spark
Italian inSight

Quick Start Guide

Argo

V1.6

Confidentiality Notice

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, playback, export images, etc.
- Argo Config: for managing users and connected devices, set events, etc.

1.2 Argo Recorder

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

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

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

- CPU: Allocate 90 CPU marks per camera. You can search for suitable CPU specifications on the following website (https://www.cpubenchmark.net/high_end_cpus.html)

  e.g.: If you need 50 cameras, the required CPU score would be 90 multiplied by 50, resulting in a total of 4500. After calculating the total score, you can visit the above website to find an appropriate CPU. Additionally, we recommend adding a buffer of 1800 points to ensure the system operates perfectly.
- RAM: 160GB or more
- Operating system: Windows 10(64-bit)
- HDD: Requirement varies depending on camera quantity, recording time and resolution.
  - 1 camera recording 20MP for 24hrs requires 211GB.
  - 1 camera recording 5MP for 24hrs requires 63GB.
  - 1 camera recording 2MP for 24hrs requires 42GB.

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)

Contents

1. START

Follow these steps to download, install, and set up Argo to ensure it runs properly.

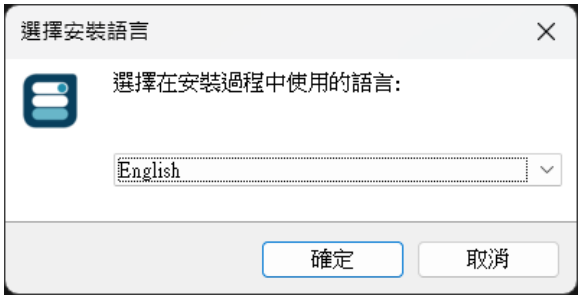
For a quicker start, we recommend referring to the tutorial video. If you havent downloaded the installer yet, please get the latest version first, then contact us via our official LINE account to request a trial license.。

▲ Watch Tutorial Video ▲Download Installer ▲Request Trial License

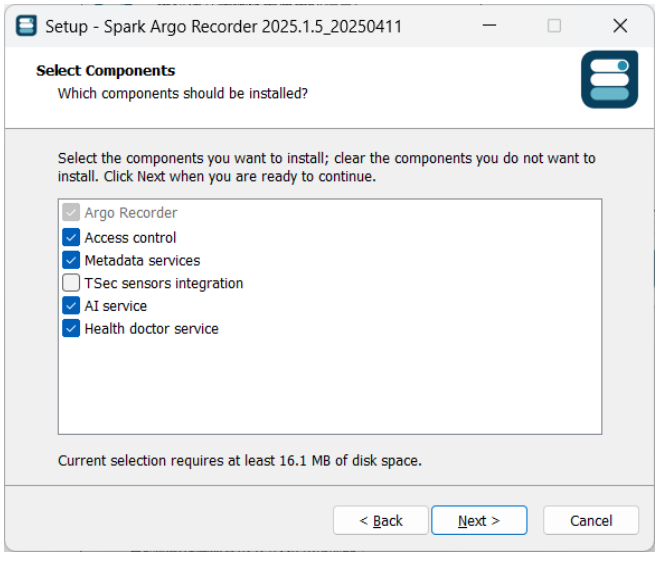
1.1 Argo Installation

This section covers how to download, install, and set up the Argo system to ensure a smooth start.

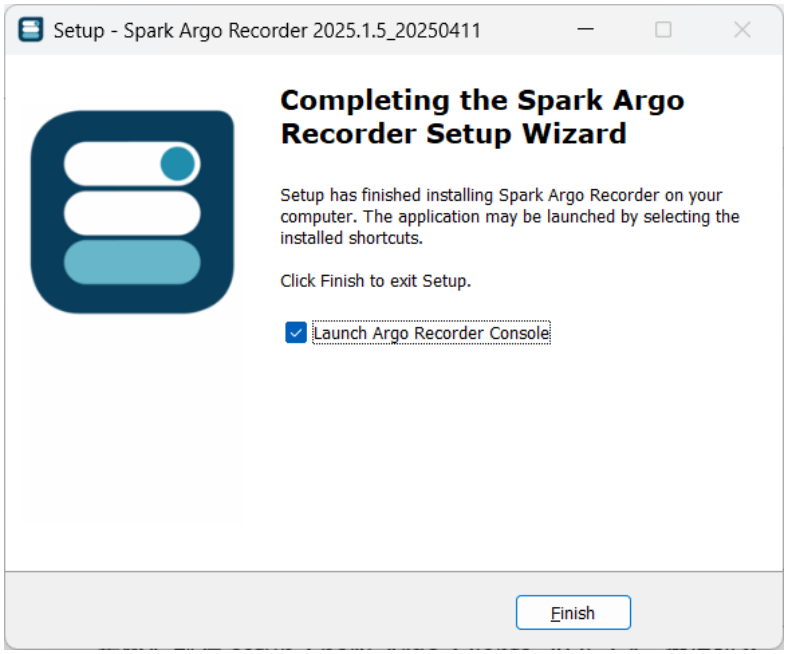
Step1 Run setup_Spark_Argo_Recorder_2025.1.4, select your preferred language, and proceed with the installation.



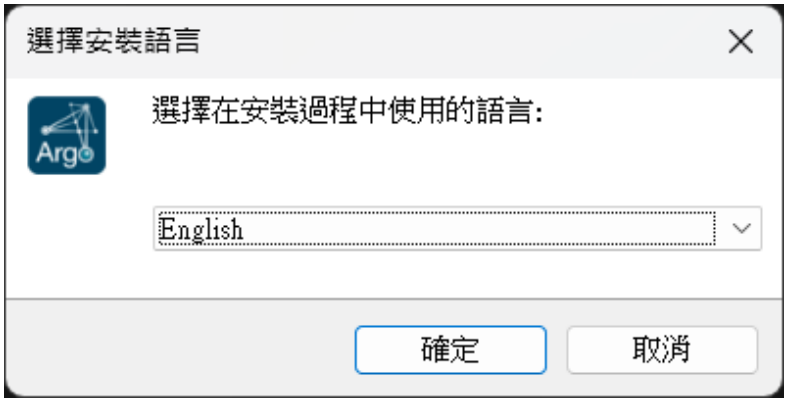
Step2 Click to install the selected components.



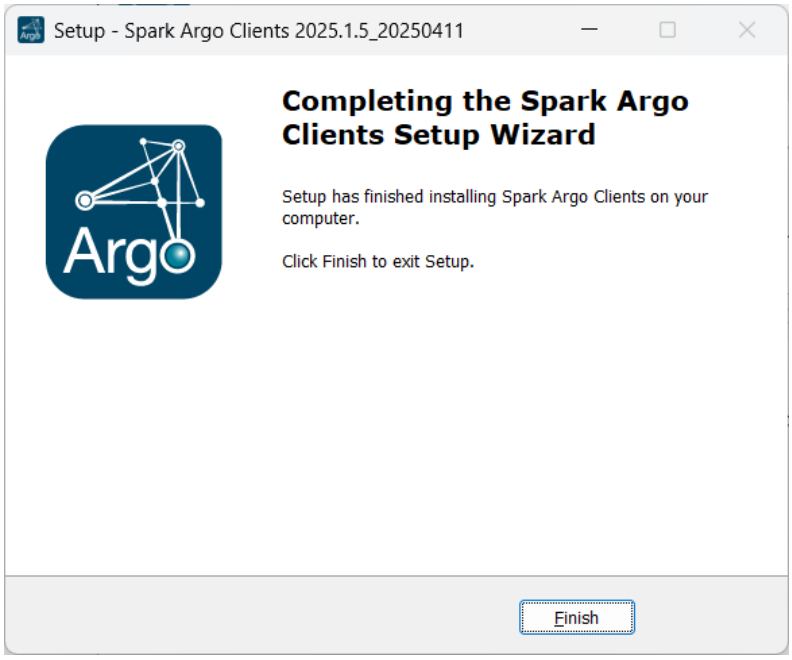
Step3 Click **[Finish]** to complete the Recorder installation.



Step4 Run setup_Spark_Argo_Clients_2025.1.4, select your language, and start the installation.



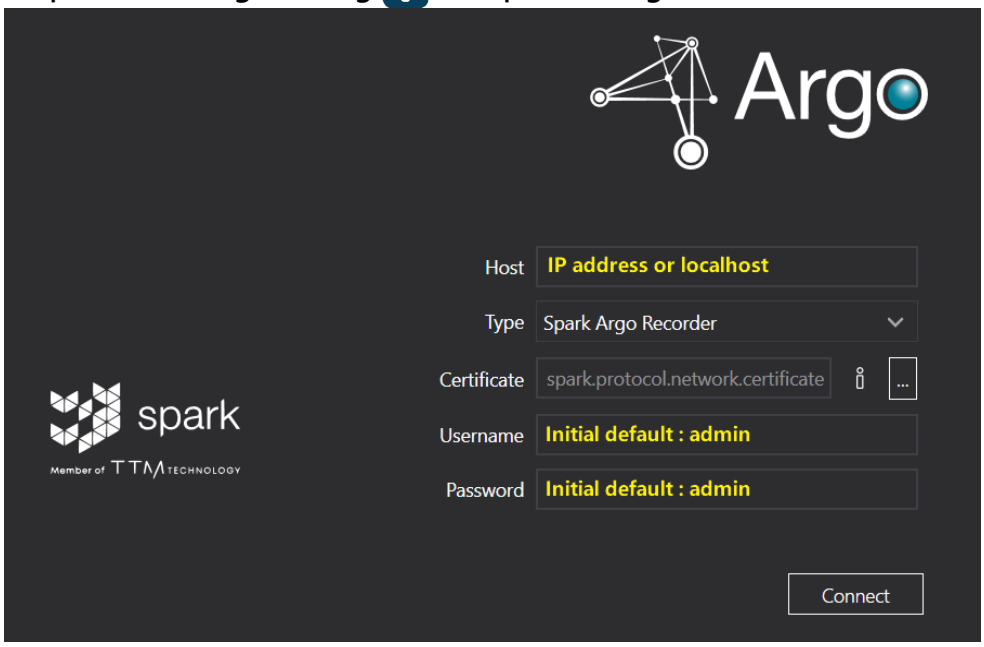
Step5 Click **[Finish]** to complete the Client installation.



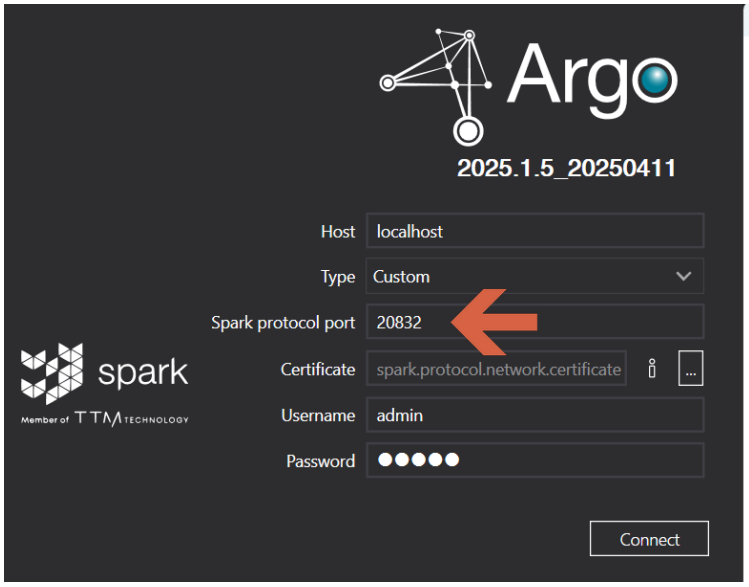
1.2 Config Login

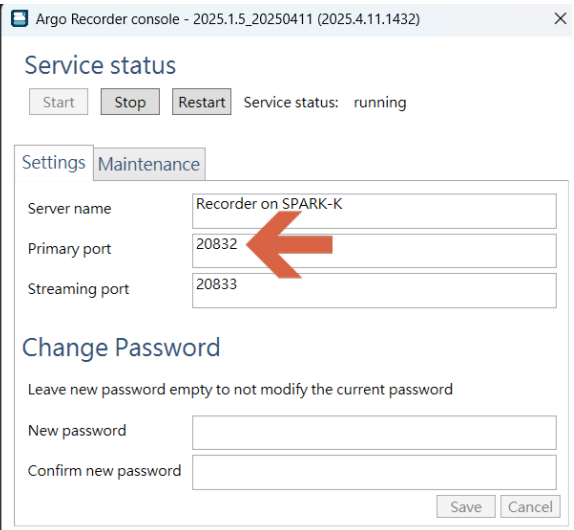
This section explains how to log into the system — the first step before configuration. Users must enter the correct login information to access the configuration interface.

Step1 Launch Argo Config to open the login screen and connect.



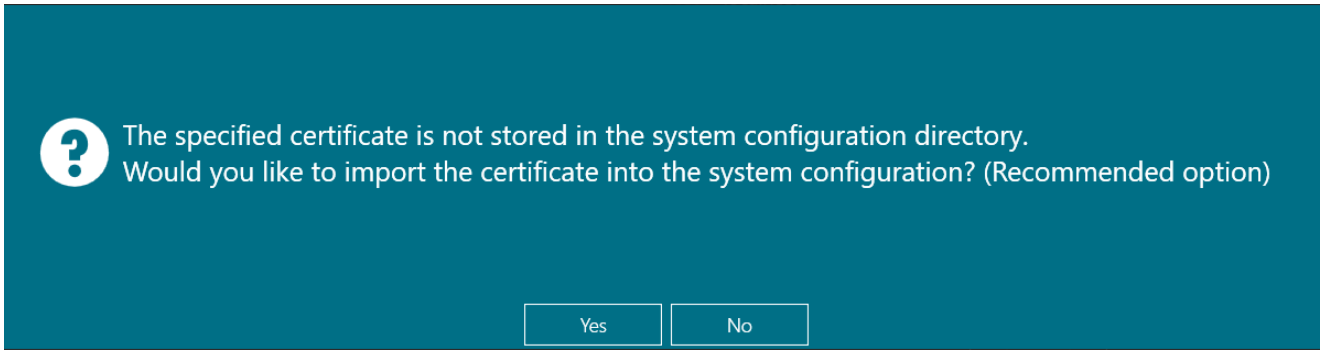
- Server: Enter the computer’ s **IP address** or **localhost**
- Type: Select the default Spark Argo Recorder. If choosing Protocol Port Setup, set the main port in Argo Recorder as shown below：



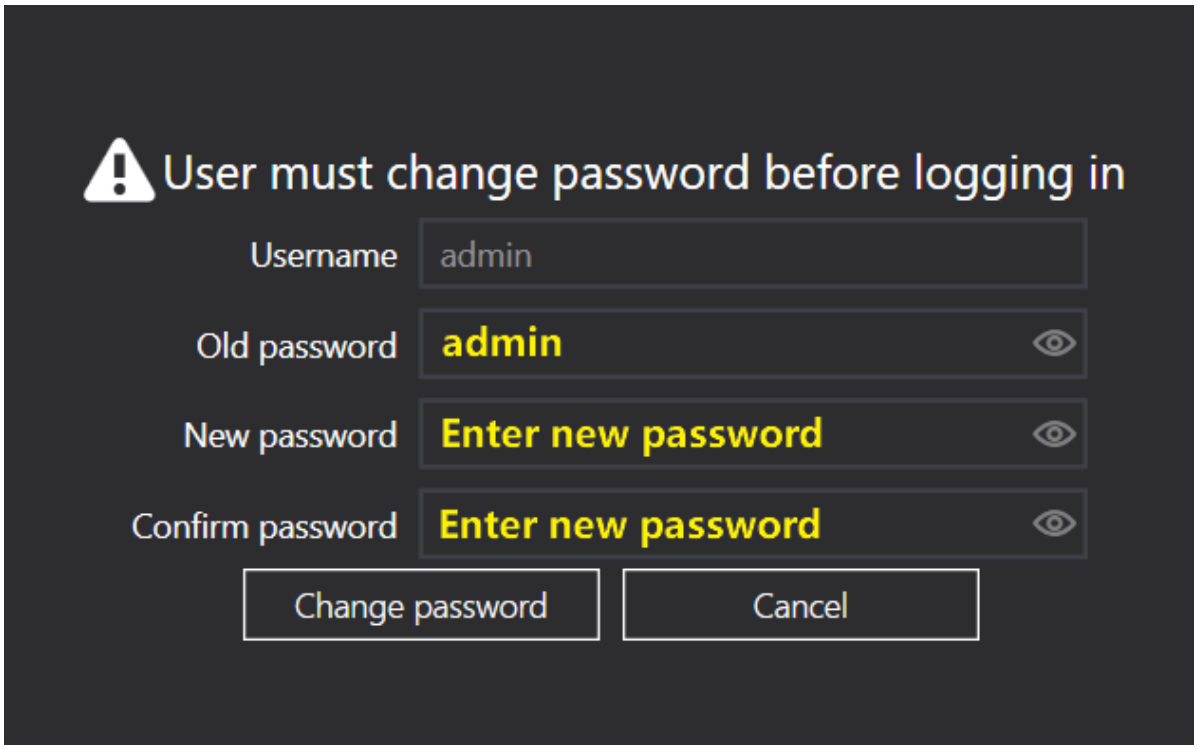


- **Username & Password: admin(Default)**

Step2 When prompted to import the certificate system, click [Yes].



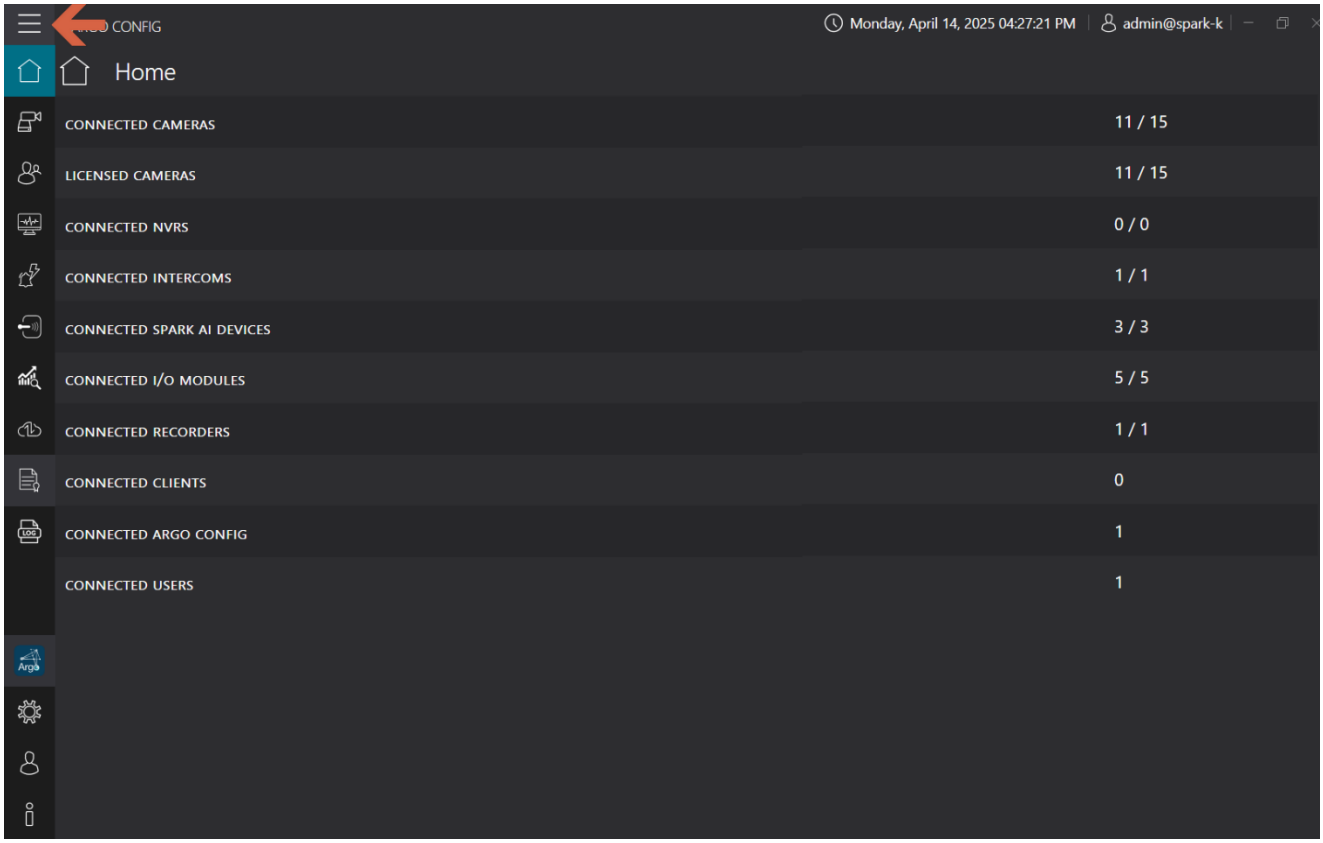
Step3 After logging in, you'll be required to change the password.



Step4 Once the password is updated, you will return to the login screen.

1.3 Argo Config Interface

This section provides a detailed guide on how to navigate the Argo configuration interface. Simple steps will help users familiarize themselves with the system setup and begin configuring devices and features.



- Click the [☰] to view the icon guide.

- Menu List：Devices/User Management/Health Doctor/Events and Alarms/Access Control/Analytics Data Collection/Backup and restore/Licensing/Logs/Argo Client/Options/Users/About

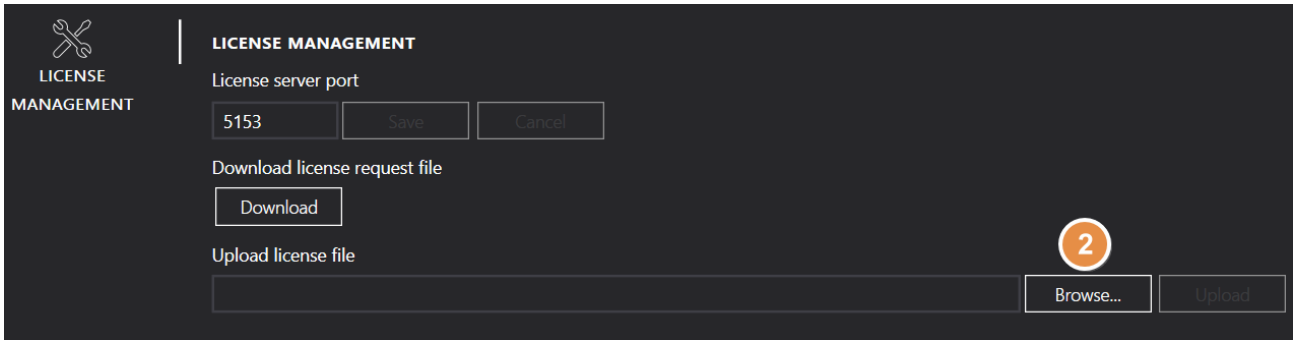
1.4 License Upload

This section explains how to upload the license file, a crucial step to enable all features of the Argo system.

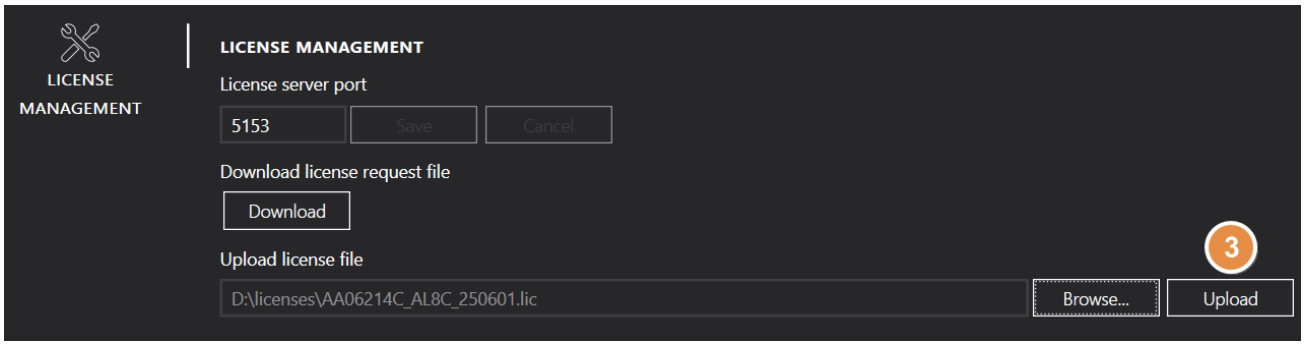
Note: Specific license keys are required for devices and AI features. To request a trial license key, contact us via LINE (@twspark).

Step1 Go to the License page.

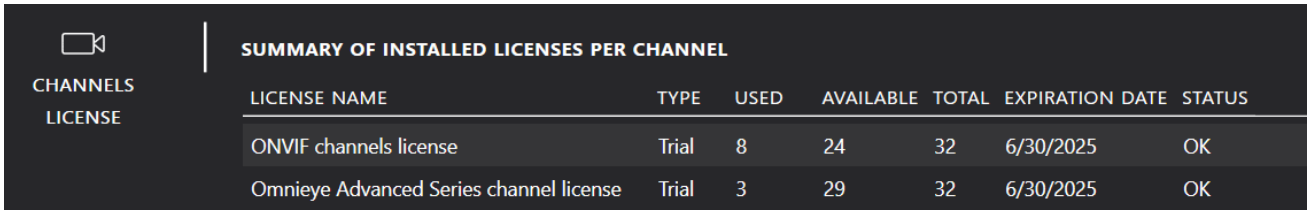
Step2 Click [Browse] and select the license file (choose based on the file location).



Step3 Click [Upload] to upload the license.



Step4 Once the license is successfully uploaded, you will see the license status.

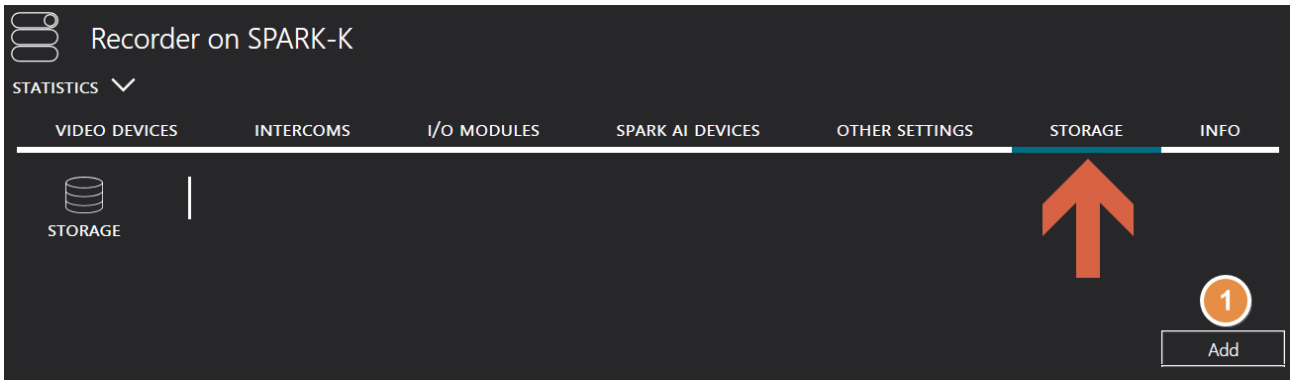


1.5 Storage Setup

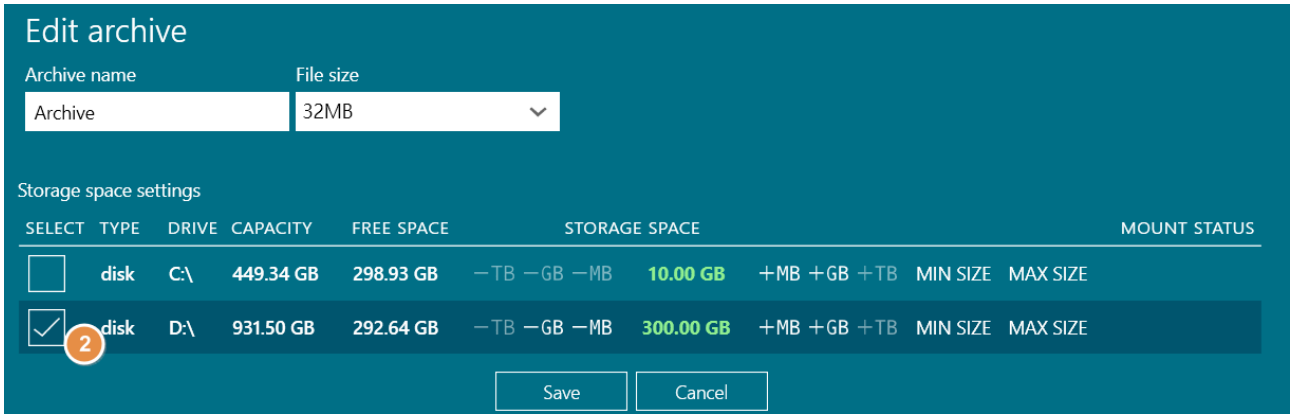
This section explains how to configure storage space and select the appropriate location to store recorded data. The recording feature requires proper storage setup.

Step1 Select Devices 

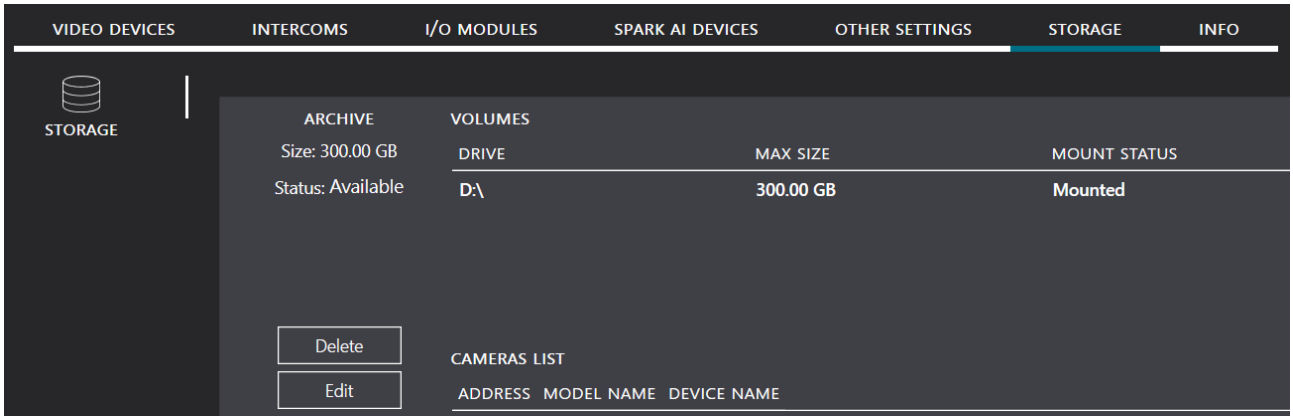
, then choose Storage and click [Add].



Step2 Select the hard disk slot, adjust the Storage to the desired recording space, and click [Save].



Step3 Once completed, you can view the storage status.

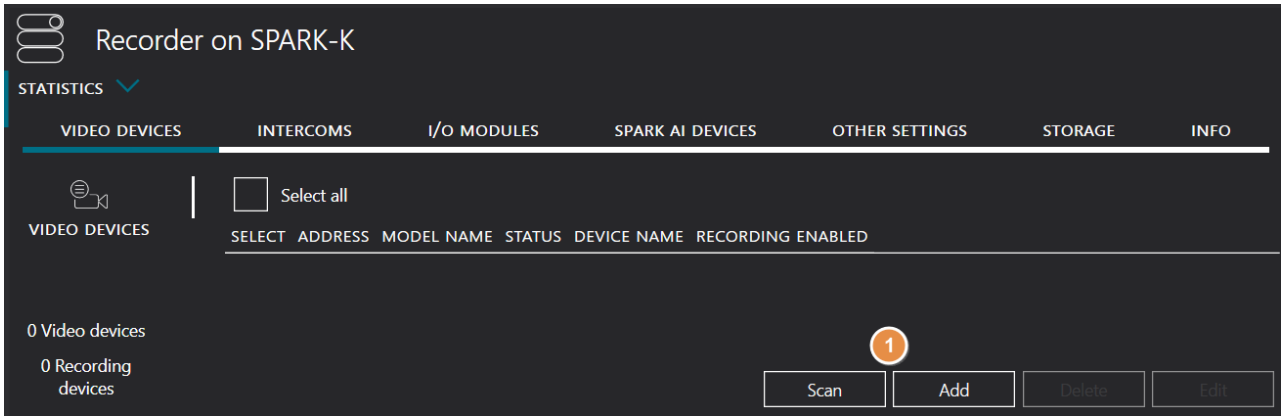


1.6 Add Camera Device

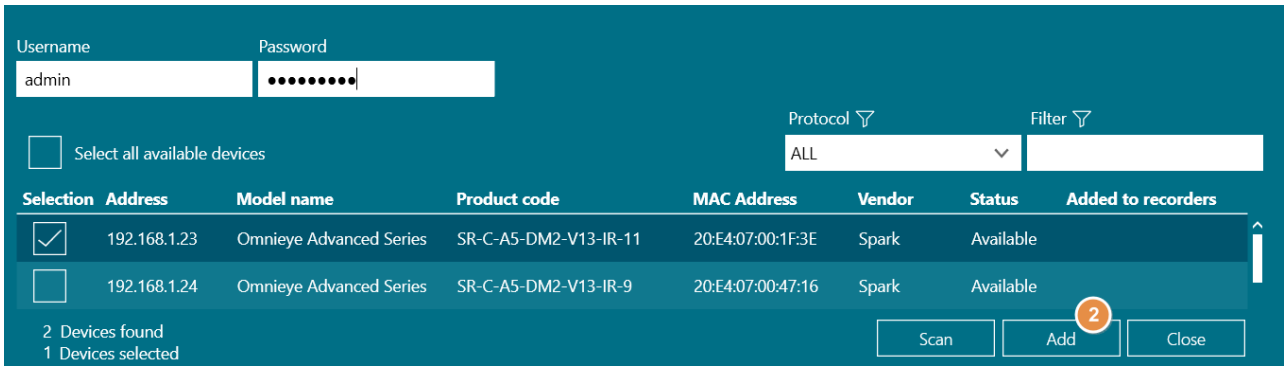
This section explains how to add a camera device to the Argo system, helping users successfully connect physical devices and enable video surveillance.

Step1 Go to Devices 

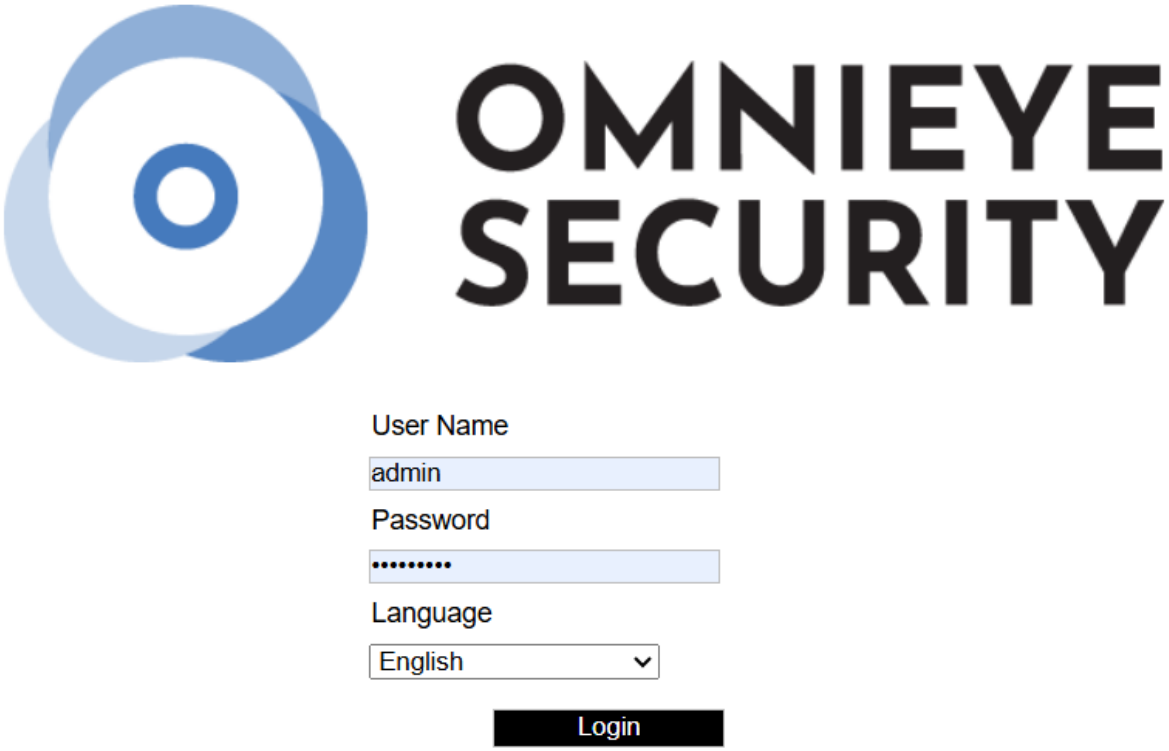
, select Video Devices, and click [Scan] (to auto-search devices) or [Add] (to manually add a device).



Step2 Select the device to add, then enter the camera's Device Username and Password and click [Add].

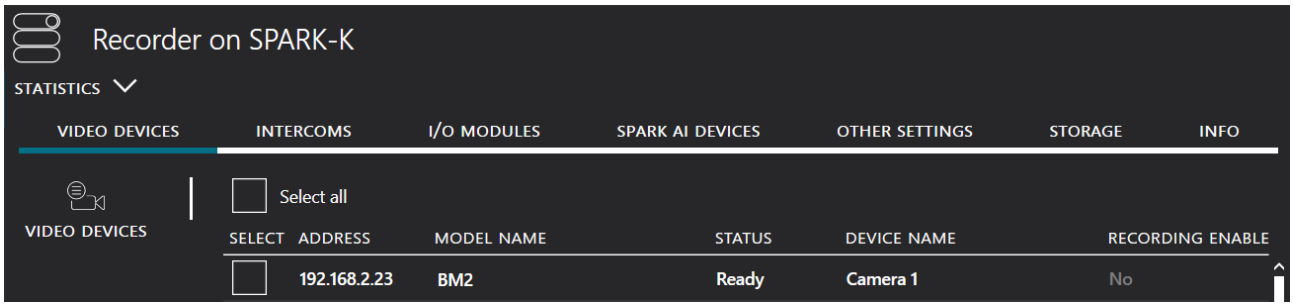


- Set the username and password based on your camera device.
- For Argo, use the Omnieye camera device’ s username and password.



- Enter the camera’ s IP address in the web interface to configure.

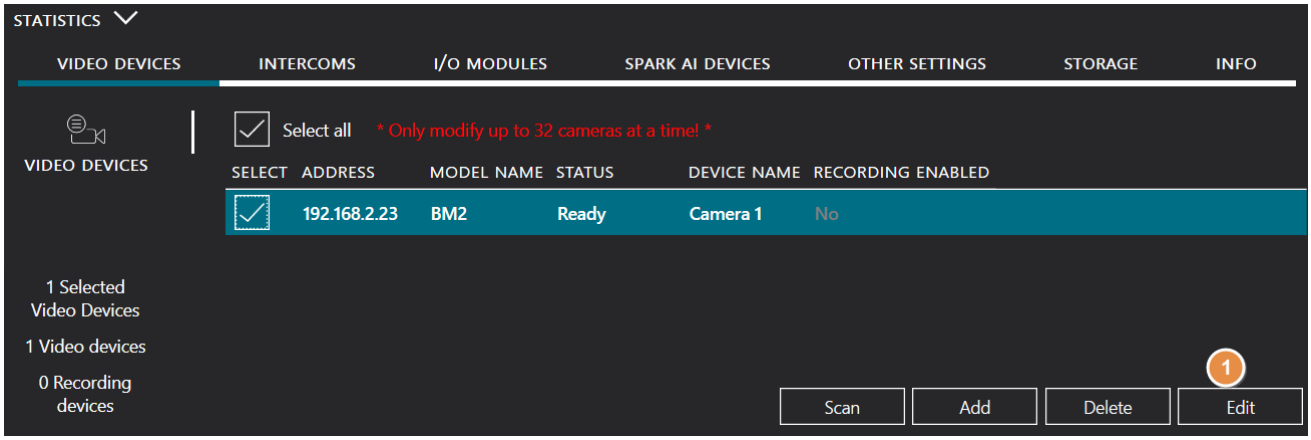
Step3 Once completed, the status will show as Available.



1.7 Enable Camera Recording

This section explains how to enable the camera recording feature. Once set up, the system will start recording video data from the camera, ensuring continuous surveillance.

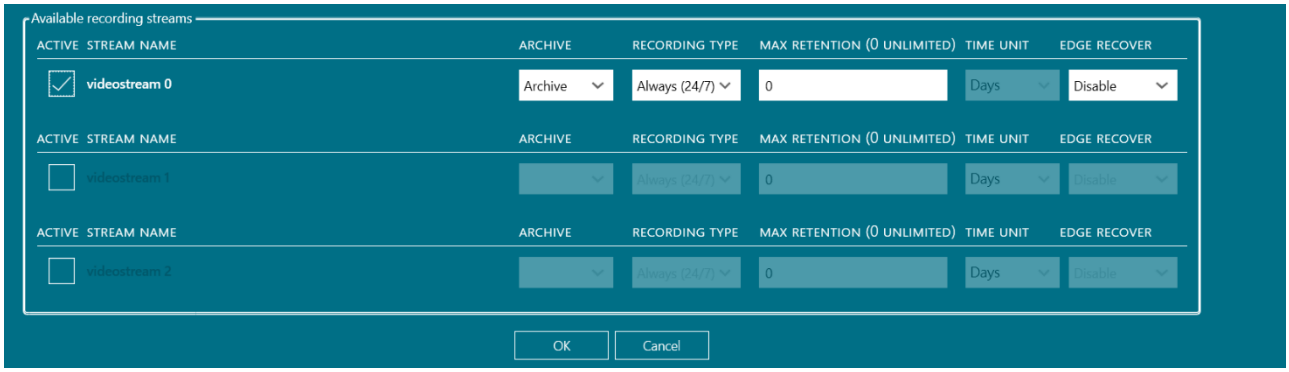
Step1 Select the device for recording, then click [Edit].



