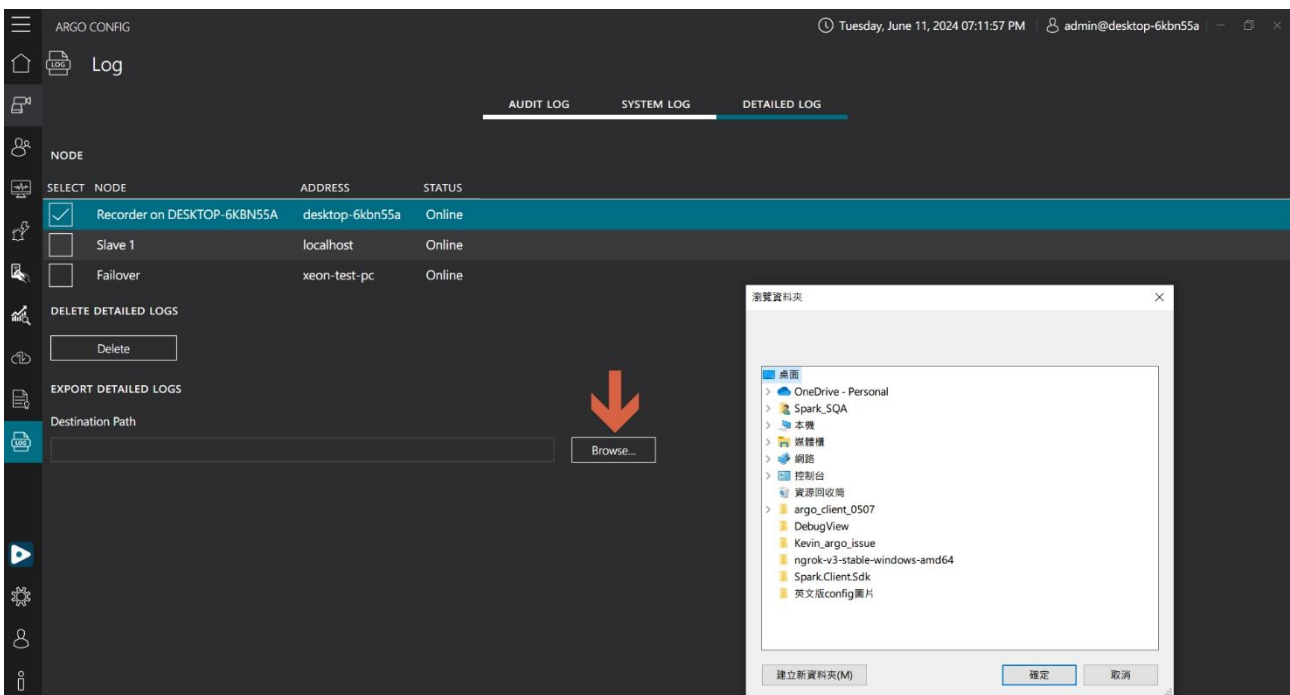
9.2 Detailed log

A. Delete detailed log



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

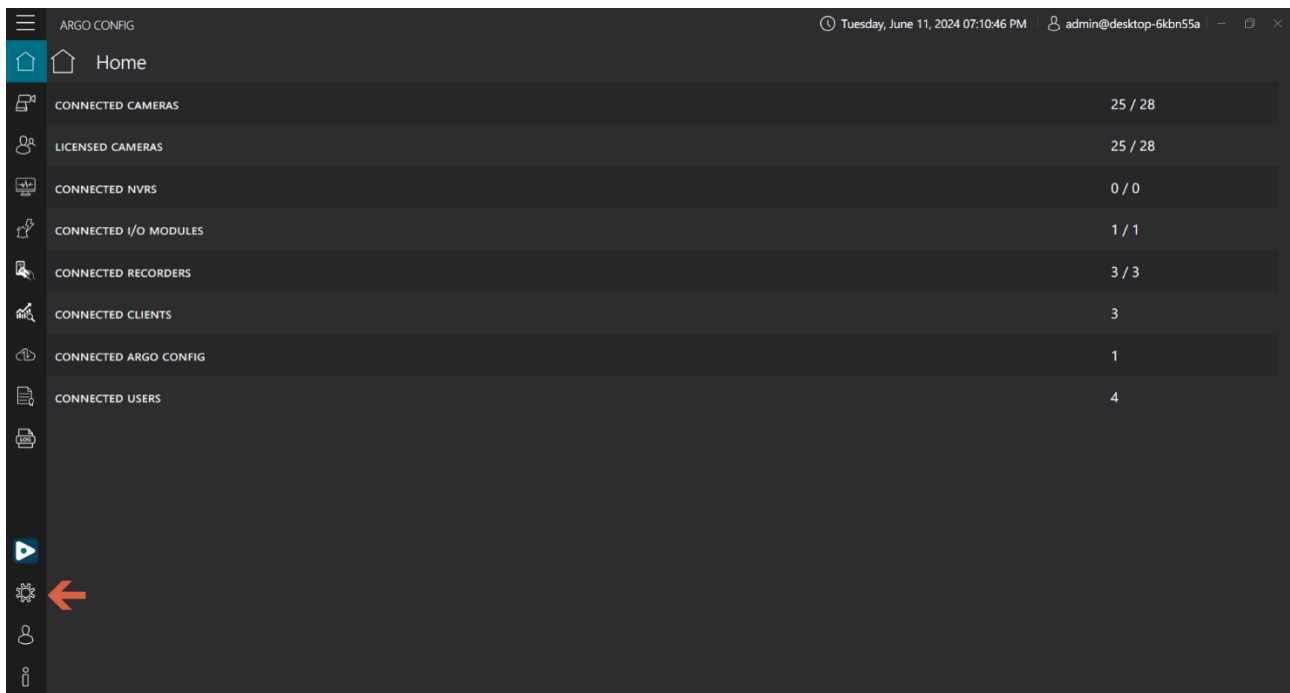
B. Export detailed log



