GANZ

User Manual

Device setting Guide

For AI AIBOX

V.1.0.8

Caution: The contents of this manual are subject to change at any time without prior notice.

1. Overview	5
1. Safety	5
Before Installation	5
During Operation	5
Disassembling and Cleaning	5
During Installation	5
During Use	5
2. Caution	5
Warning	5
2. Components	5
1. Components	5
2. Names and Functions	5
3. AI AIBOX Device Settings	7
1. Device installation	7
1.1 Installing the AI AIBOX Device	7
2. Search for devices on the network	8
2.1 Download the Device Management Tool	8
2.2 Running screen	8
2.3 Setting screen	9
2.4 Screen after settings applied	9
3. Initial access settings	
3.1 Device language settings	10
3.2 Device Time-zone settings	10
3.3 Initial password setting of Device	11
3.4 Accessing to Device and setting the remote support settings	11
4. Video source setup	
4.1 Camera Video Input Setting	12
4.2 Video Stream For Each Channel Setting	13
4.3 Check The Video Stream Connection Setting	13
4.4 Multiple channels of video stream at once	14
4.5 Searching for setting ONVIF cameras	14
4.6 Searching for setting ONVIF cameras	16
5. Remote support settings	17

5.1 Remote support Settings	17
4. Application usage guide	17
1. Application Activate	17
2. Event Action Setting Guide	19
2.1 Alarm setting example (Intrusion)	20
3. Counter Setting Guide	25
3.1 Counter working process	25
3.2 Counter Setting Example (Occupancy Counting)	26
3.3 Counter Action Rule Setting Example	31
3.4 Periodic Reporting Setting Example	35
3.5 Counter Statistics Report Format Guide	
5. Reduce False Detection Setting	41
1. Object Size Filter	41
1.1 Object Minimum Size Filter	42
1.2 Object Maximum Size Filter	42
2. Exclusion Area	46
2.1 Exclusion Zone Settings	46
2.2 Save, Load, And Reset The Settings	49
6. Arm/Disarm Setting Guide	49
1. Arm/Disarm Overview	49
2. Global Disarm	49
3. Arm/Disarm Instant Settings	50
4. Arm/Disarm Rules	50
4.1 Alarm Input	51
4.2 Schedule	52
7. Action setting guide	52
Utilizing Event Meta Tokens & Creating Action Message Guide	53
1. System	62
1. Relay	62
2. Camera speaker Output	63
3. RS485(RS232)	64
2. NETWORK	68

1. HTTP		68
2. FTP Upload		75
3. AWS S3 Upload .		77
4. MQTT Publish		79
5. Email Alarm		
3. VMS		89
1. Cortrol Plug-in In	tegration Guide	
2. AIAIBOX Plugin I	ntegration Guide for Network Optix VMS	
3. AIAIBOX Integrat	ion Guide for Milestone XProtect VMS	

7. Schedule Setting Guide	134
1. Schedule Overview	135
2. Create a New Schedule	135
3. Weekly Schedule	136
4. Monthly Schedule	136
5. Yearly Schedule	137
6. Time Schedule Setting	138
7. Exclusion Schedule	138
8. Combined Rule Setting Guide	139
1. Overview of Compound Rule Conditions	139
2. Combined Rule Conditions Setting	139
3. System I/O Combined Condition Settings	141

1. Overview

2. Components

1. Components







Cable clamp

Adapter

Screw

2. Names and Functions





No.	Item	Description
0	LED	Indicator LED for POWER / STATUS
0	LED	Indicator LED for ALARIM IN / ALARM OUT
0	RESET	Factory reset button.
0	MICRO SD	Slot for inserting a micro SD card.
6	USB	Universal Serial Bus(USB) port for additional devices such as USB Memory Stick
6	AUDIO	Connect the audio line input and output.
0	LAN1	RJ-45 port for connecting internet and other platforms such as interoperable VMS, recorders and IP cameras.
8	LAN2	RJ45 port for connecting IPCs and other devices through a separate LAN.
9	RS-232	Connect the remote control device for RS232 communication.
0	CAN	Connect the remote control device for CAN communication.
0	ALARM IN	Connect the sensor / alarm input signal wires.
Ð	RELAY OUT	Connect the relay output signal wire.
ß	RS-485	Connect the remote control device for RS-485 communication.
12	WIEGAND	Connect the Wiegand input and output signal wires.
Ð	DC JACK	Connect the power plug of the provided 12V adapter.
T:	CLAMP HOLE	DC JACK cable clamp fixed hole

Basic Layout.



3. AI AIBOX Device Settings

AI AIBOX is an AI video analysis device that analyzes multi-channel video using various types of AI algorithms to extract meaningful objects or identify various situations visually detected on the screen.

Al algorithms can be used to extract objects and follow the event after judging the situation with Al metadata. Based on Al analytics information, event condition and alarm types can be set as wanted. You can also accumulate and visualize your data to create analytical data that enables you to gain insights from continuous, otherwise meaningless data.

The document below explains the basic connection method of AI AIBOX, the structure of the system setting UI, and the setting method.

1. Device installation

1.1 Installing the AI AIBOX Device



1. Install AI AIBOX on a network connected to the Internet and run a DHCP server.

2. Connect the network cable to the ETHERNET 1 port of AI AIBOX.

3. The AI AIBOX boots up immediately when the adapter is powered on due there does not have separate power button.

4. It takes about 1 minute for connecting to the PC after the device completes booting.

2. Search for devices on the network

2.1 Download the Device Management Tool

Download and install the Device Management Tool from the link below. AI AIBOX is possible to search the device's IP and set the network via the Device Management Tool program provided by GANZ. DeviceManagementTool-v1.03

When the install file runs, the firewall setting window will appear as below. For smoothly using, it is recommended to allow the entire network.

iiii Windows Security Alert						
Windo app	ws Defend	er Firewall has blocked some features of this				
Windows Defender public and private r	Firewall has blo networks.	cked some features of devicemanagementtool-v1.04 on all				
	Name:	devicemanagementtool-v1.04				
	Publisher:	Unknown				
	Path:	C:₩users₩사용자₩downloads₩devicemanagementtool- v1.04₩devicemanagementtool-v1.04.exe				
Allow devicemanag	ementtool-v1.0	4 to communicate on these networks:				
🔽 Private netw	vorks, such as m	y home or work network				
Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)						
What are the risks	of allowing an a	pp through a firewall?				
		Cancel				

2.2 Running screen

			Network Interfac	e: ALL			~	Search
Model	Mac Address	Туре	IP Address	Netmask	Gateway IP	DNS 1	DNS 2	WebPo
AlBridge Pro	24:76:25:9a:4a:84	DHCP	192.168.100.224	255.255.252.0	192.168.100.1	168.126.63.1	0.0.0.0	8443
AlBridge Pro	24:76:25:96:36:8b	STATIC	192.168.100.227	255.255.252.0	192.168.100.1	168.126.63.1	8.8.8.8	8443
	Setup Network	¢						
	- Setup Network	C DHCP O S	TATIC					
	Setup Network	c ⊙ DHCP ○ S	TATIC		IC) admin		
	Setup Network	€ ● DHCP ○ S	TATIC DNS1 DNS2		IE Passwore	admin		

- When run for the first time, it shows a list of AI AIBOXs connected to the network. In the ID / Password field, admin / 1234 is entered by default.
- When the AI AIBOX is in "factory default or factory reset" status, "1234" is set as a temporary password for network settings in the tool
- If the AI AIBOX is not shown, please check the network cable is connected to ETHERNET 1 properly.