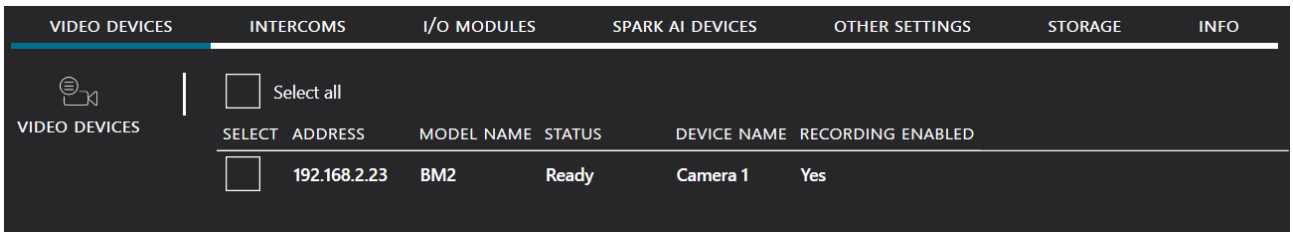
Step2 In the streaming section, check the desired recording streams and click [OK] to save.

- **For initial setup, use the default settings (as shown below). If the camera supports Disconnect Recovery, enable this feature (it is disabled by default).**

  Note: Disconnect Recovery allows the system to automatically restore lost footage after the camera reconnects.



Step3 Once completed, the recording status will show as Enabled.

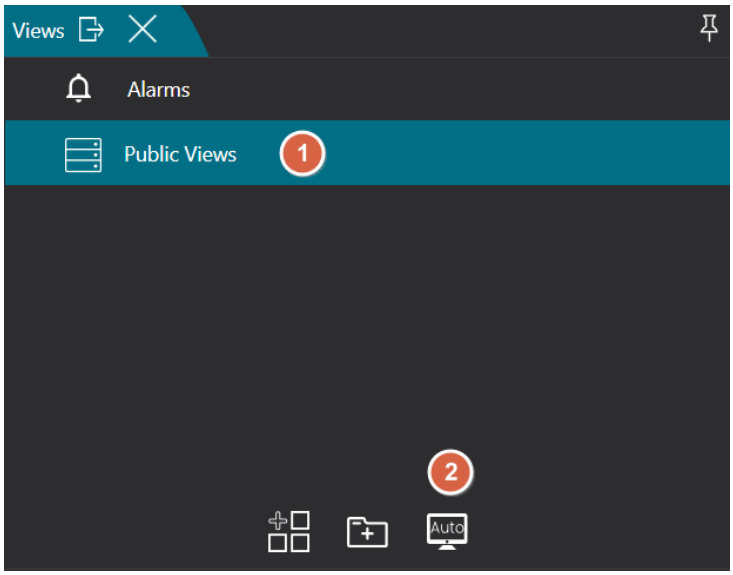


1.8 Client Real-Time Layout (Auto)

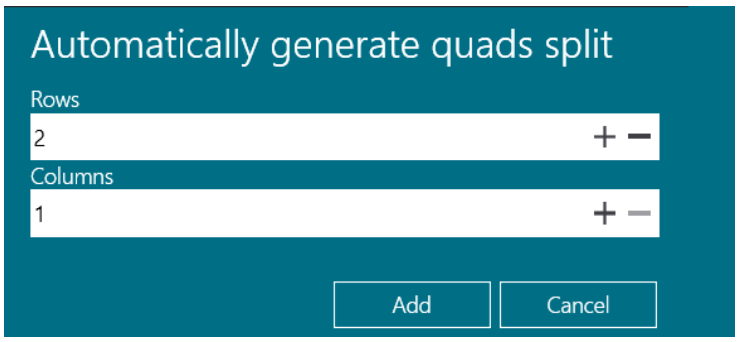
This section explains how to set up the automatic Client layout and camera arrangement. The system will automatically adjust the camera feeds based on the number of devices and the user’ s chosen layout without needing to manually add cameras.

Step1 Click [Public Views]➔ select [Auto]

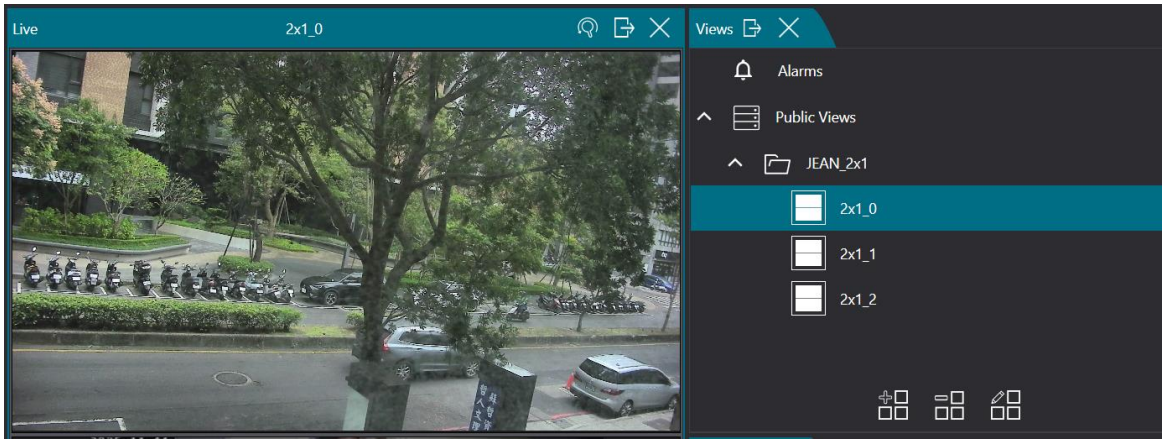
(After completing camera setup in Config, the Client will guide the user through a quick setup on first login.)



Step2 Adjust the screen layout by changing the rows (horizontal) and columns (vertical), then click [add] to confirm



Step3 Click on the divided screen icons to view the live feed.

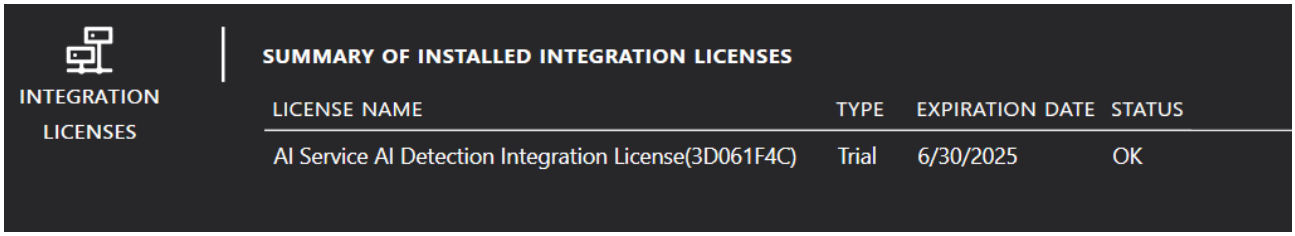


2. HOW TO ENABLE AI DEVICES

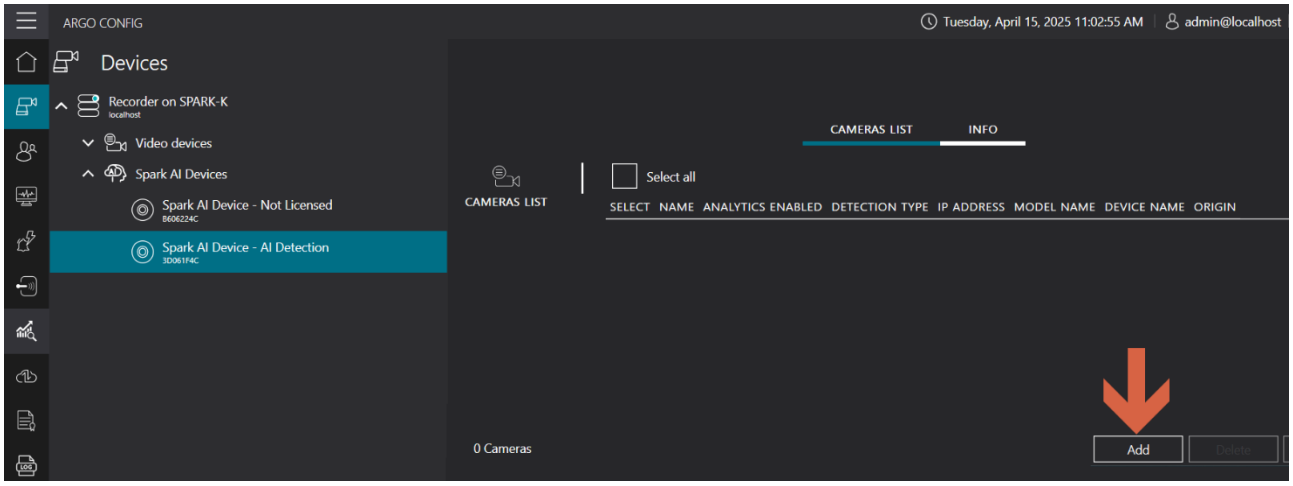
This section explains how to enable Argo's AI devices. To use AI devices, the system must have a valid license (contact Spark sales). These features improve monitoring efficiency and enable data analysis and event processing.

2.1 How to Use Human/Vehicle (Object) Detection

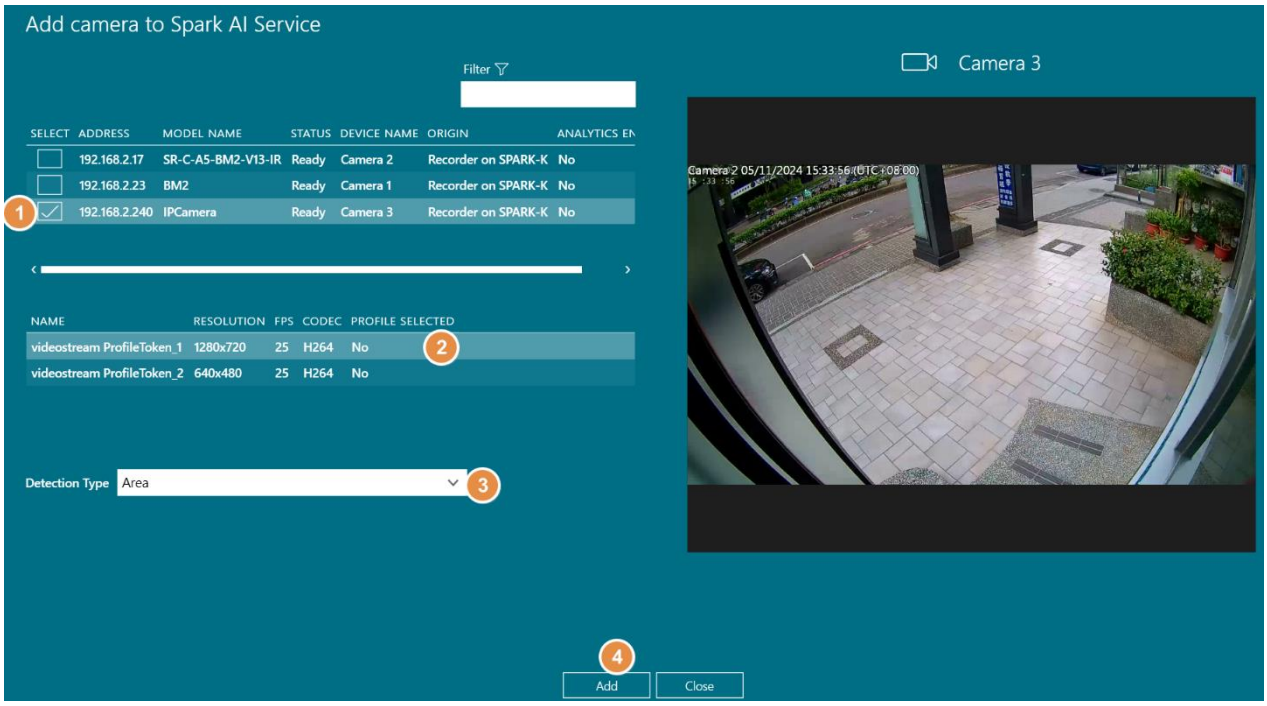
Step1 Config➔ click the License Key page on the left menu➔check if the license status is valid. If there' s no license, import one first



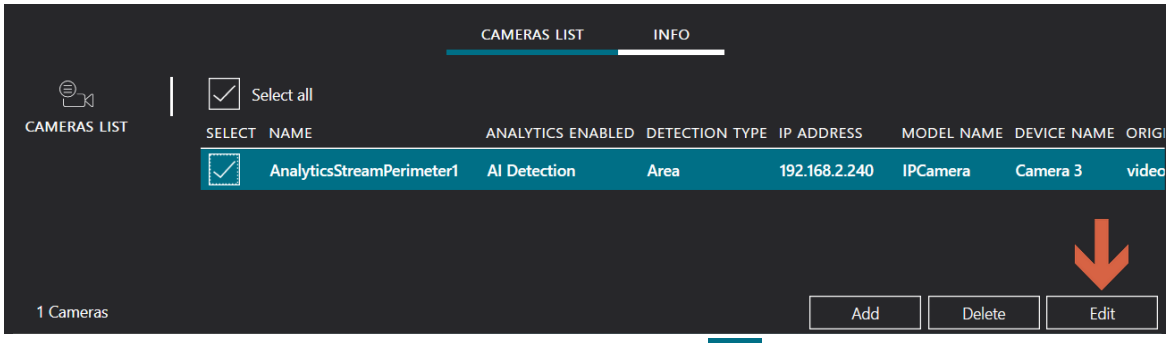
Step2 In the Device section➔ click the SPARK AI device under SPARK AI Devices -AI Detection➔ then click [Add] to proceed.



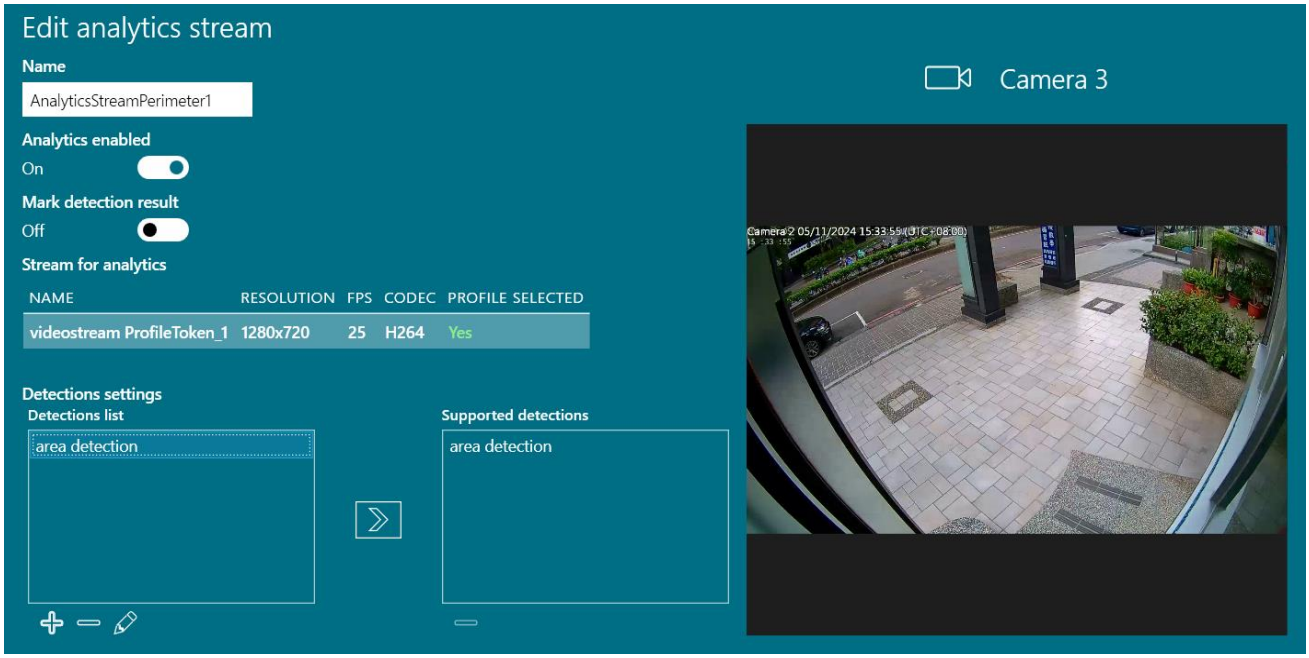
Step3 Select the camera device➔ choose the analysis stream➔ set the detection type to Area➔ click [Add] to proceed



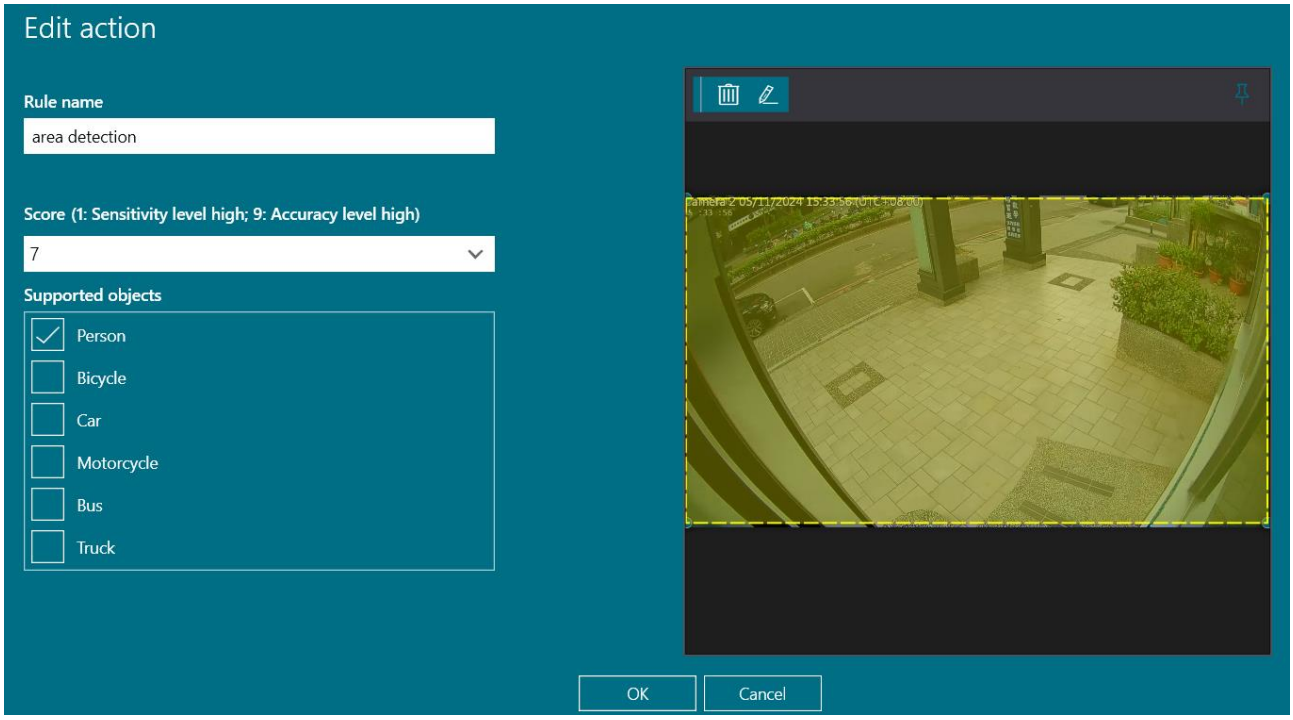
Step4 Click [Edit] to edit the analysis stream.



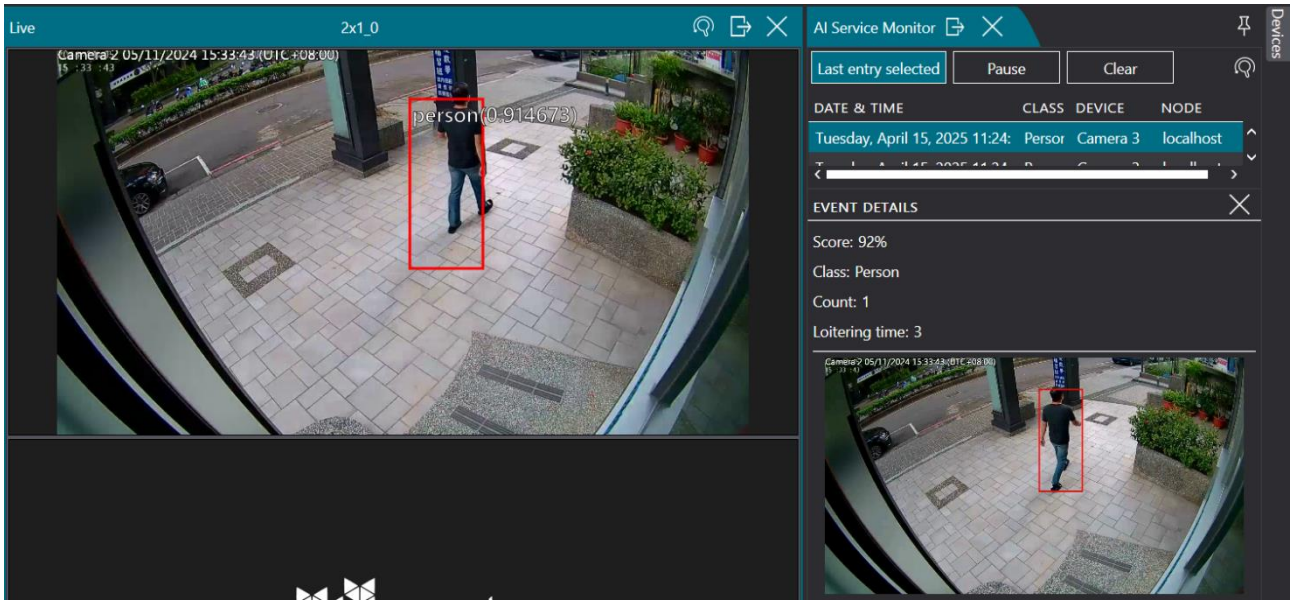
Step5 Edit the analysis stream name, then click Edi to define the detection area.



Step6 Set the detection area, then click [OK] to save.



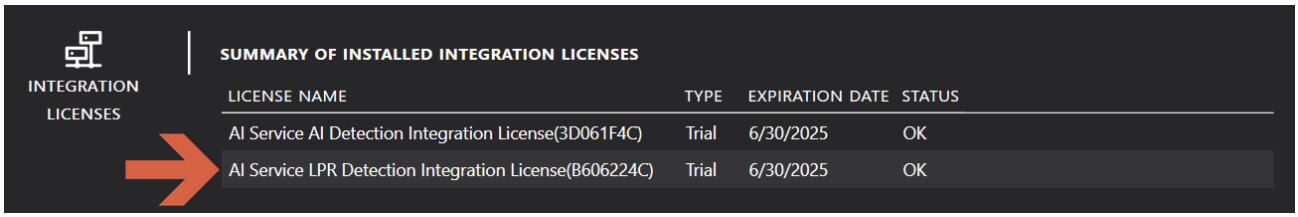
Step7 Open the Client live window and AI service monitoring window to view the detection results.



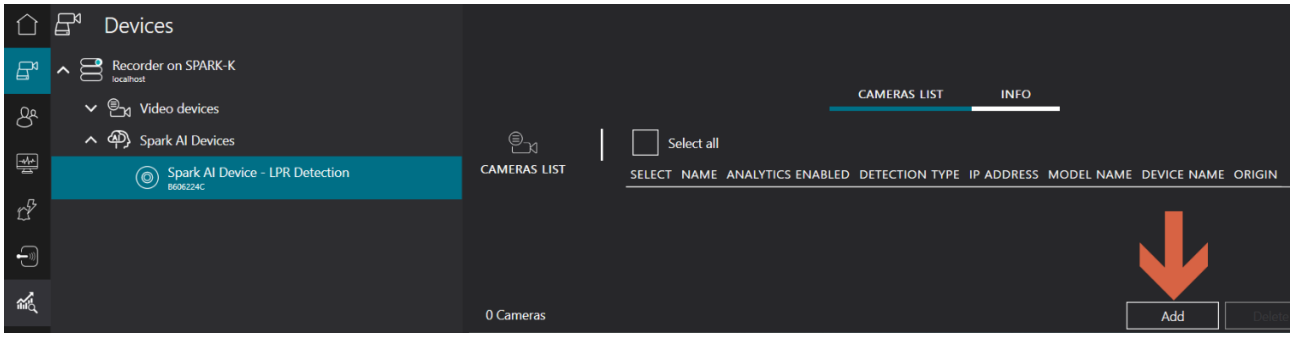
2.2 How to Use Taiwan License Plate detection

The license plate recognition feature identifies vehicle entries and exits, linking license plates to events for automated management. It enhances efficiency and, with access control, restricts unauthorized vehicle access for better security.

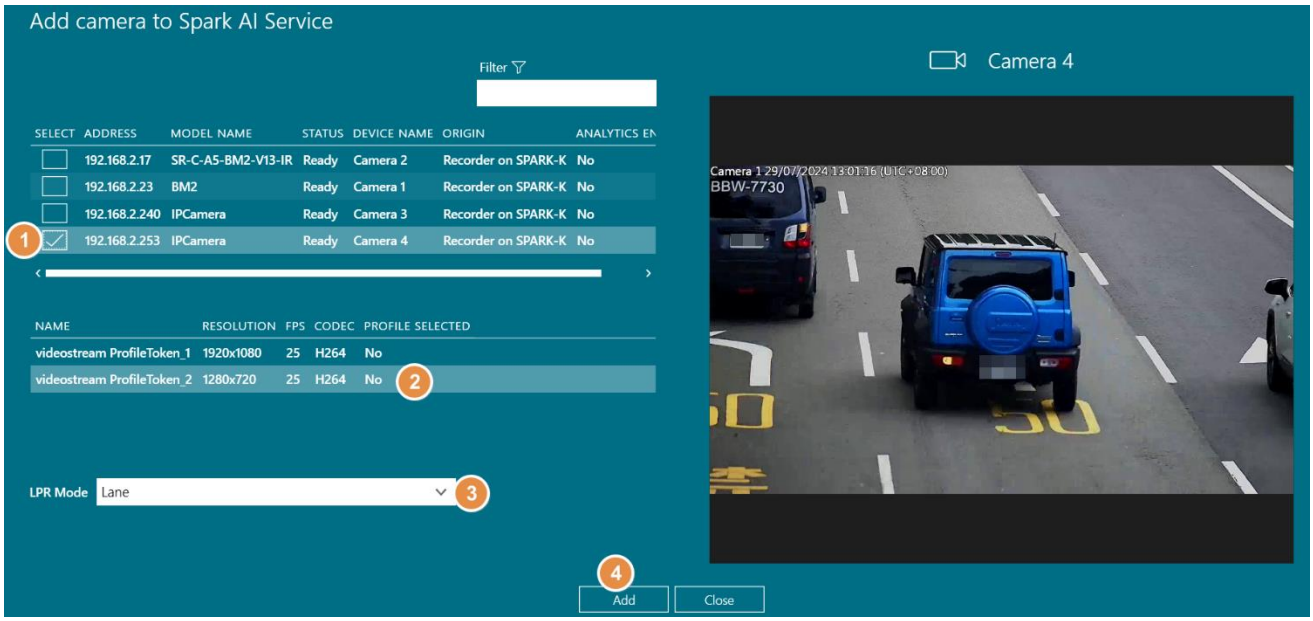
Step1 Config→ click the License Key page on the left menu→ check if the license status is valid. If there' s no license, import one first.



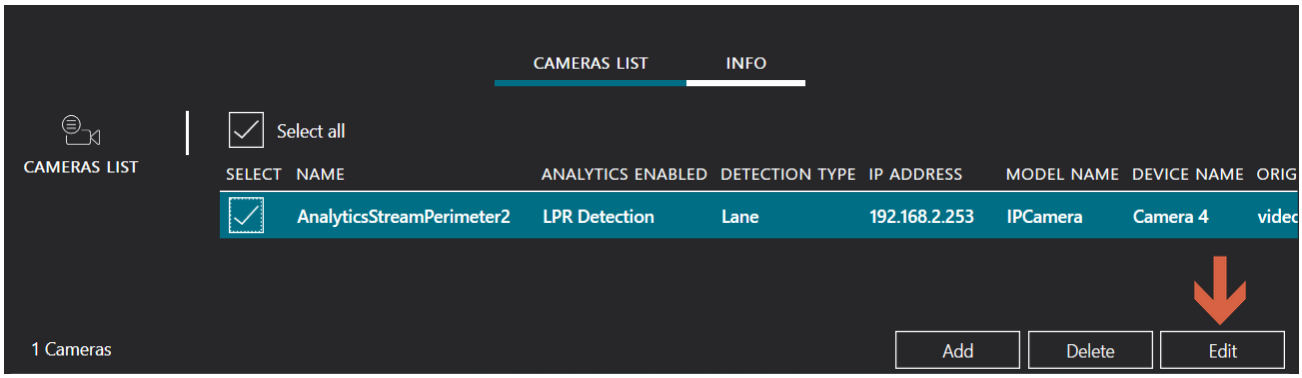
Step2 In the Device section, click SPARK AI Devices, then choose Device - License Plate detection, and click Add to start configuring the analysis stream.



Step3 Select the camera device➔ choose the analysis stream➔ set the mode to Lane or Parking ➔ and click [Add] to complete the setup

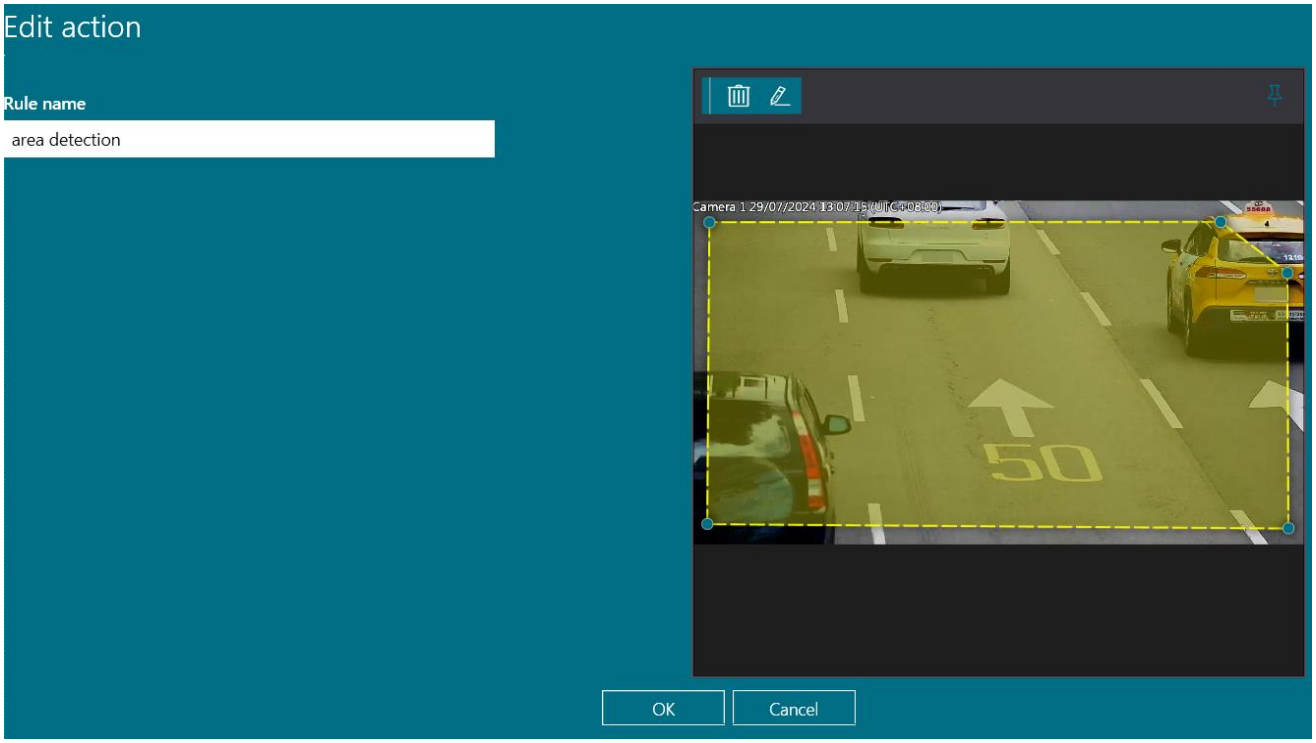


Step4 Click [Edit] to modify the intelligent analysis stream.

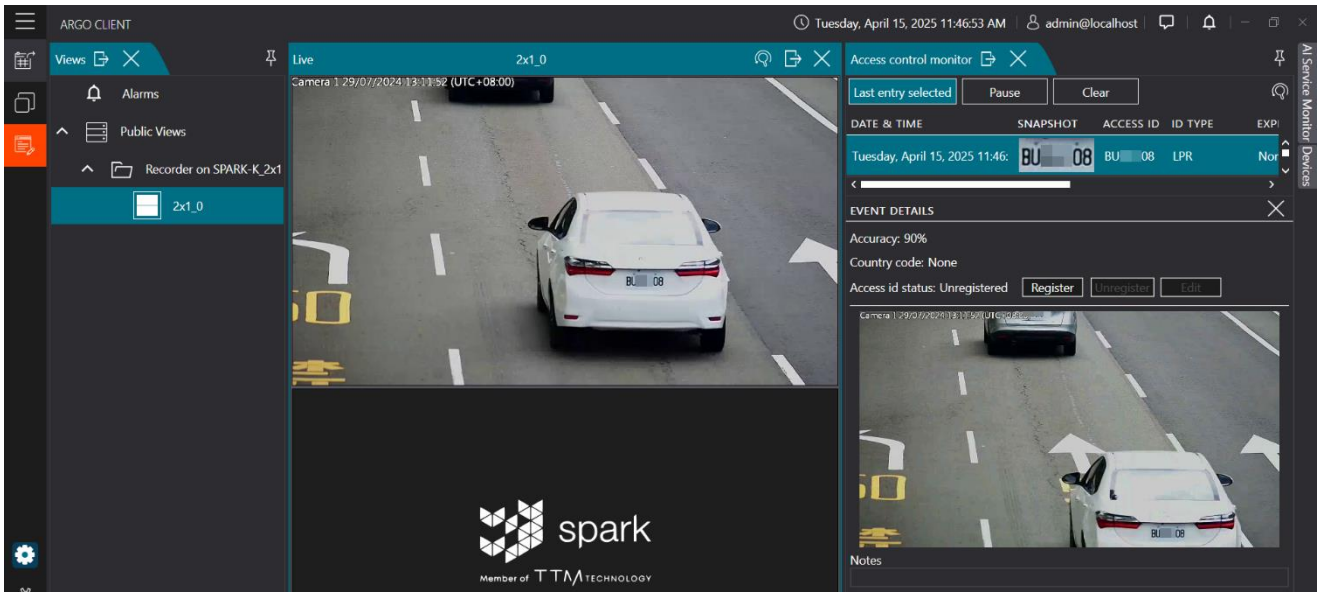


Step5 Edit the stream name and click Edi to define the detection area.

Step6 Click Edit to draw or delete the detection area, then click [OK] to finalize the configuration.

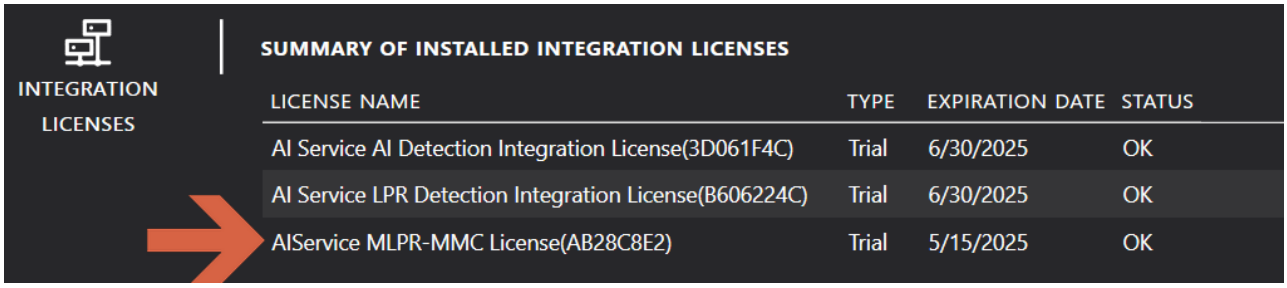


Step7 Open the Client real-time window and access control monitor window to view detection results.

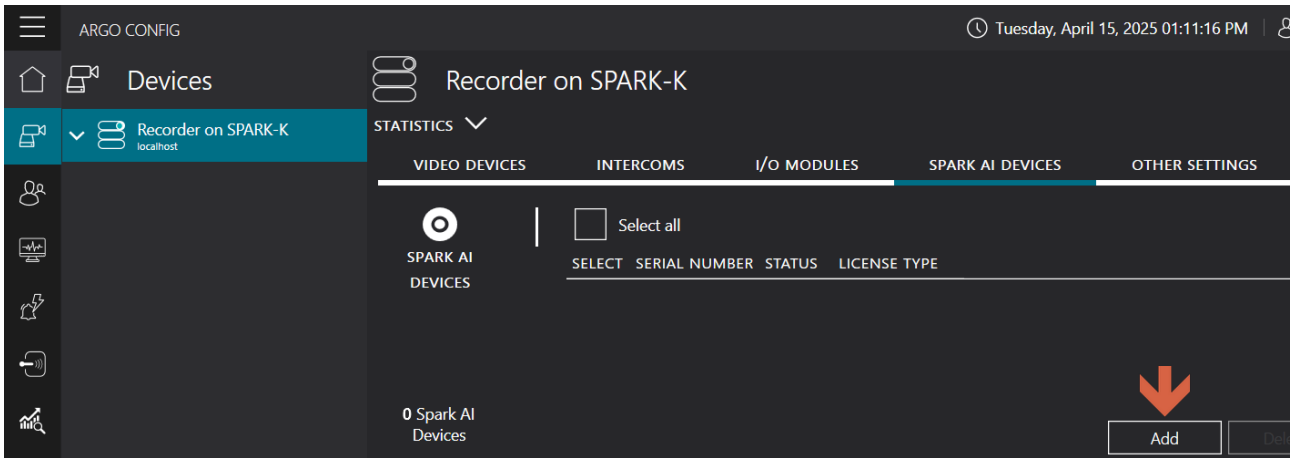


2.3 How to Use MLPR Detection

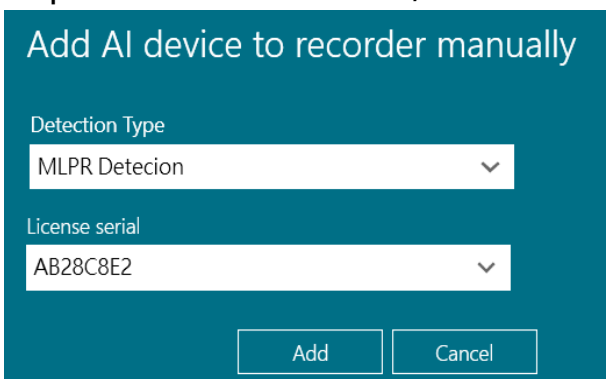
Step1 Config→ click the License Key page on the left menu→check if the license status is valid. If there’ s no license, import one first.



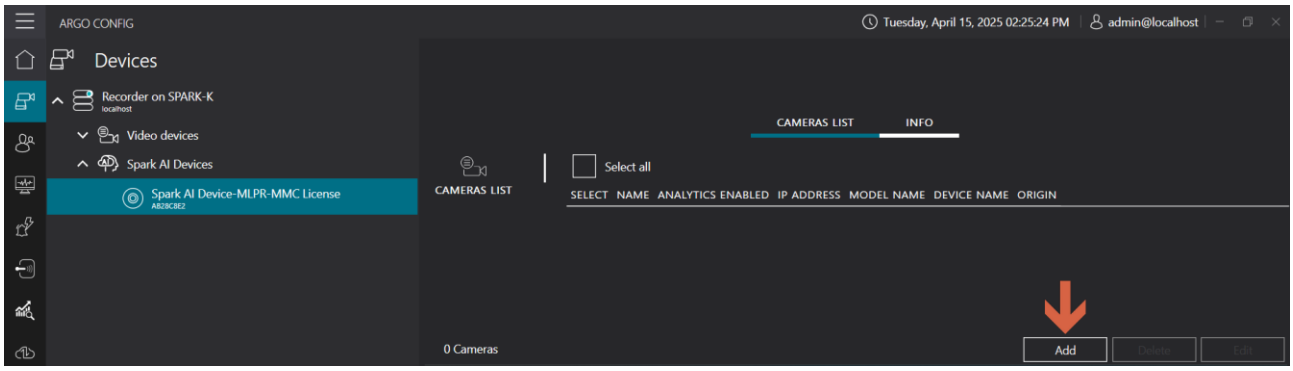
Step2 In the Device section, click SPARK AI Devices, then click [Add].