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



10. ARGO CLIENT

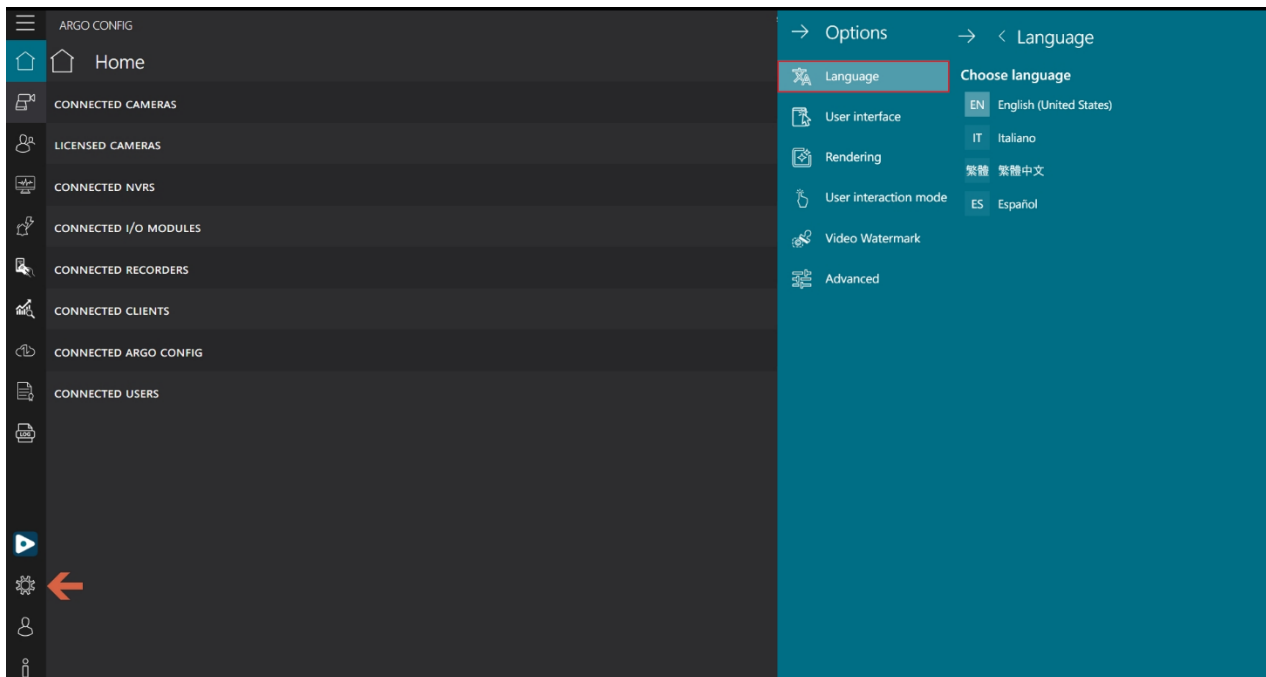


- Click the **[Argo Client icon]** on the bottom left
- Link from Argo Config to Argo Client