2.3 Setting screen

🔍 Al Bridge Device Mana	agement Tool - 1	1.01						- 🗆 X
			Network Interfac	ce: ALL			~	Search
Model N	Mac Address	Туре	IP Address	Netmask	Gateway IP	DNS 1	DNS 2	WebPort
AlBridge Pro 24	:76:25:9a:4a:84	DHCP	192.168.100.224	255.255.252.0	192.168.100.1	168.126.63.1	0.0.00	8443
AlBridge Pro 24:	:76:25:96:36:8b	STATIC	192.168.100.227	255.255.252.0	192.168.100.1	168.126.63.1	8.8.8.8	8443
	- Setup Netwo IP Address Netmask Gateway	rk O DHCP	DNS1	8.8.8.8 8.8.4.4 Apply	Passwor	D admin d •••••	•••	

- 1. Click the device that wants to change the network settings from the list.
- 2. Enter the network information to set in the Setup Network section below.
- 3. Enter the ID / Password of the device.
- If the AI AIBOX is in "factory default or factory reset", enter admin / 1234.
- 4. Click the Apply button.

2.4 Screen after settings applied

🔍 Al Bridge Device	e Management Tool - 1.	01						- 🗆 X
			Network Interfac	e: ALL			~	Search
Model	Mac Address	Туре	IP Address	Netmask	Gateway IP	DNS 1	DNS 2	WebPort
AlBridge Pro	24:76:25:96:36:8b	STATIC	192.168.100.227	255.255.252.0	192.168.100.1	168.126.63.1	8.8.8.8	8443
AlBridge Pro	24:76:25:9a:4a:84	STATIC	192.168.101.23	255.255.252.0	192.168.100.1	8.8.8.8	8.8.4.4	8443
	Setup Networ	k						
		O DHCP O ST	ATIC					
	IP Address		DNS1		I	D admin		
	Netmask		DNS2		Passwo	d		
	Gateway			Apply				

After a while by pressing the Apply button, the network setting of the device will be updated in the list.
 If the network settings have not been changed, it is due ID or Password being incorrect, please check again.
 After setting the network, double-click the device information in the list to access the AI AIBOX.
 The AI AIBOX webpage will open in the default browser in Windows.

3. Initial access settings

When accessing the AI AIBOX for the first time, the initial setting wizard is displayed. To use the AI AIBOX, complete the setup in the order shown in the UI.

3.1 Device language settings

Language/言語/	^번 어	
English		
Ligisi		
		Apply

The appropriate language is set as the default to match your browser's language settings. If you want a different language, select the desired language from the drop-down box.

3.2 Device Time-zone settings

Timezone	
GMT+09:00 Asia/Seoul	~
DST	
OFF	~
	Apply

Set the password want to use. The password can use the alphabet, numbers, and special characters, and it should be set to 8 to 16 characters.

3.3 Initial password setting of Device



When accessing the AI AIBOX for the first time, the initial password setting UI is displayed. Set the password want to use.

The password can use the alphabet, numbers, and special characters, and it should be set to 8 to 16 characters.

	GANZ.
2	Username
θ	Password
Lo	gin
	Forgot password?

3.4 Accessing to Device and setting the remote support settings

Log in using the device's account information using admin as the ID and the password set in the previous step.

4. Video source setup

4.1 Camera Video Input Setting

To enable the AI AIBOX to receive and analyze video from a camera, you must first set up the camera's connecting information.

VIDEO	Home / Vid	o Stream				
Video Stream						
False Alarm Reduction	Al Engine Video Deo	Resource ()	26%			1044 / 4000 160 / 1000
• Event Rule List	Video Res	olution Resource ()	15%			148 / 1000
↔ Network <	() strea	minto			CL Search Cameras	Na Calt Video
System <	1	W.O Bldg. Connect	ed 1920x1080 8.0tps	rtsp://192.168.101.7:5554/video/1080p.mp4	@ 🖶 😑	
Cloud Service	2	LPR.PL Connect	1920x1080 30.11ps	rtsp://192.168.101.7:5554/video/lpr_pl.mp4	@ <mark>:</mark>	
	3	AES Connect	ed 1920x1080 3.9fps	rtsp://192.168.101.7:5554/video/aes3_15.mp4	ń. ii 📑	
🔢 Explore Al Apps	4				Configure Al	Арр
	5				Configure Al	App
System Event Settings	6				Configure Al	App
	7				Configure Al	App

Click the **'Video Stream'** in the sidebar navigation menu displays the settings menu for receiving video from the camera.

(1) The **'Al Engine Resource'** displays usage relative to maximum Al processing capability. Each app requires a different Al processing capacity, so be careful not to set over the maximum processing. The **'Video Decoding Resource'** shows current usage based on the maximum amount of video the Al AlBOX can receive and process from the camera. The **'Video Resolution Resource'** shows the usage against the maximum resolution available on the Al AlBOX. No item will exceed the limit.

(2) The **'Video Stream'** settings allows you to set the video stream information accessible over the network.

4.2 Video Stream For Each Channel Setting

Attribute		
Channel Name	Channel Name	
Video Source		
URL	rtsp://	
Transport	TCP 🗸	
HTTP(S) Port	0	
Authentication		
Username		
Password		
Etc		
Use Cam Speaker	Connect additional audio session for transmitting sound sources.	
Video Buffering	~500ms	

Click the **channel** for which you want to set the video in the list of video streams.

1 Enter the **Channel Name**

(2) Enter the **RTSP URL** of the camera.

(3) Select a transport protocol. The transport protocol specifies the protocol of the transport layer used to import the video stream.

(4) Set the credentials needed for receiving the video stream. Usually, the ID and password of the IP camera are used.

(5) If you want to use a camera speaker, check the **'Use Camera Speaker'**.

(6) Set the maximum video buffering time. If, due to network conditions or camera types, video information is not transmitted smoothly and is received in a sudden burst, AI AIBOX can redistribute it into smooth videos according to the buffering setting. As the 'Video Buffering' setting is a maximum value, the actual buffering will be less than the set value if there are no problems with the camera and network performance.

4.3 Check The Video Stream Connection Setting

You can check that the video stream you have set up is being received correctly. To check the receiving video stream, click the **'Video Preview'**.



4.4 Multiple channels of video stream at once

Set up multiple channels of video streams at once. You can set up multiple channels of video streams in bulk using copy and paste, as well as features such as Apply to All.

To use the Bulk Setup feature, click the 'Edit Video' button in the Video Stream Settings area.



The 'Batch Setting' allows you to set the name, RTSP URL, transport, and authentication information for all channels at once.