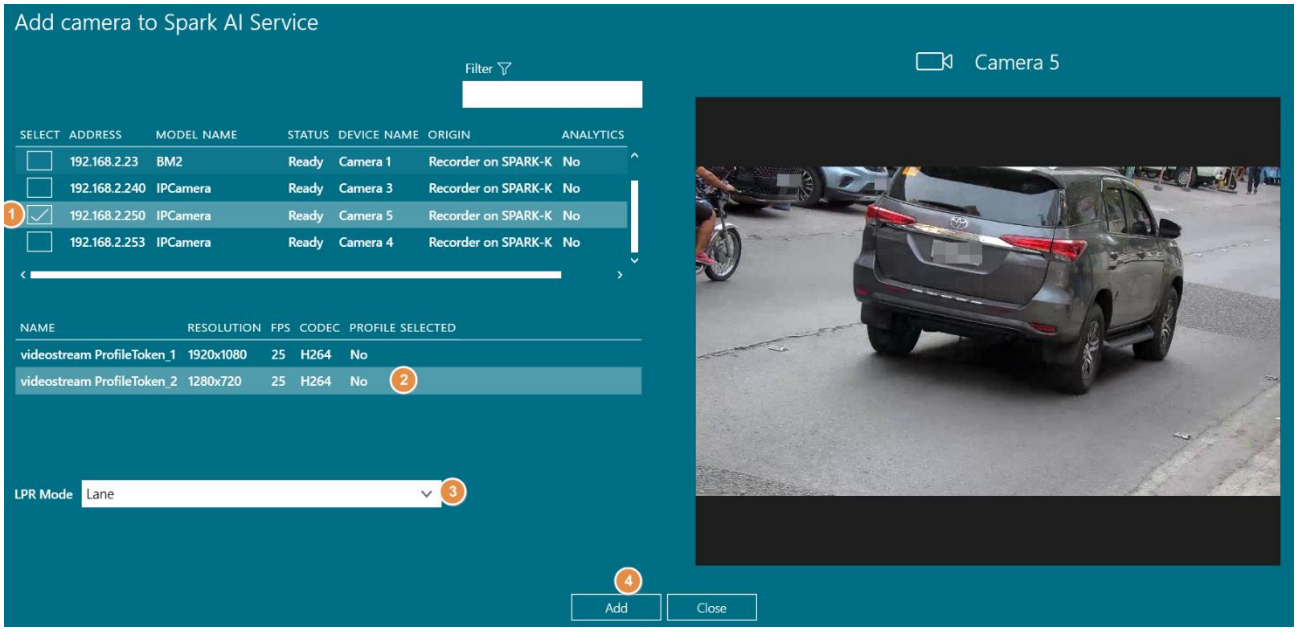
Step3 Select MLPR Detection, and choose the license serial number



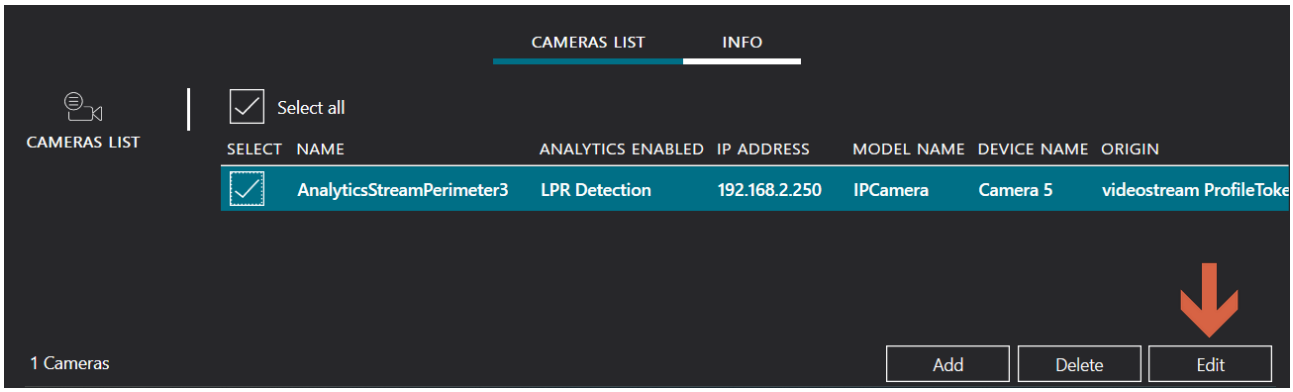
Step4 Select the camera device



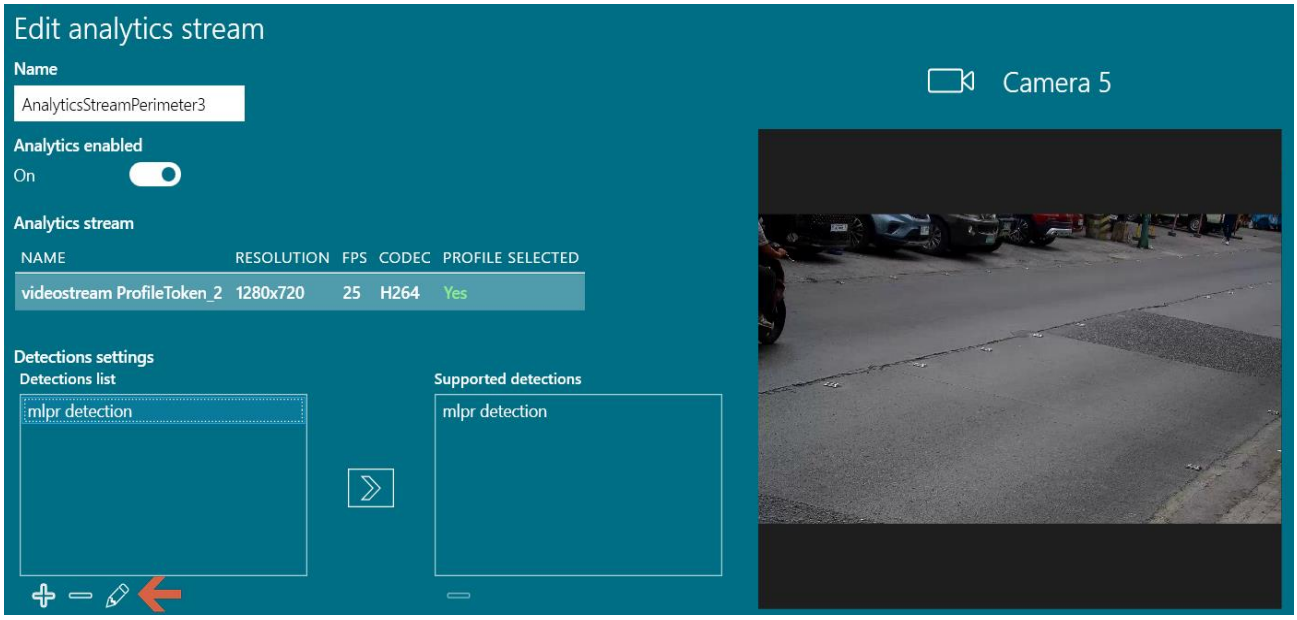
Step5 Choose the analysis stream, set the mode to Lane or Parking, and click [Add] to complete the setup.



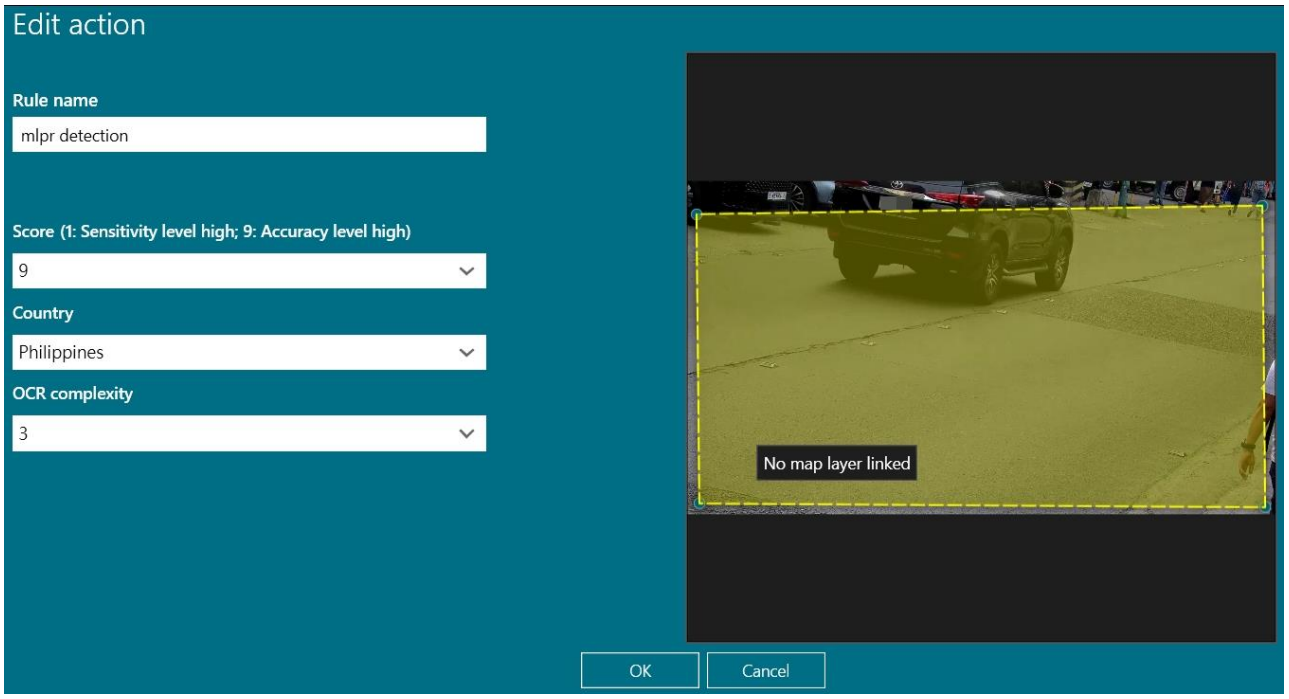
Step6 Click [Edit] to edit the analysis stream.



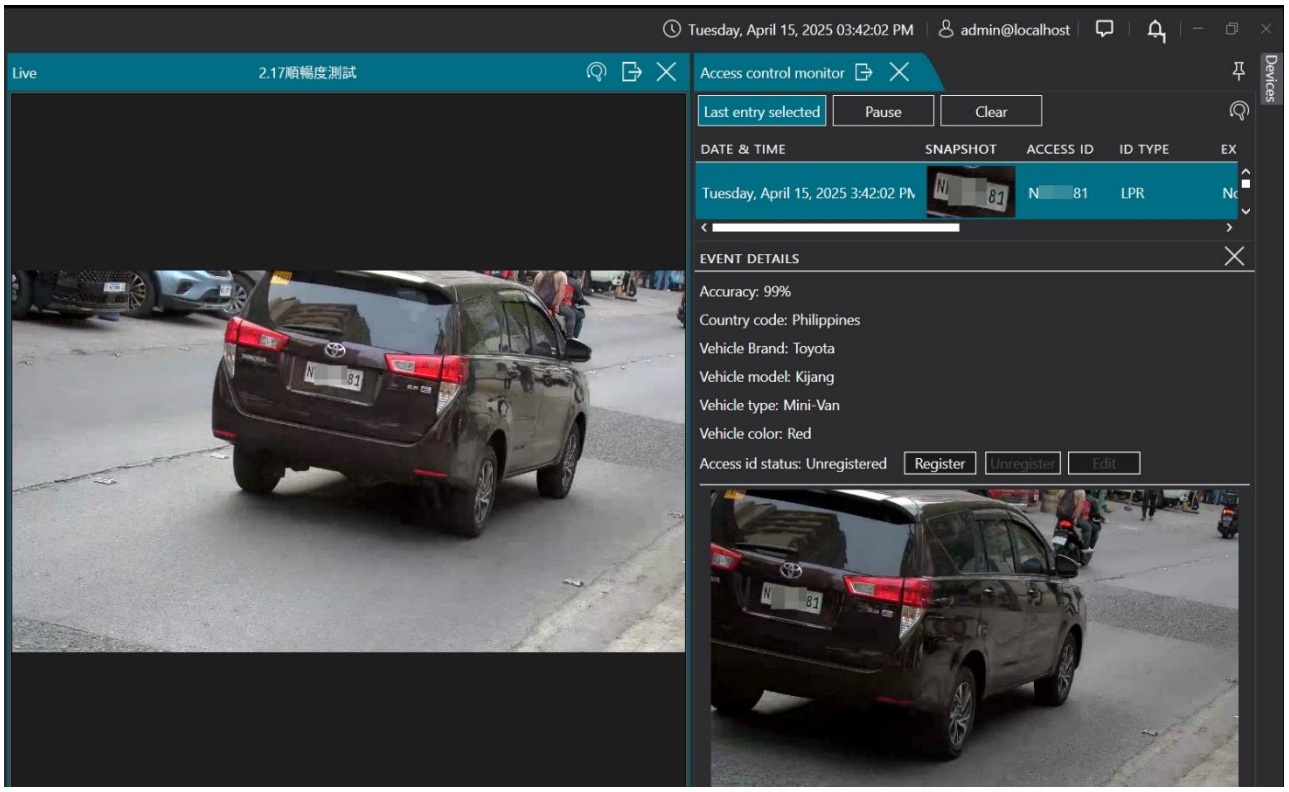
Step7 Edit the stream name and click Edit to define the detection area.



Step8 Click Edit to draw or delete the detection area, then click [OK] to finalize the configuration.



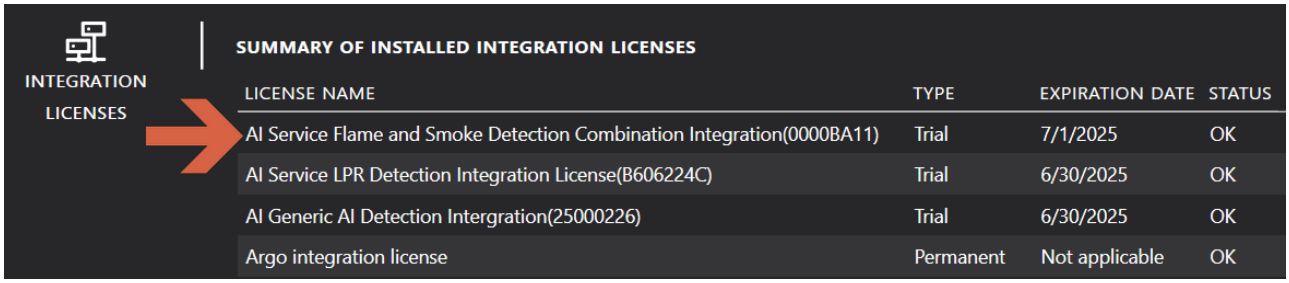
Step9 Open the Client real-time window and access control monitor window to view detection results.



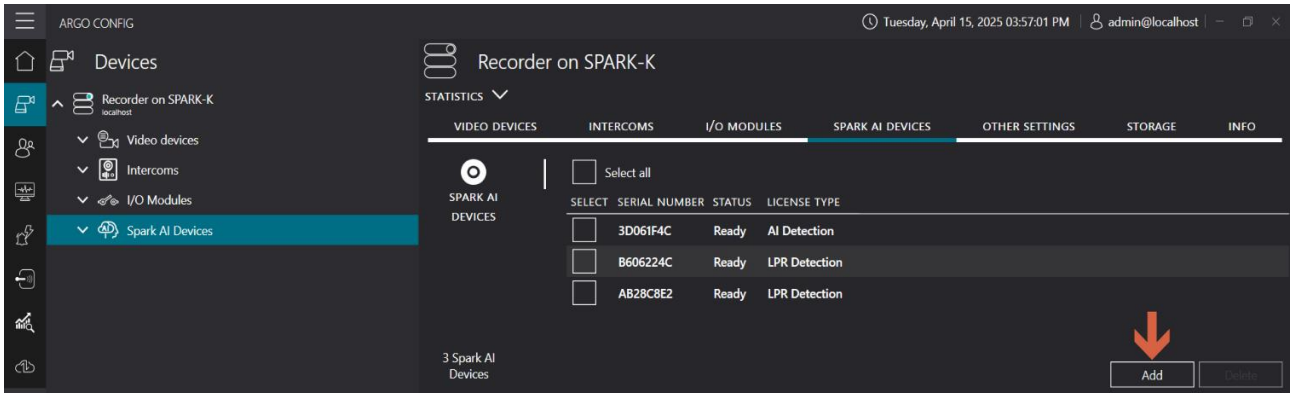
2.4How to Use Fire and Smoke Detection

The fire and smoke detection feature improves safety by detecting potential fire hazards. Once fire or smoke is detected, the system immediately alerts, reducing accident risks.

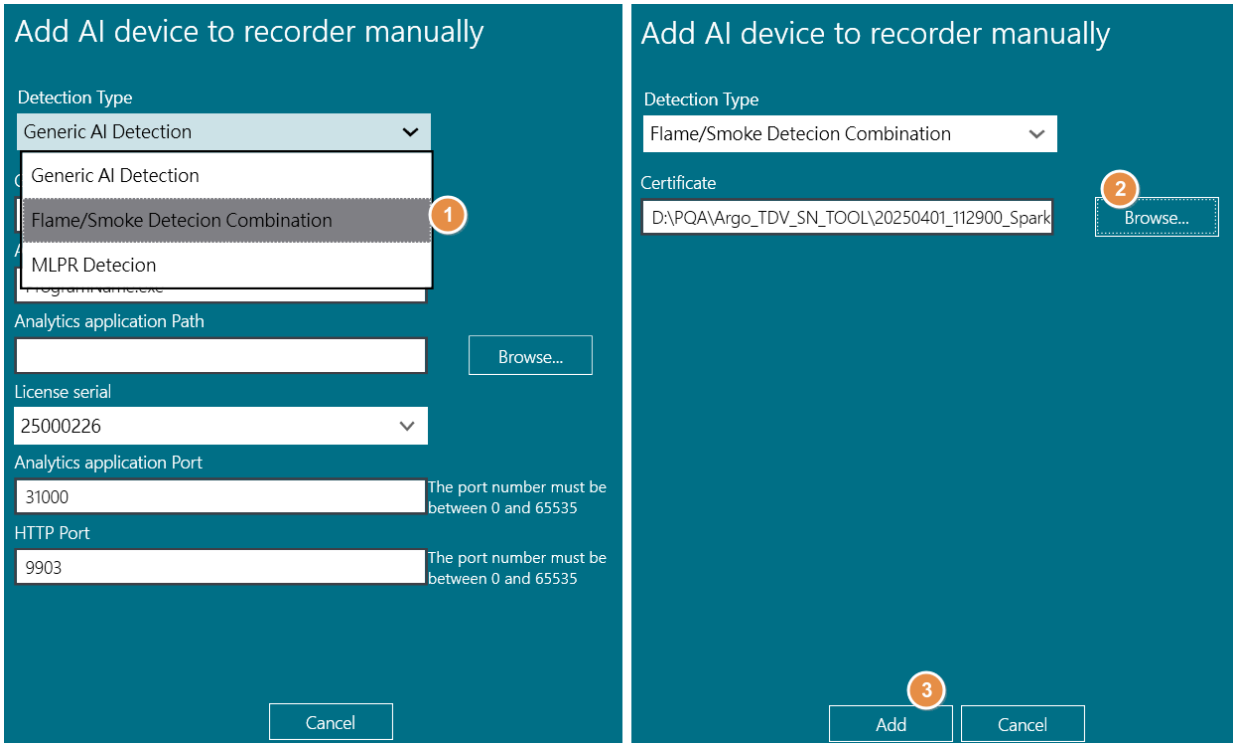
Step1 Config→ click the License Key page on the left menu→check if the license status is valid. If there' s no license, import one first.



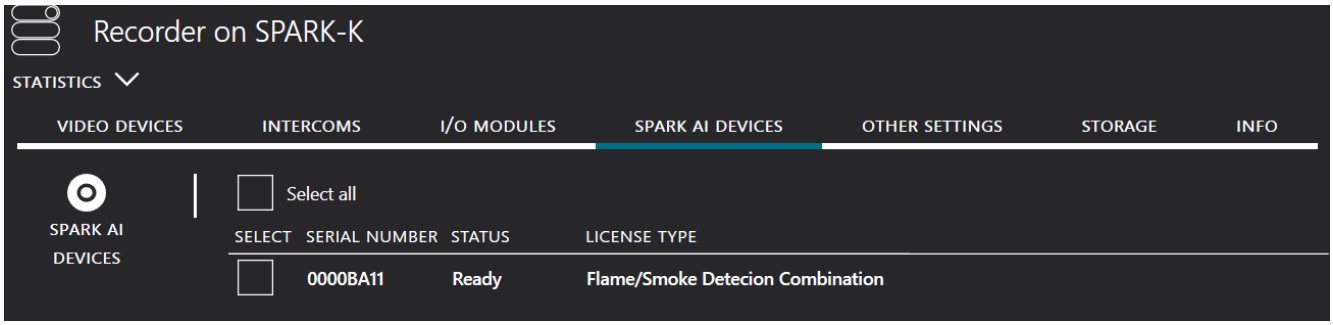
Step2 Select SPARK AI device on the device page and click [Add].



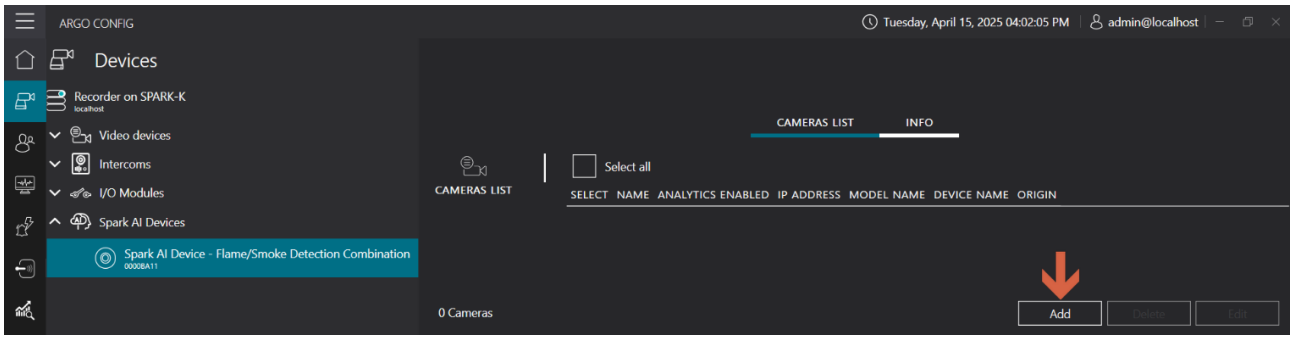
Step3 Choose flame / smoke detection→browse and import the certificate→click [Add].



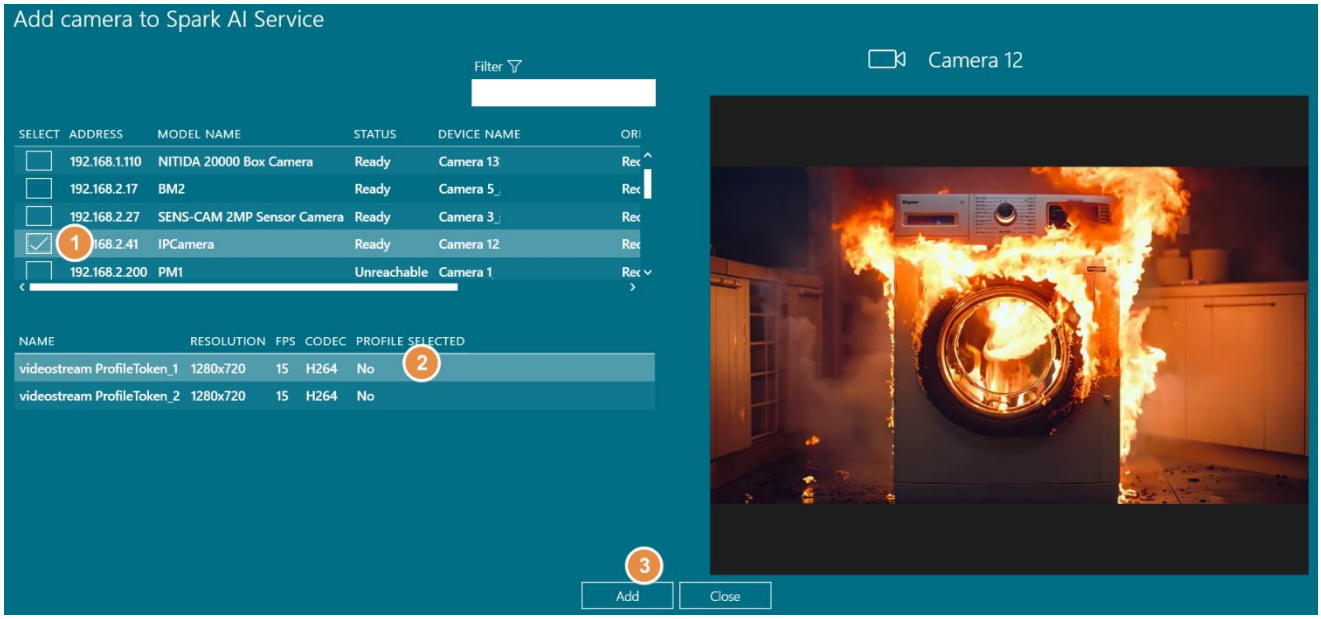
Step4 Check the status of Flame / Smoke detection under SPARK AI device.



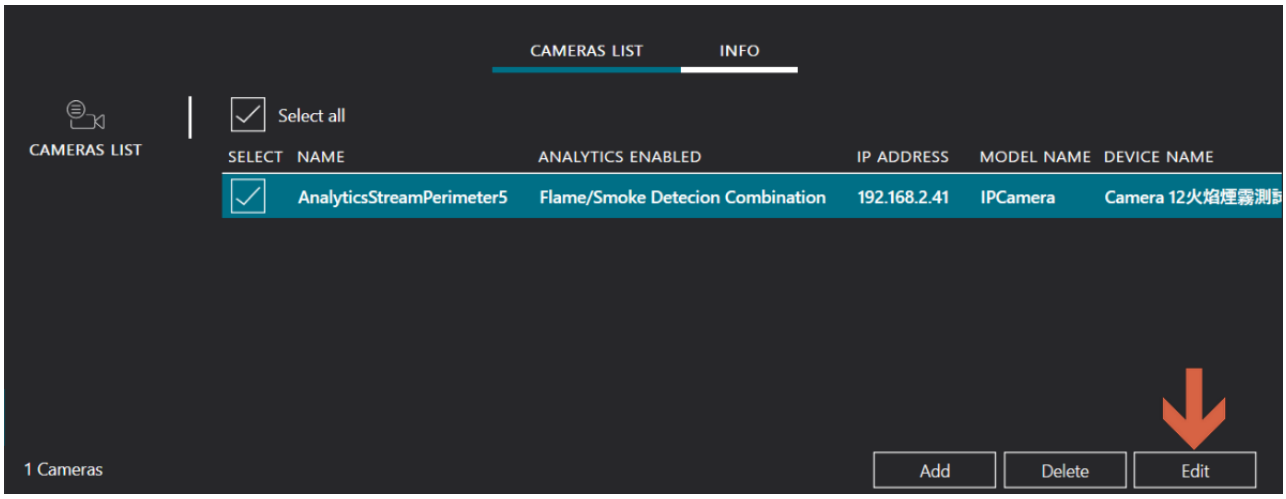
Step5 Expand Recorder on node and select SPARK AI device➔ Flame / Smoke Detection, then click [Add].



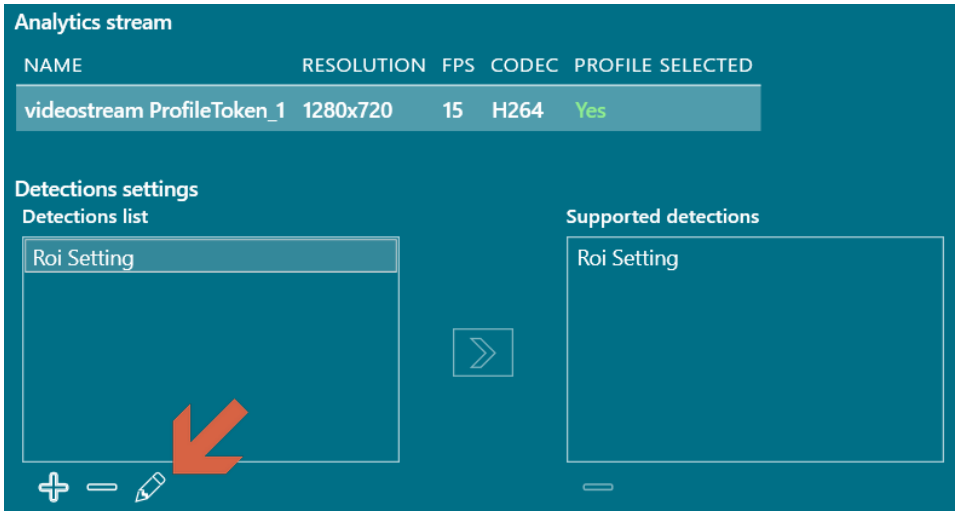
Step6 Select the camera and analysis stream for AI recognition, then click [Add].



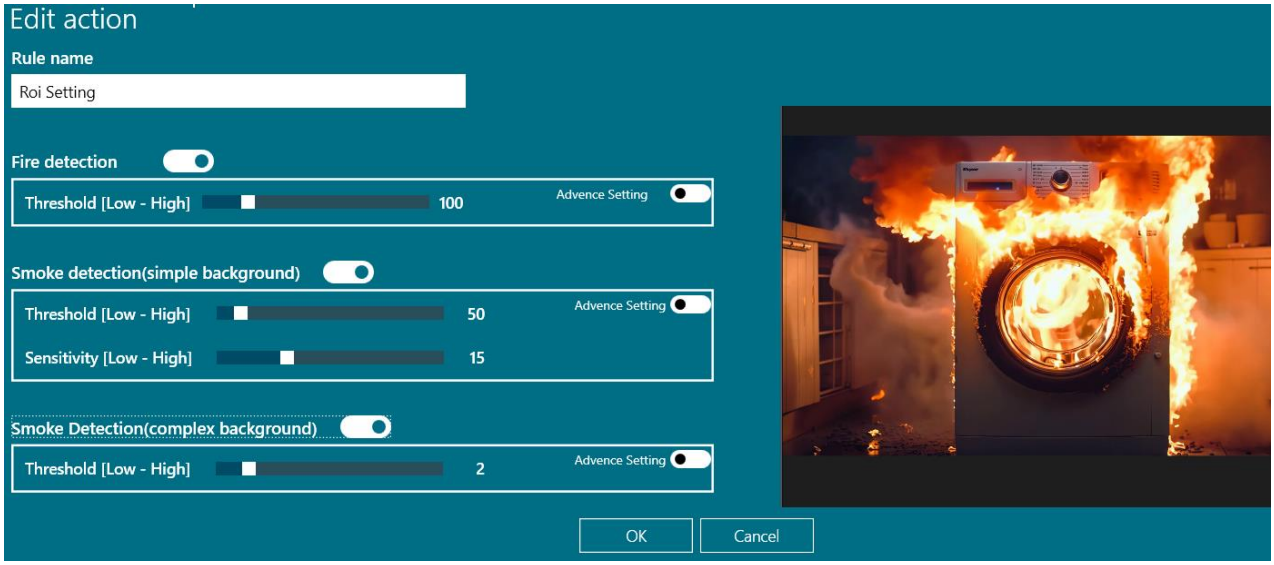
Step7 Select the new analysis stream and [Edit]



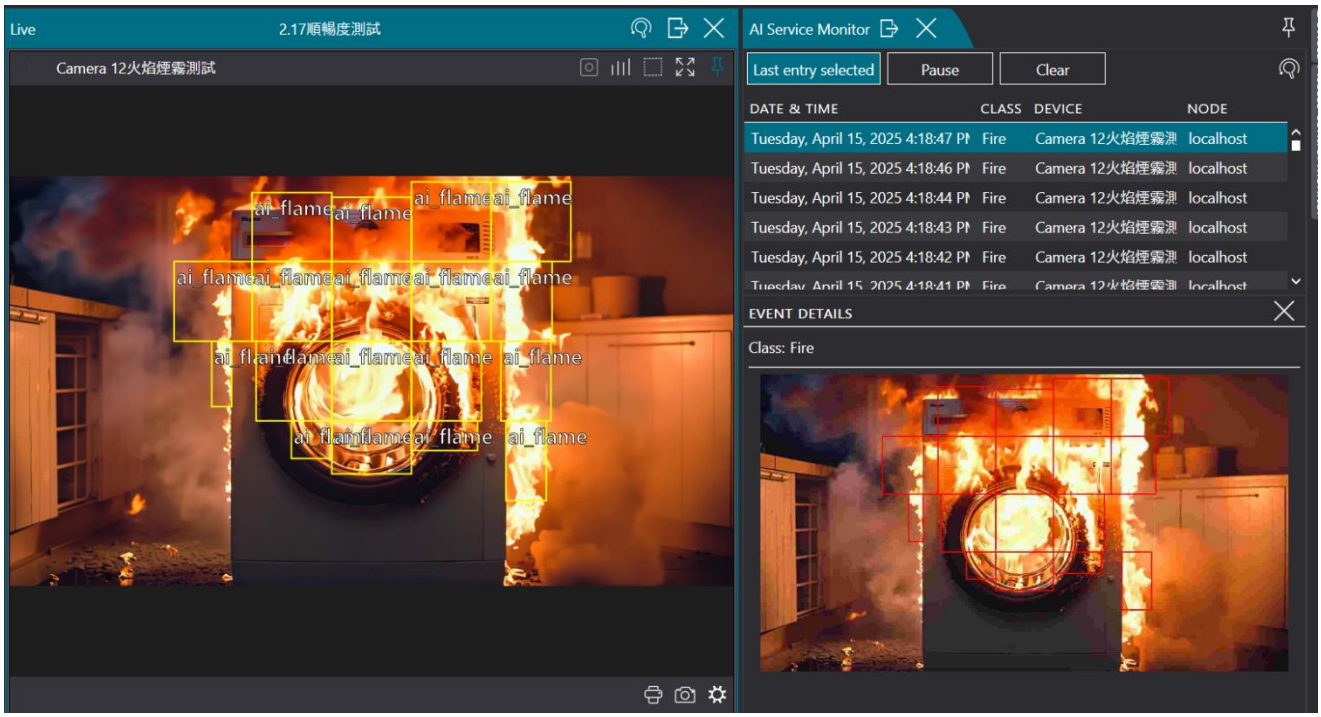
Step8 Click  to enter detailed settings



Step9 Enable the desired detection options



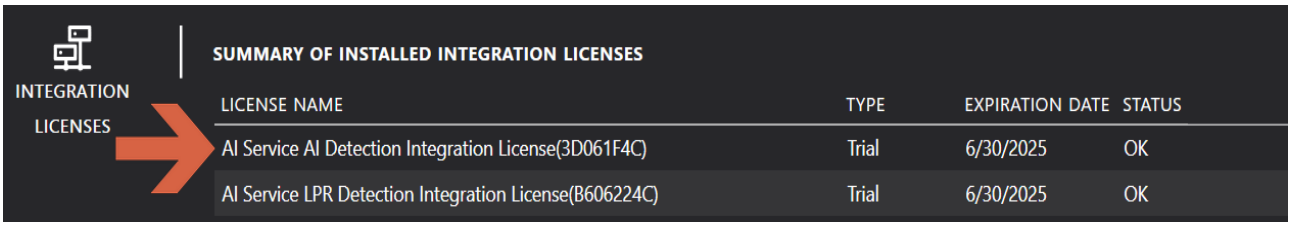
Step10 Open the Client live view and the AI service monitor window to see the Flame / Smoke detection results.



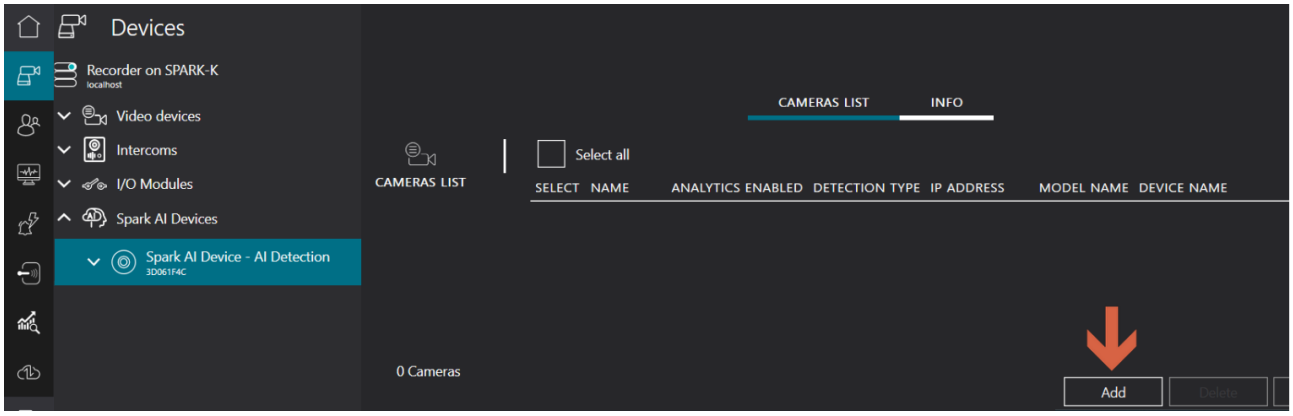
2.5 How to Use Line-Crossing Detection

Line-Crossing detection monitors if objects cross specific virtual boundaries. It’ s widely used for security and area monitoring, detecting human and vehicle crossings for applications like flow counting and violation detection.

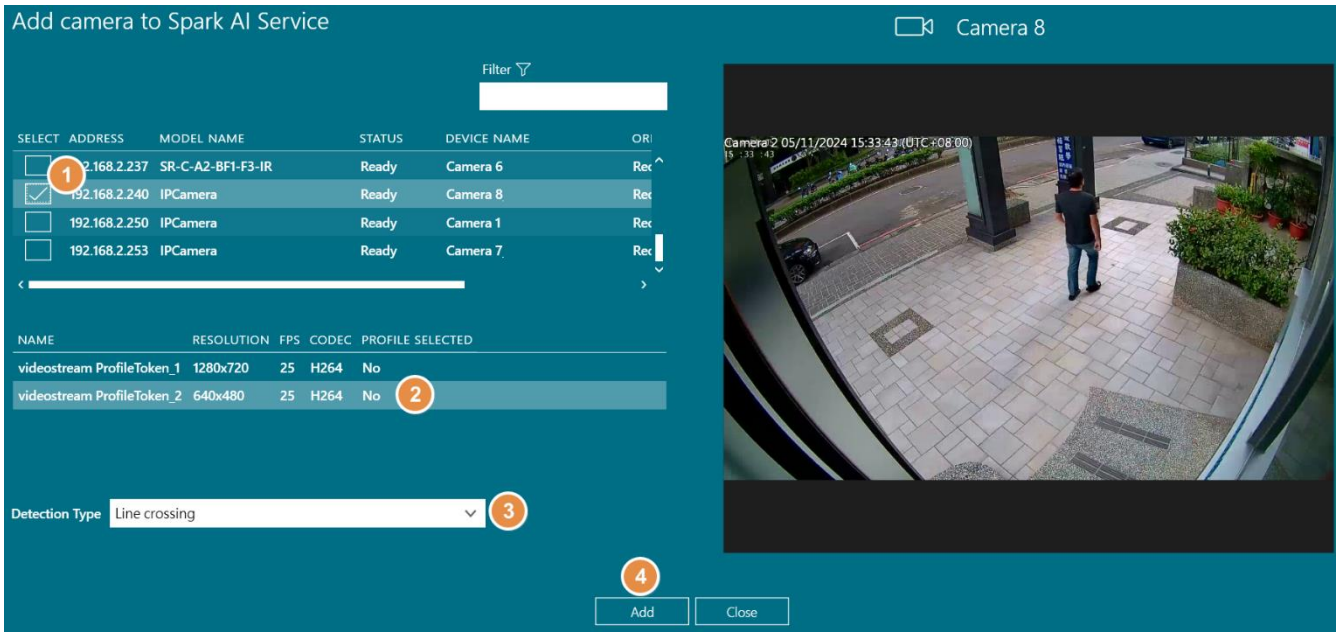
Step1 Config→ click the License Key page on the left menu→ check if the license status is valid. If there’ s no license, import one first



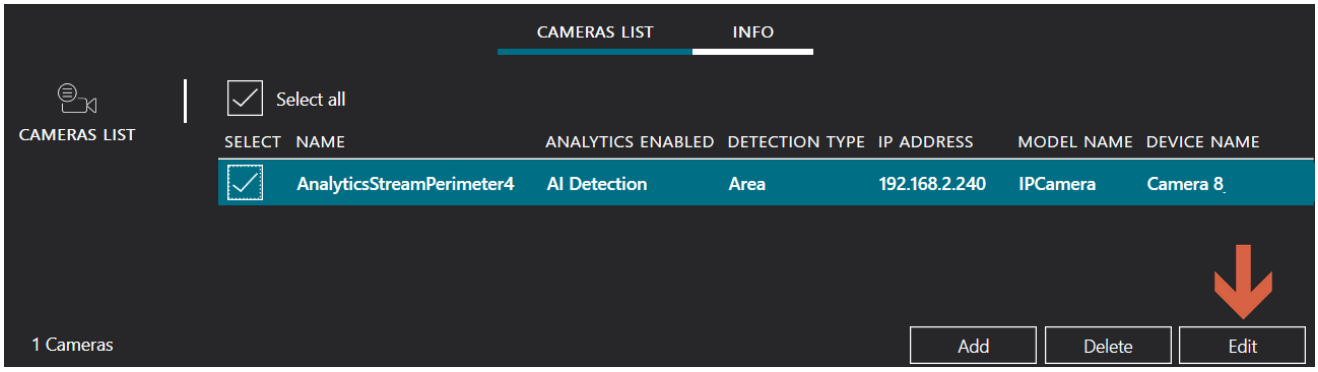
Step2 In the device list, select SPARK AI device AI Detection, click [Add].