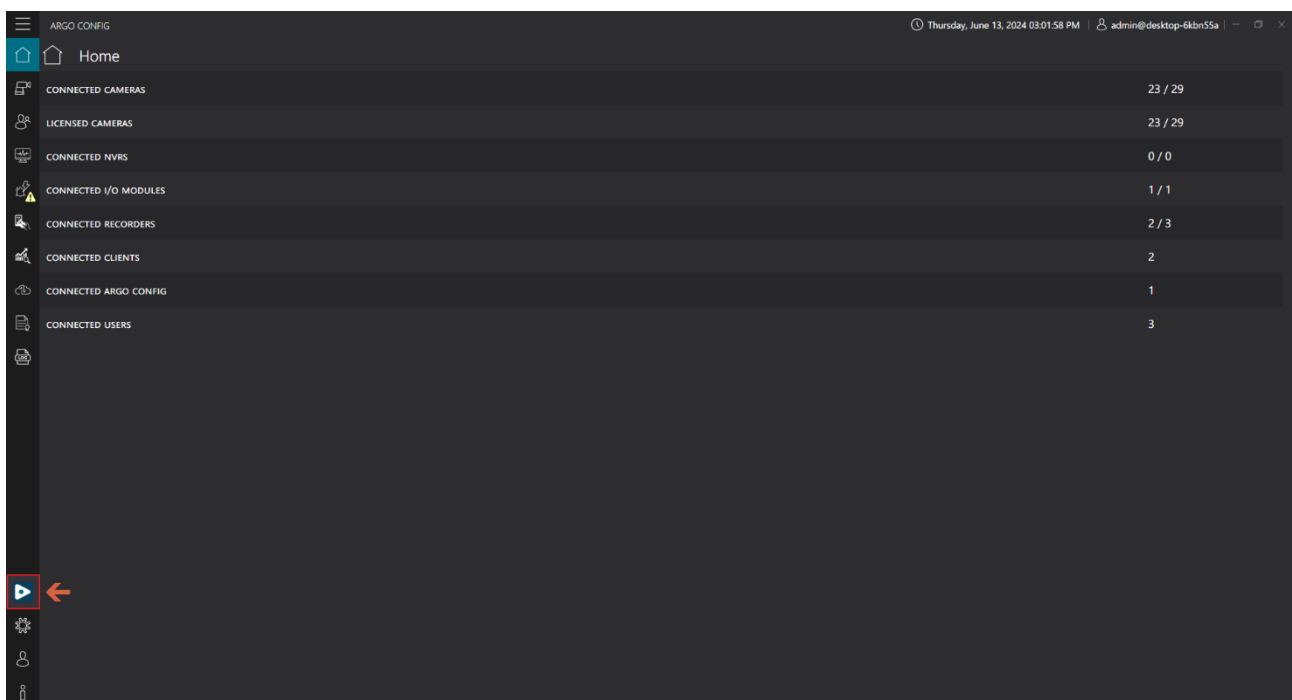
11. OPTIONS

11.1 Language

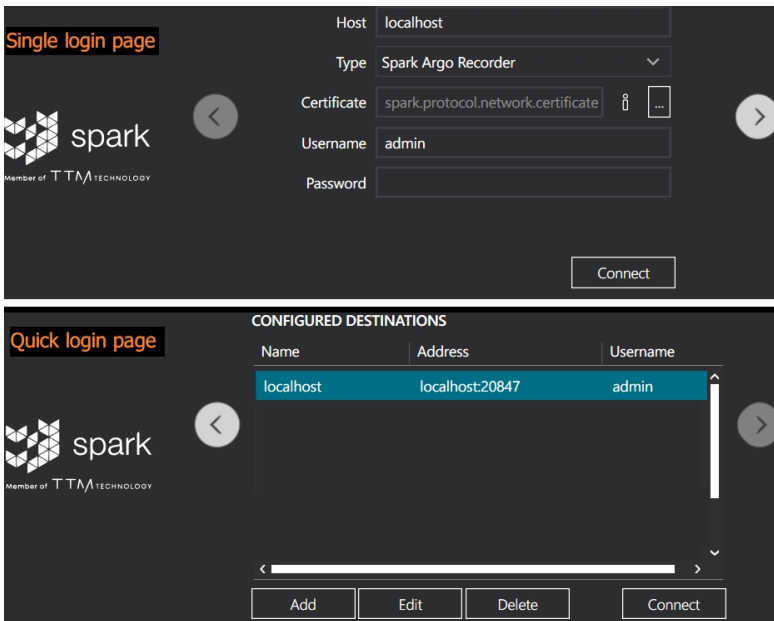


- Click the bottom left [**Options**] and select [**Language**].