The settings you enter in the Apply All line at the top can be applied to all channels by clicking the tick button for each setting.

Video clip guide (Refer to the on-line <u>Technical document)</u>

4.5 Searching for setting ONVIF cameras

ONVIF is a standard for the interoperability of physical security devices. For network cameras that support the ONVIF standard, you can set up video streams using Discovery. To use the discovery feature, click the **'Search Cameras'**.



Search for your camera in the ONVIF search pop-up, then enter your credentials to see a list of video streams supported by your camera. Assign the streams you wish to analyze to a channel on the AI AIBOX.

Search Cameras	×
 Click 'Search Cameras' to auto-detect compatible cameras. Log in, get RTSP URLs, and assign to desired channels. 	Q Search Cameras
	Cancel Submit

Search Cameras			×
 Click 'Search Cameras' to auto-detect compatible cameras. Log in, get RTSP URLs, and assign to desired channels. 		Q Search (Cameras
QPX_0824M5C 192.168.101.191	Username	Password	Login
IPX 192.168.101.137	Username	Password	Login
VUHDIP-32 192.168.101.46	Username	Password	Login
CSB2-5M4C-1MPAR7 192.168.101.128	Username	Password	Login
VUHDIP-8-3 192.168.102.8	Username	Password	Login
CSB-8MP-1VKAR5 192.168.103.214	ADMIN		Login
CSB-8MP-1VKAR5 192.168.103.213	Username	Password	Login
CSB-8MP-1VKAR5 192.168.103.215	Username	Password	Login
NHC-IR22T 192.168.101.90	Username	Password	Login 🗸
		Cancel	Submit

earch Cameras				
Click 'Search Car Log in, get RTSP	neras' to auto-detect compatible cameras. URLs, and assign to desired channels.		Q Search (Cameras
QPX_0824M5C 192.16	58.101.191	Username	Password	Login
IPX 192.168.101.137		Username	Password	Login
VUHDIP-32 192.168.1	01.46	Username	Password	Login
CSB2-5M4C-1MPAR7	192.168.101.128	Username	Password	Login
VUHDIP-8-3 192.168.	102.8	Username	Password	Login
CSB-8MP-1VKAR5 19	2.168.103.214		_	
rtsp://ADMIN:	@192.168.103.214:554/live/main 1920x1080 / ~15 f	FPS	CH1	^
rtsp://ADMIN:	@192.168.103.214:554/live/second 640x360 / ~30 F	FPS	None	
CSB-8MP-1VKAR5 19	2.168.103.213	Username	Passv CH1	n
			cup	
			CH3	ıbmit
			CH4	
			CH5	
			CH6	

4.6 Searching for setting ONVIF cameras

Once the video stream is set up and connected, click the 'Configure AI App' button, select the appropriate app, and set the event action rule.

Q Search	Cameras	Fedit Videos	
	Configure AI A	Арр	
	Configure AI A	Арр	

5. Remote support settings

5.1 Remote support Settings

	E Device 98838 Arm/Disarm	admin 风
VIDEO	Home / System / System Management System Management	
Display <	System Management	
e Event Rule List	F/W Update I Update	
↔ Network <	Factory Default S Default	
System ~	System D8 🛓 Import 🏦 Export	
Date / Time User	Certificate Update 🛱 Update	
System Management	System Reboot 🕐 Reboot 🗖 Schedule	
System Information Security		
Log	Technical Support	
API Document	Debug Logs 🛛 🚍 Download	
License Management Cloud Service	Remote Assistance	
	MAC Address 24 Remote Code 59	
Explore Al Apps	Provide the device's MAC address and remote support code to the technical support specialist. The specialist can access the user's device through the internet. After the remote support scasion is completed, remember to disable this feature.	
System Event Settings	Fort forwarding is not required when using this remote support feature. ● Terms and Conditions	

Enable the Remote Assistance function in the System > System Management > Technical Support menu. You can receive remote technical support by sharing the Mac Address and Remote Code displayed on the UI.

4. Application usage guide

Al AIBOX works by adding various applications in the form of add-ons. To add and use the application to the device, a license to use the application should be issued from the device dealer.

1. Application Activate

To activate additional apps, you need a license for each application.

Licenses are issued by the seller of the device in the form of a .json file, which you register and use in the 'License Management'.



If the device has a license, the app will appear as a green header in the 'Explore AI apps' menu.



In the 'Explore AI apps', you can click on the app that you want to use to go to the settings menu for that app.

2. Event Action Setting Guide

Many of the various applications supported by AI AIBOX have a structure that performs predefined actions for events detected based on AI.

By defining events and setting related actions, notification on real-time events can be used for a variety of purposes.



When an event is triggered by the event action setting, the schedule is checked. If the event occurs at other times with the schedule, the event is dropped without any event action.

If the action run time is set, the action that can be run on the edge is run first.

2.1 Alarm setting example (Intrusion)

То

na ngation me				
VIDE	0			Licensed A
₽	Video Input	<		_
	Display	۲.	Intrusion Detection	_
。	Event Action List			ata
SYST	EM SETTINGS			"ŤŤ
<>	Network	<	Detect people in no-entry zones,	send
¢	System	<	notifications, and configure vario actions.	us other
õ	License Management		8 CH Licensed	No Rules in Use
6	Cloud Service		Stay & Go	
APP S	SETTINGS			
000	Explore Al Apps			
~	Active Al Apps	<	Ř Ś	
¢	System Event Settings		Detect objects that stay in and o	ut of the
To set a new d	letection rule, click the	+ Add Rule	button in the intrusion detec	tion settings.
2.1.1 Event Ac	ction Rules Setting			
		Rule Name	Rule #8975	

To set up an intrusion detection event action, click the 'Explore AI Apps - Intrusion Detection' in the sidebar navigation menu.

1. Enter a name for the rule. A random default value is entered, change this if necessary. You can also identify the rule by the name you enter in the action performed by the action handler.

Active

2. If you want to activate the event action rule upon creation, turn on the 'Active' switch.

2.1.2 Event Setting

1. Click the	Add but	tton to set	up the event.			
	Event Setting	Add				
		Video	Event Type	Event Name	UUID	Operation
				-		

2. Select the video want to detect via the dropdown to the right of the Event Type.



Please refer to the video to properly set the detection zone. The detection zone can be set using the functions below. Alternatively, you can select zone information generated from other event settings by importing zone information.

Video clip guide (Refer to the on-line <u>Technical document)</u>

<u>00:00</u>
00:26

• Drag the detection zone to **move the entire area**.

- Drag the **vertex to move** it.
- Click the yellow line to **add a new vertex** at that point.
- Right-click the vertex to remove it.
- Drag the gray box to move the label position.

After done, the video will look like below with the event zone ad label set up above.



3. Click the

button to save after setting for each option.