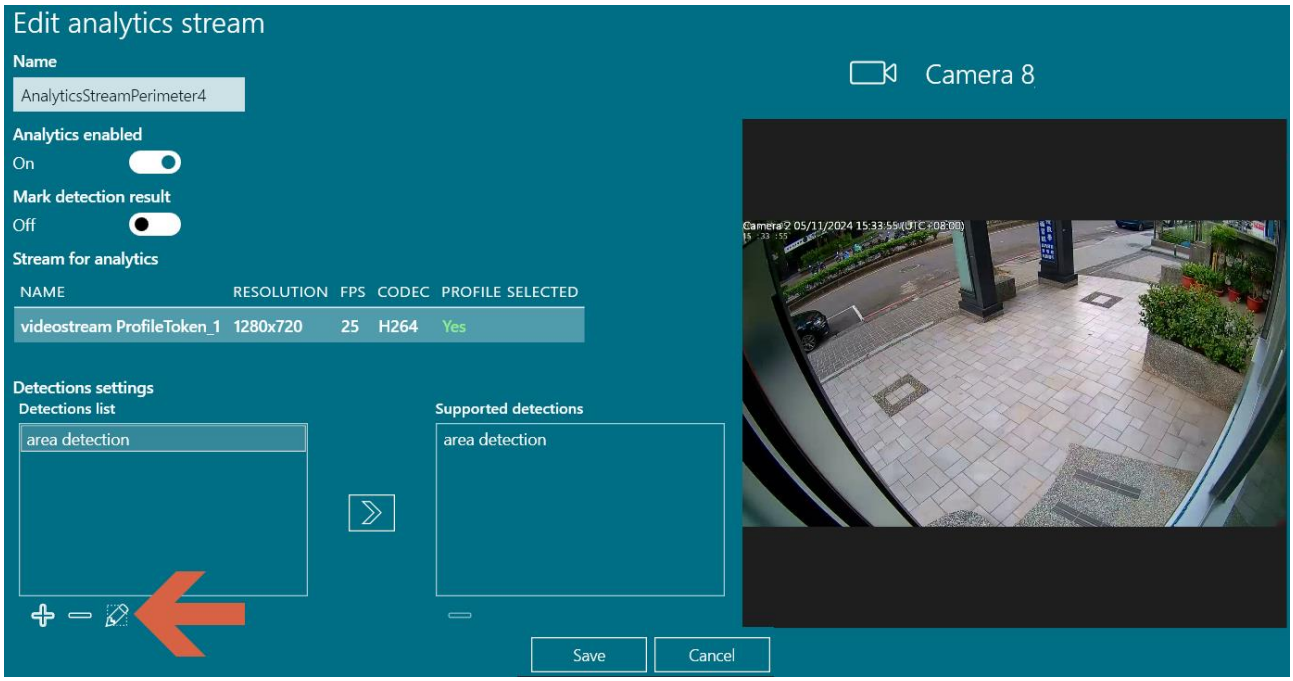
Step3 Select the camera➔ select analysis stream➔ set detection type to line crosssing➔ click [Add].



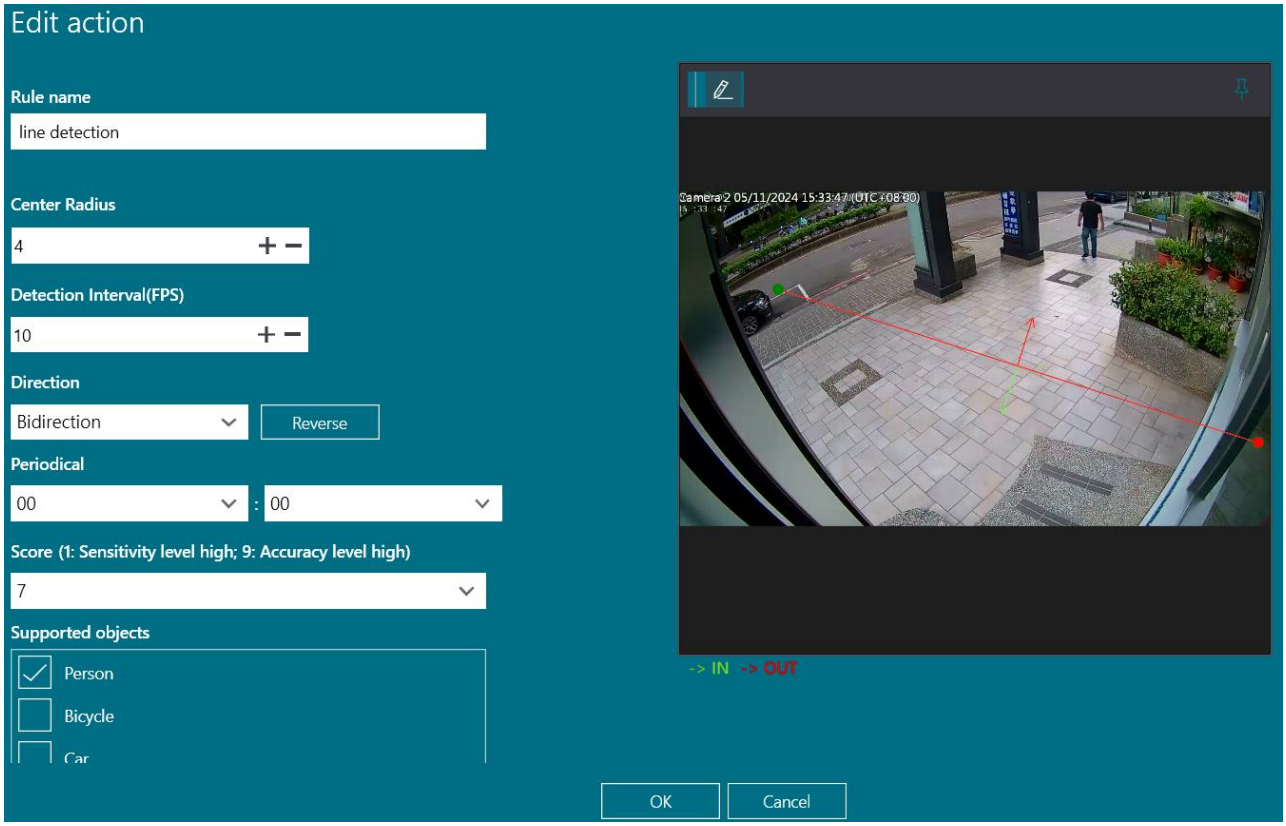
Step4 Click [Edit] to edit the smart analysis stream.



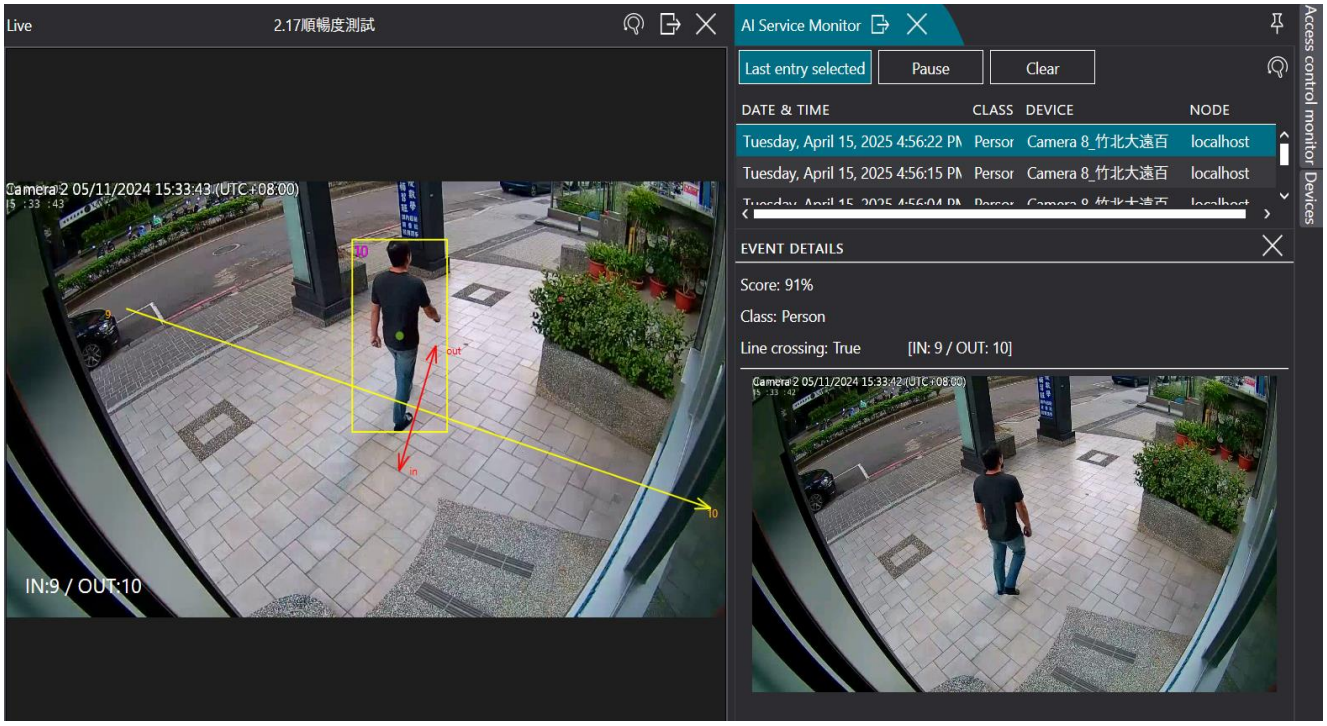
Step5 Edit the stream name and click  to draw detection areas



Step6 Click  to create the detection area, then click [OK]



Step7 Open the Client real-time window and AI service monitor window to view results.



3. HOW TO SET UP EVENTS AND LINE NOTIFICATIONS

This section explains how to configure events and notifications in the Argo system. Event settings ensure the system can respond based on specific conditions, while notification settings help users stay informed of monitoring activities.

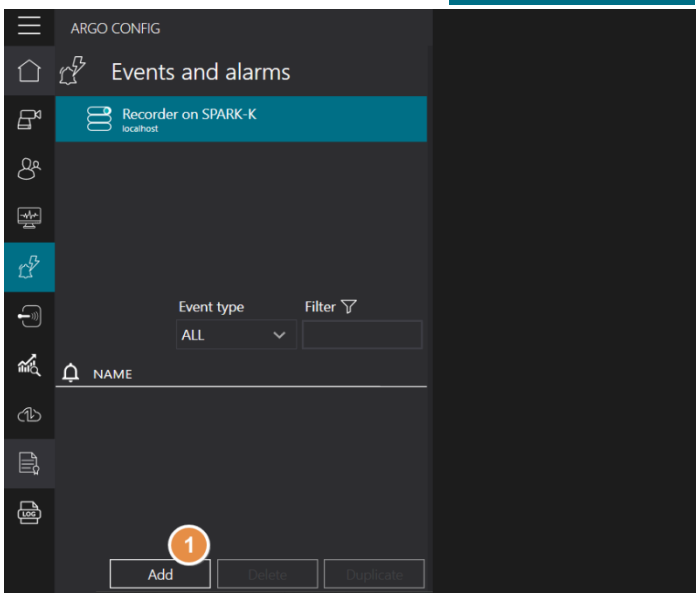
3.1 Event Setup Process

This part outlines how to configure various event trigger conditions. It covers the basic trigger setup and later sections (3.2 LINE and 3.3 Mail notifications) for managing alerts accurately.

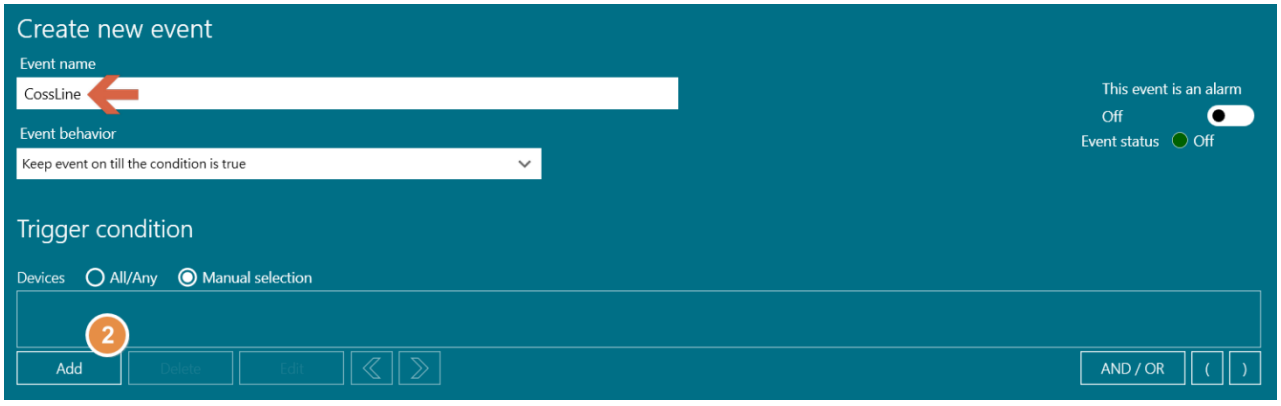
Step1 Make sure the AI analysis stream for object detection is configured. For details, refer to Chapter 2. This section uses "Human detection" as an example.

Step2 Go to Events and Alarms 

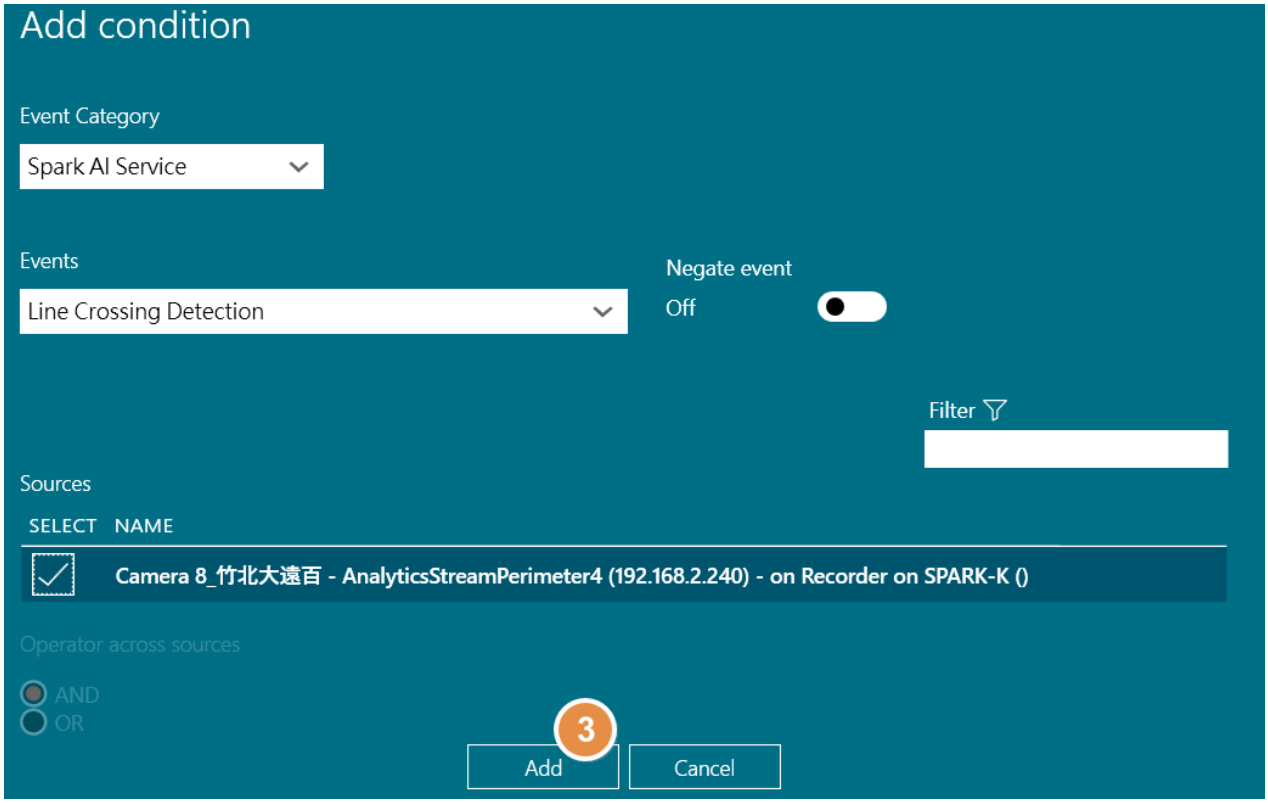
, and click [Add] to create a new event.



Step3 Enter the event name, then click [Add] to proceed to trigger configuration.

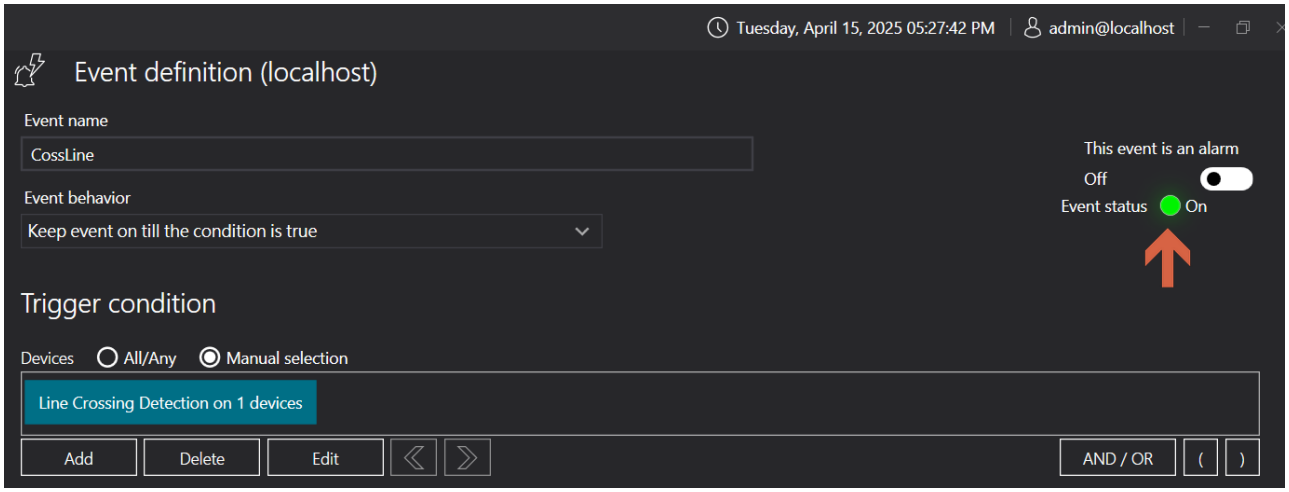


Step4 Select the event category and trigger condition, then click [Add] to complete the



setup.

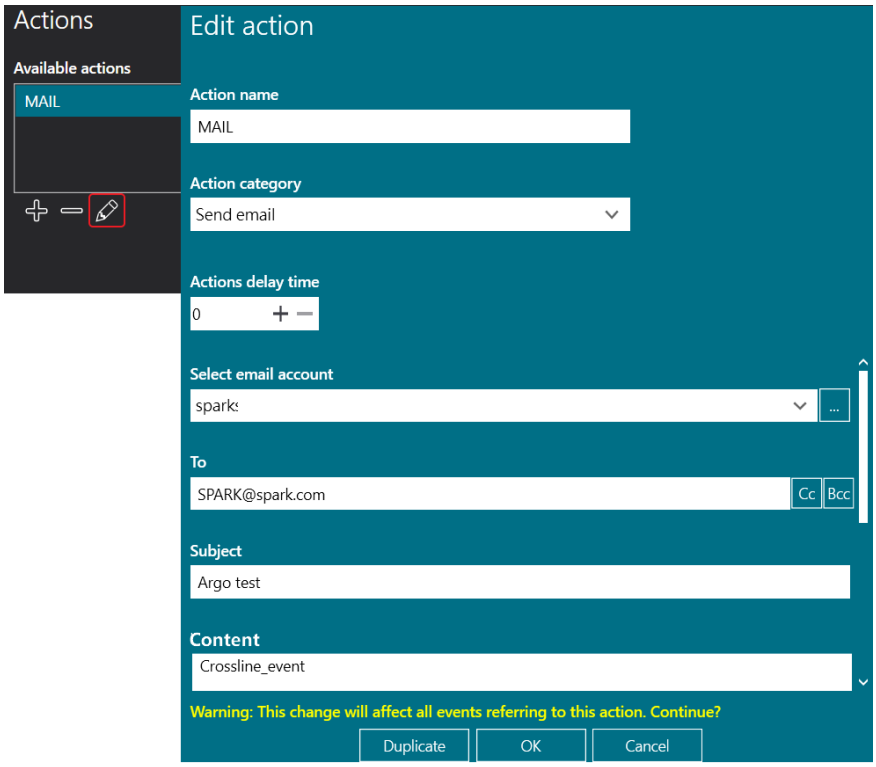
Step5 Once configured, you can check the event status. When the indicator light turns green, it means the event was triggered and set up successfully.



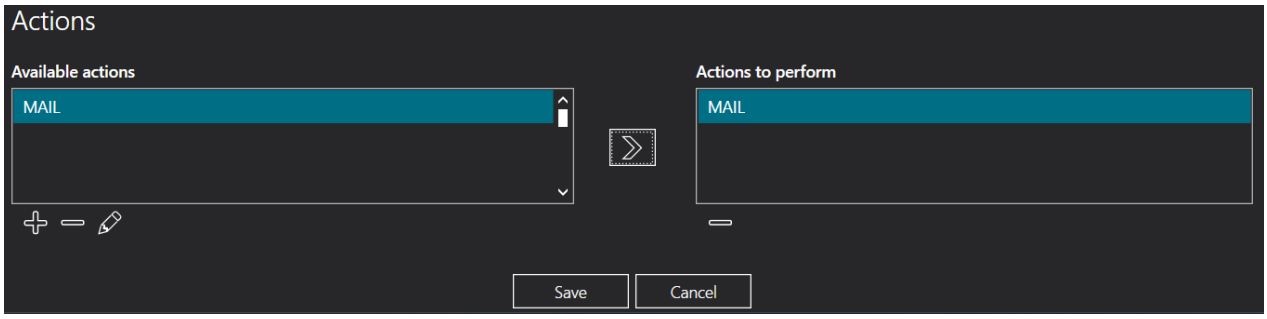
3.2 Editing Response Actions

This section explains how to edit existing response actions to meet new requirements or situations, ensuring the system can respond quickly and effectively to abnormal events.

Step1 Select the desired available action and click [✎]



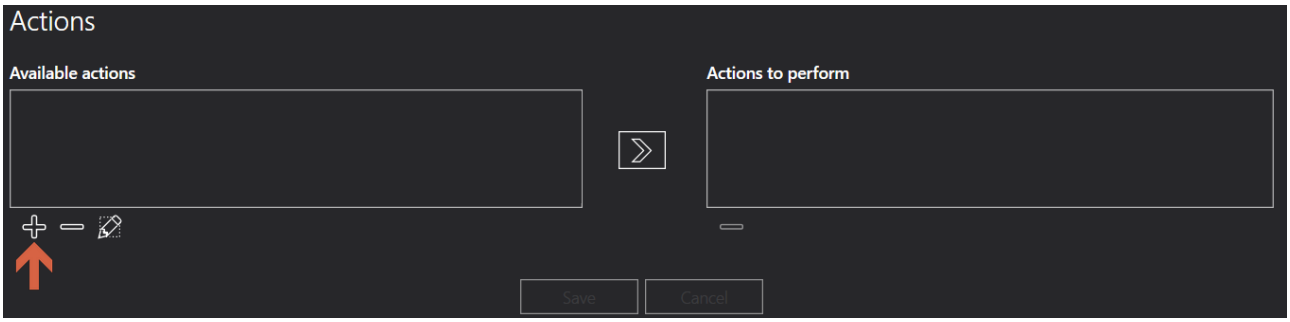
Step2 Click [>] to add the selected action to the list of active response actions. Click [Save] to complete the notification setup.



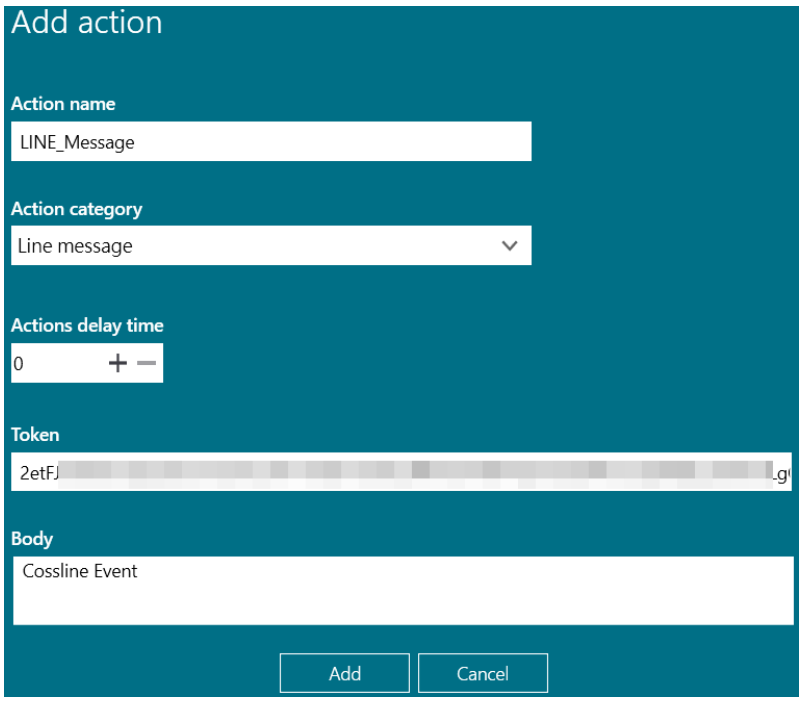
3.3 Basic Event Setup: LINE Event Notification

This section explains how to set up LINE as a notification method. When an event occurs, the system sends real-time alerts via LINE so users can respond promptly.

Step1 Under "Available Response Actions," click [+] to add a new actions.



Step2 Configure the notification settings:



- Enter a name for the response action
- Select [LINE message] as the action type
- Set a delay time (how long to wait after the event is triggered before sending the alert; default is 0)
- Enter the Token (If it's your first time, please refer to Step 3 for account setup)
- Enter the LINE message content
- Click **[Add]**

Step3 Apply for a LINE Messaging Token (If already completed, you may skip this step.)

Starting from March 31, 2025, LINE Notify has been upgraded to LINE Messaging API. To use the messaging feature, users must create an official LINE Official Account.

Message delivery costs are calculated according to LINE’ s official pricing. See the table below for details: :

	Communication	Light	Standard
Monthly Fee	Free	50 USD	150 USD
Free Messages	Up to 500	Up to 10,000	Up to 40,000

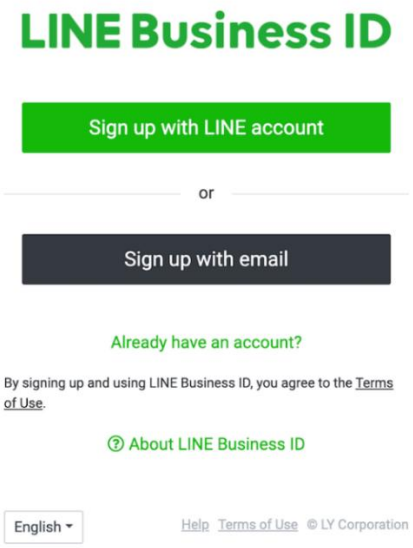
Source：LINE Biz-Solutions

Note: Unlike LINE Notify, LINE Messaging API charges per recipient.For example, if you send a message to a group of 100 people, it will count as 100 messages

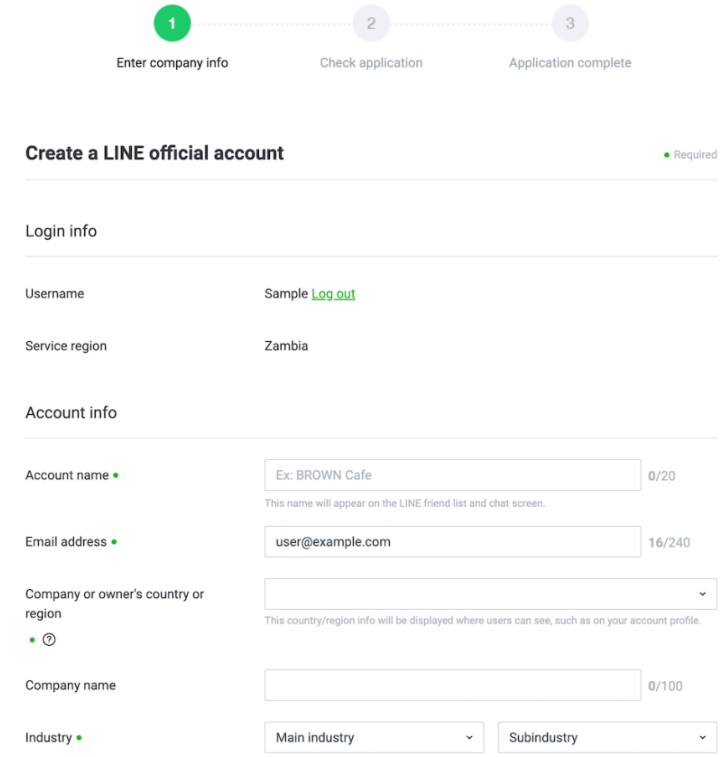
(1) Click on https://developers.line.biz/en/services/line-login/ to access the official LINE Business Account page.

(2) Register for LINE Business ID

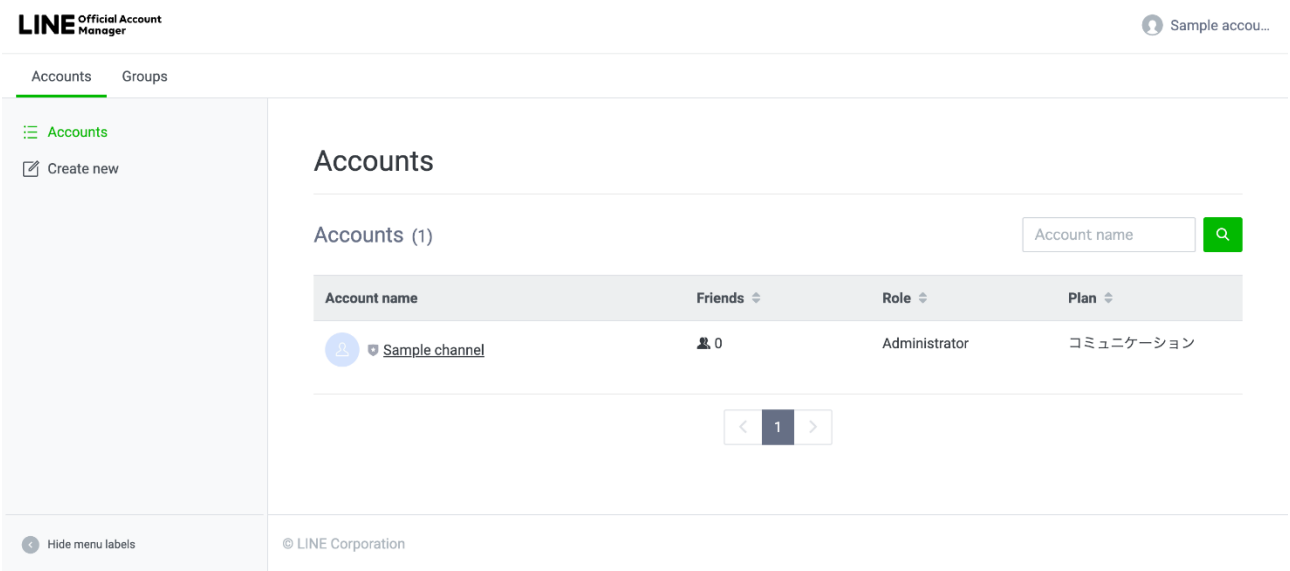
To create a LINE Official Account, you need to register for LINE Business ID (opens new window). You can register for LINE Business ID using your LINE account or email address.



(3) Fill in the entry form

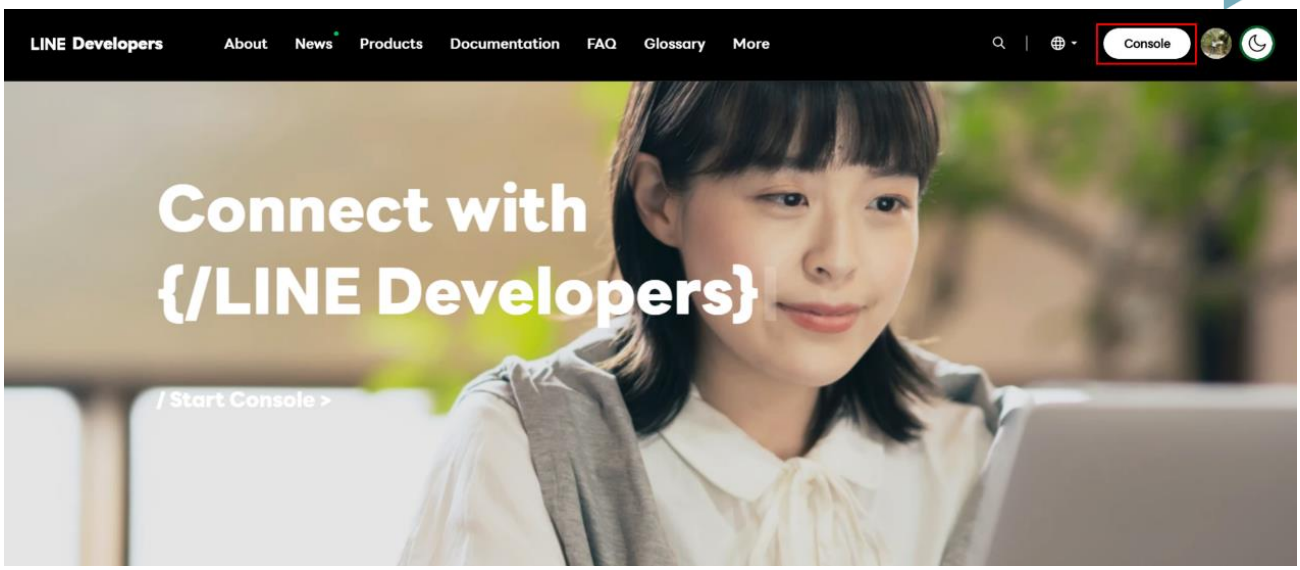


(4) Check your LINE Official Account

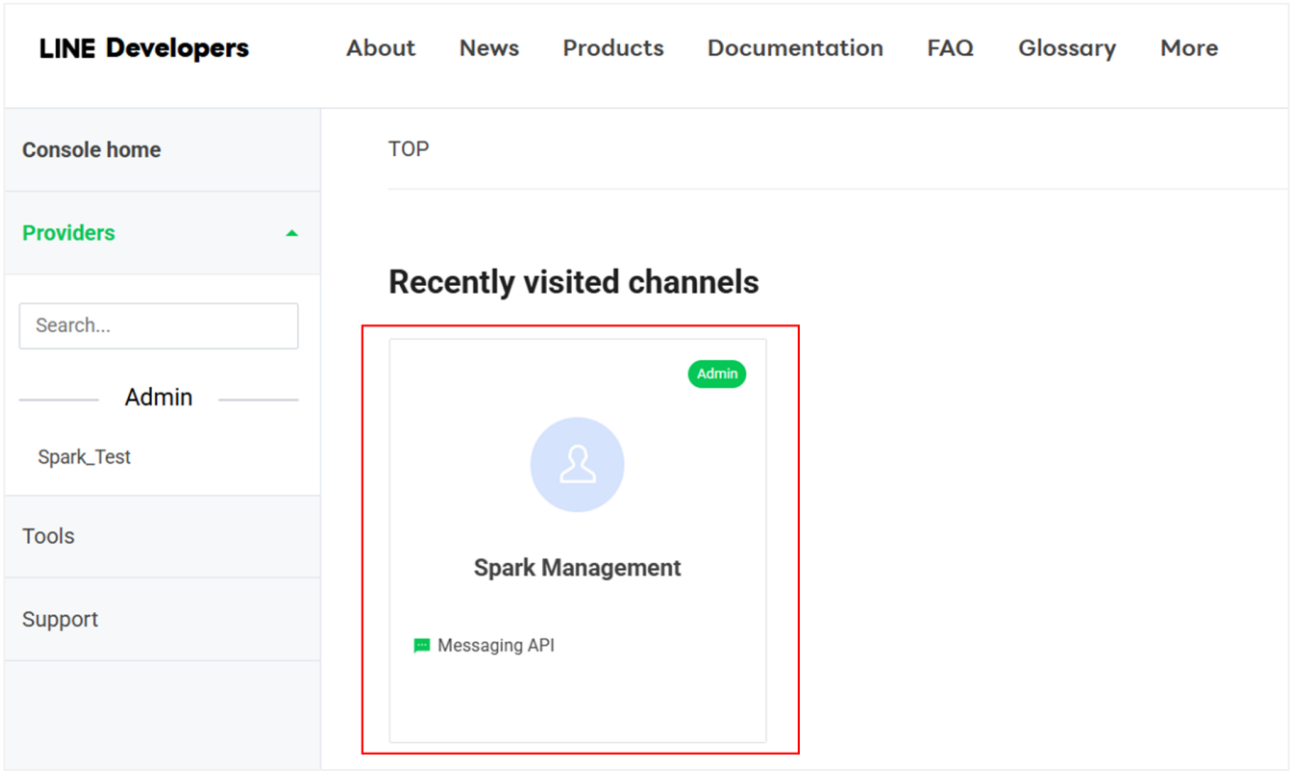


(5) Enable the Messaging API for your LINE Official Account

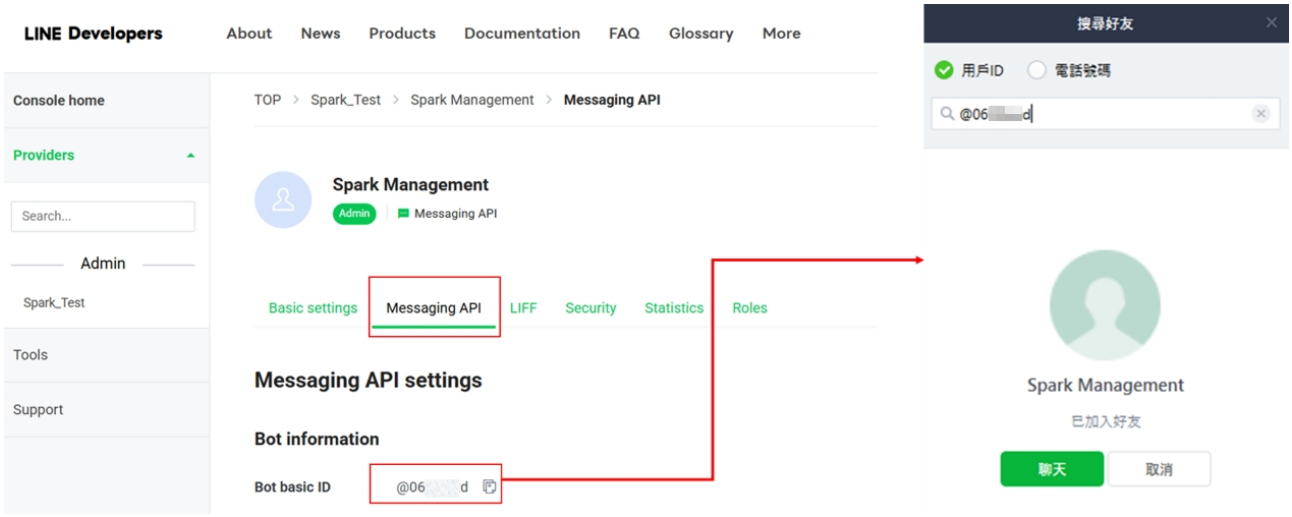
To link your LINE Official Account with the Messaging API, go to the LINE Official Account Manager (opens new window)and enable the Messaging API. This creates a channel.



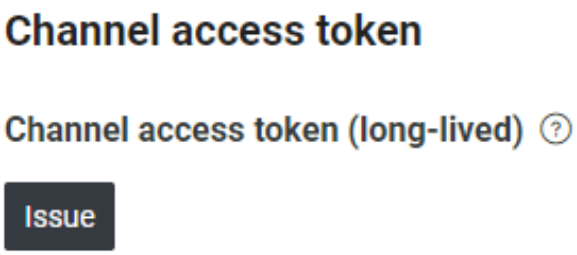
(6) Select the LINE account to which you want to send notifications.



(7) Click on [Messaging API], and obtain the ID to add the LINE account as a friend.



(8) Scroll down to the bottom of the page and locate the "Channel Access Token" section. Click [Issue].



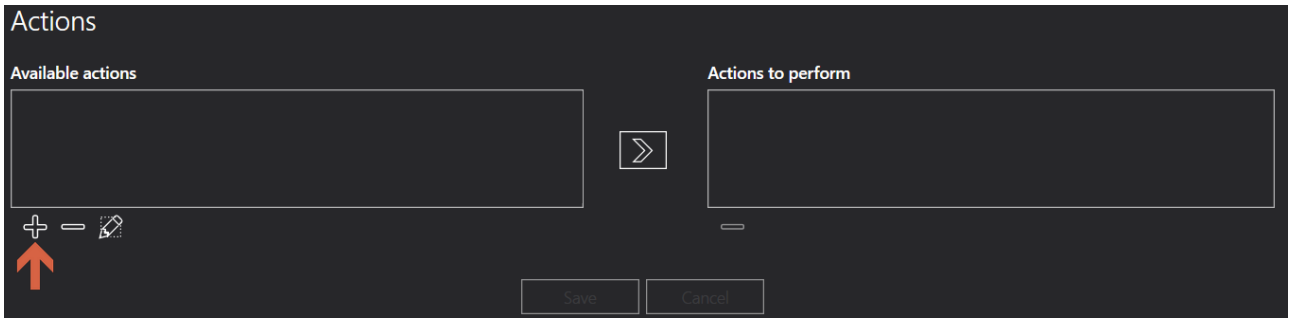
(9) Copy the Channel Access Token to obtain the authentication token.

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

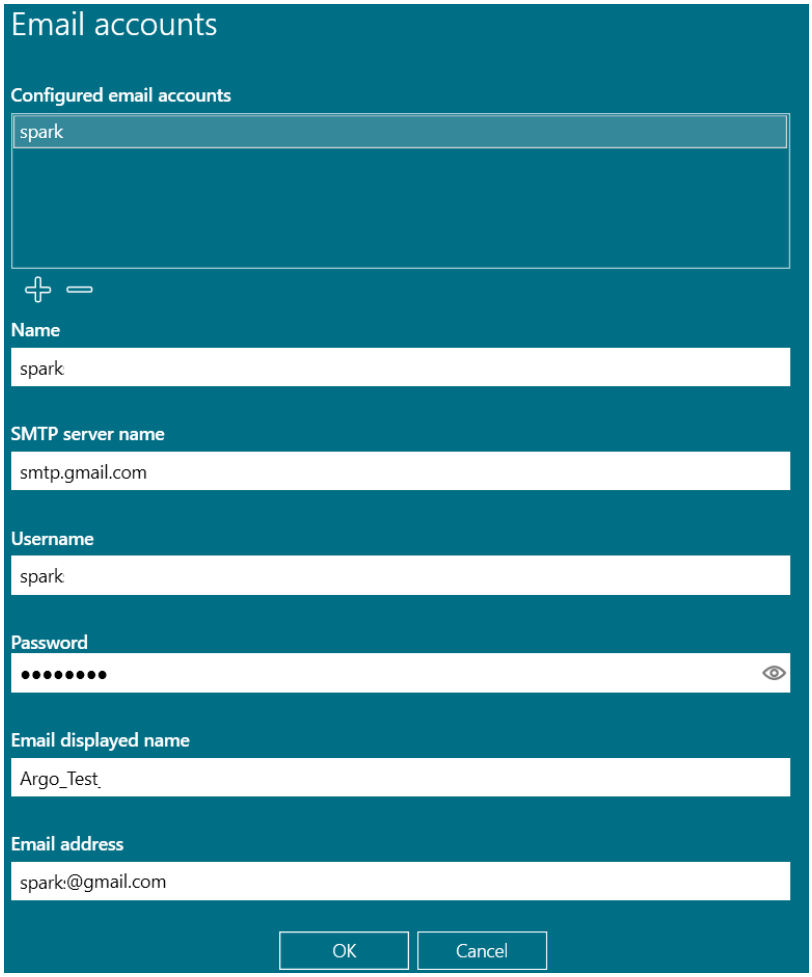
3.4 Basic Event Setup: Email Notification

This section explains how to configure the email notification feature. When an event occurs, the system automatically sends an email alert so that users can stay informed even when off-site.