- Language options: English / Italiano / 繁體中文 / Español

■ Interface

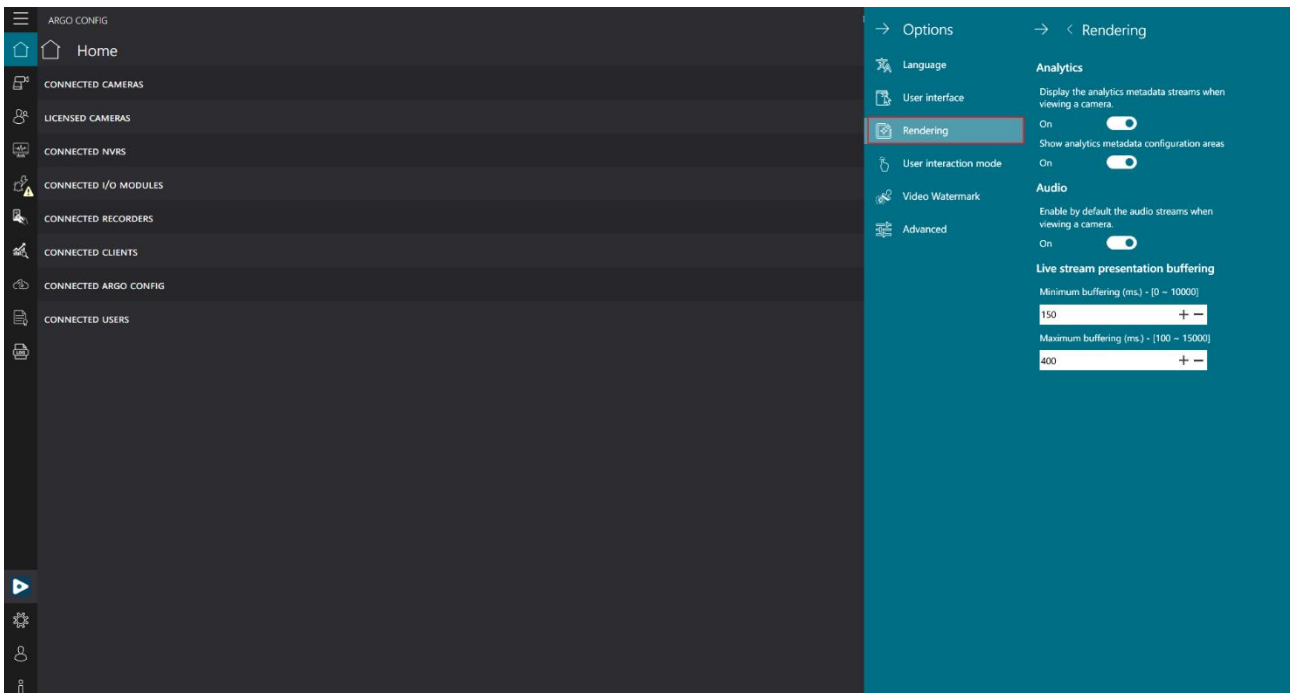


- Click the bottom left [**Options**] and select [**User interface**].