Event Name	Intrusion Detection	Detection Policy	Careful Detection	~ 0
Event Count Label	Intrusion	Target Object	Person 🛞	~
Event Count Reset	00:00 ~ Reset	Ignore Duplicate Object	0	
		Skip Consecutive Events	0	
		Re-trigger Interval		second(s) 🕐
		Ignoring Interval	3	<pre>> second(s) ()</pre>

- Event Name : Enter the name of the event zone you created above.
- Detection Policy : Select whether to make event judgments about objects quickly or cautiously. When setting up a careful detection policy, objects are observed for a period of time to ensure that events are raised as accurately as possible. This can reduce false alarms at the expense of slightly delayed events. When setting a fast detection policy, the event is raised as soon as the object is detected. In this case, the time to observe the object is minimized in order to make a quick decision, which may result in false positives.

- Event Count Label : Enter the name of the label widget drawn over the video.
- Target Object : Select the event detection target. Person, Vehicle, and bike can be set.
- Event Count Reset : Set whether the event counts value or not. When enabled, the count value is reset at the set time.
- Ignore Duplicate Object : When checked, the same object will be ignored if it enters the event area again.
- Skip Consecutive Events : When checked, ignores events caused by new objects as long as the detected event target remains in the event zone.
- Re-trigger Interval : When Ignore Duplicate option is enabled, if there are still detected event targets in the zone, the event will occur again every set time.
- Ignoring Interval : Do not occur new events during the set time after an event occurs.

2.1.3 Action Settings

Define the event action to take when the event set occurs in Action Setting.

1. Click the	Ac	ld bu	utton to add a new action item.	
Action Settir	ng	Add		
		Action	а Туре Ор	eration
			-	

2. Set each action want to perform when an event occurs. Please refer to the Action setting Guide for the types of actions supported and how to set them up.

2.1.4 Finish setup



1. Click the button at the very bottom to save intrusion detection event settings after setting up the event, action in the event action rule set page.

2. If everything is set up correctly, you can see the new event in the list on the Intrusion Detection application screen.

Intrusion	Detection (1)		≡ ₊ Add
No	Name	Activation	Operation
1	Hazardous Area Access	\mathbf{C}	•••

2.1.5 Filter settings (optional)

Schedule and Combined Rule filters can be used to set up event filters to drive actions. The schedule and Combined Rule filter settings described below are not required to configure an action rule, so you only need to set them if necessary.

2.1.5.1 Schedule settings

Set up event action schedules that operate over a period of time to set the time for sending the notification whenever an event occurs.

1. Click the	Setti	ing t	outton to set the event action schedule.	
Schedule Se	etting	Settin	q	
	2		2	
		Name		Operation
			-	

2. Add a schedule to drive action when an event occurs. Please refer to the <u>Schedule Setting Guide</u> for more information on how to set up a schedule.

2.1.5.2 Combined Rule condition settings

Set compound conditions on event actions to perform more complex forms of event filtering. The following items can be set as compound conditions.

- Rules set in the application in the form of an event action
- Events that make up a rule are set in an application in the form of an event action
- System I/O devices, such as alarm inputs or virtual alarm inputs

1. Click the

Add

button to set the combined rule condition.

Combined Rule	Add			
	UUID	NOT	Time Range	Operation
			-	

2. Please refer to the <u>Combined Rule Setting Guide</u> for more information on setting up.

3. Counter Setting Guide

The counter application counts the number of AI-detected objects. The count value can be utilized by defining various actions.

3.1 Counter working process



By setting up a counter application, AI AIBOX counts objects internally and archives the counting data to internal storage at regular intervals.

The stored data can be retrieved directly from the edge through the API. Edge storage has limitations in areas such as storage period, network configuration, and service delivery performance.

3.2 Counter Setting Example (Occupancy Counting)

Utilize the Occupancy Counting application to count people in real-time not only in stores, but also in buildings, specific areas of buildings, floors, or any other unit.

3.2.1 Counting Method

Occupancy counting operates according to the following methods.

1. Count the number of people entering from all possible entrances to the target space.

2. Count the number of people exiting at all possible exits from the target space.

3. Aggregate and store **the number of people entering – the number of people exiting** for each data collection cycle.

3.2.2 Counting Condition

To ensure that the count value is as accurate as possible, follow these guidelines.

- Compliance with entrance and exit camera installation guide.
- No one enters or leaves the target space other than the designated entrances and exits.
- Specify a daily counter reset time when no one is inside the target space.

3.2.3 Camera Installation Condition

Camera tilt angle	10º~25º
Camera installation height	2m~5m
Camera horizontal angle	40º~110º
Camera resolution	Over 1280×720, 16:9 Ratio
FPS frame per second	6~30
Transmission bitrate	2Mbps~10Mbp
Minimum detection object size	Horizontal 32px, Vertical 64x
Distance between camera to object	~ 15m



3.2.4 AI AIBOX Counter Setting

1. To set up counting people in a space, click the **'Explore AI Apps' – 'Occupancy Counting'** in the sidebar navigation menu.



2. Click the button to create a new counter in the upper-right corner of the Occupancy Counting list.

3. Enter the name in the **"Name"** session to distinguish this event action from the other events. Later, you can use the name you enter here to distinguish the event in event history lookups or in actions performed by the action handler.

Name	Counter #50	54		
Entry Counting	Add Zone			
	сн	Name	UUID	Operation
Exit Counting	Add Zone			
	сн	Name	UUID	Operation
		-		

Add Zone

4. Click the button to add the enter/exit zone. If there are multiple entrances and exits, every entrance and exit be added as a counting zone.

3.2.5 Counting Zone Setting

1. Select the video you want to count from the **Select Video dropdown** in the top right corner.



2. To properly set up the counting area, please refer to the video. The counting area can be set using the functions below.

Video clip guide (Refer to the on-line <u>Technical document)</u>

00:00
00:20

- Drag the vertex to **move it**
- Click the yellow line to **add a new vertex** at that point

- Right-click the vertex to remove it
- Drag the gray box to move the label position

```
3. Click the Apply button to save af
```

3. Click the button to save after setting each option. Set the counting zone to every entrance and exit the same as above to count the whole passengers.

- Zone Name : Enter the name of this zone.
- Counting Zone : Select the direction of people passing by needed to count as an event

3.2.6 Schedule settings (optional)

You can reset the counter at times when there are no people in the target space, such as at night or during nonbusiness hours.

You can set up a wipe schedule as a daily, weekly, or monthly wipe. You can also add multiple wipe schedules.

1. Click the	Setting	button to s	et the event action schedule.	
	Sebadula Se	atting C. ut-		
	Schedule Se	Setting Setting		
		Name		Operation

2. Add a schedule to drive action when an event occurs. Please refer to the <u>Schedule Setting Guide</u> for more information on how to set up a schedule.

3.2.7 Finishing the setup

1. When you've finished setting up all the entry and exit people counters and reset schedules, click

the submit button at the bottom of the page to submit your in-space people counter settings.

2. If everything is set up correctly, you can see what you've set up in the list of people counters in the space.

ounters (1)			+ Add Counter
Name	Occupancy Count $\ \mathbb{C}^{l}$	Channels In Use	Operation
Counter #5054	0	1 2 3 4 5 6 7 8	

3.2.8 Setting up real-time reporting (optional)



This feature allows you to send count values to a user-configured HTTP server in real time. Not setting it does not affect the behavior of the counter.