Step1 Click [+] under Available Actions to add a new action.



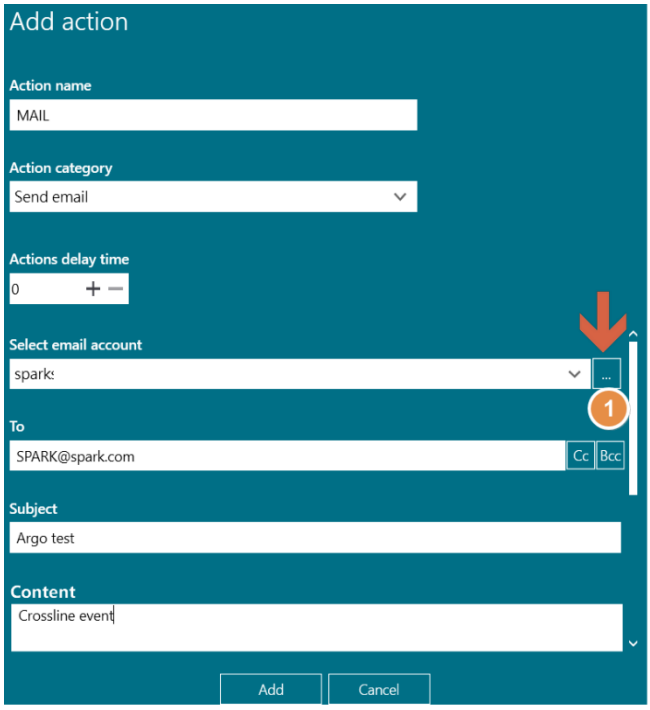
Step2 Configure the email notification:

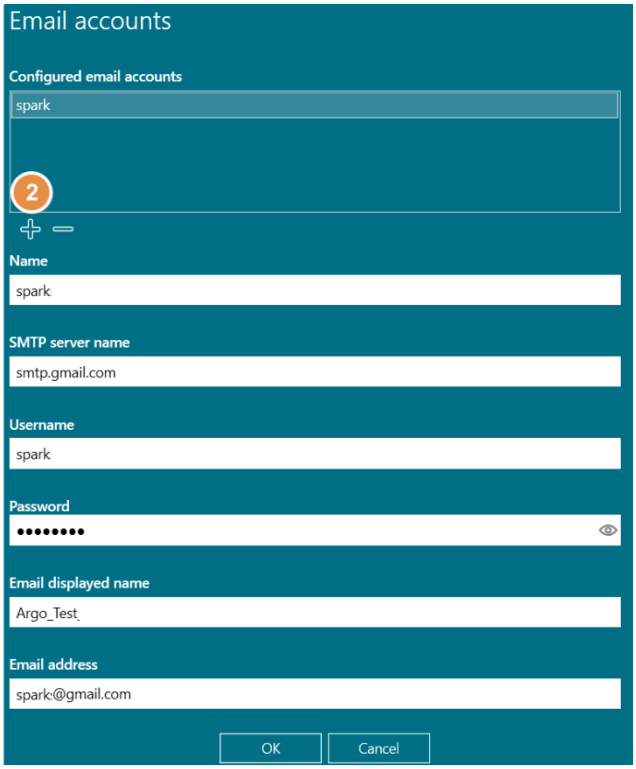


- Enter a name for the response action
- Select [Send Email] as the response action type.
- Choose an email account (if not set up yet, refer to Step 3).

- Enter the recipient email address in the To field ➔Enter the email subject.
- Enter the email content.
- Click [Add] to complete the setup.

Step3 Email Account Setup (skip if already configured):





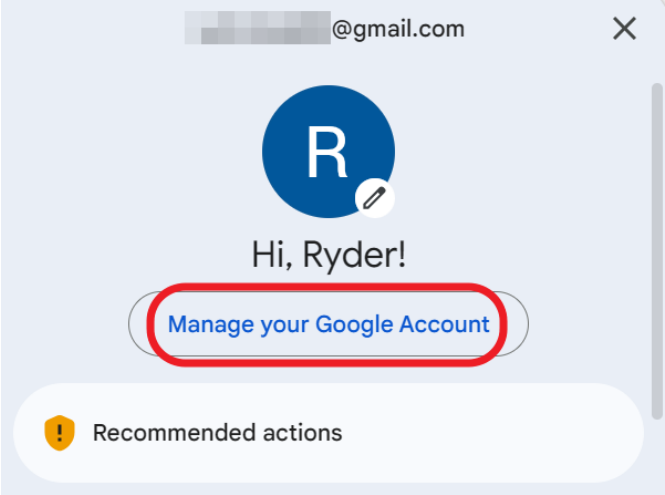
- SMTP Server Name: Use the SMTP server and default port 587 based on your email provider.

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

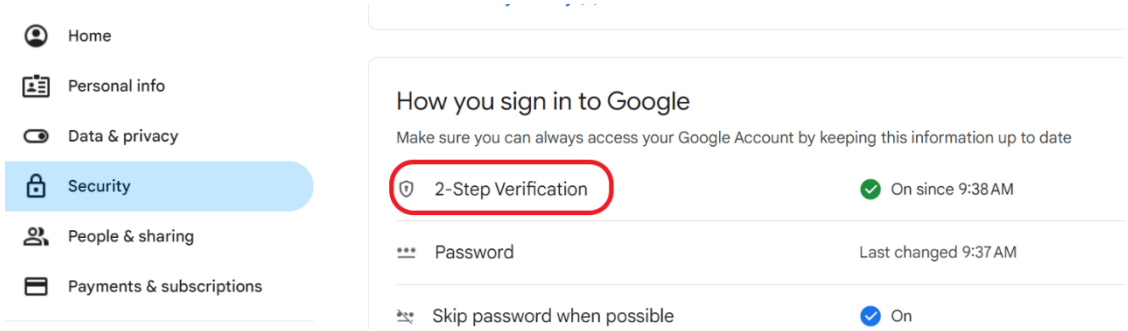
Note: If your email provider is not listed, search using keywords like "[email provider] smtp server name".

- Account: Enter your email address.
- Password: If using Gmail, generate an app password through 2-step verification.

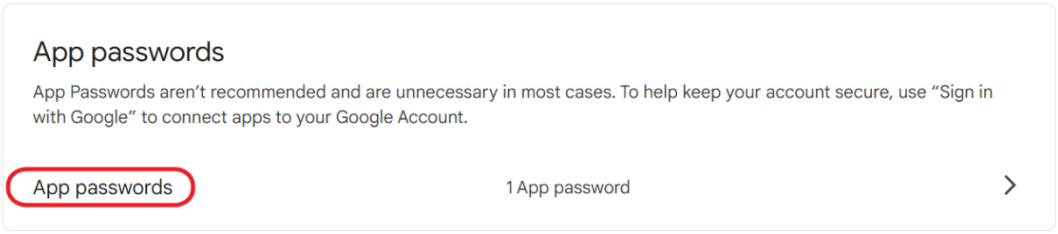
(1) Go to the Gmail homepage, click on "Manage your Google Account."



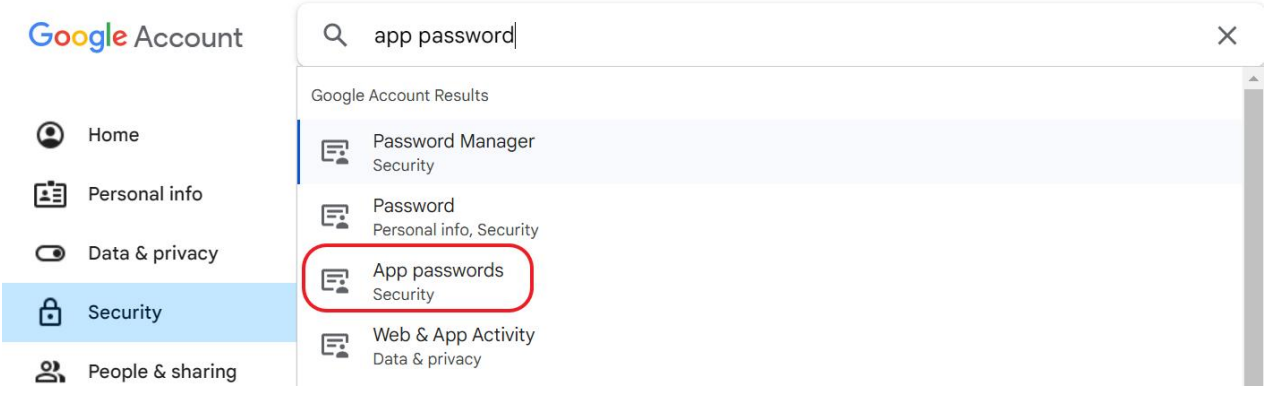
(2) Click on "Security" to enter two-step verification, then enter your account password.



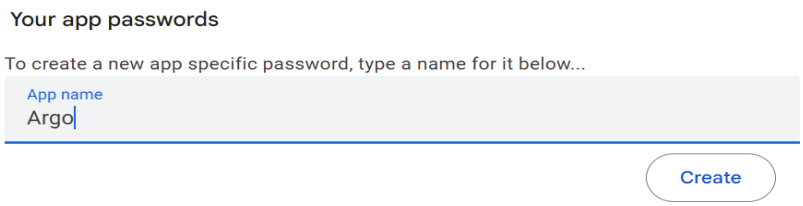
(3) On the two-step verification page, click on application password



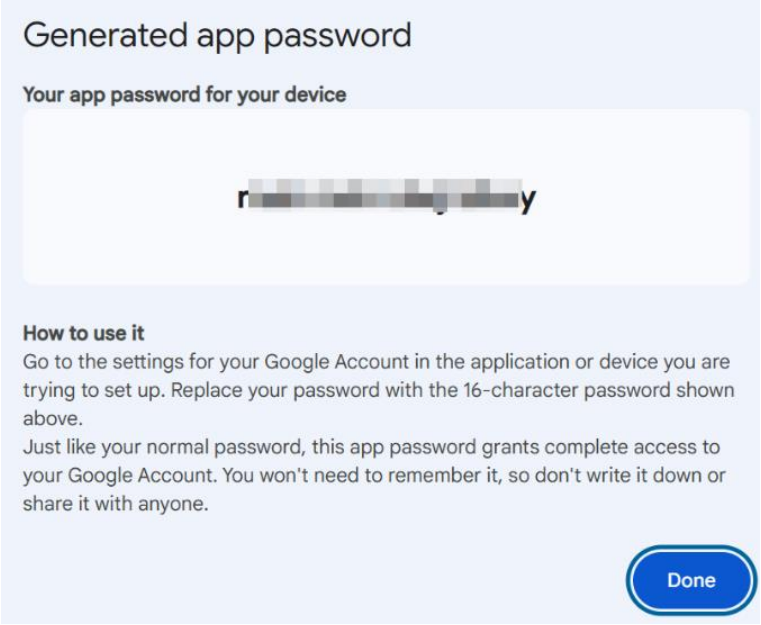
If the application password does not display correctly, key-in the application password in the search field to set up.



(4) Create an application name.

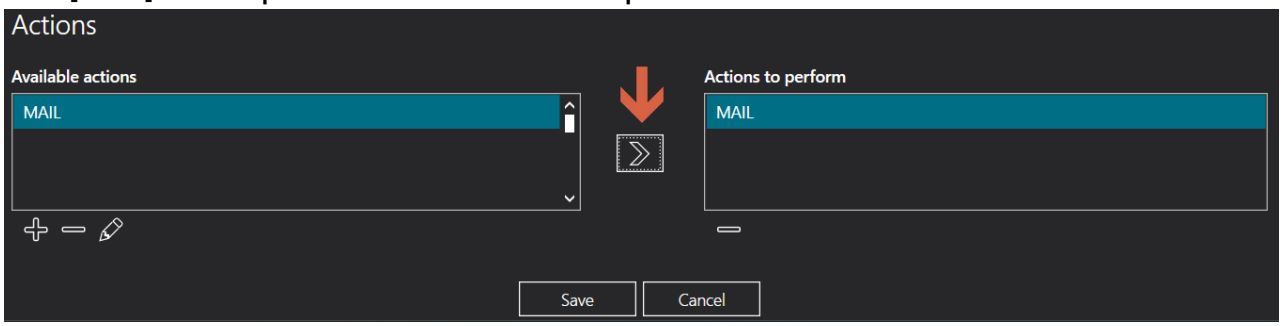


(5) Backup the generated password, then click Finish to complete the setup process.



Note: This password serves as the email password.

Step4 Click [>] to add the available action to the selected actions to be executed, then click [Save] to complete the notification setup



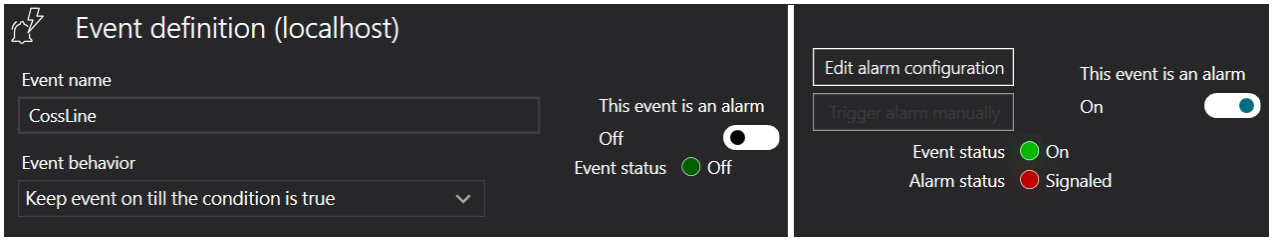
4. HOW TO CONFIGURE EVENT ALARMS

This chapter introduces how to configure the alarm system and its triggering conditions. The Client features a dedicated alarm page, helping users respond quickly to issues and allowing assignment of alarms to specific roles for efficient management.。

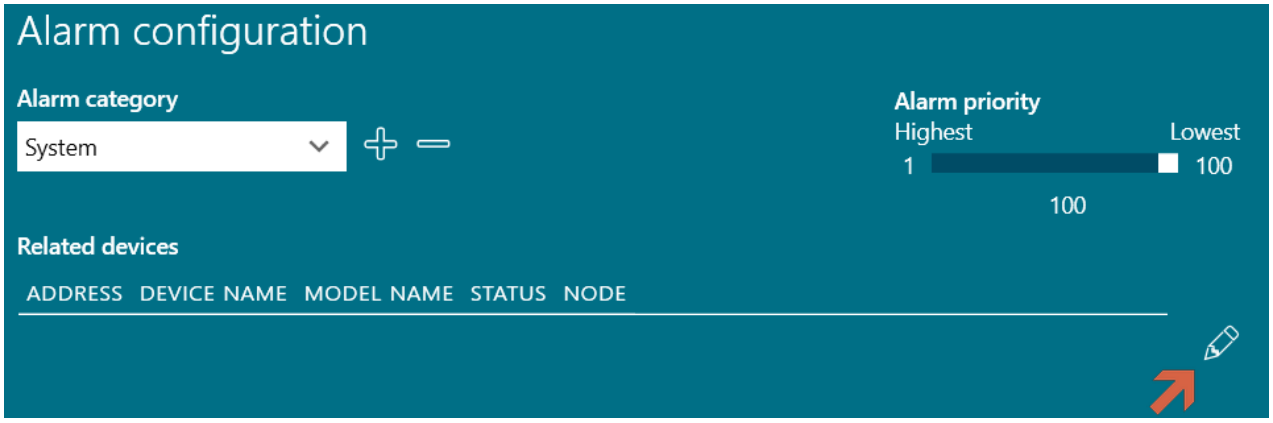
4.1 How to Enable the Alarm Bell

This section explains how to set up the alarm bell. When an event is triggered, the bell icon activates and logs the alert in the playback timeline for easy video retrieval.。

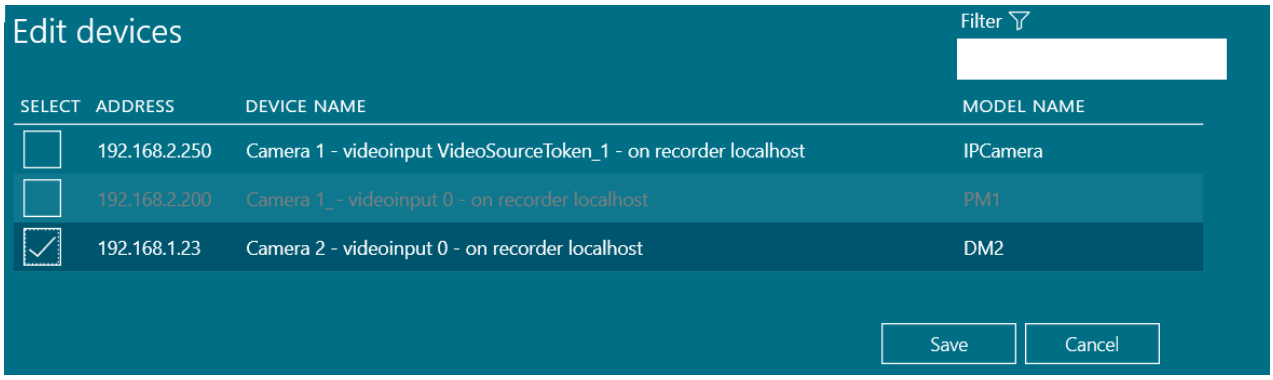
Step1 Enable [This event is an alarm] and click [Edit Alarm configuration]



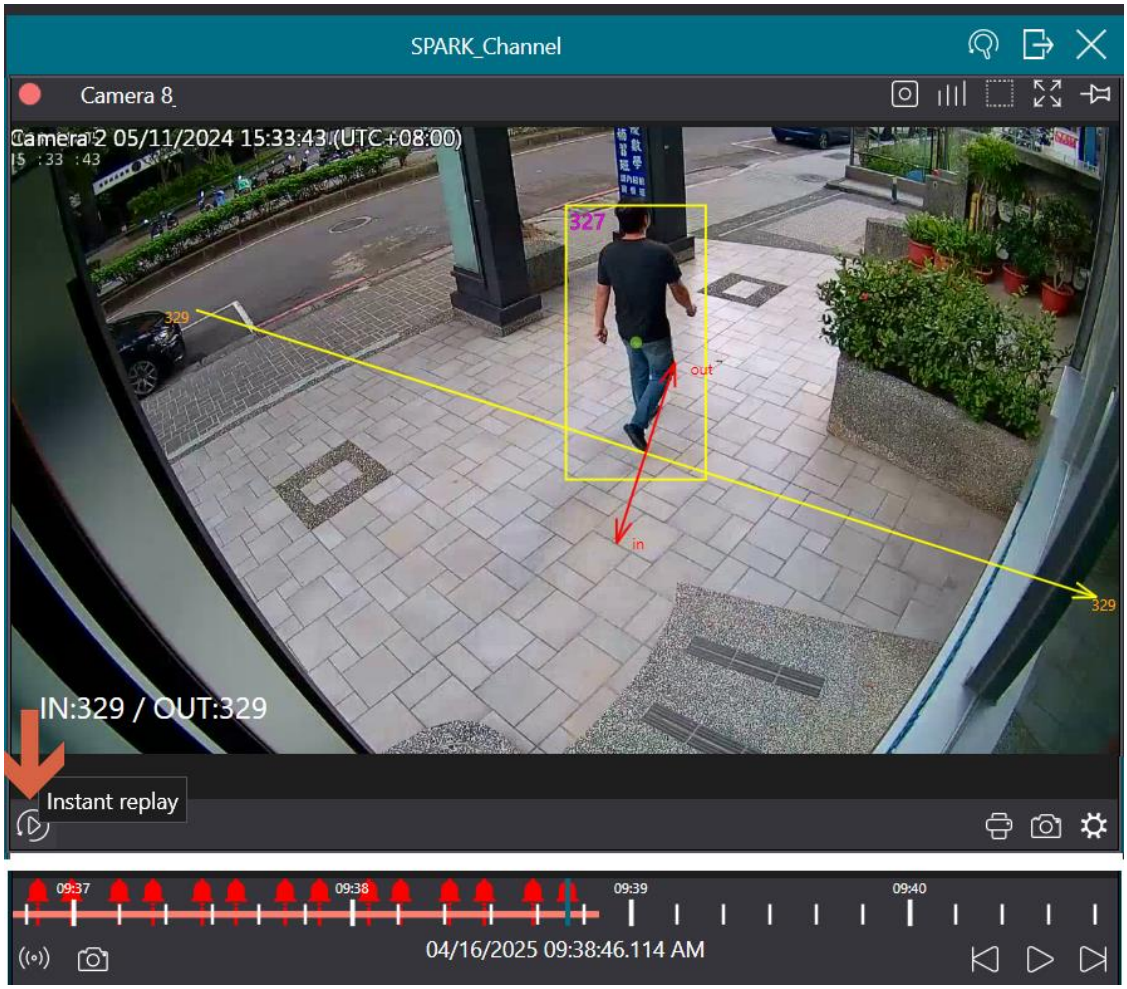
Step2 Click [Edit] (pencil icon)



Step3 From the device list, select the associated camera(s) and click [Save]



Step4 In the Client's live view window, click [Instant replay] to view alarm markers



4.2 How to Set an Alarm SOP

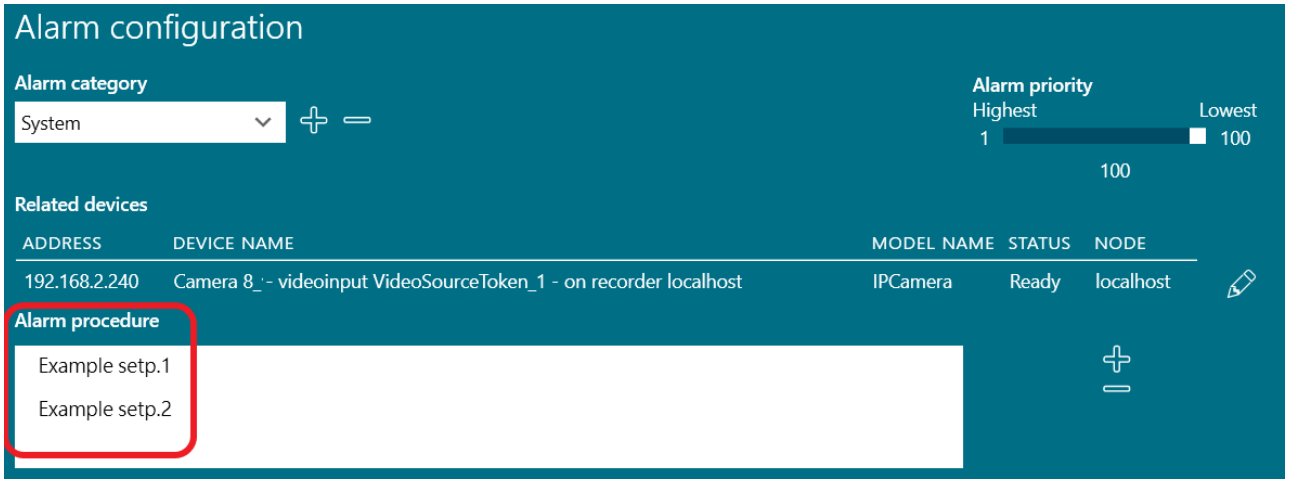
This section shows how to define an SOP for handling alarms. Users can follow a structured process to resolve alarms quickly.

Step1 Complete alarm setup in Section 4.1

Step2 In the alarm page, click [+] in the Alarm Procedure section

Step3] Enter instructions for the handling step in the [Procedure] field and click [Add]

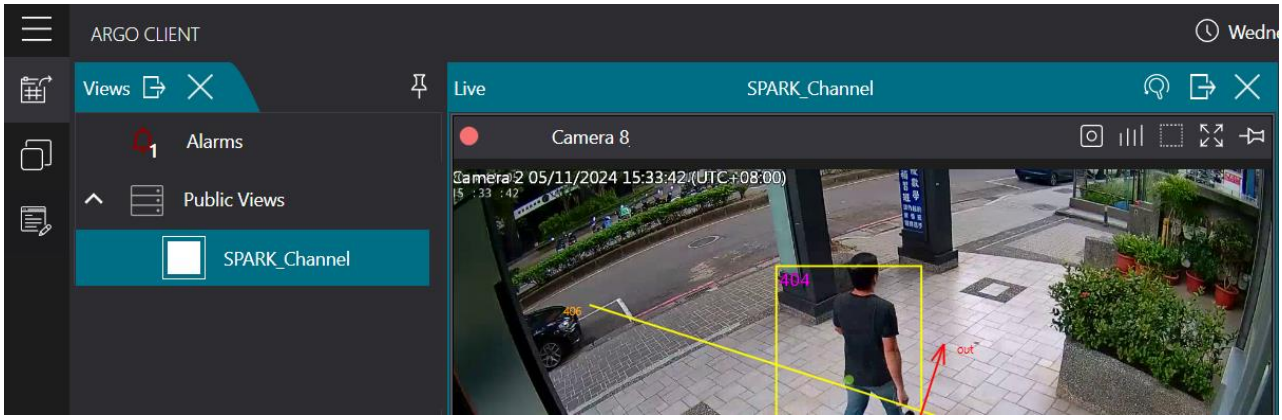
Step4 Once added, the steps will appear in the procedure list. Click [OK] to save



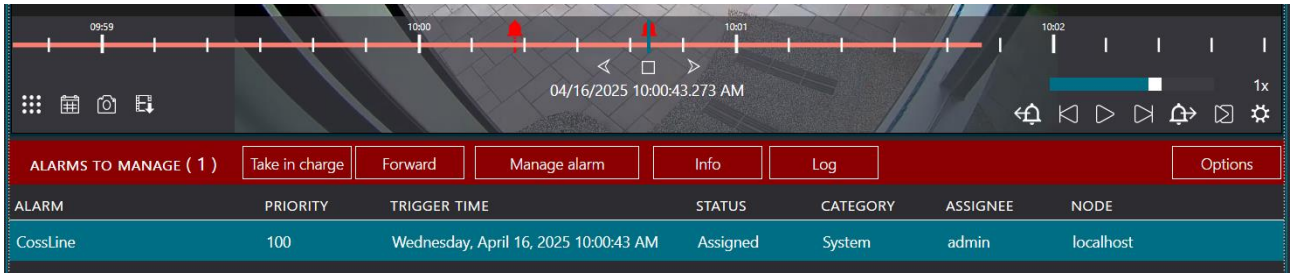
4.3 How to Use Alarm Management in Client

Learn how to use the Client interface to manage alarm responses and ensure proper handling.

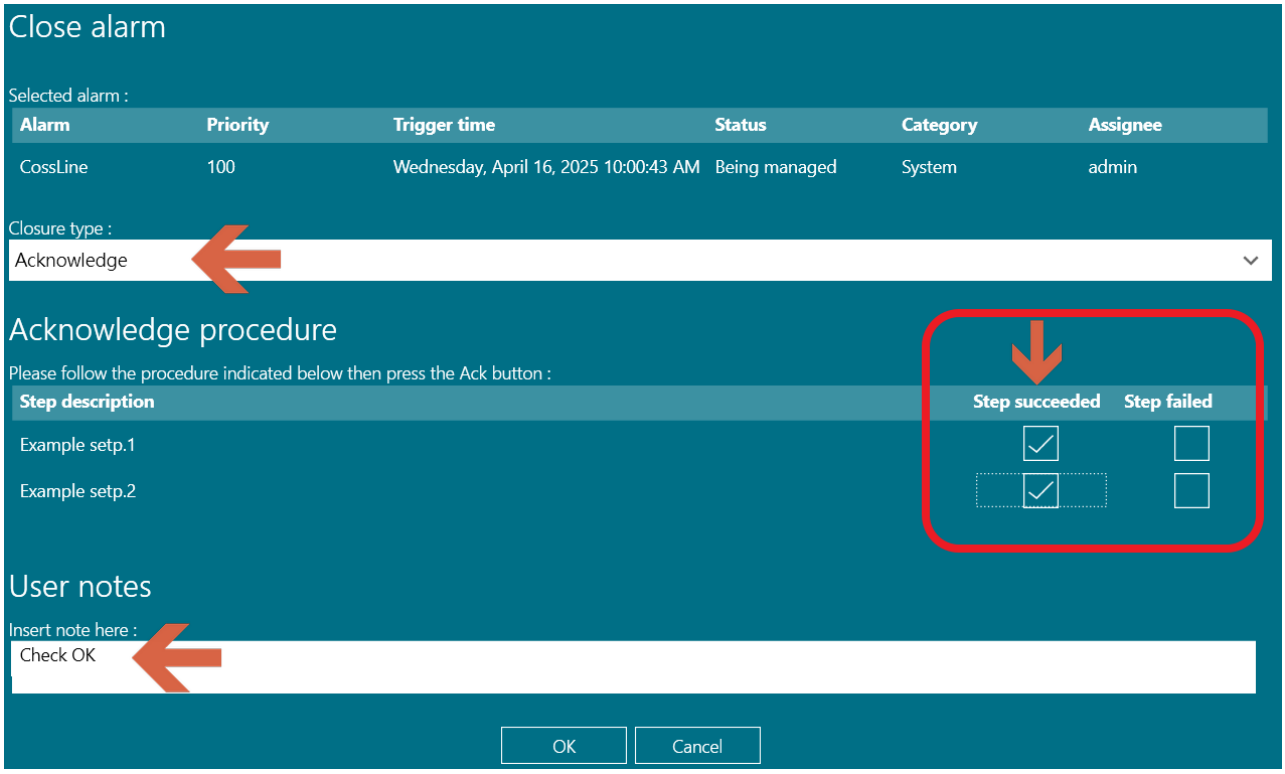
Step1 When an alarm is triggered, click the Alarms to open the Alarm Management page



Step2 In the Alarm Management page,click [Take Over] ➔ [Manage Alarm]



Step3 Select alarm type to dismiss ➔ If handling steps were completed, check [Step succeeded] ➔ Add notes in the User Notes section ➔ click [OK] to complete alarm handling



5. HOW TO RECEIVE SYSTEM ABNORMALITY NOTIFICATIONS

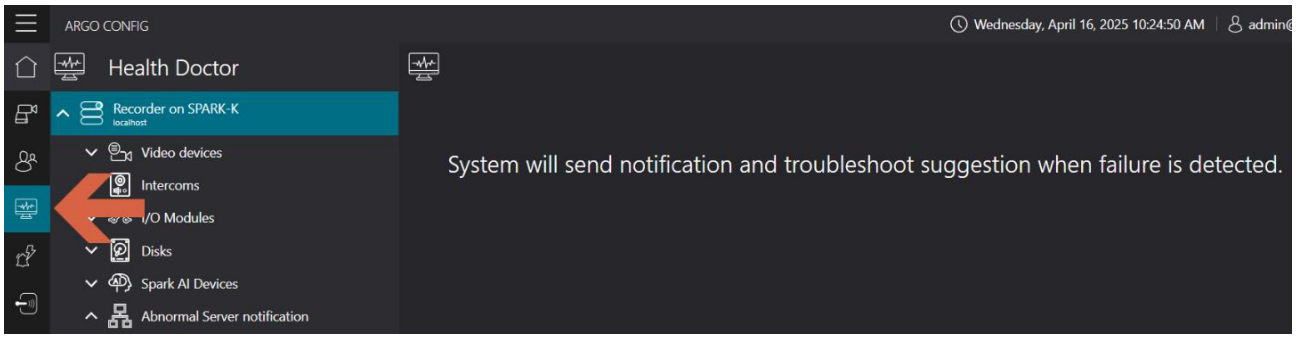
This chapter explains how to configure notifications when devices are disconnected or encounter errors. The system will proactively notify relevant personnel, ensuring timely responses to abnormal events.

5.1 Enabling the Health Doctor

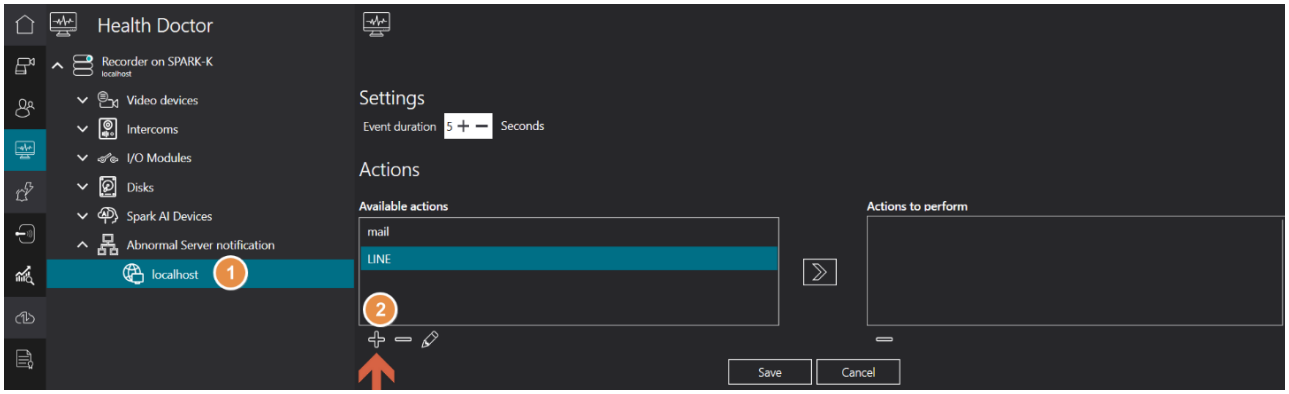
This section explains how to use the Health Monitor to track system status. It helps users detect problems early and respond effectively.

Step1 Upload the Member ID from the License page

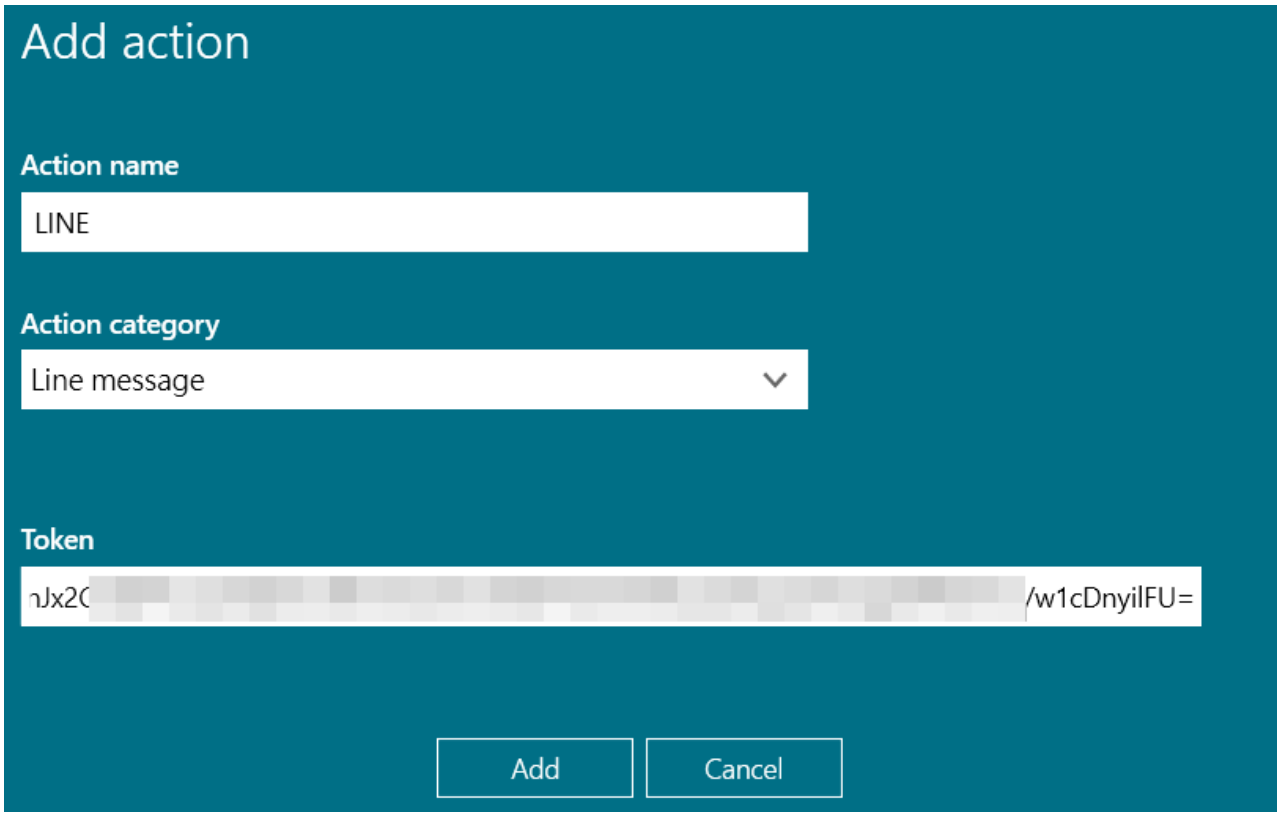
Step2 Click the Health Doctor icon to enter the settings page



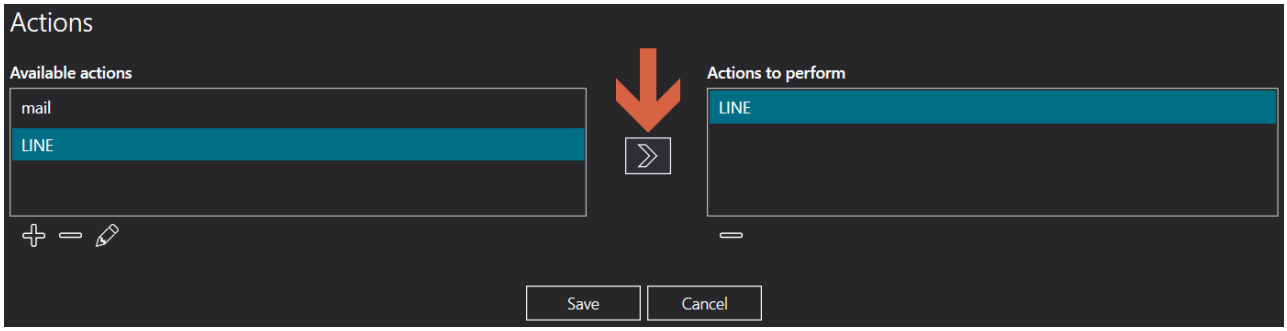
Step3 Select the device(s) requiring host error notifications, then click [+] to add available action



Step4 Enter the action name ➔ Select [LINE message] as the action type ➔ Paste the token (applied via LINE Messaging API, see Section 3.2) ➔ Click [Add] to save the action



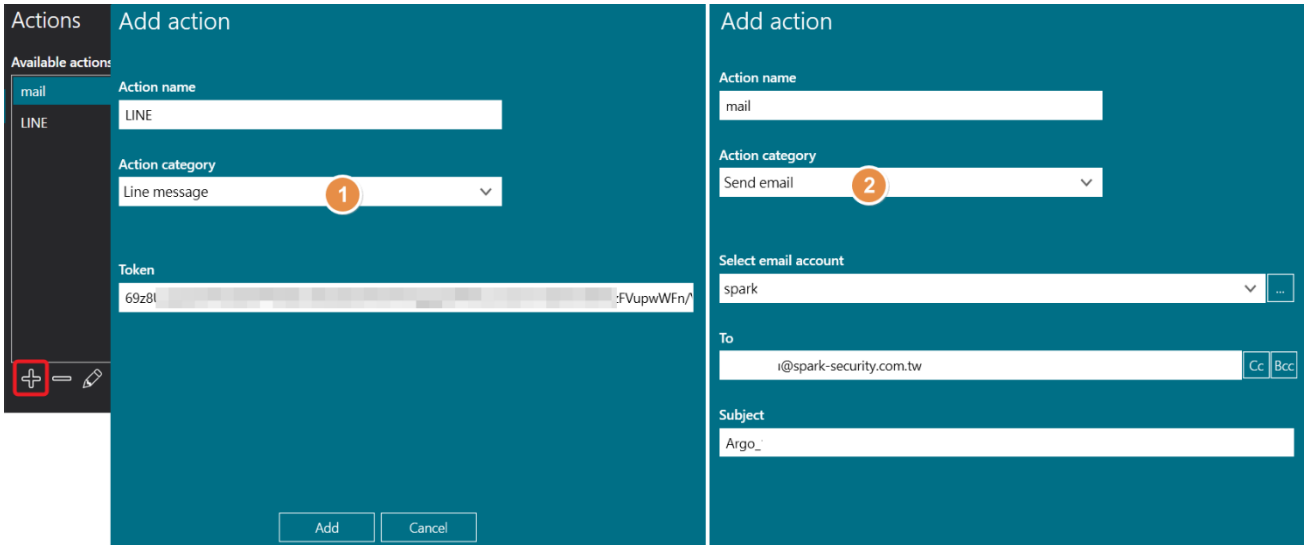
Step5 Move the newly created available action from [Available Actions] to [Actions to perform] using [>], then click [Save] to apply



Note: Host error notifications are confirmed by the server and do not follow event duration settings. The first notification is sent 5 minutes after disconnection, followed by hourly notifications if the issue persists

5.2 Adding Notification Methods in Health Monitor

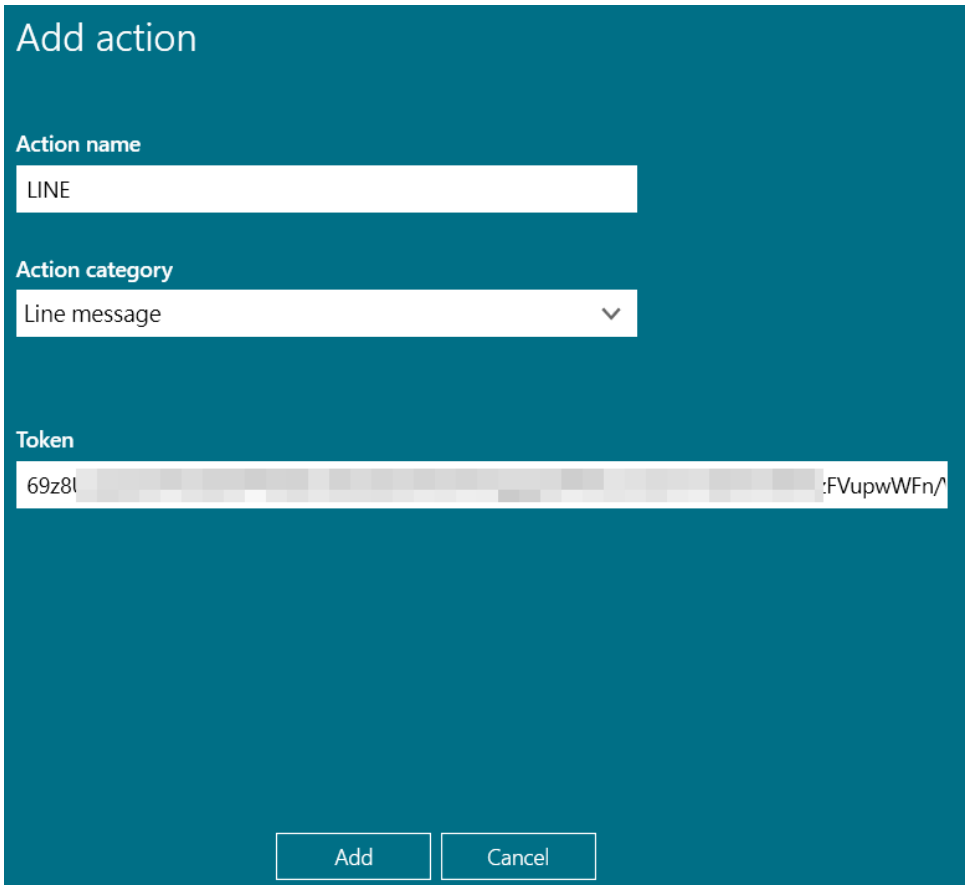
This section explains how to define new [Actions] for abnormal events. The system will automatically send troubleshooting instructions based on the defined actions.