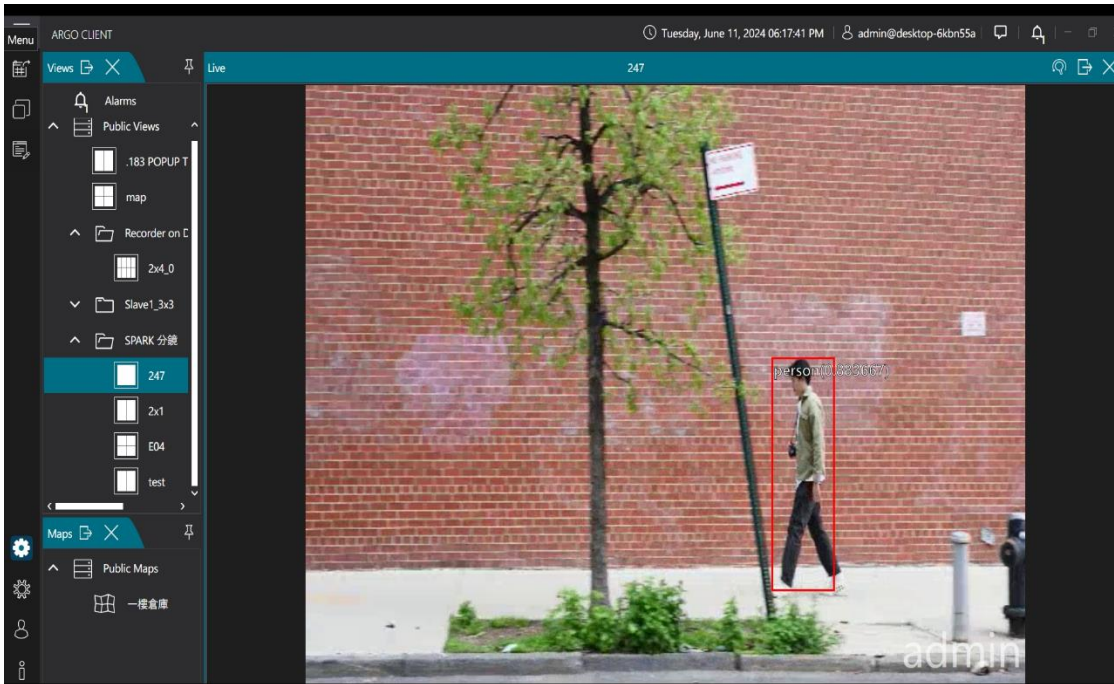


- Log in
Single login page: password is required to log in.
Quick login page: log in without a password for direct connection.