Click the "Settings" button to configure the real-time count reporting feature.

3.2.8.1 Reporting setting

Report Setting		
Activation	\bigcirc	
Reporting Cycle	60 second(s) V	

To enable real-time reporting, turn on the switch in the Activation button. The frequency of real-time reporting is set in the **Reporting cycle** item.

3.2.8.2 Data Receiving Server

Data	Receiving	Server
Data	Receiving	Server

Http(s) URL	https://your-domain-name.com/path
Authentication	None ~
	Test

To receive real-time count data, configure the server information.

Add the HTTP or HTTPS server URL and authentication settings if you have authentication capabilities.

The authentication method can be configured as **Basic**, **Digest** or **Token**.

You can use the Test button to check that the device can send data to the server normally once you've set up the data receiving server. When the "Test" button is clicked, data will be sent to the configured HTTP server in the same format as the real time count data of the actual meter.

3.2.8.3 Data Transfer Format

Data Transfer Format

View Format	\sim



3.3 Counter Action Rule Setting Example

You can set events and create action rules based on the counter values of the counters you set.

Each counter app includes a separate menu where you can set up rules.



1. Enter a **name** for the rule. A random default value is entered, change this if necessary. You can also identify the rule by the name you enter in the action performed by the action handler.

2. If you want to activate the event action rule upon creation, turn on the 'Active' switch.

3.3.2 Event setting

1. Click the

to set the event.

Event Setting	Add				
	Video	Event Type	Event Name	UUID	Operation
			-		

2. Select the channel on which you want the event widget to appear and specify the location of the widget. The channel on which the event occurs will also be set to the channel on which the widget will be displayed.



3. Specify the target counter for the event in Counters. If there are any counters set up in the Counters application, they will be displayed in the list.

- There are two event types.
 - Conditional the event is triggered when the specified counter's value meets a specified condition.
 - Every Count N Triggers an event when the count value of the counter goes above or below a multiple of the N you set. For example, if N=10, an event is fired when the count value changes from 9 to 10, 19 to 20, or 10 to 9, etc.
 - If you added a range condition, such as greater than/less than, to the condition for every count N – Even if the interval N changes, the event will not occur if the range condition is violated.
 - If the item greater than the setting is greater than the item less than the setting the event is fired if only one of the two conditions is met. ex) True if "X>10 OR X < 5" if X>10, X<5
 - If the item Greater than the setting is less than the item Less than the setting the event is fired only when both conditions are satisfied. ex) True if "X>5 AND X<10" if 5<X<10
 - Greater Than The event is triggered the moment the counter's count value becomes greater than the setting.
 - Less Than The event is triggered the moment the counter's count value becomes less than the setting.
 - The Greater Than or Less Than events are mutually independent, so there is no condition under which one must be greater or less than the other. The event is triggered when the count value becomes greater or less than the number you set.

Event Name	Occupancy Counting	Counter	Counter #5054	~
Counter Value Label	Occupancy Now	Event Type	Conditional	~
Event Count Label	Event Count	Every Count N	10	<u>^</u>
Greater Than Count Label	Greater Than Count	Greater Than	10	<u>~</u>
Less Than Count Label	Less Than Count	Less Than		
Event Count Reset	00:00 V Reset			

- Periodic The count event occurs at regular time intervals.
 - Events occur at regular intervals based on the event cycle you set.
 - If you have added a range condition such as greater than/less than setting as a condition every cycle – every count N, the range condition will operate the same way as the setting.

Counter	Co	ounter #5054		~
Event Type	Pe	riodic		~
Event Cycle		60	~ ~	second(s)
Greater Than		10		^ ~
Less Than		0		<u>^</u> 0

3.3.3 Action Settings

Define the event action to take when the event set occurs in Action Setting.

Action Setting Add	1. Click the	Add	button to add a new action item.				
Action Setting Add							
	Action Setting	Add					
Action Type Operation		Action	Type Op	eration			
· · · ·			-				

2. Set each action want to perform when an event occurs. Please refer to the <u>Action Setting Guide</u> for the types of actions supported and how to set them up.

3.3.4 Finish setup

Submit

1. Click the button at the very bottom to save intrusion detection event settings after setting up the event, action in the event action rule set page.

2. If everything is set up correctly, you can see the new event in the list on the Intrusion Detection application screen.

vent-Action Rules (1)		+ Add Rul
Rule Name	Activation	Operatio
Rule #9465	\bigcirc	ß 🗓
	\sim	

3.3.5 Filter settings (optional)

Schedule and Combined Rule filters can be used to set up event filters to drive actions. The schedule and Combined Rule filter settings described below are not required to configure an action rule, so you only need to set them if necessary.

3.3.5.1 Schedule settings

Set up event action schedules that operate over a period of time to set the time for sending the notification whenever an event occurs.

1. Click the	Setti	ng butto	on to set the event acti	ion schedule.	
Schedule Se	etting	Setting			
		Name			Operation
				-	

2. Add a schedule to drive action when an event occurs. Please refer to the <u>Schedule Setting Guide</u> for more information on how to set up a schedule.

3.3.5.2 Combined Rule condition settings

Set compound conditions on event actions to perform more complex forms of event filtering. The following items can be set as compound conditions.

- Rules set in the application in the form of an event action
- Events that make up a rule are set in an application in the form of an event action
- System I/O devices, such as alarm inputs or virtual alarm inputs

1. Click the	Add	button	to set the	e combined rule c	ondition.	
Co	ombined	d Rule	Add			
			UUID	NOT	Time Range	Operation
					-	

2. Please refer to the <u>Combined Rule Setting Guide</u> for more information on setting up.

3.4 Periodic Reporting Setting Example

You can periodically report the counts collected by the counters you have set up to storage, such as FTP, email or AWS S3.

Each counter application has a separate menu where you can set up reporting.

	Home / A	pplications / C)ccupancy	Counting /	Report	
	Counter	Event-Action	Report			
	Report					
To add a nev	v counter rule, cli	ck the + Add R	eport buti	ton in the top rig	ht corner of the re	port list.

3.4.1 Reporting Preferences Settings

Report Name	Report #3122		
 Activation 	\bigcirc		
Counter	All	~	Generate Merged File 🕖
Data Format	CSV	~	

- 1. **Report Name** : Enter the name to identify this report setting. A random default value is inserted, change this if required.
 - Once you have set a report name, you can use the {{REPORT NAME}} token in the report file name or the directory name in the receiver settings to specify this report name in the report file name or the directory name in the receiver settings.
- 2. **Activation** : Check the Enable box if you want to enable the report function simultaneously with generation.
- 3. **Counter** : Set Counters specifies the counters that are included in the report. Counters must be set in advance. The report will include **all counters** that are set when you select **All**.
- 4. **Data Format :** The Data Format setting specifies the type of reporting data. You can report data in CSV or JSON format.