- Click [+]
- Action Name: Define the action name
- Action Type: Choose LINE Message (see Section 5.2.1) or Email Notification (see Section 5.2.2)

5.2.1 LINE Notification

Explains how to configure LINE Message for system abnormalities. When triggered, the system sends a LINE message immediately.

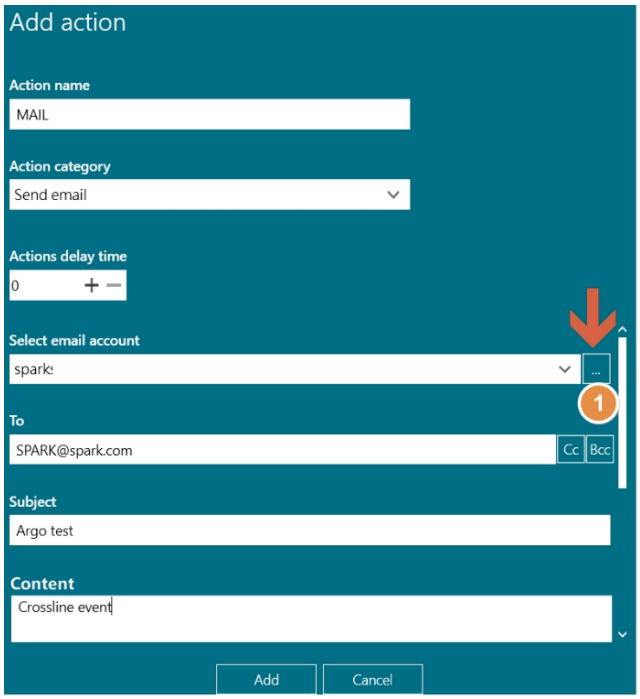


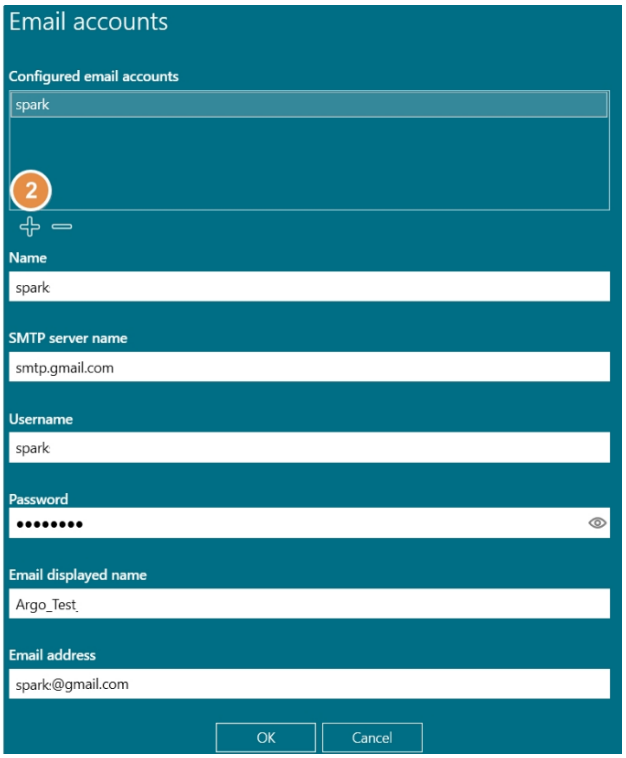
- Photo Send Interval (seconds): Set the time interval for image sending
- Token: Paste the LINE Messaging API token (see Section 3.2)
- Notification Message: Default content for device disconnection or malfunction

Default Message: The device is experiencing issues and cannot provide service temporarily. Please perform simple troubleshooting. We will notify you again once the system recovers

5.2.2 Email Notification

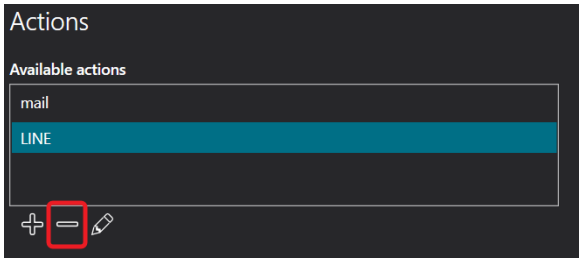
Set up email notifications to alert users immediately when an error occurs. Emails include error descriptions and instructions for further action.





5.3 Deleting a Response Action

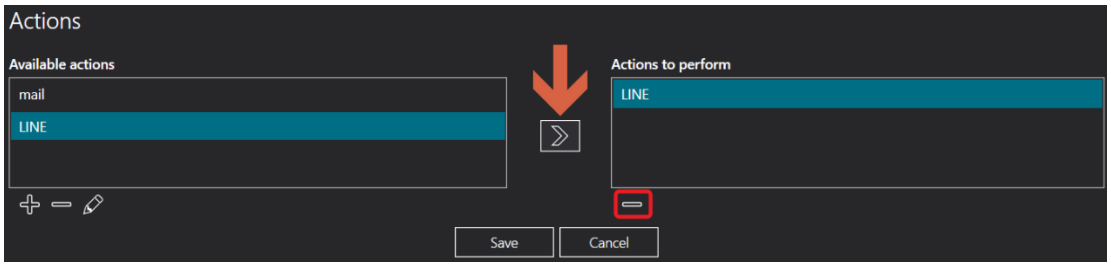
When certain actions are no longer needed, users can delete them to simplify management.



- **Select the response action to delete from Available Actions and click [-]**

5.4 Executing a Response Action

After configuring a response action, it must be applied to take effect.



- **Apply to Actions to perform: Select the action from Available Actions and click [>]**
- **Delete from Actions to perform: Select the action in Actions and click [-]**

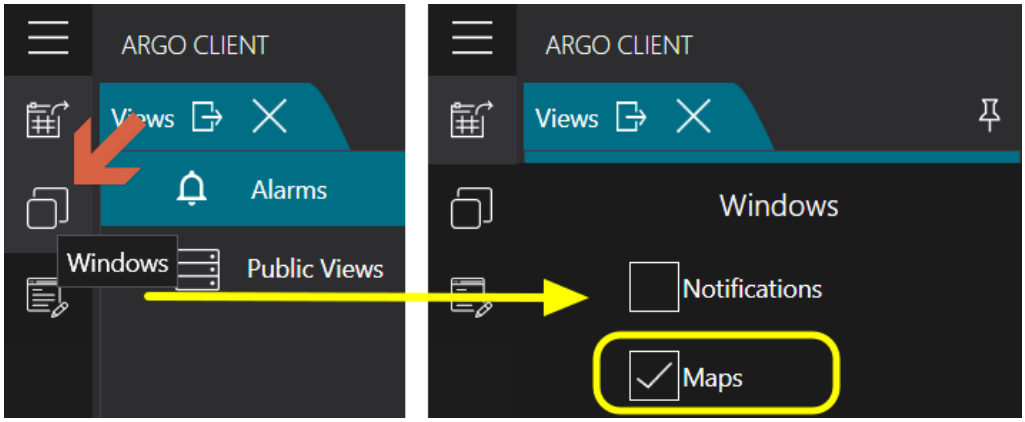
6. HOW TO USE THE E-MAP FOR VISUALIZED DEVICE MANAGEMENT

This chapter introduces how to use the E-Map feature to manage devices visually. Devices can be placed on the map for intuitive and efficient management.

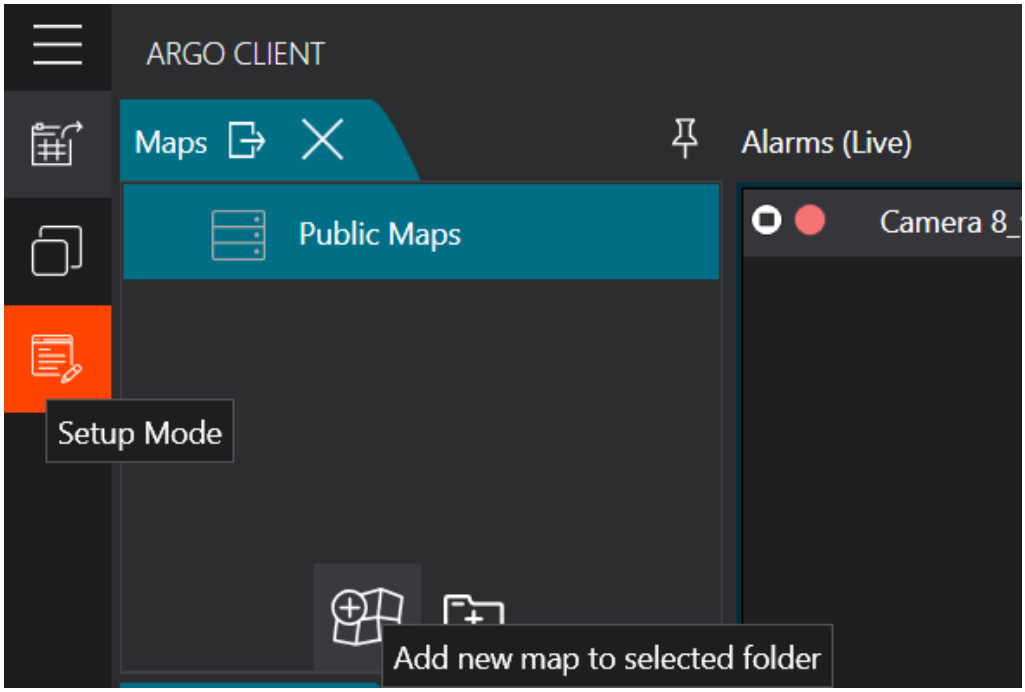
6.1 Add a New E-Map

Set up a new E-Map as a base for device management. Users can clearly visualize the device locations on the map for easier operations and maintenance

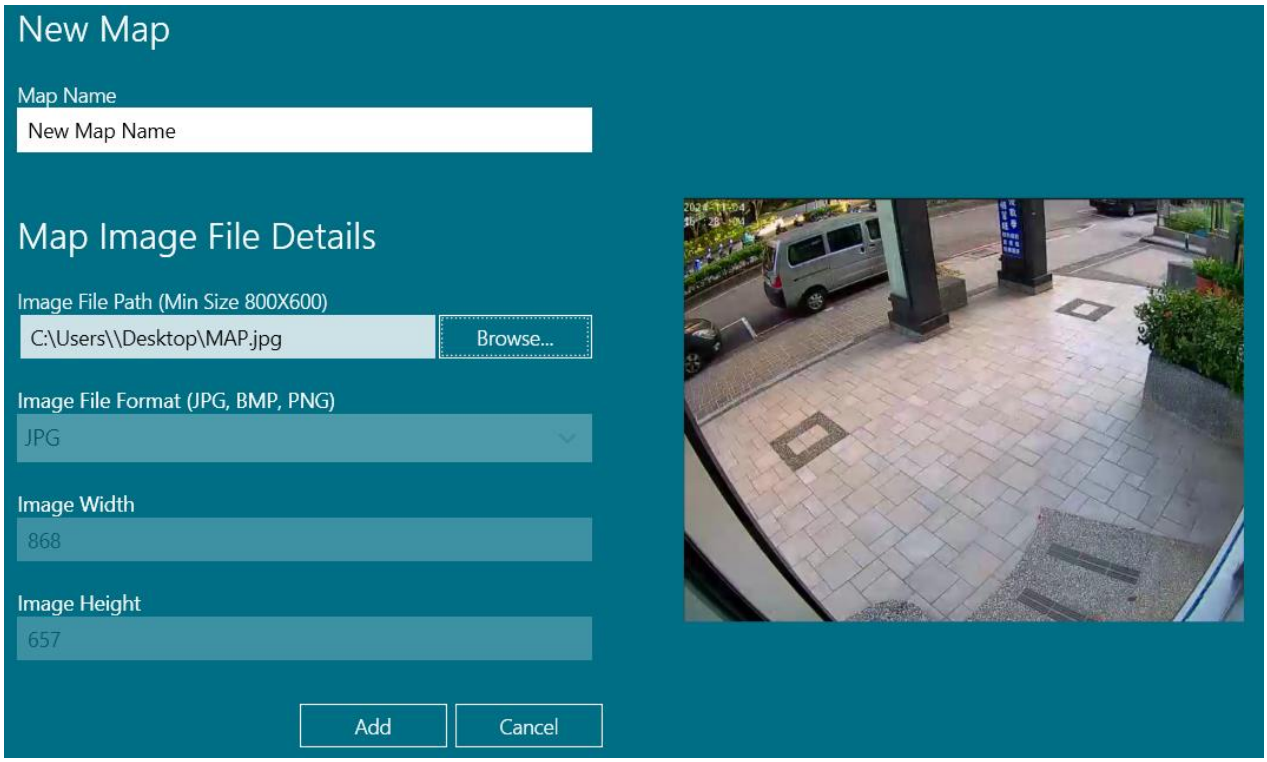
Step1 On the Client application, click the left-side window icon and enable the map function.



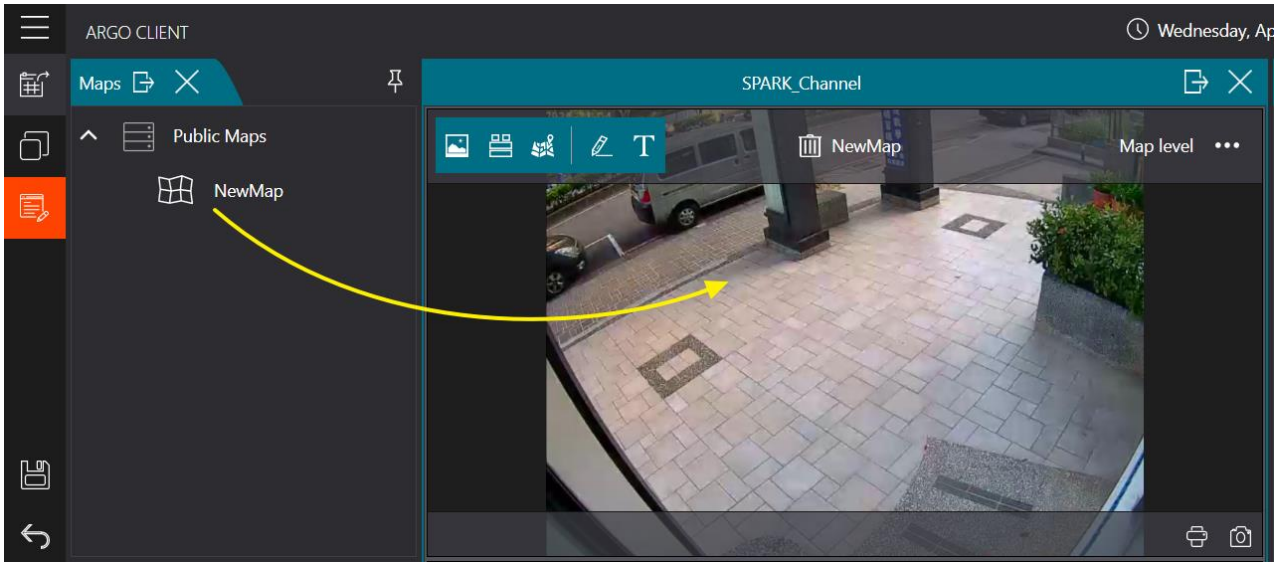
Step2 Enter Edit Mode and click [Add New Map to Selected Folder] to start editing a new map.



Step3 Enter a name for the E-Map, click [Browse] to select an image file, preview the image on the right, and click [Add] to save



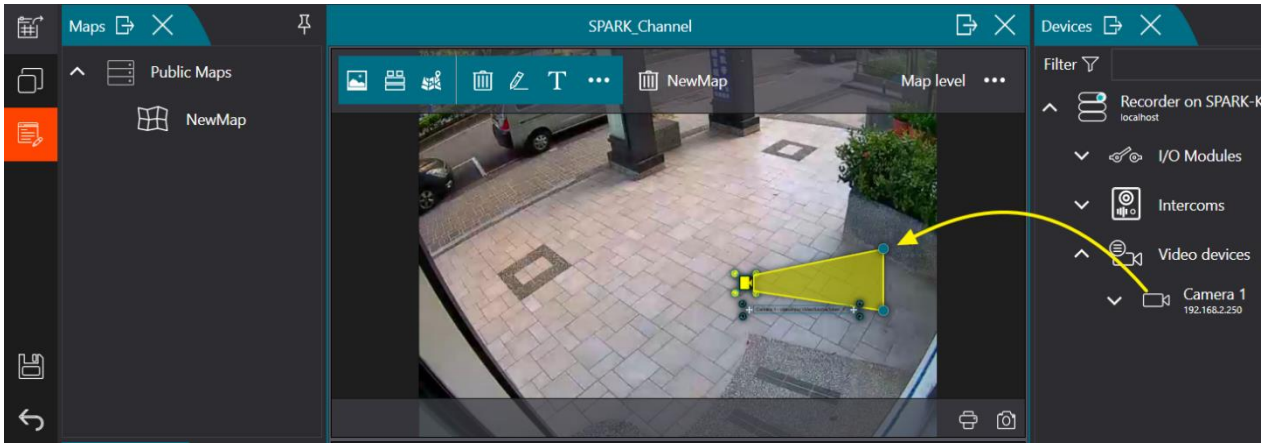
Step4 Drag the newly added E-Map into the live view area on the right, then click [Save] to apply changes



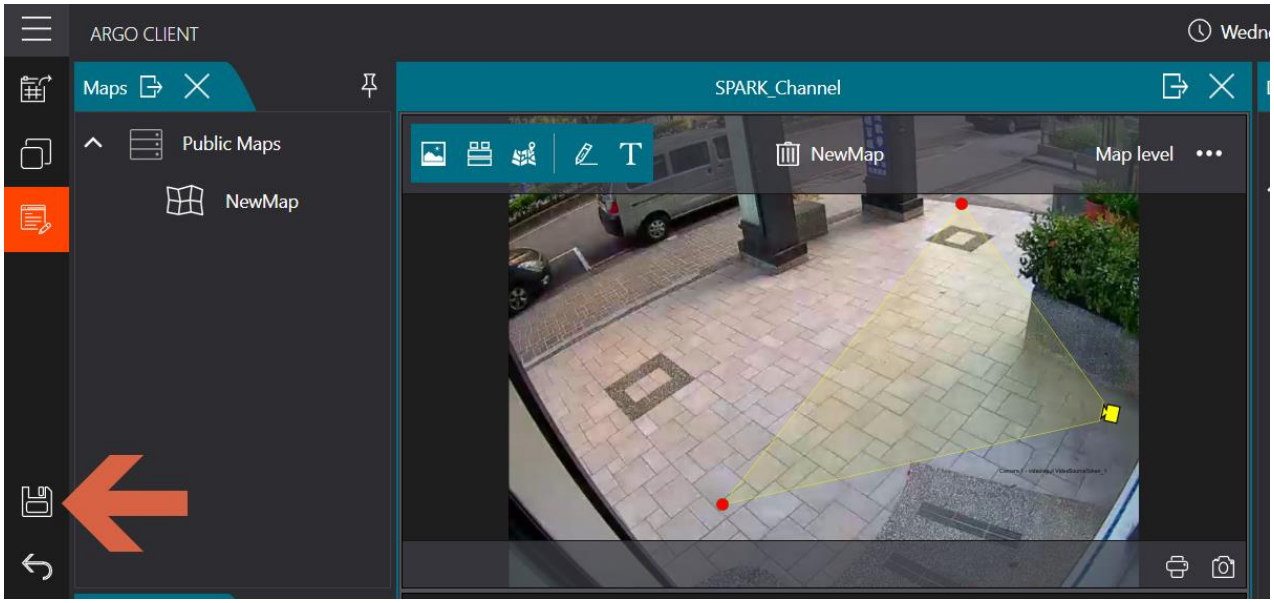
6.2 Place Devices on the E-Map

This section explains how to accurately place devices on the E-Map, allowing users to see each device' s location and status on the map.

Step1 In Edit Mode, drag and drop video devices into the live view window to display them on the map



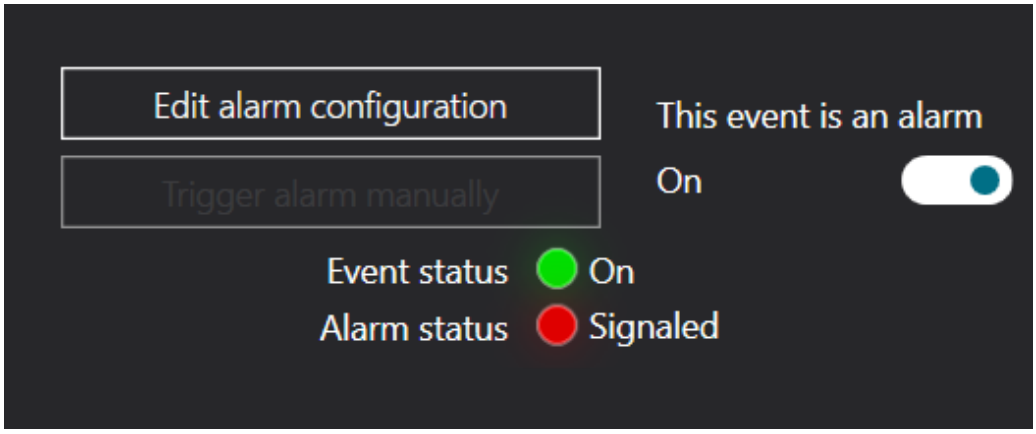
Step2 Drag alarm icons to desired locations, then click [Save] to apply changes



6.3 Enable Alarm Flashing Alerts

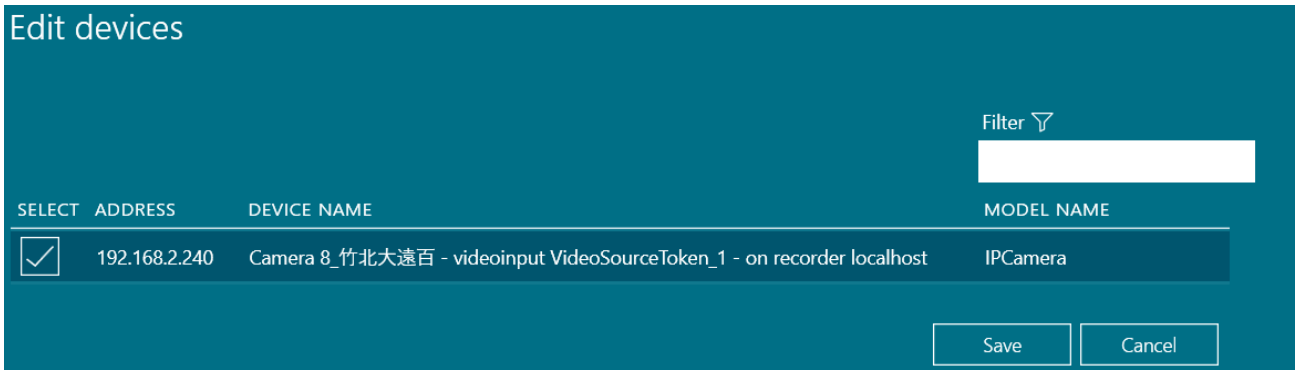
Configure flashing alerts on the E-Map when alarms occur. This helps users notice devices that require attention.

Step1 On the Config > Events and Alarms page, select the event to link, then click [Edit Alarm configuration]

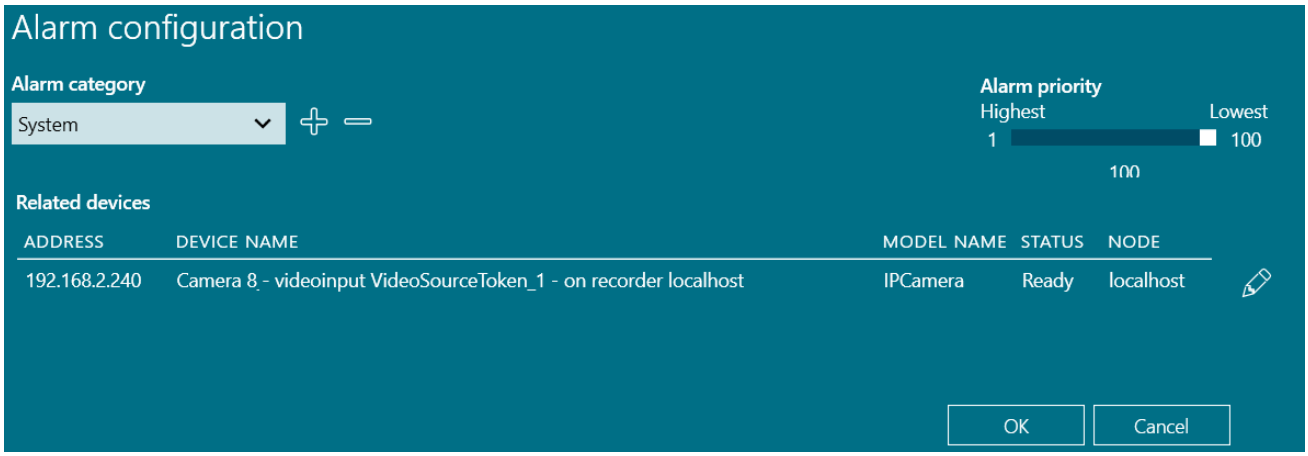


Step2 Click the related device to enter the device edit page

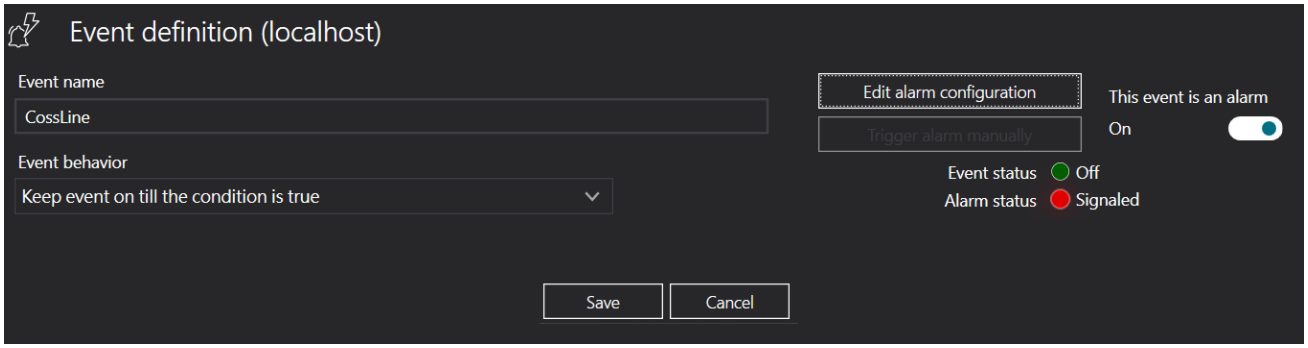
Step3 Select the camera to link with the alarm icon, then click [Save]



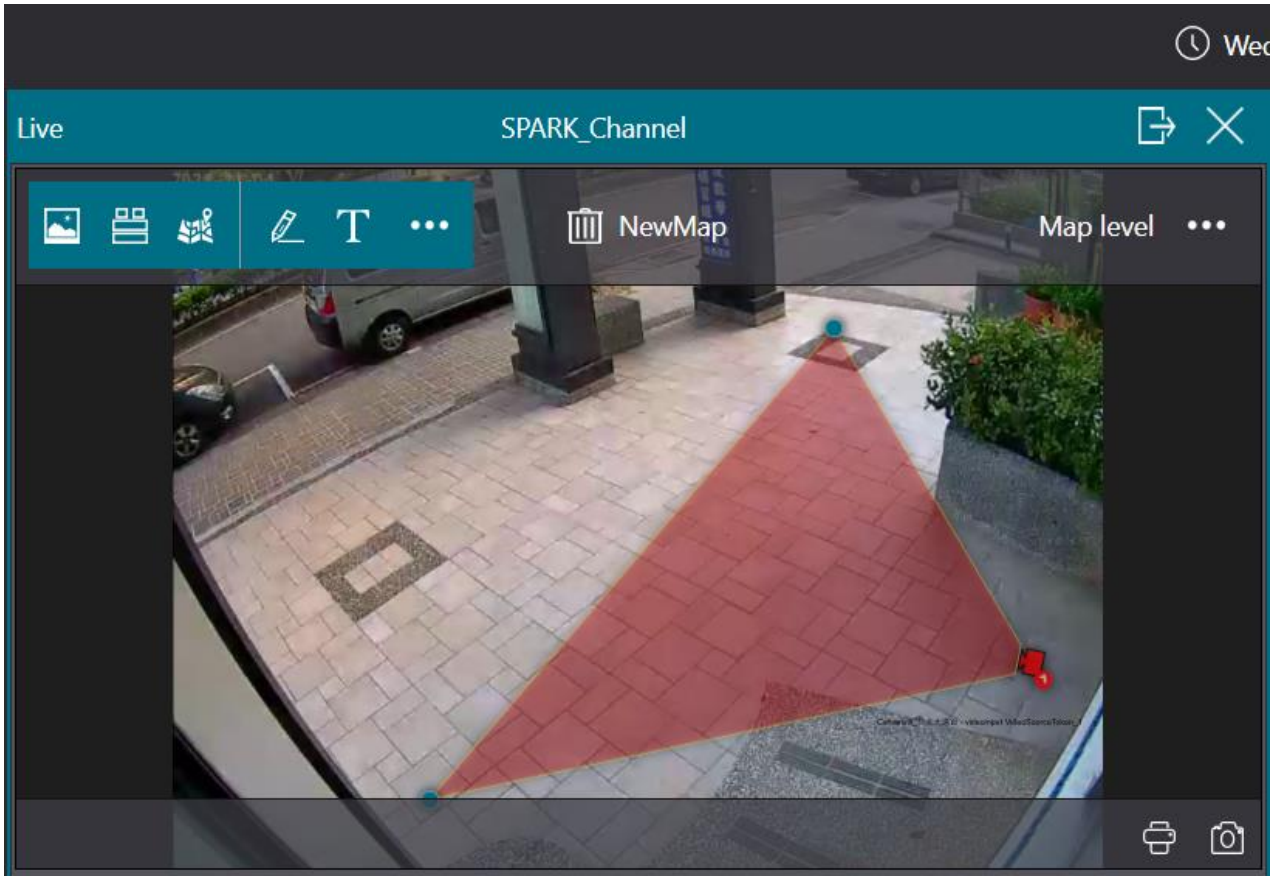
Step4 Return to the Alarm Configuration page and click [OK] to save



Step5 Return to the Event Definition page and click [Save] to finalize



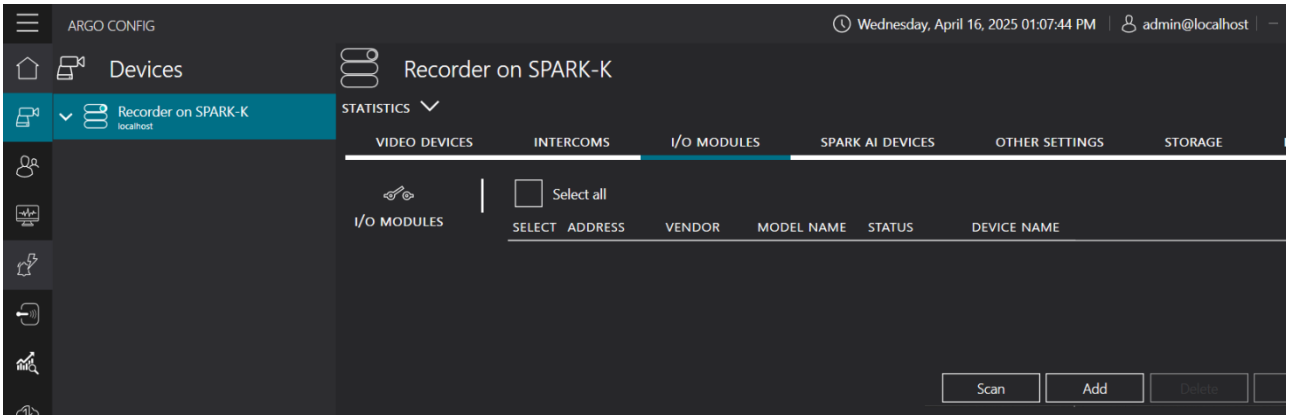
Step6 When an alarm occurs, the linked device will flash on the E-Map to alert the user



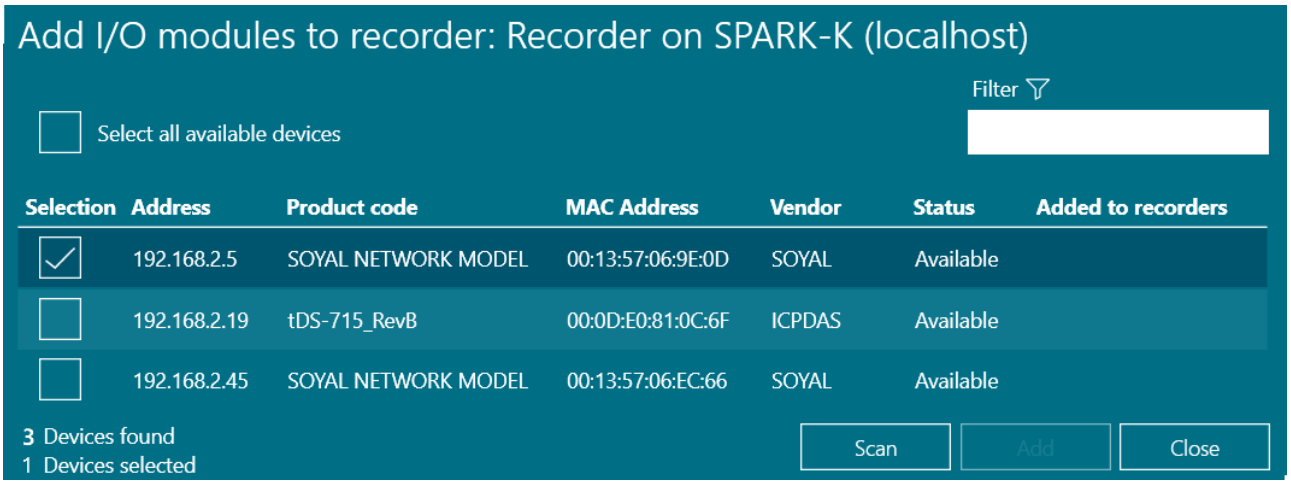
6.4 Remote Control of I/O Devices via E-Map

This section explains how to use the E-Map to remotely control I/O devices, enhancing remote device management convenience.

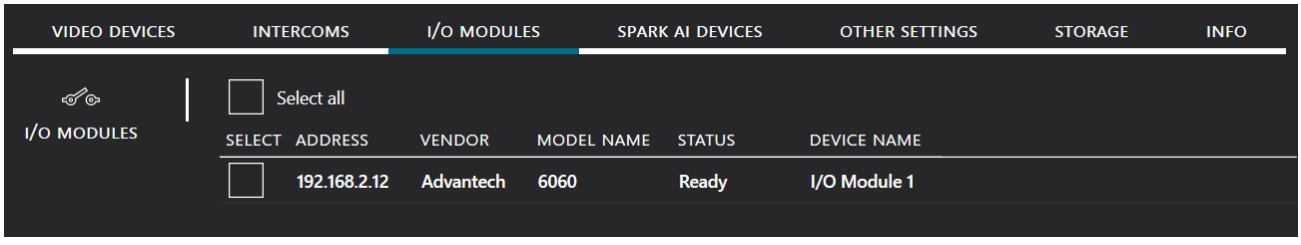
Step1 On the Device page, click the I/O Module, then click [Scan] to auto-discover and add I/O devices.



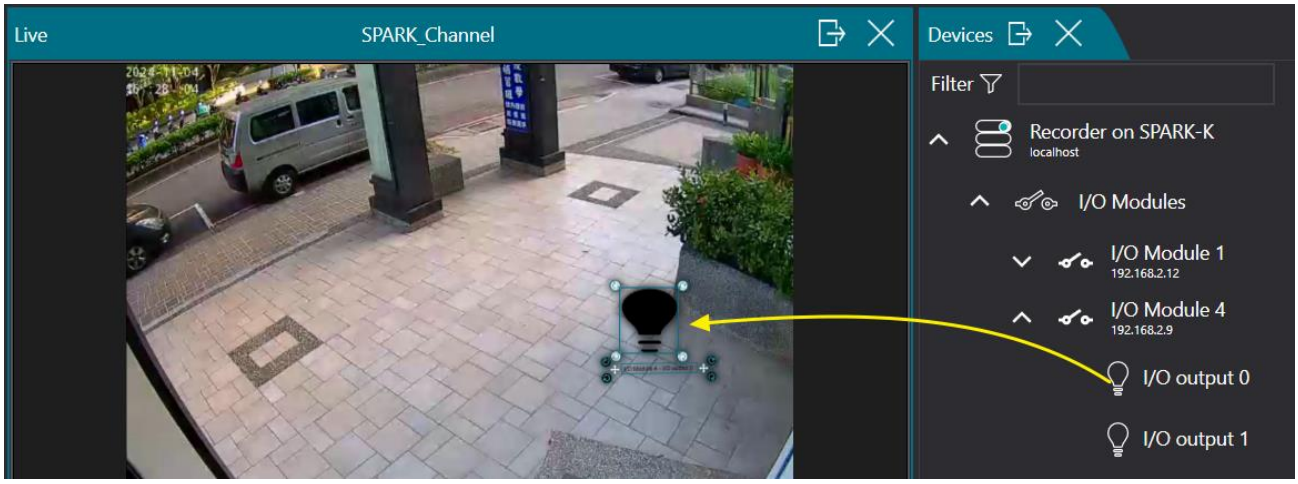
Step2 Select the newly discovered I/O device



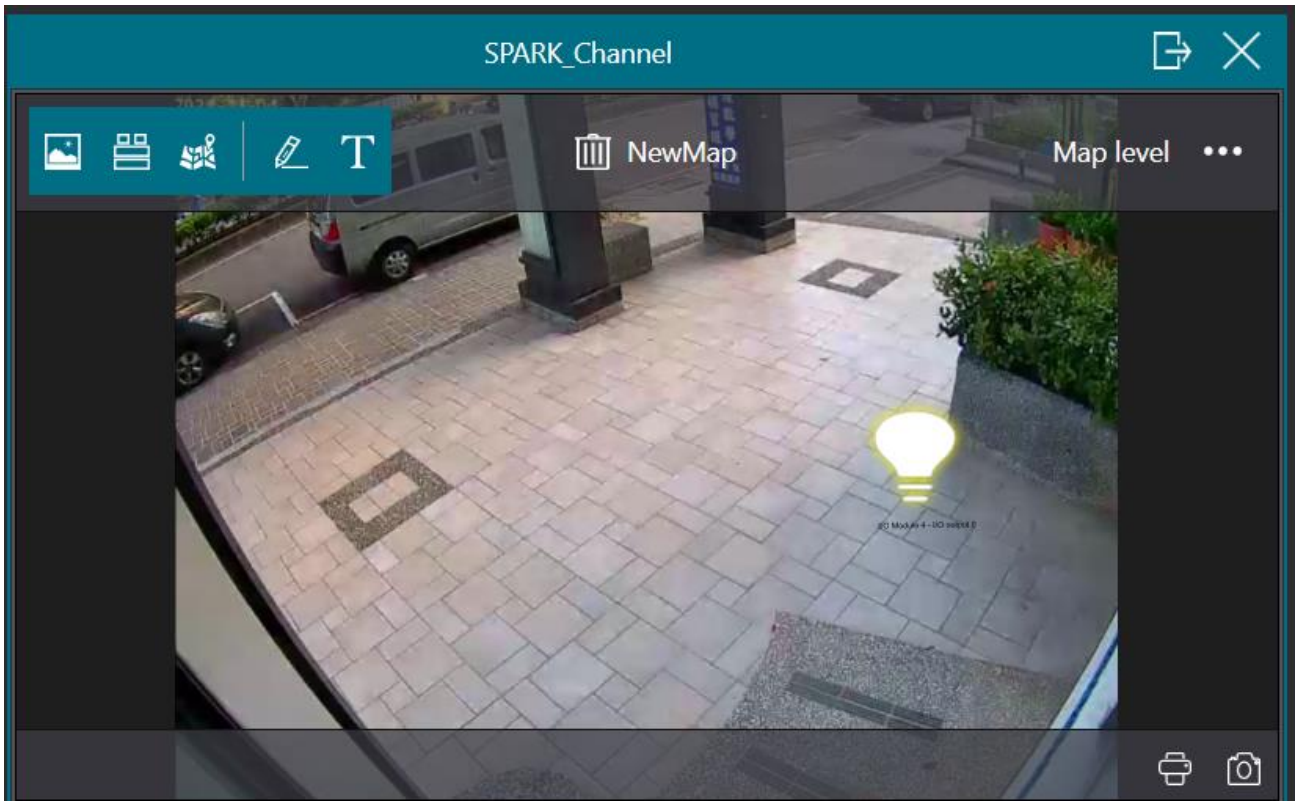
Step3 Once added, the I/O device status will be displayed



Step4 In Edit Mode on the Client, drag the I/O Output switch onto the live view window, then click [Save]



Step5 Exit Edit Mode, click the I/O icon on the map to control the device's on/off status



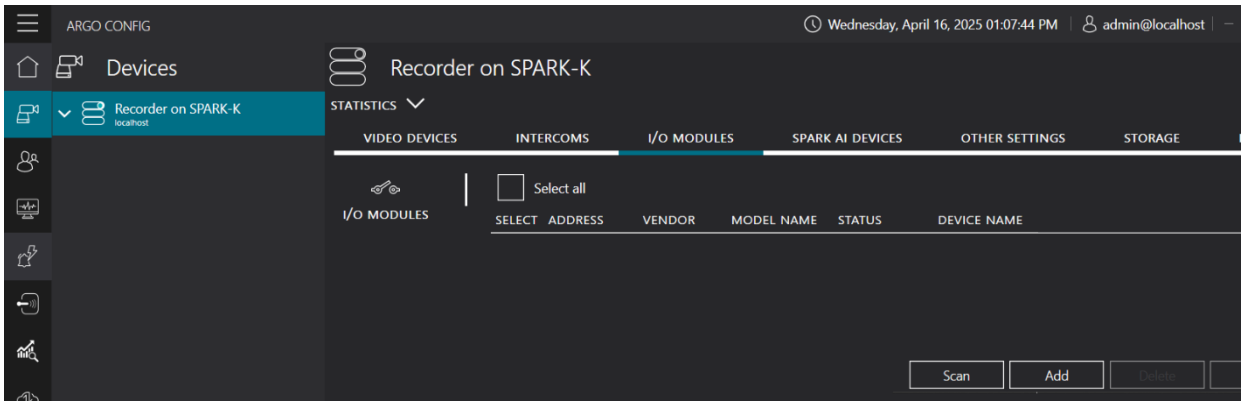
7. HOW TO USE ARGO FOR ACCESS CONTROL MANAGEMENT

This chapter explains how to manage access control using ARGO. After completing the setup in this chapter, users can monitor and control personnel and vehicle entry using I/O or RFID devices through the Access Control interface, ensuring safety and efficient management.