■ Drawing



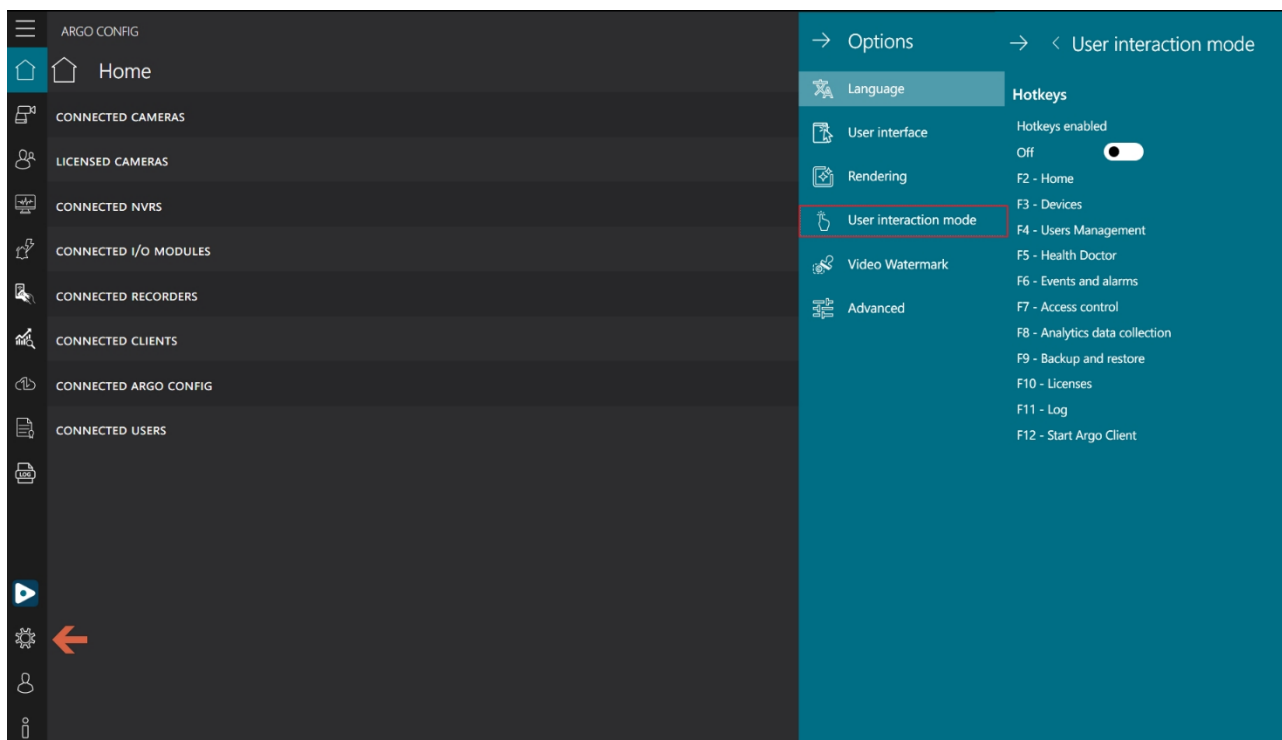
- Click the bottom left [**Options**] and select [**Rendering**].



- Analytics
 - Display the analytics metadata steams when viewing a camera: the monitoring screen will display a red frame on detected object.
 - Show analytics metadata configuration areas: 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.
 - Live stream presentation 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.