3.4.2 Schedule Settings

Schedule settings allow you to set reporting frequency, reporting time, reported data scope and reported data units. You can register multiple schedules. Each schedule will send data independently.
Schedule Setting		
Reporting Cycle	Every 5 minutes	~
Report Time	00 ~ : 00 ~	
Data	Previous 5 Minute	~
Resolution	5 Minutes	~
		Close Apply

- 1. Reporting Cycle : Set the frequency of data reports.
- 2. **Report Time** : Set when to report based on reporting cycle.
- 3. Data : Set the scope of reporting data.
- 4. **Resolution** : Set the units for aggregating report data.

3.4.3 Recipient settings

Recipient settings are similar to action settings in Event action rule settings. You can set a destination for the report to be delivered to.

File transfer protocols are supported such as FTP (SFTP), email and AWS S3. For detailed settings, refer to the <u>Action Settings Guide</u>.

3.4.4 Finish the setup

Once you've finished setting up your preferences, schedule settings and recipients, click the button at the bottom of the page to submit your reporting settings.

You will see your settings in the list on the Counter Reporting screen if everything is set up correctly.

Home / Applications / O Report Counter Event-Action	Report	
Report (1)		+ Add Report
Report Name	Activation	Operation
Occupacny_Report		۲ D

3.5 Counter Statistics Report Format Guide

3.5.1 Reporting data format

If you've set up <u>reporting</u>, then a statistical report is sent when the next cycle comes around.

Statistical reports are sent as CSV or JSON type data, depending on your settings.

Multiple zones can be set for a single counter. For example, **Counter #1234** can have multiple zones set for it, such as **Zone #1234**, **Zone #1235**, **Zone #1236**, ... etc.

Therefore, the format of the statistics report sent is also variable depending on the counter's settings.

In general, the format of the statistical report will include the following data according to the **counter-zone** hierarchy.

- 1. Total sum data from the counter
- 2. Data by each zone

You can see the format of the data being sent referring an example below.

3.5.2 [People counting] Example of statistical reporting data

If you have the following counters and report set up to periodically receive data from them through reporting settings.

Name	Gangnam Station Traffic Counter					
Ø UUID	ad5d5d0c-10e5-4c4e-baac-501dc3283b52 💭					
People Counting	Add Zone					
	сн	Name				
	CH 1	Gate 6 Crosswalks				
	CH 1	Gate 5 Front				

The counter is named **Gangnam Station Traffic Counter**, and it has two counting areas set up: the **Gate 6 Crosswalks**, and **Gate 5 Front**.

By adding reporting settings in the PeopleCounting app, you can receive statistical reports periodically for these counters.

Below is an example of a statistical report set to send in CSV format every 5 minutes.

3.5.3 Example data in CSV format

Example data in JSON format

timestamp,datetime,[cumulative]-Gangnam Station Traffic Cour 1695107700,09/19/2023 16:15:00,45888,224,33,31,21,8,12,23

[{
"timestamp": 1695171300,
"datetime": "09/20/2023 09:55:00",
"[cumulative]-Gangnam Station Traffic Counter": 28321,
"[count]-Gangnam Station Traffic Counter": 230,
"[A]-Gangnam Station Traffic Counter": 131,
"[B]-Gangnam Station Traffic Counter": 96,
"[A]-Gangnam Station Traffic Counter-Gate 6 Crosswalks": 96,
"[B]-Gangnam Station Traffic Counter-Gate 6 Crosswalks": 38,
"[A]-Gangnam Station Traffic Counter-Gate 5 Front": 35,
"[B]-Gangnam Station Traffic Counter-Gate 5 Front": 58
}]

Each line contains the following data

Aggregation start time from counters

- 1. timestamp
 - The Unix Epoch value of when the data started being collected.
- 2. datetime
 - Date and time values from when the data started being collected. It is set in the format specified in the System-Date and Time setting.

Aggregated statistical data from counters

- 1. [cumulative]-counter name (Ex. [cumulative]-Gangnam Station Traffic Counter)
 - \circ ~ The total sum of the counting data aggregated since this counter was last reset.
 - The cumulative value of the aggregated data from all zone is set in the counter.
 - [cumulative]-counter name = the [cumulative] value of the previous time data + the [count] of the current time data.
 - o If there is a count reset schedule, the cumulative value is initialized at that time.
- 2. [count]-counter name (Ex. [count]-Gangnam Station Traffic Counter)
 - The number of aggregates this counter during at that time.
 - Equal to the sum of all counts counted this time in each zone.
- 3. [A]-counter name (Ex. [A]-Gangnam Station Traffic Counter)
 - Sum of all A-direction counts set in this counter
- 4. **[B]-counter name** (Ex. [B]-Gangnam Station Traffic Counter)
 - Sum of all B-direction counts set in this counter

Statistical data from the individual areas that configure the counter

- [A]-counter name-zone name (Ex. [A]-Gangnam Station Traffic Counter-Gate 6 Crosswalks)

 Aggregate value in the A direction for the zone
- 2. [B]-counter name-zone name (Ex. [B]-Gangnam Station Traffic Counter-Gate 6 Crosswalks) • Aggregate value in the B direction for the zone

3.5.4 [Vehicle Counting] Example of statistical reporting data

This is the same as the report format in the PeopleCounting app.

3.5.5 [Occupancy] Example of statistical reporting data

Example data in JSON format

[{
"timestamp": 1695171300,
"datetime": "09/20/2023 09:55:00",
<pre>"[occupancy]-Building_Occupancy": 2626,</pre>
<pre>"[increase]-Building_Occupancy": 11,</pre>
<pre>"[entry]-Building_Occupancy": 92,</pre>
<pre>"[exit]-Building_Occupancy": 81,</pre>
<pre>"[entry]-Building_Occupancy-Front_Door": 5,</pre>
<pre>"[exit]-Building_Occupancy-Front_Door": 7,</pre>
<pre>"[entry]-Building_Occupancy-Back_Door": 86,</pre>
<pre>"[exit]-Building_Occupancy-Back_Door": 74</pre>
}]

Aggregation start time from counters

- 1. timestamp
 - The Unix Epoch value of when the data started being collected.
- 2. datetime
 - Date and time values from when the data started being collected. It is set in the format specified in the System-Date and Time setting.

Aggregated statistical data from counters

- 1. [occupancy]-counter name (Ex. [occupancy]-Building_Occupancy)
 - The number of people currently occupied by this counter.
 - [occupancy]-counter name = All entering counting All exiting counting, since this counter was last reset
- 2. [increase]-counter name (Ex. [increase]-Building_Occupancy)
 - The change in the number of occupied people that this counter has counted at this time.
 - The sum of the (Entry-Exit) values of all zones set in this counter.
- 3. [entry]-counter name (Ex. [entry]-Building_Occupancy)
 - The sum of entering count from all zones that is set in this counter.
- 4. [exit]-counter name (Ex. [exit]-Building_Occupancy)
 - \circ ~ The sum of exiting count from all zones that is set in this counter.