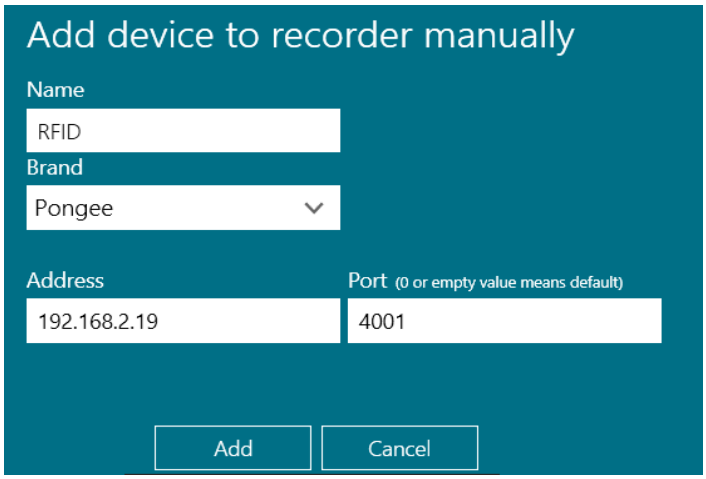
7.1 Add I/O Access Devices

Set up I/O access devices and add them to the ARGO system for management. ◦

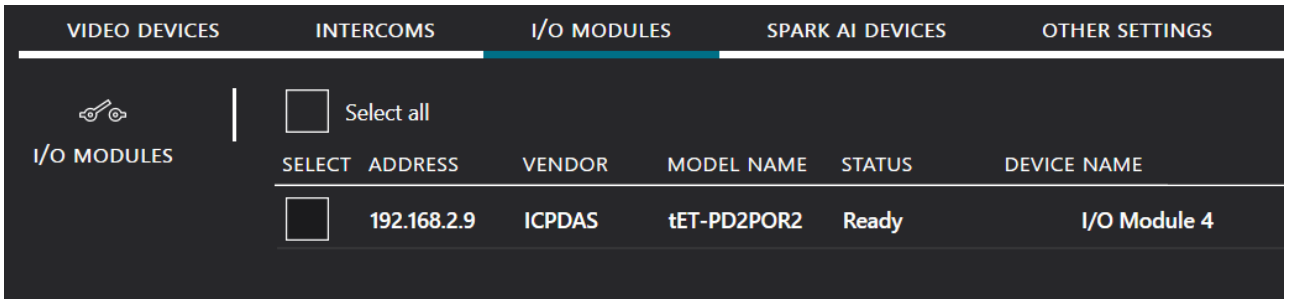
Step1 On the Device page, click the I/O Module, then click [Add] (manual input) to add the I/O device



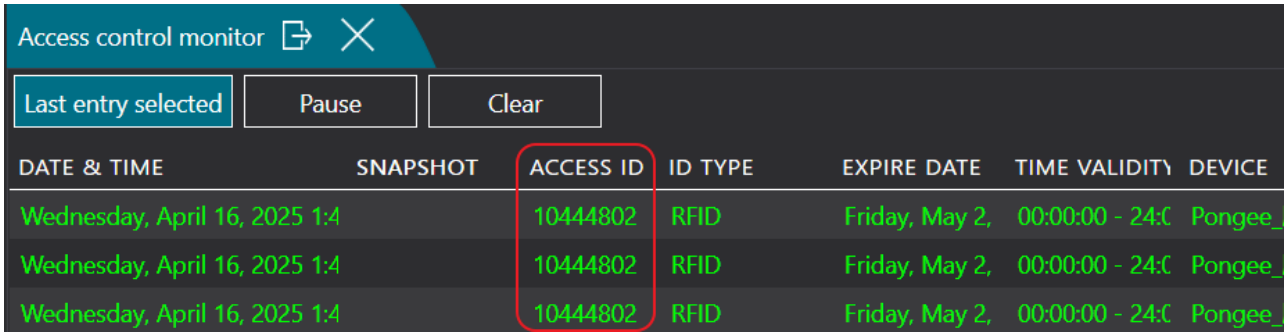
Step2 Enter the device name➔ Select brand➔ Enter IP address and port 4001 ➔ Click [Add] to save



Step3 Once added, the device status will be shown as available



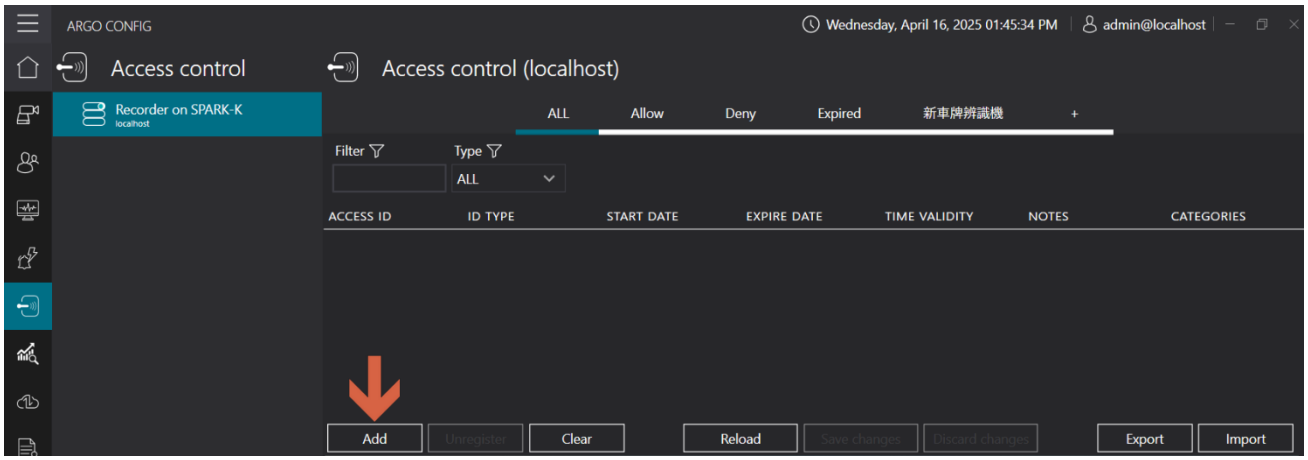
Step4 Open the Access Control monitoring view on the Client to view identification results



7.2 Add Access List

Configure access lists to grant entry permissions to specific personnel, ensuring only authorized individuals can access certain areas.

Step1 On the Access Control Service page, click [Add]

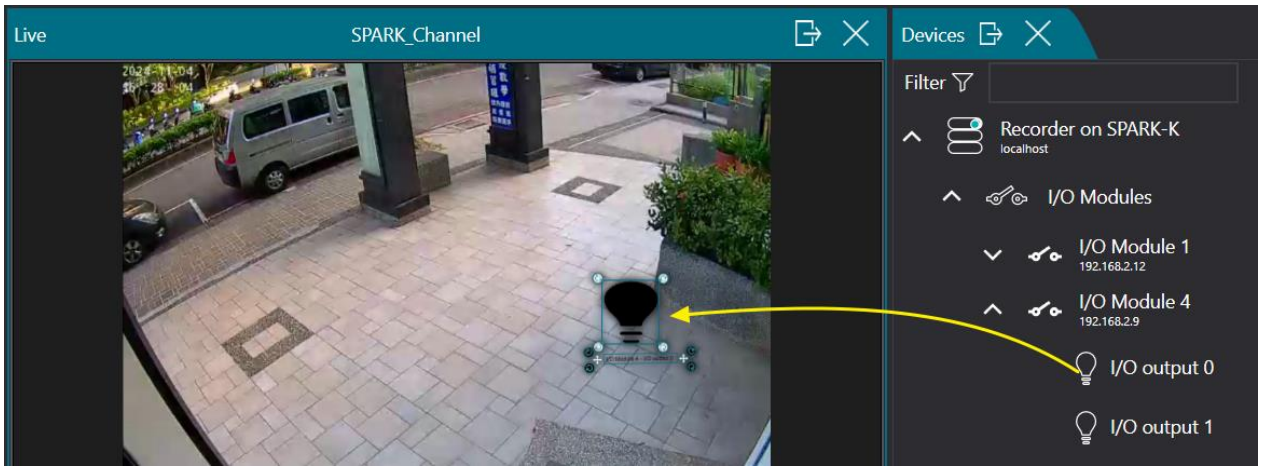


Step2 Enter access ID information➔ Select ID type (RFID)➔ Set valid date range➔ Set valid time range➔ Add remarks➔ Select whitelist or blacklist➔Click [Add] to save

7.3 Place I/O Devices on the E-Map

Add I/O devices to the E-Map for easier monitoring and control.

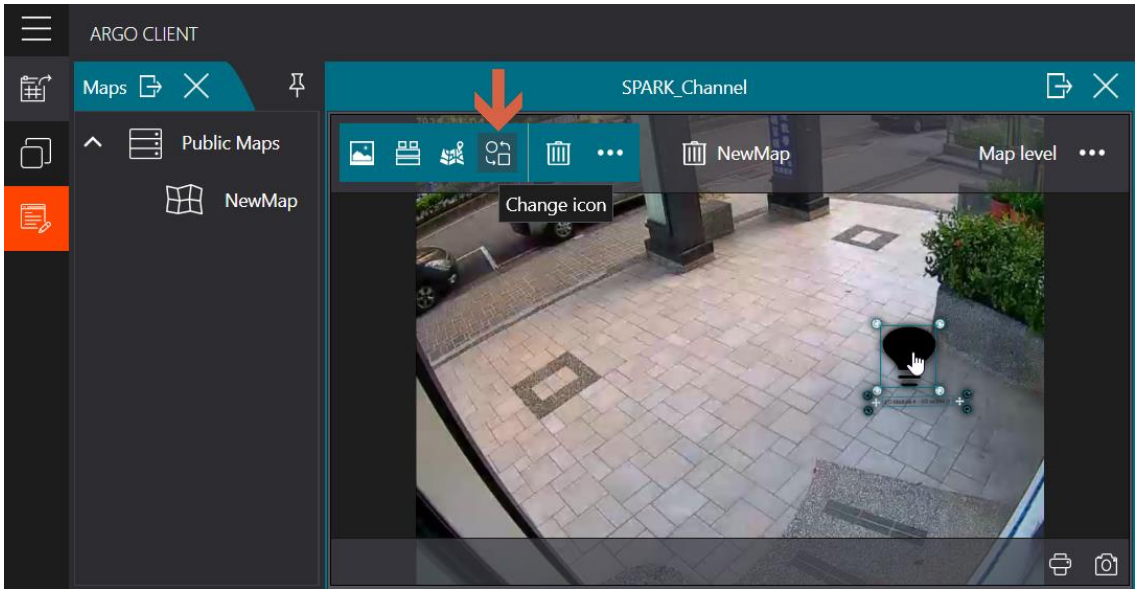
Step1 In Edit Mode on the Client, drag the I/O Output switch into the live view window, then click [Save] to apply changes



7.4 Change Device Icons on the E-Map

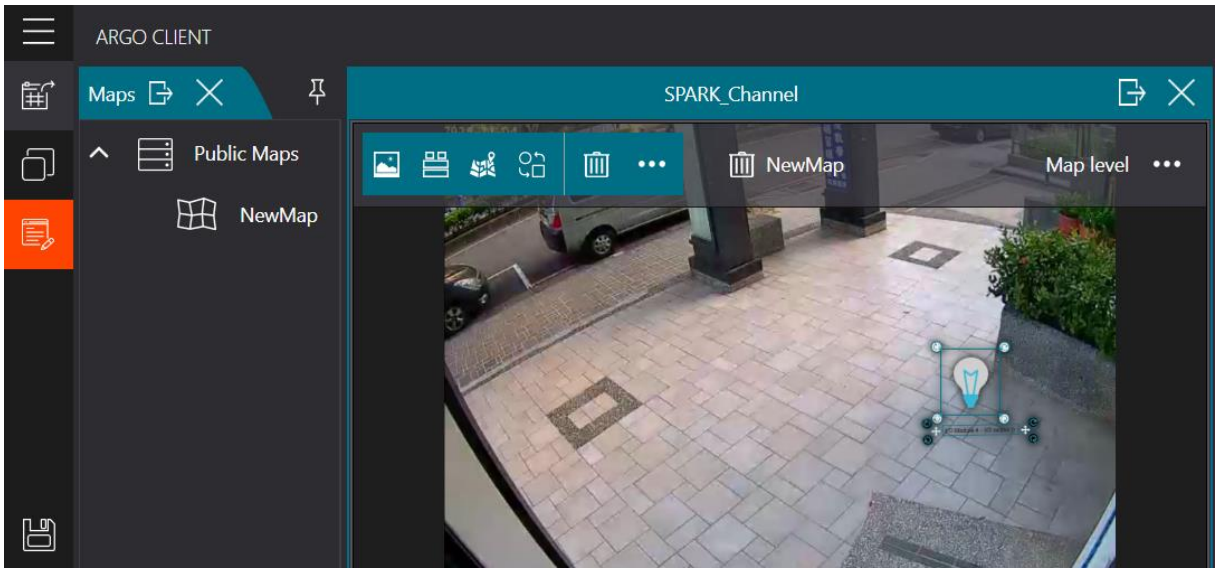
This section explains how to update or change icons for I/O devices on the E-Map for better visualization.

Step1 In Edit Mode, select the I/O device and click [Change Icon].



Step2 Choose the new icon and click [OK] to save

Step3 After changing the icon, click [Save] to apply changes

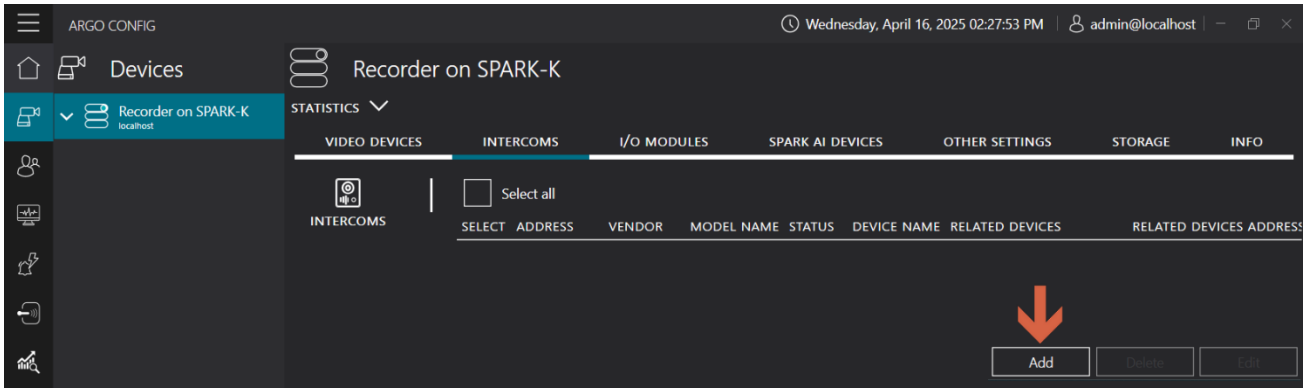


8. HOW TO USE INTERCOM FOR REAL-TIME COMMUNICATION AND MANAGEMENT

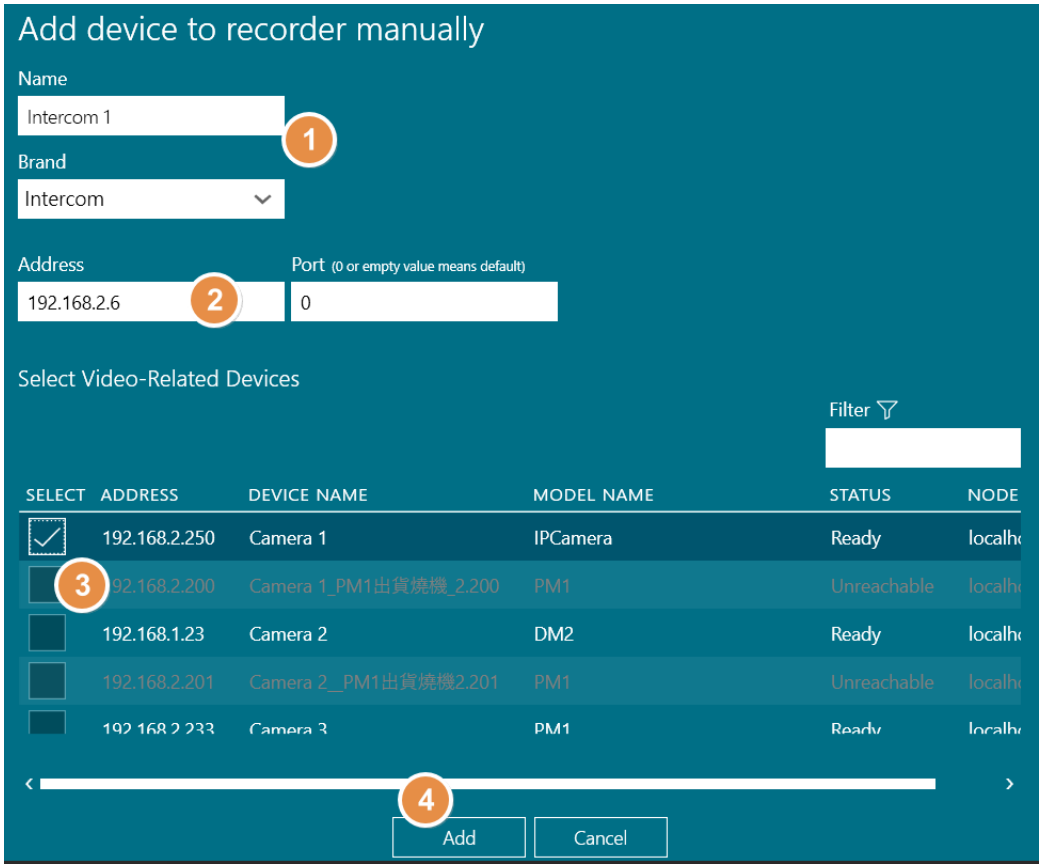
Argo supports SIP-based intercom devices, enabling real-time two-way voice communication. Some devices also support video intercom, displaying live camera views during calls.

8.1 How to Add Intercom Devices

Step1 Click [Add]

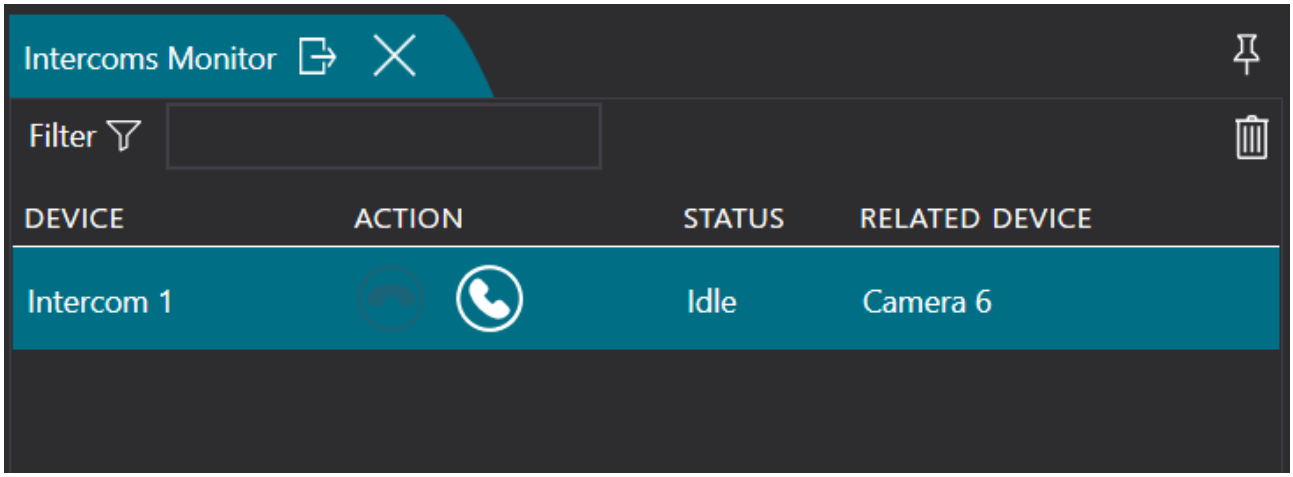


Step2 Manually input the device information, then select the camera to associate with the intercom for displaying video during calls

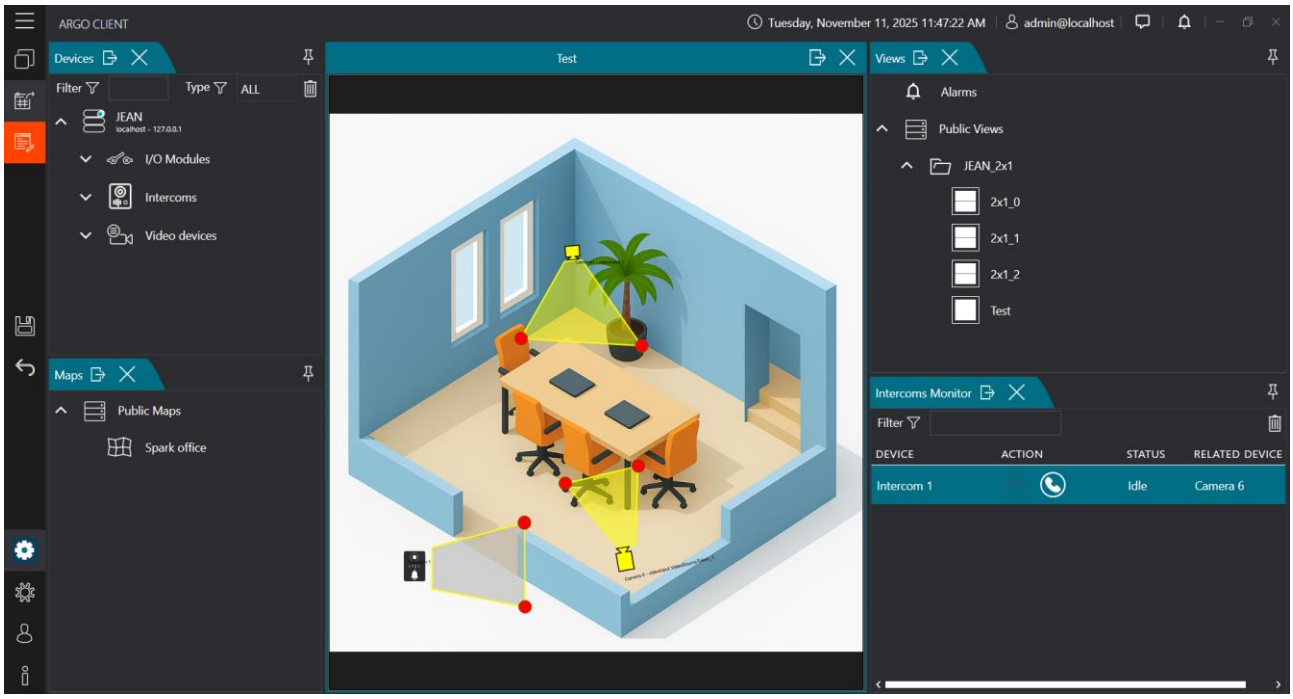


8.2 How to Use Intercom in the Client

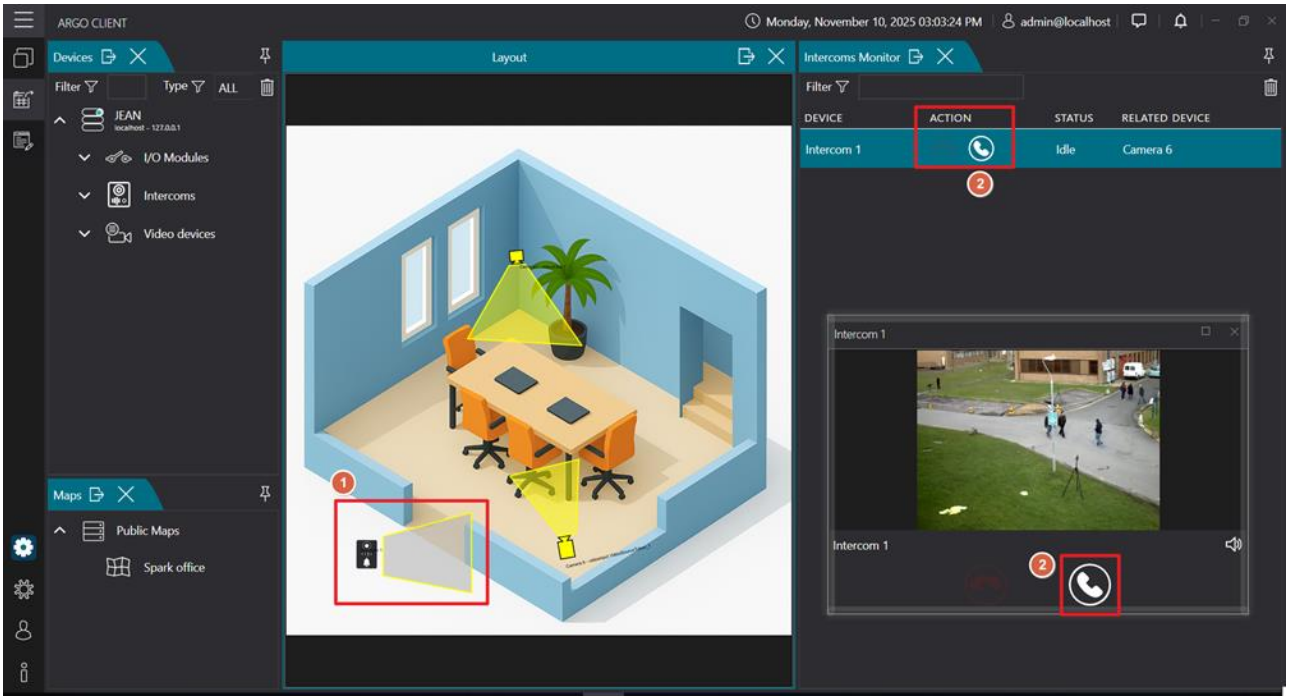
Step1 Open the Intercom Monitoring page to access call control features.



Step2 In Edit Mode, place the intercom device on the E-Map. When a call comes in, the video will be displayed, and you can answer directly.



Step3 After adding the intercom device to the E-Map, click it to open a real-time call window for dialing, or make calls through the Intercom Monitoring interface.



Step4 Hang up

Step5 Call / Answer

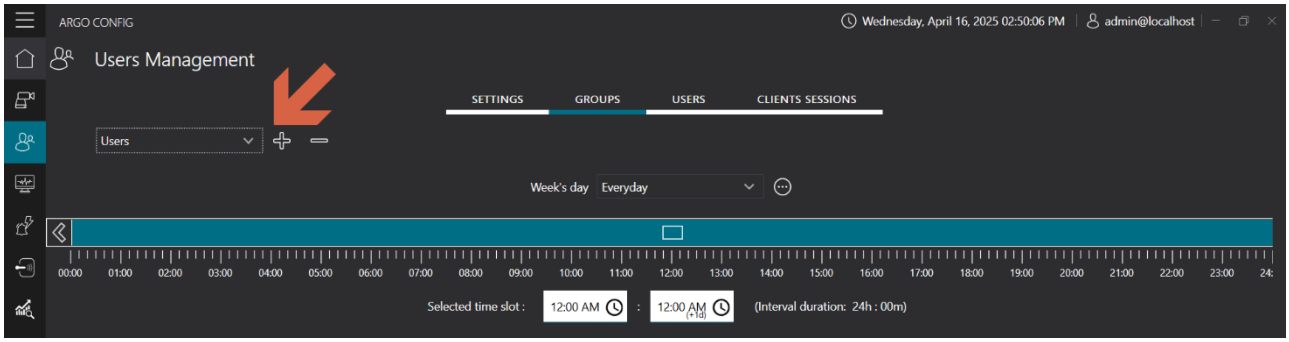
9. HOW TO ASSIGN USER PERMISSIONS

This chapter explains how to set different user privileges to ensure system security and stability. By assigning permissions, you can control access to sensitive functions and restrict unauthorized operations, protecting data and system integrity.

9.1 User Permissions

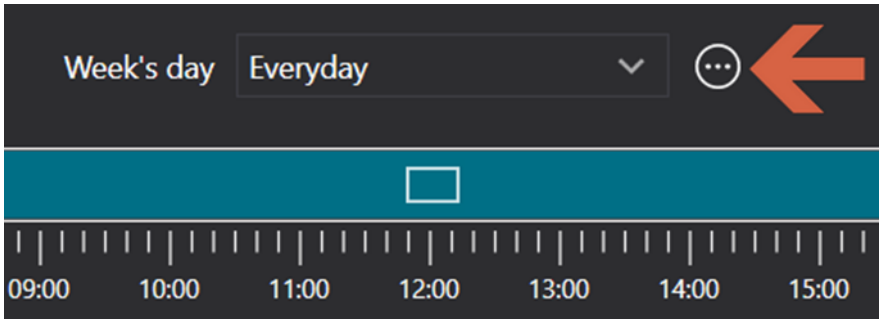
This section details how to configure permissions for each user. You can limit access to system settings, data, and sensitive features, improving overall security.

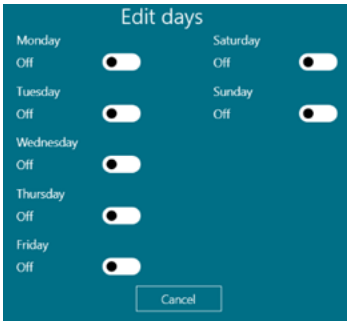
Step1 Go to User Management and click [User Group] to configure group permissions



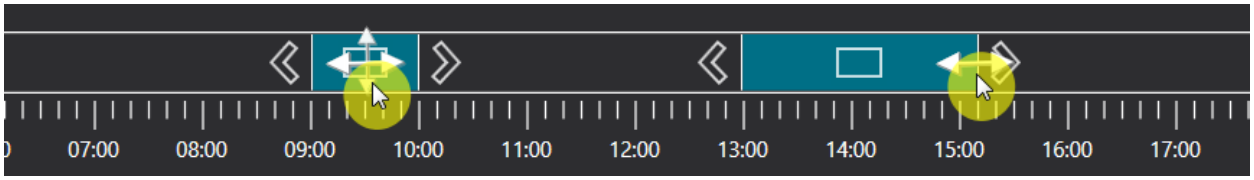
Step2 Set viewing schedule restrictions:

(1) Schedule: Click  **to edit weekly viewing schedules**

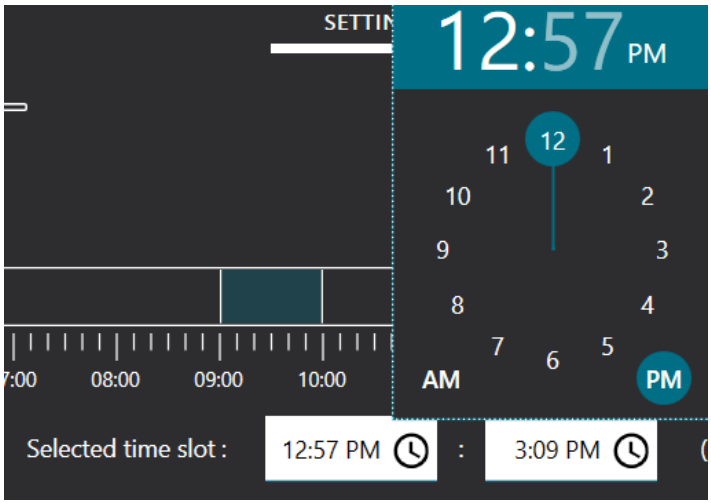




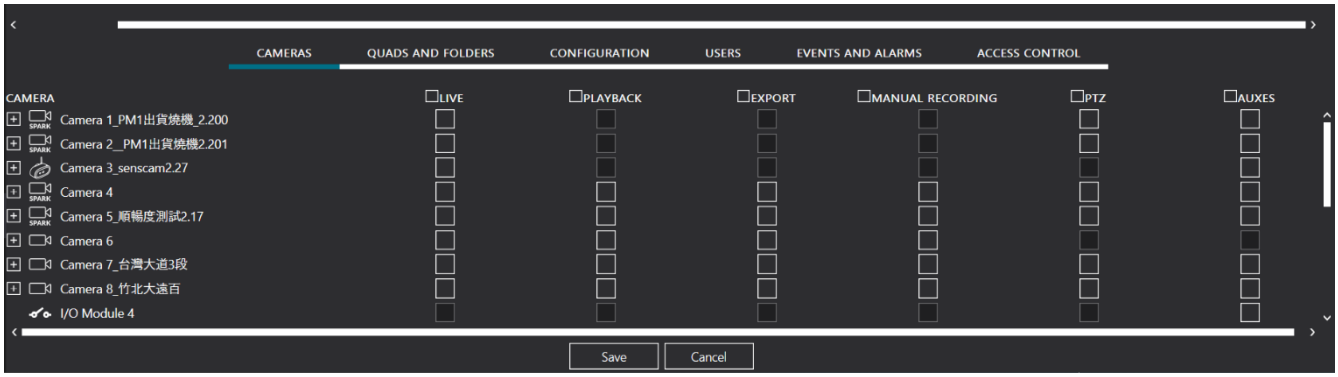
(2) Time Segments: Drag arrows to adjust time range.
Click [+] to add or remove time periods



(3) Time Picker: Click the clock icon to adjust time slots



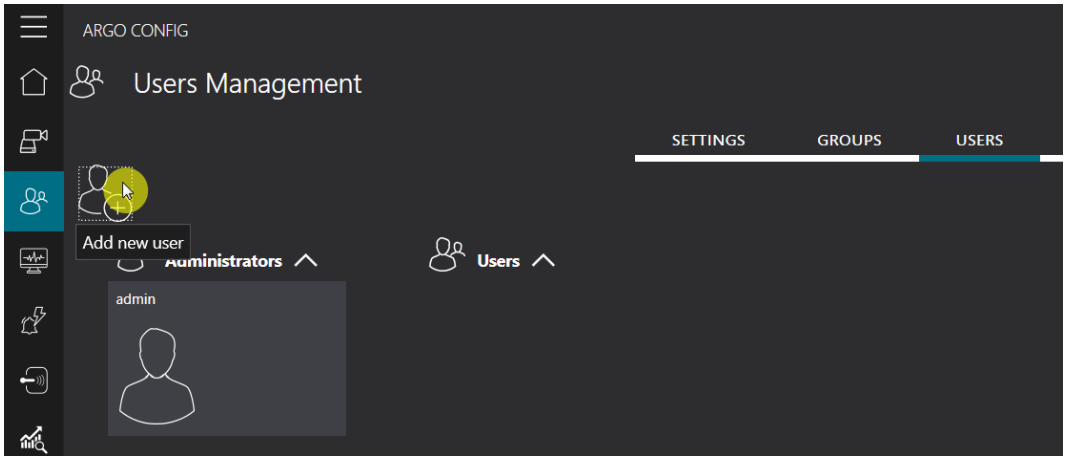
Step3 Assign permissions for cameras, quads and folders, configuration, user, events and alarms, and access control ➔ Click [Save] to apply



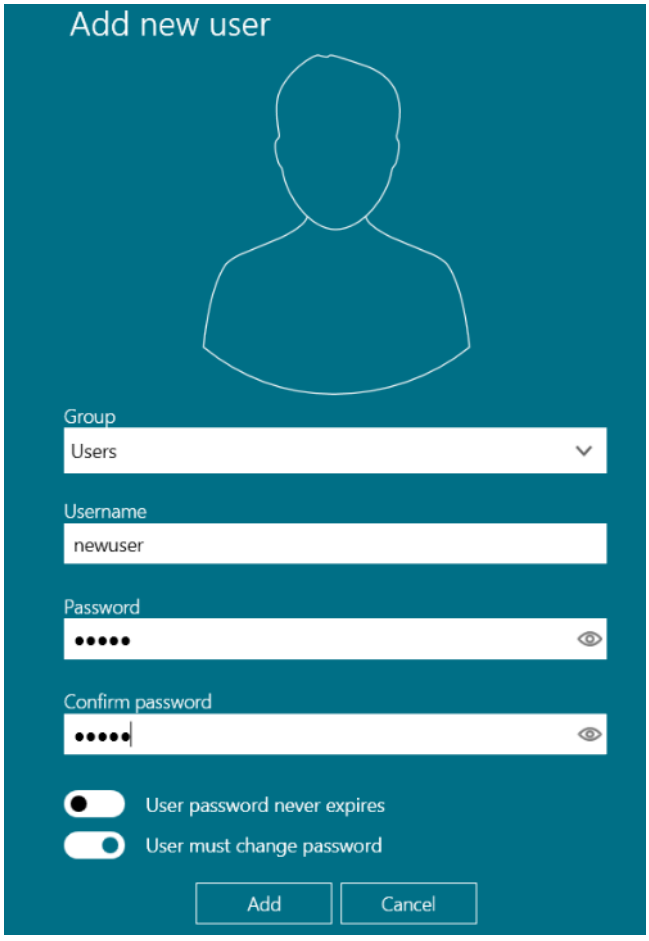
9.2 User Management

User Management simplify permission management. Assign specific permissions to each group for centralized control. This helps organize users efficiently and reduces the need for individual settings.