11.2 User interaction mode

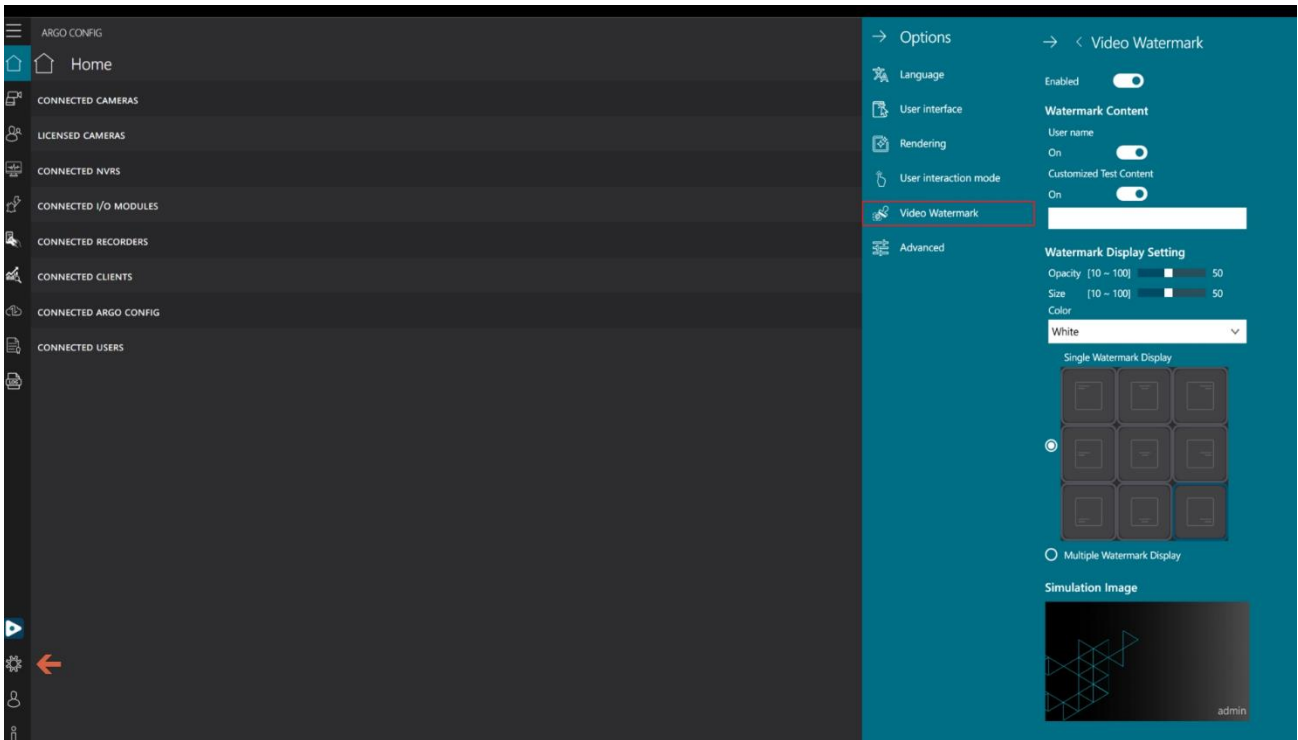


- Click the bottom left [**Options**] and select [**user interaction mode**].
- Hotkeys: when enabled, users can use below hotkeys.

F2	Home	F8	Analytics data collection
F3	Devices	F9	Backup and restore
F4	User management	F10	Licenses
F5	Health doctor	F11	Log
F6	Event and alarm	F12	Start Argo Client
F7	Access Control		