Statistical data from the individual areas that configure the counter

- [entry]-counter name-zone name (Ex. [entry]-Building_Occupancy-Back_Door)

 The aggregate number of people entering the zone
- 2. [exit]-counter name-zone name(Ex. [exit]-Building_Occupancy-Back_Door))

 The aggregate number of people exiting the zone

5. Reduce False Detection Setting

Deep learning object detection cannot be 100% accurate.

There are several tools to reduce false detections and false alarms. Learn more about these features below, and add settings to reduce false detection.

Object Size Filter

Object Exclusion Area

1. Object Size Filter

Within the same field of view, the size of objects of the same type will be approximately constant, or if the field of view is narrow and the distance is close, the size of objects at the top and bottom will increase and decrease at a constant rate and be detected.

These characteristics can be used to exclude detected objects from events if their size is too large or small compared to expectations.

1.1 Object Minimum Size Filter

The Object Minimum Size Filter is a setting that allows a detected object to be recognized as an object only if the size of its bounding box is greater than the size of the box you set.

To access the settings, click Object Size Filter in the sidebar menu and select Min Size Filter in the body area.



1.1.1 How To Filter The Minimum Object Size



If the bounding box of an object is even larger by one horizontal or vertical dimension than the minimum size filter of the object, it will not be filtered out. Only when the object's bounding box is completely within the minimum size filter will the object be filtered out. See the illustration above to see how the minimum size filter works and which objects are filtered based on the object's bounding box size.

X Notes

The object minimum size filter is not applied to fire detection. The object minimum size filter is not applied to fallen detection.

1.2 Object Maximum Size Filter

The Max Size Filter is a setting that only recognizes a detected object as an object if its bounding box is smaller than the specified box size.

To access the settings, click Object Size Filter in the sidebar menu and select Max Size Filter in the body area.



1.2.1 How To Filter The Maximum Object Size



If the bounding box of an object is even larger by one horizontal or vertical dimension than the maximum size filter of the object, it will be filtered out. Only when the object's bounding box is completely within the maximum size filter will the object not be filtered out. See the illustration above to see how the maximum size filter works and which objects are filtered based on the object's bounding box size.

X Notes

The object maximum size filter is not applied to fire detection.

1.2.2 Filters Set Up

1. Select the channel you want to set the Minimum Size Filter.

CH 1			^
СН	1		
CH 2	2		
СН 3	3		
CH 4	4		
CH S	5		
CH 6	5		
CH 7	7		
	- AND IN	and the same	

2. Select a Minimum Size Filter type.



3. Drag the filter area to move the filter position.



4. Drag the vertex of the filter box to change the size of the filter.



1.2.3 Filter Types

1. Not Used

1) No use Minimum Size Filter for this channel.

2. Normal

1) Use a Normal type of Minimum Size Filter.

2) Typically used when the viewing angle is distant, and the screen area contains objects of approximately similar size.

3) Set a single box and compares all objects to the size of that box. Objects smaller than the box are filtered out.



3. Perspective Correct Interpolation

1) Set two boxes based on perspective.

2) Set the Near Object Min Size box smaller than the size of objects in the near part of the screen at the bottom.

3) Set the Far Object Min Size box smaller than the size of objects in the far part of the screen at the top.

4) A minimum size filter box, calculated as a percentage of the near box and far box, is applied per screen area.

5) Minimum Size Filter with perspective applied based on where the object appears.



1.2.4 Save, Load, And Reset The Settings

1. Save : Click the button at the bottom of the screen to save the position and size information of the filter setting.

2. Load : Click the button to load the most recently saved information of the filter that is set on that channel.

3. Reset : Click the button at the bottom left of the screen to delete and reset the filter settings for that channel.

2. Exclusion Area

Exclusion zones can be used to filter out the same type of false detection that is consistently occurring in the same location. Objects in the area you added as an exclusion zone will be ignored and will not trigger an event.

2.1 Exclusion Zone Settings

1. Click the "False Alarm Reduction > Exclusion Area" in the sidebar menu to access the settings menu.



2. Select the channel you want to exclude.



3. Click the

🛨 Add Zone

button to create an exclusion zone box. Up to 10 exclusion zones can be set.



4. Drag the exclusion zone to move it.



5. Drag the vertex of the exclusion zone box to change the size of the zone.



6. Double-click or right-click the exclusion zone to delete it.



XCaution

It is recommended that the exclusion area is as small as possible to prevent actual objects from being filtered out by the exclusion area settings.

Even if the exclusion zone does not cover the entire object, the object is excluded as long as its center is within the exclusion zone.

2.2 Save, Load, And Reset The Settings

1. Save : Click the button at the bottom of the screen to save the position and size information of the filter setting.

2. Load : Click the that channel.



🛌 Load

t button at the bottom left of the screen to delete and reset the filter settings

Arm/Disarm

button to load the most recently saved information of the filter that is set on

Arm

button in the top

3. Reset : Click the for that channel.

6. Arm/Disarm Setting Guide

In the Disarm settings, you can set the disarm for whether the action is triggered when an event occurs.

1. Arm/Disarm Overview

In a disarmed state, no actions are triggered when an event occurs. In addition to the settings that are enabled by default on **webpage**, you can change the state by entering **alarm input**, **schedule**, etc.

You can change the global disarm status of the device via header.

If you checked the Arm activation button even when disarmed in the Arm/Disarm rule settings, the action will run.

2. Global Disarm



The global disarm status is synchronized with the status of the selected alarm input.

When linked to an alarm input, the disarm status cannot be changed via the webpage and API.

3. Arm/Disarm Instant Settings

Disarm Status(Arm/Disarm)	1 2 3 4 System Event Action Rule
Alarm In	1 2 3 4

X Disarm Configuration

- Global: t can be configured in the top header of the UI, allowing you to control the operation of all device actions. This setting takes priority over per-channel settings and system action disarm rules
- All: You can configure the Arm or Disarm operation of all channels and specified actions..
- Per channel: You can configure the operation of all channels and the specified actions
- System Event Action Rule: You can set whether an action set in a system event/action rule is triggered or not.

All							
Arm	Disarm						
CH 1		CH 2		СН 3		CH 4	
Arm	Disarm	Arm	Disarm	Arm	Disarm	Arm	Disarm
System Eve	nt Action Rule						
Arm	Disarm						

In the Arm/Disarm instant settings, you can set the status of all, per-channel, and system event action rule individually via the buttons. In Arm/Disarm Instant Settings.

If the status of the global disarm is set to disarmed, the event action will not run regardless of the per-channel armed status.

4. Arm/Disarm Rules

Arm/Disarm Rules					+ Add Rule
Rule Name	Activation	Handler	Disarm Status Set	Arm/Disarm Target	Operation
On the Arm/D	isarm Settings scr	een, you can	add a rule by clicking	+ Add Rule button.	

Rule Name	Enter the name				
Active					
Handler	Alarm In Schedule				
	Sun Mon Tue Wed Thu Fri Sat				
	© 00:00				
Disarm Status Set	Arm O Disarm				
Arm/Disarm Target					
	CH 1 CH 2 CH 3 CH 4				
	System Event Action Rule				

- 1. Enter a **rule name** to distinguish of rule.
- 2. The **activate button** sets the rule's activation status.
- 3. The handler specifies whether this rule is for alarm input or schedule.
- 4. **Disarm state set** configures the arm/disarm state when the rule triggers.
- 5. Arm/Disarm target chooses the entities affected by the rule.