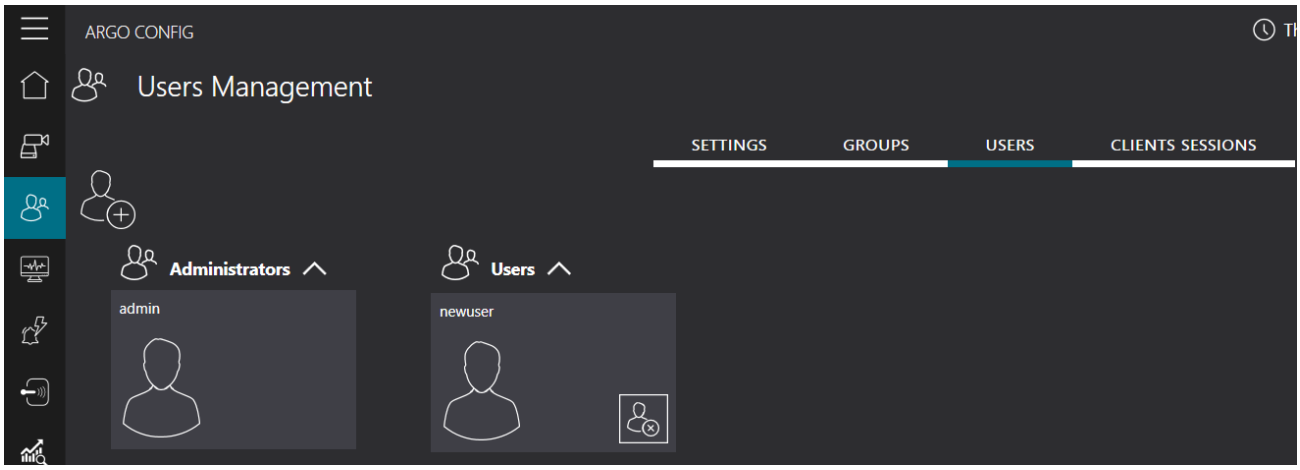
Step1 Click [Add New User]



Step2 Choose a group (Admin/User Group)➔ Enter username➔ Enter password➔Click [Add] to save



Step3 Upon success, the new user will be added to the designated group



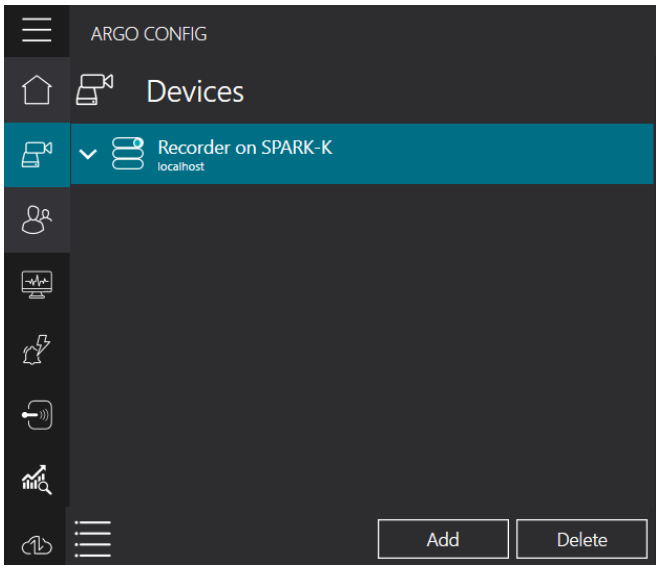
10.HOW TO SET UP THE SERVER AS MASTER/SLAVE/FAILOVER ARCHITECTURE

This section explains how to configure the server as part of a master-slave or failover architecture to improve system reliability, ensure data redundancy, and enable load balancing. This ensures the system continues to operate even in the event of a failure.

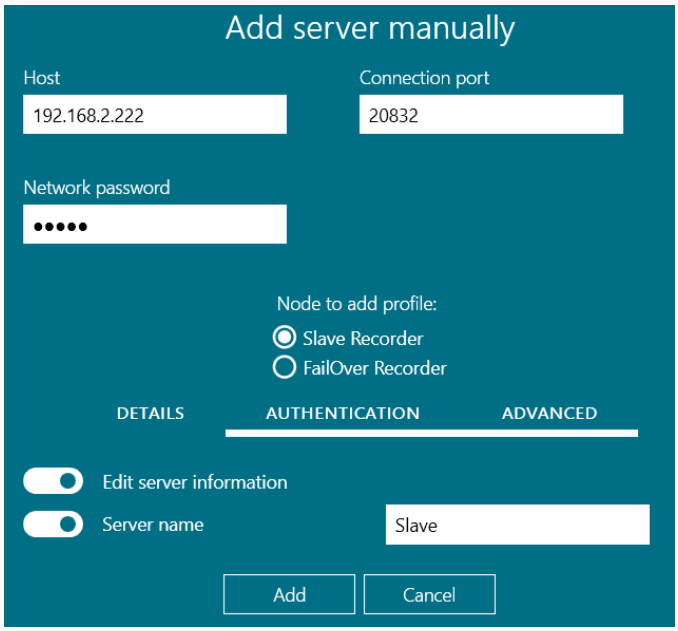
10.1 Adding a Server as a Slave

Setting up a slave server enables data redundancy and load balancing, improving system stability and performance. By configuring a master-slave server architecture, multiple servers can be linked, with a unified monitoring screen and settings. The slave server can also share part of the workload, ensuring continuous system operation.

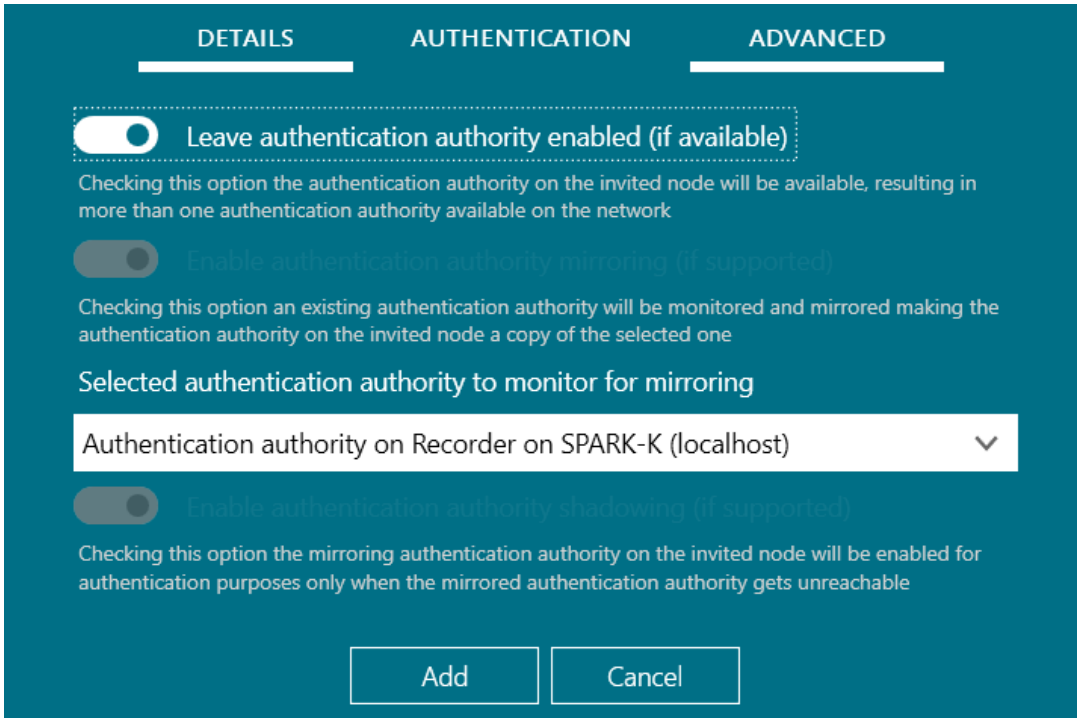
Step1 On the device page, click [Add] to manually add a server.



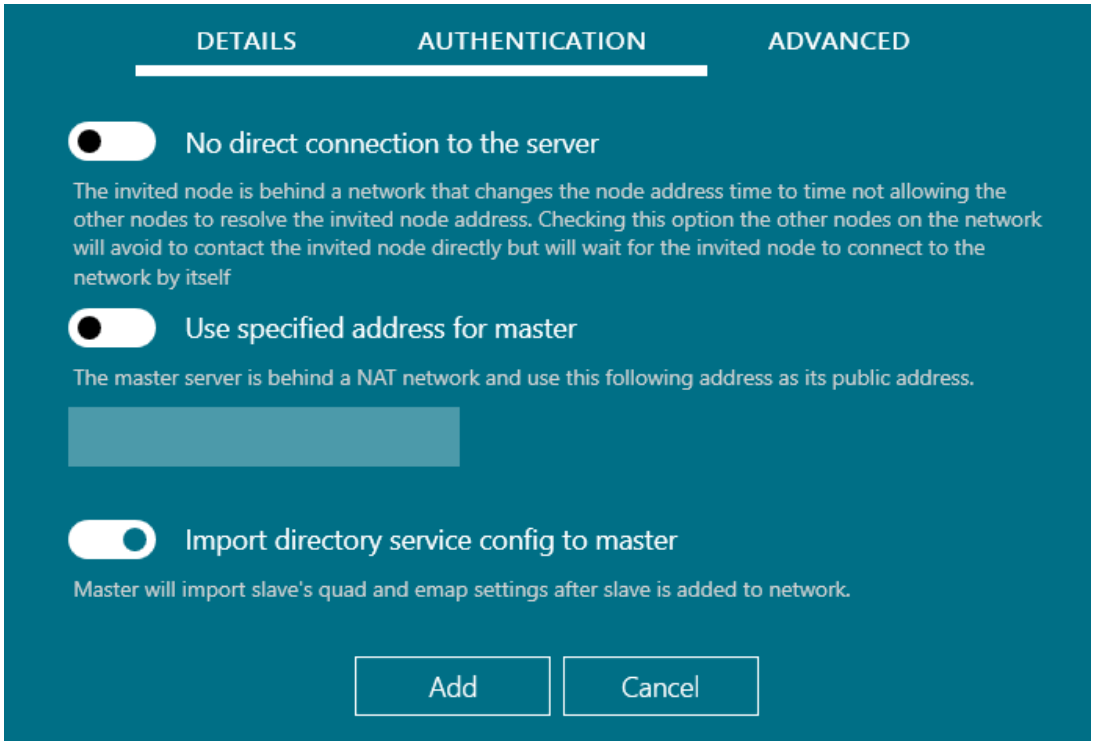
Step2 Enter the server IP address, input the port (default: 20832), and the password (default: admin). Select the slave server option, then edit the server information and name.



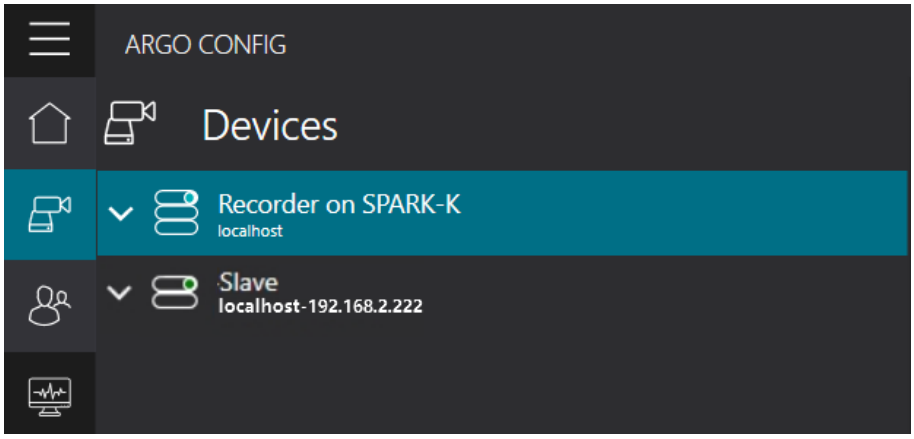
Step3 Enable [Allow Authentication Service]. This feature ensures that after the master-slave server fails, the slave server can continue with the authentication process to allow login.



Step4 Activate [Import Directory Service Config to Master]. This will display the slave server’s monitoring content on the master server’s monitoring screen. Press [Add] to complete the setup



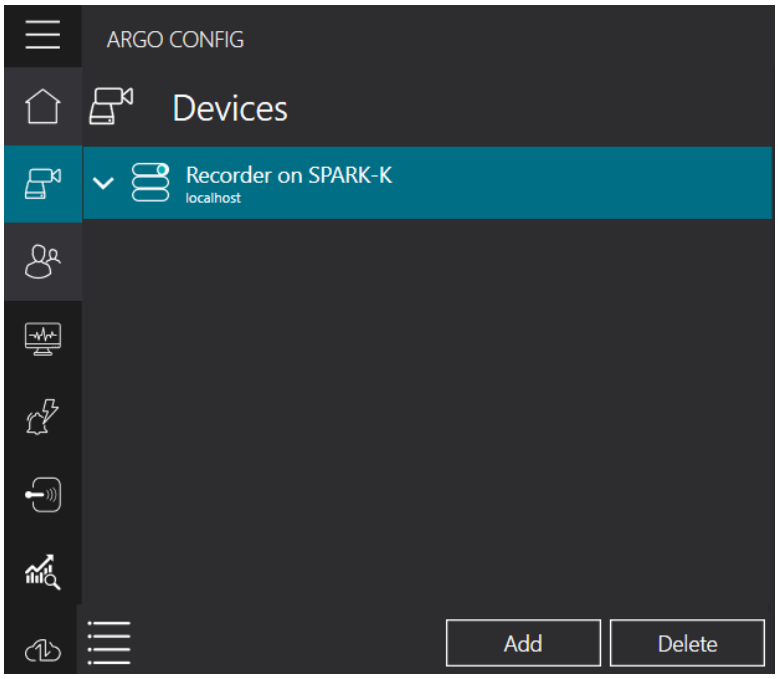
Step5 After completing the steps, you can view the slave server’ s successful addition in the device node field



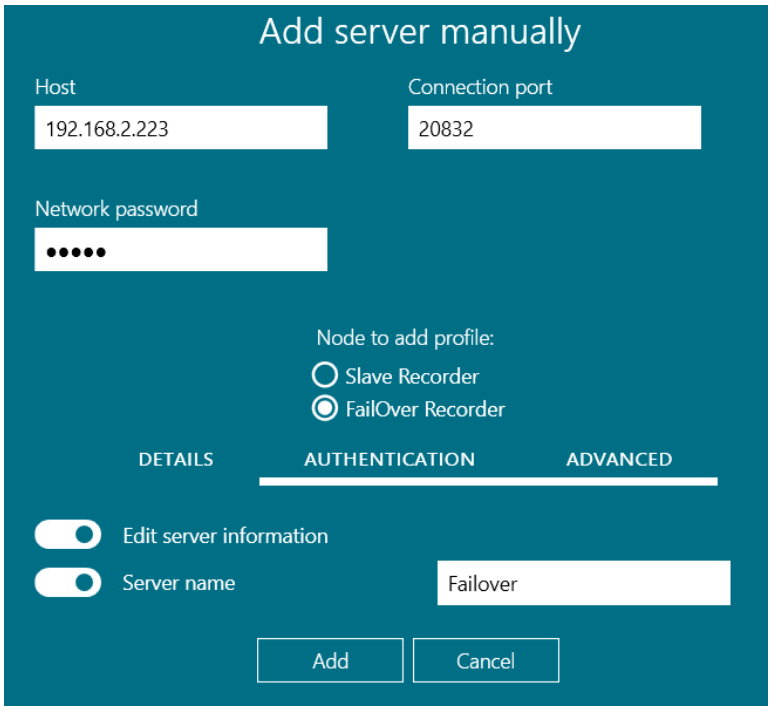
10.2 Adding a Server as a Failover

Set up a failover server to ensure that when the master server fails, the system can quickly switch to the backup server, preventing service disruption

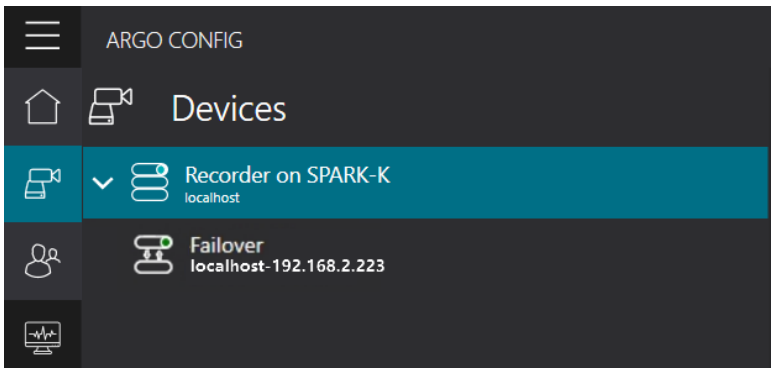
Step1 On the device page, click [Add] to manually add a server.



Step2 Enter the server IP address, input the port (default: 20832), and the password (default: admin). Select the failover server option, then edit the server information and name. Press [Add] to complete the setup



Step3 After completing the setup, you can view the failover server’ s successful addition in the device node field.



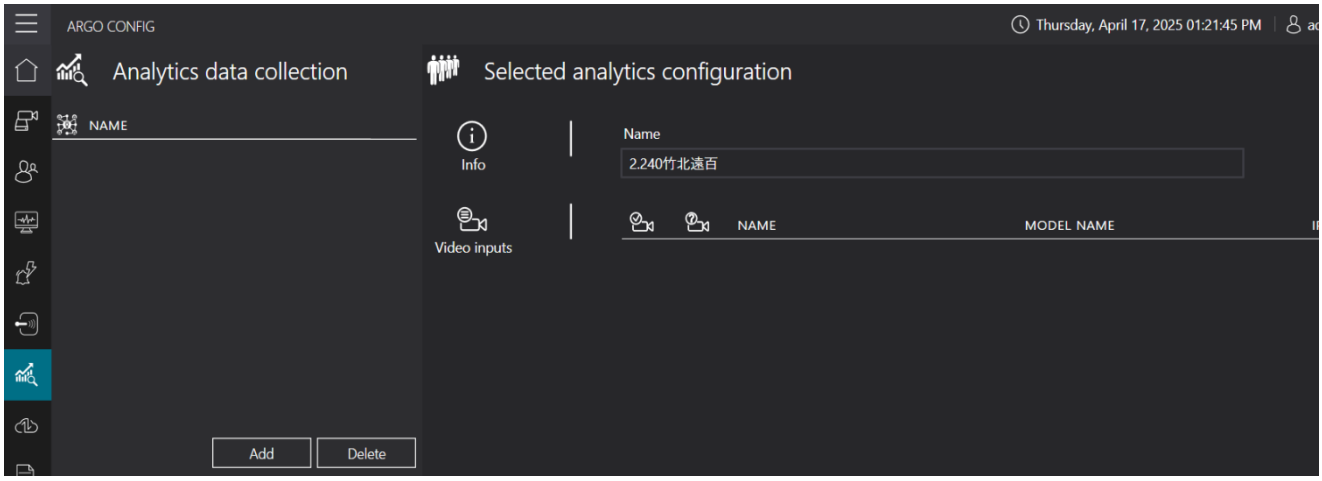
11. HOW TO DISPLAY ANALYSIS DATA ON THE DASHBOARD

This section explains how to display AI analysis data on the dashboard. Through the dashboard, you can visually view statistical results and analysis data after image analysis, including people flow, vehicle flow, and real-time violation cross-line counting information.

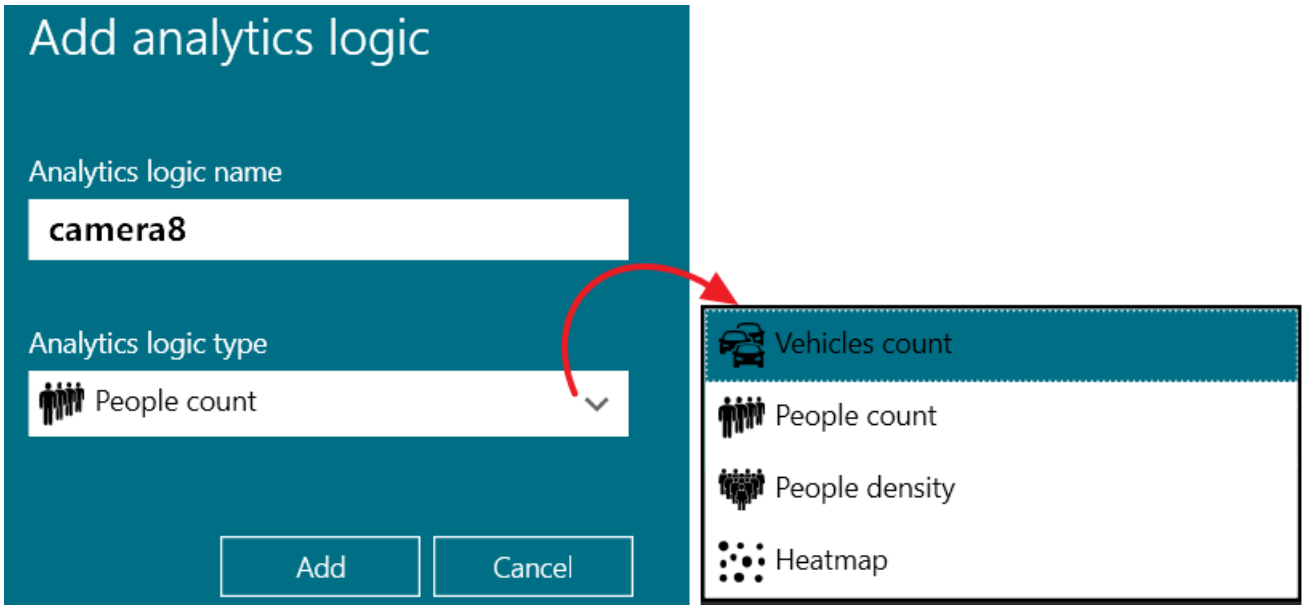
11.1 How to Use Line-Crossing Counting for Object Statistics

Utilize line-Crossing detection for object counting and statistics, and display the results on the dashboard. This feature helps monitor the movement of objects, enabling more accurate statistics and data analysis

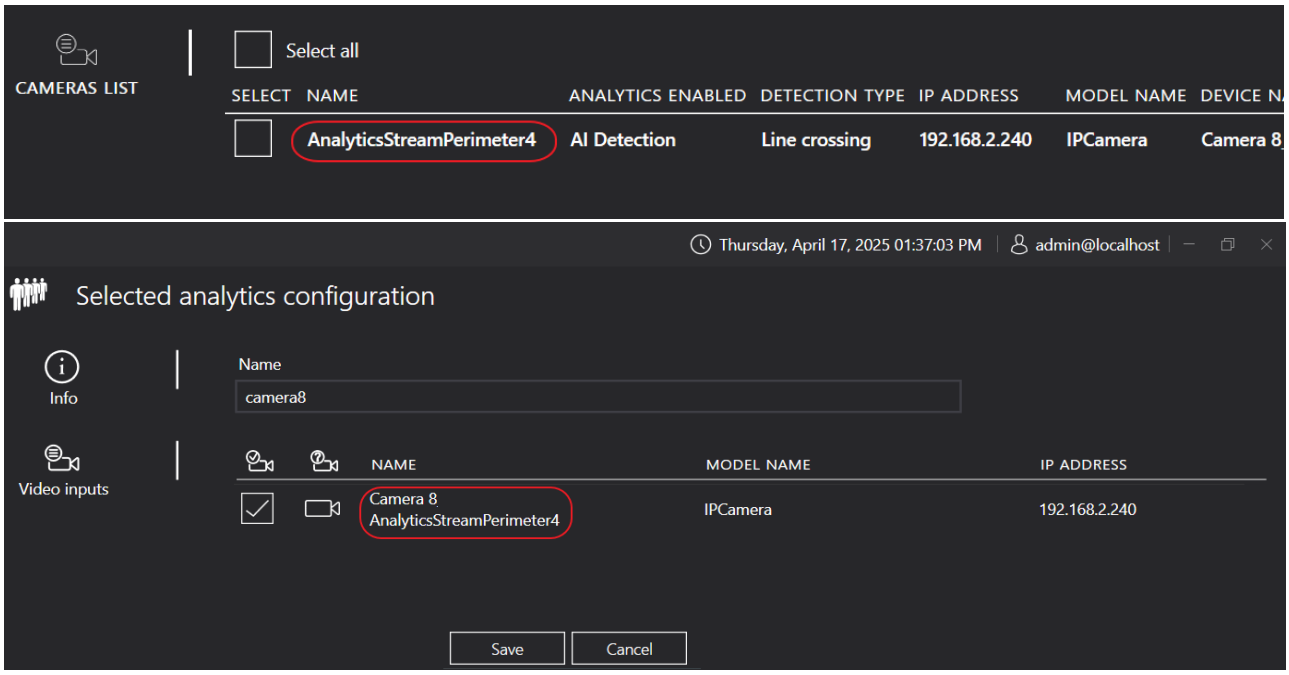
Step1 Click on  for image analysis data and press [Add] to proceed.



Step2 Enter the name for the image analysis logic, and select the logic type, such as People counting

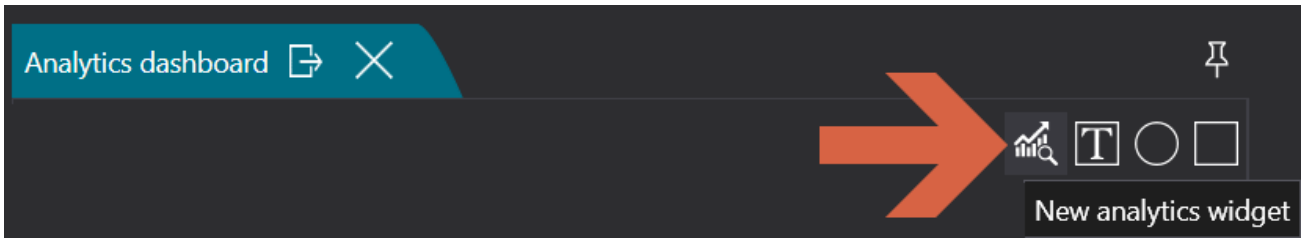


Step3 Select the image input source from the image analysis parameters, which refers to the stream that requires data analysis.

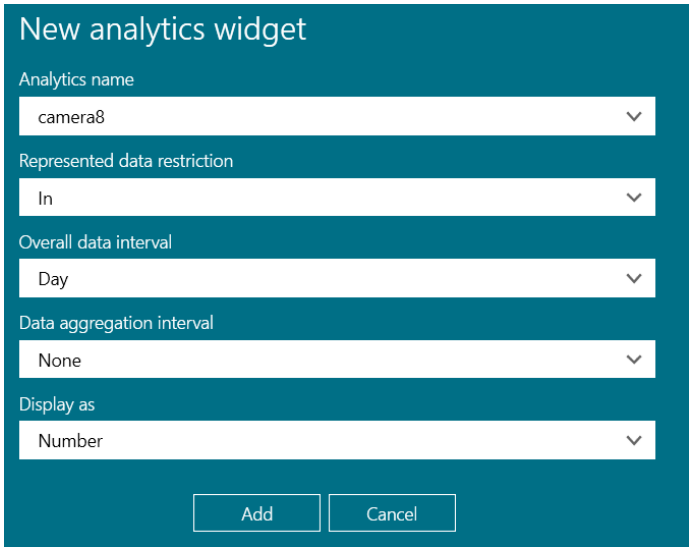


Step4 Open the Client, click on  window, and check 

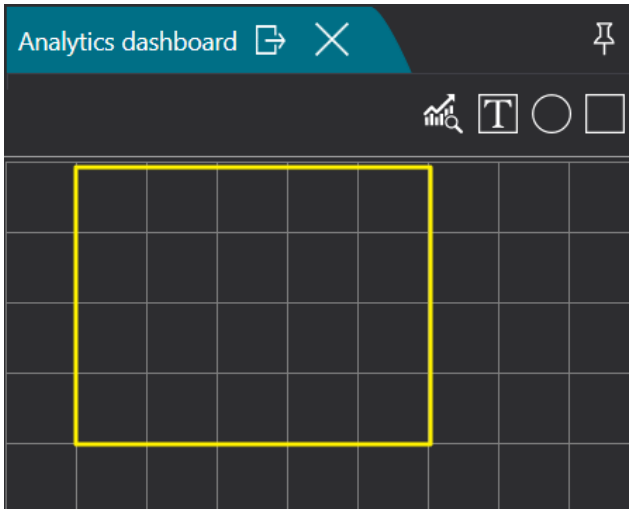
Step5 Press  in edit mode ➔click  ➔Add Image Analysis Component to proceed.



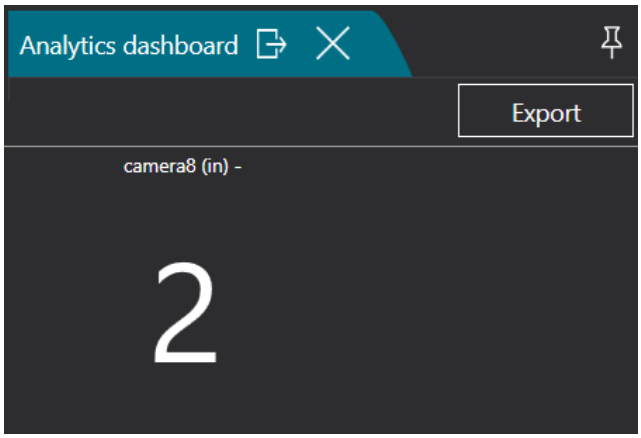
Step6 Select the analysis name➔display data conditions➔total data range➔data aggregation range➔choose the display graph, such as a number, then press [Add] to complete the setup.



Step7 Drag the yellow box to resize the component, and press to save the changes and complete the setup



Step8 You can now view the recognition results and synchronize data to the analysis data report.



12.HOW TO PERFORM ONE-CLICK BACKUP AND RESTORE

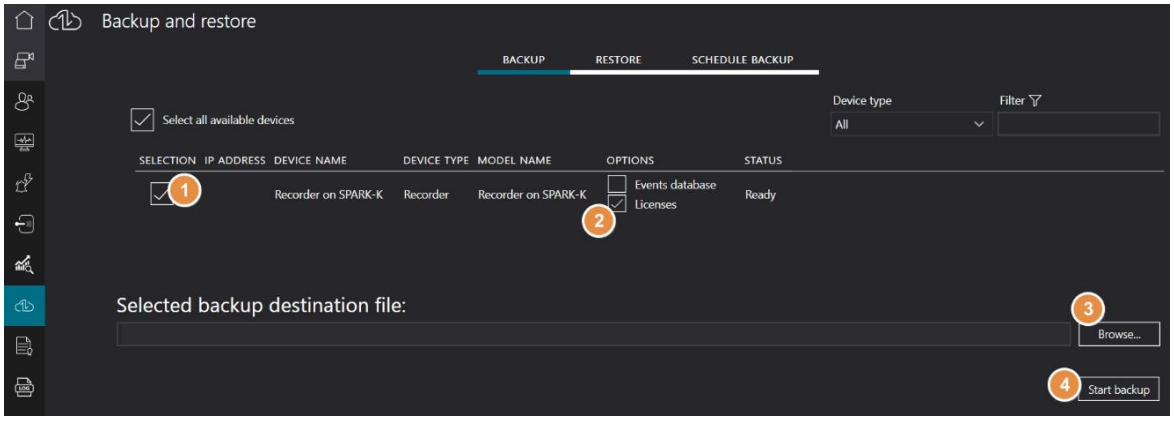
This section explains how to back up and restore the Config system settings, including camera device settings, event and alarm settings, health check settings, user management settings, etc., to avoid data loss. Through simple operations, you can easily back up system settings and recording data and restore them as needed.

12.1 Backup System Settings

Set up backup functionality to periodically save system settings and data, ensuring the security of critical information. Regular backups can prevent data loss and make it easy to restore in the event of system failure.

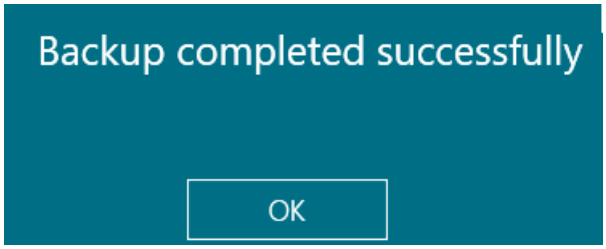
Step1 Click  on Backup and Restore

Step2 Check backup host➔authorization key ➔browse to select the backup file storage location➔start backup



Step3 You can input backup record details in the information fields, and then press [Start] to initiate the backup

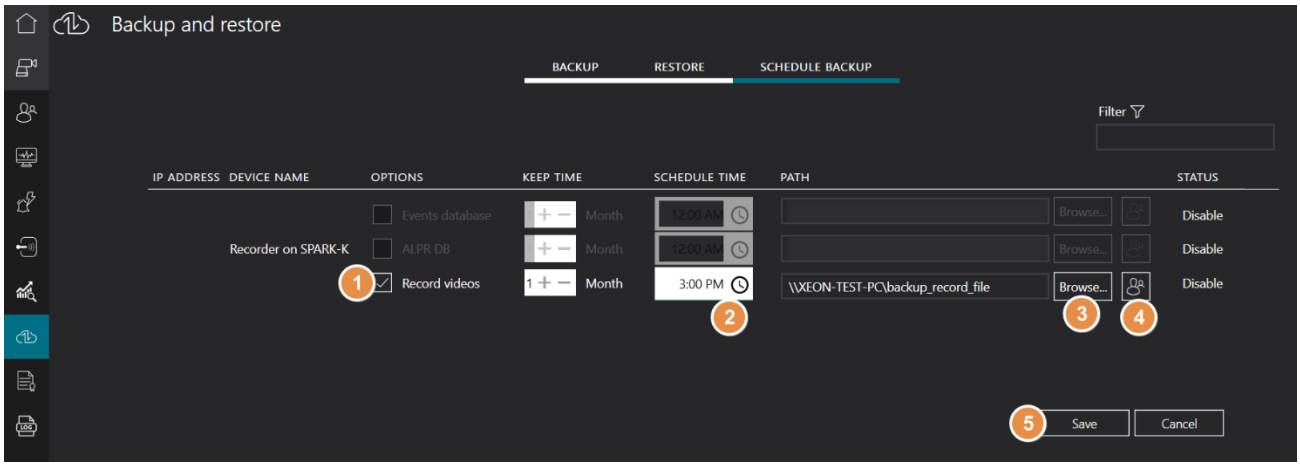
Step4 Once the progress is complete, the backup success message will be displayed.



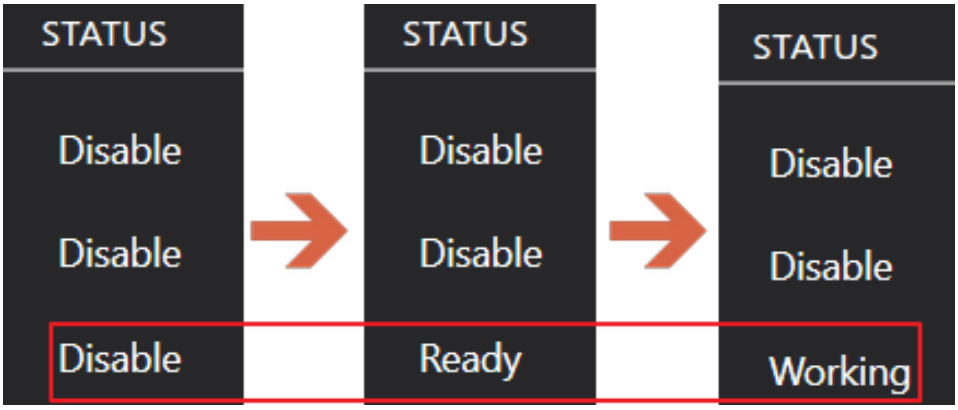
12.2 Schedule Backup for Recording Data

Set up scheduled backups for recording data to prevent data loss or damage. Through the scheduling settings, you can ensure that recording data is automatically backed up at specified times to maintain data security.

Step1 For data scheduled backup, select the host for which video files need to be backed up➔adjust the daily backup start time➔browse the backup storage location➔ input the backup host username and password➔complete the [Save] settings.



Step2 Once the backup schedule is set, the status will change to "Ready." When the backup start time is reached, the status will change to "Working."

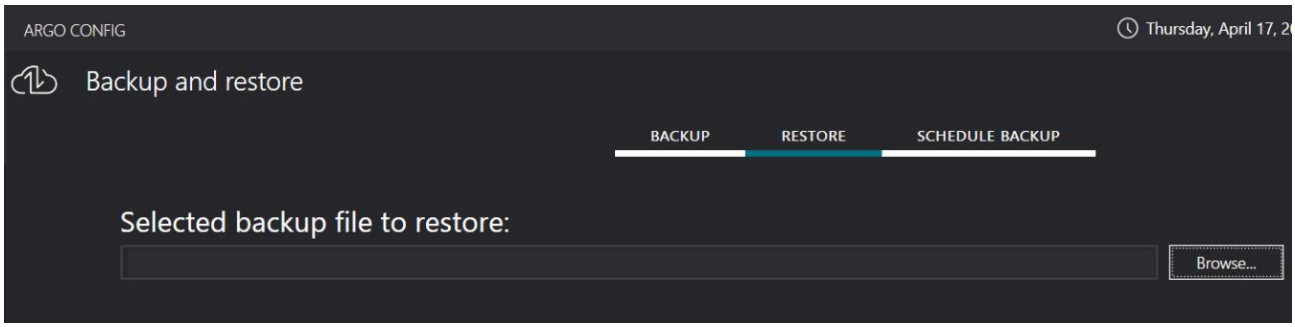


Step3 After the backup is complete, you can check the folder content at the storage location. The file naming structure is: the previous day's date \ computer name \ hour \ camera name.

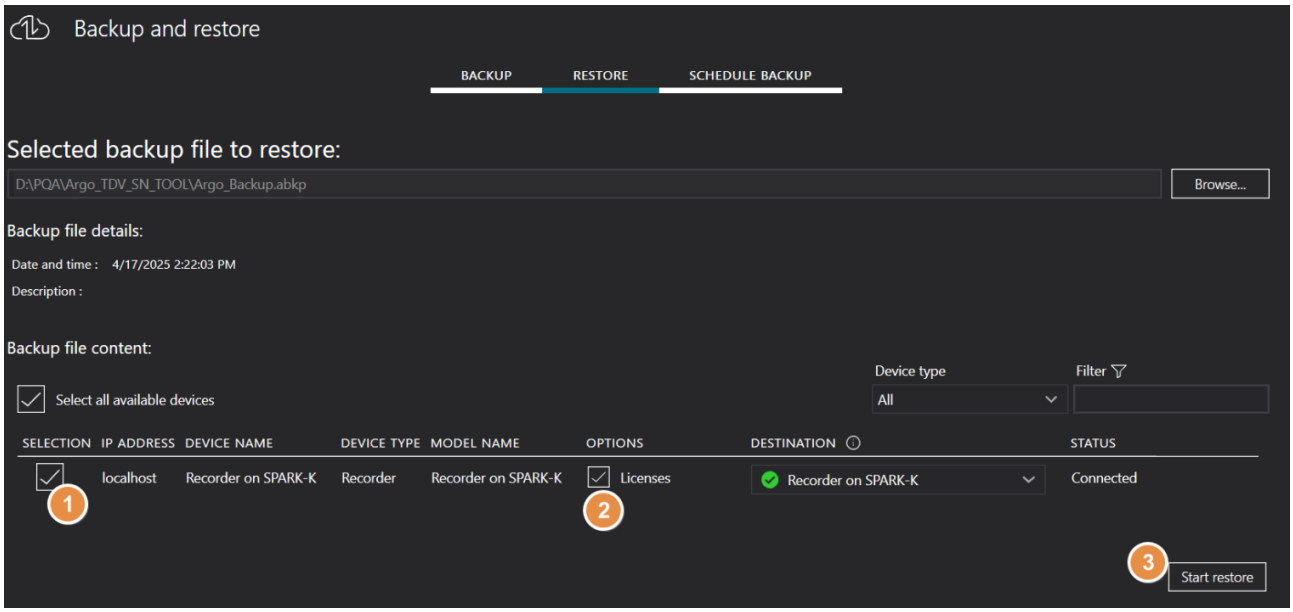
12.3 How to Restore Backup Settings

This section explains how to restore system settings from a backup. This feature ensures that the system returns to its previous configuration state.

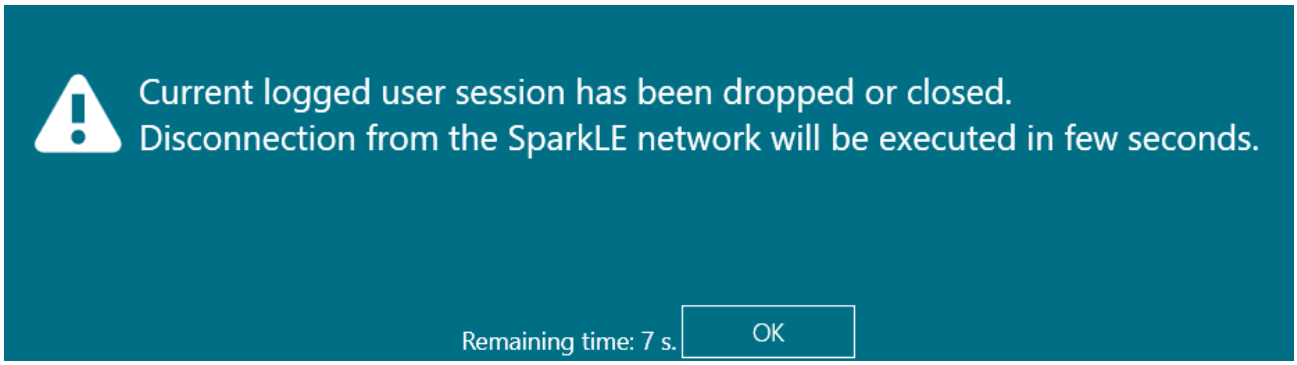
Step1 Click on the restore page, and browse to the backup file location to select the restore file.



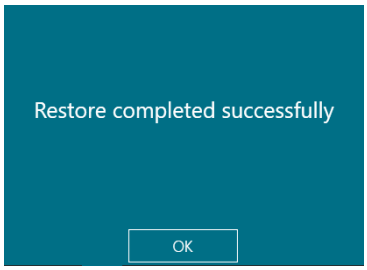
Step2 After importing the backup file, check the restore host and authorization key, and press [Start Restore].

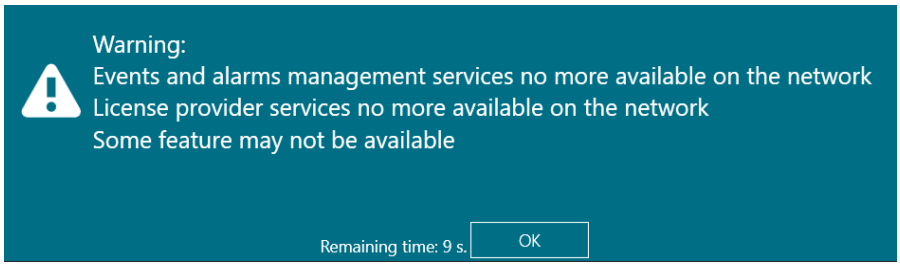


Step3 Click [OK] to proceed with the restoration



Step4 Once the restoration is complete, click [OK], and after the Directory Service restarts, you can log in normally.





Spark S.r.l
Via Antonl/O Gramsci, No. 86/A
42124 Reggl/O Emilia, Italy
+39 0522 929850
info@spark-security.com

Taiwan Spark
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