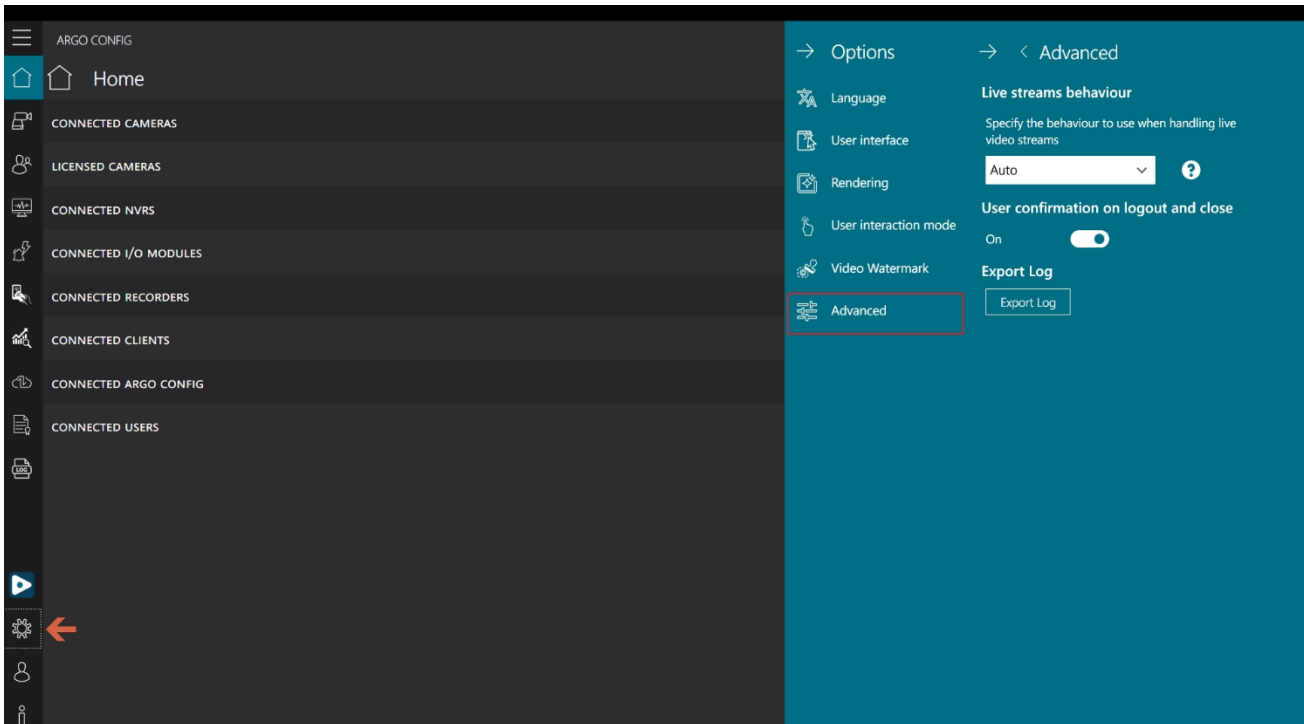
11.3 Watermark



- Click the bottom left **[Options]** and select **[Video Watermark]**.
- Watermark content: edit the username and custom content.
Username: when enabled, the watermark will display the username.
Customized Test content: when enabled, users can custom watermark content.
- Watermark Display Setting:
Edit the text opacity, text size, text color, single watermark display position, or multiple watermarks filling the image.
Opacity: edit the transparency of the watermark text, ranging from 10 to 100.
Size: edit the size of the watermark text, ranging from 10 to 100.
Color: edit the watermark text color, choosing between white or black.
Single watermark display: 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 Display: display watermarks at all nine positions, filling the image with watermark content.
Simulation Image: preview the watermark settings.



11.4 Advanced



- Click the bottom left **[Options]** and select **[Advanced]**.
- Real-time streaming behavior
Live streams 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.
- User confirmation on logout and close
On: a confirmation prompt will be displayed when logging out or closing the program.
- Export log: Click **[Export logs]** to export complete system program log

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



12. USER

12.1 Change password

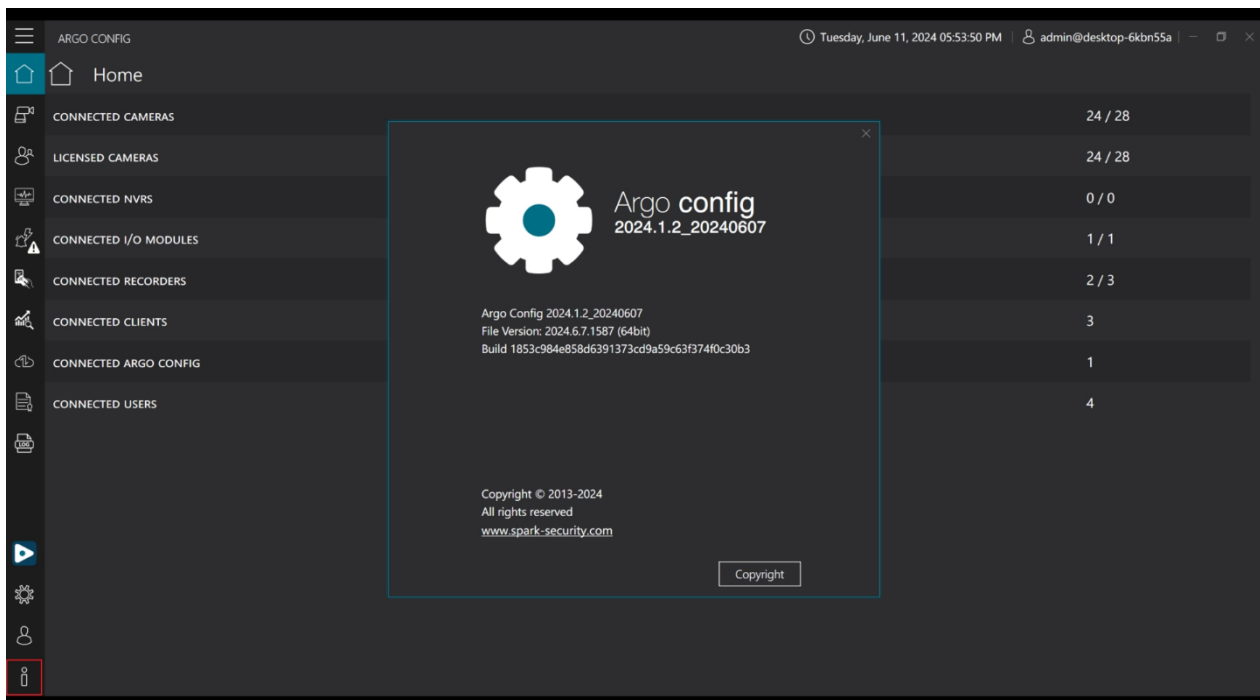
- Click on **[User]** then click **[change password]**. After changing password, click **[change password]** to confirm.
- Username: usernames cannot be modified.
- Old password: insert username old password
- New password: insert new password
- Confirm password: retype the password

12.2 Logout/Close

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



13. 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.



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**