4.1 Alarm Input

Handler	Alarm In	O Schedule			
	Alarm In 1	^			
	Al				
Status Set	Alarm in 1				
	Alarm In 2				
rm Target	Alarm In 3				
	Alarm In 4				
)			

You can set up a rule by specifying the alarm input to use.

4.2 Schedule

Handler	 Alarm 	In 💿 So	hedule				
	Sun	Mon	Tue	Wed	Thu	🗌 Fri	Sat
	© 00:00)					

You can set a schedule to change disarm status.

You can set a schedule by setting a target day and specifying a time. For example, you can set a rule to disarm every Saturday at 00:00.

7. Action setting guide

Various types of actions you want to trigger when an AI event occurs can send alarm notifications by defining the event actions in the event action settings.

Users can send real-time events over the network to specific servers or clients, such as **alarm output, voice audio through the camera speaker**, as well as **HTTP, FTP, etc**. And the system can be configured in conjunction with various pre-integrated **VMS**, such as Nx Witness, Cortrol, Milestone, Genetec, etc.

Utilizing Event Meta Tokens & Creating Action Message Guide

Action handlers that use the network can send messages using various event meta-information, such as the **event name** and the **event occurring time**.

When you set up an action handler of the type that sends a message from a device, the action message you want to send is configured in a format that you edit yourself.

By using the various event meta tokens provided when editing an action message, you can easily add dynamic event meta information to your action message.

This approach to action handlers allows users to write and use protocols with a high degree of freedom, depending on the protocols of the target device or server you want to interact with, without requiring additional development.

1 Edit Action Message UI Components

The Edit Action Message UI consists of a **template settings control**, a token settings control, an edit box, an example box, and a test button.

String Construction	Use template	~	Use	
	Select to add tokens	~	Add	
Editable Box	CH{{CH}} - {{EVENT NAME}}	- {{TIMESTA	MP}}	
Message Example	CH3 - My Event Name - 15	51961100.12	3000	
Send example message	Test			

1.1 Edit box, Example box, and Test button

Typically, when composing a message, you type the message you want to send into the edit box. The typed message can contain an event metadata token in the form of {{XXX}} event metadata token. A list of available event metadata tokens is displayed in the Token Settings control dropdown list.

Click the Test button to actually send the hypothetical action message you see in the example box and test the integration with the recipient you're setting up.

1.2 Template Settings Controls

Use the Set Template control to set an action message in the form of a predefined template directly in the edit box.

String Construction	Use template	Use
	Simple msg template	Add
Editable Box	Simple msg template(Json)	?} }
	Basic msg template	
	Basic msg template(Json)	
	Kronos	
	Kronos TCP	00
Message Example	Immix	00

1. Select the template you want to set from the drop-down list.

2. Click the Use button on the right.

XCaution

When you use a template message, everything in the edit box is replaced with the template message. If you are working on something, you will lose your work if you replace it with the template message, so be careful when using it.

1.3 Token Settings Controls

You can insert event metadata into the action message using the Token Settings control.

EVENT NAME	Add
сн	Channel
CH NAME	Channel Name
MAC	MAC Address
RULE NO	Rule index
RULE NAME	Rule Name
EVENT NAME	Event Name
EVENT TYPE	Event Type

- 1. Select the token you want to set from the drop-down list.
- 2. Click the Add button on the right.

The selected event metadata token is added to the edit box, and the virtual event metadata appears in the example box.

The token string can be moved anywhere in the edit box. The list of supported tokens and details of each are described below in the manual.

2 How to use object token {{::OBJ[XXX]}}

In the list of event metadata tokens, tokens of the form {{::OBJ[XXX]}} must be used according to specified rules. {{::OBJ[XXX]}} is a token representing different information about the object(s) causing the event. An event may contain multiple objects, and the event's object information token is repeatedly replaced by object count.

Therefore, to specify where to repeat the syntax from and to for object information tokens, you must use a separate token, which is a list of objects.

The rules for using the OBJ token are as follows.

• All {{::OBJ[XXX]}} tokens must be placed between two {{LIST OBJECTS}} or {{LIST

OBJECTS[PARAM=COMMA]}} tokens, with the first LIST token signifying the start of the iteration and the second LIST token signifying the end of the iteration.

• All {{::OBJ[XXX]}} tokens must be placed between two {{LIST OBJECTS}} or {{LIST

OBJECTS[PARAM=COMMA]}} tokens, with the first LIST token signifying the start of the iteration and the second LIST token signifying the end of the iteration.

• A list of object information starting with {{LIST OBJECTS}} and ending with {{LIST

OBJECTS[PARAM=COMMA]}} and a list of object information starting with {{LIST

OBJECTS[PARAM=COMMA]}} must both end with {{LIST OBJECTS[PARAM=COMMA]}}.

• Object information enclosed in {{LIST OBJECTS}} has no delimiter to separate the items, and the string inside the list is simply repeated.

• {{LIST OBJECTS[PARAM=COMMA]}} appends a comma (",") character to separate items in the list.

To understand how to use the rule, see the following sample.

Me

2.1 1st Example of using an object token

Editable Box	{{LIST OBJECTS}}{{::OBJ[CLASS]}}{{LIST OBJECTS}} {{LIST OBJECTS}}{{::OBJ[CLASS]}} {{LIST OBJECTS}}
essage Example	person person person

The "{{LIST OBJECTS}}" token repeats the string between it and the next "{{LIST OBJECTS}}" token for the number of event objects. The message between the {{LIST OBJECTS}} is repeated twice because the fictional event used to construct the example message contains two person objects.

In the above example, the string is "{{::OBJ[CLASS]}}" and "{{::OBJ[CLASS]}}[newline]". This has resulted in a different message in the example field.

2.2 2nd Example of using an object token

Editable Box	{{LIST OBJECTS}}Class: {{::OBJ[CLASS]}} Bounding Box: P1({{::OBJ[BBOX_X1]}}, {{::OBJ[BBOX_Y1]}}) P2({{::OBJ[BBOX_X2]}}, {{::OBJ[BBOX_Y2]}}) {{LIST OBJECTS}}
Message Example	Class: person Bounding Box: P1(0.145877, 0.56192) P2(0.158819, 0.63) Class: person Bounding Box: P1(0.093212, 0.512331) P2(0.121459, 0.585929)

It is an example message sending object information by adding the bounding box positions of two persons' objects containing a fictional event. The plain text remains the same, and the OBJ token repeats the object information syntax twice the number of objects.

2.3 3rd Example of using an object token

Editable Box	[{{LIST OBJECTS[PARAM=COMMA]}}{ "event_name": "{{EVENT NAME}}" "class": "{{::OBJ[CLASS]}}", "bbox": [{{::OBJ[BBOX_X1]}}, {{::OBJ[BBOX_Y1]}}, {{::OBJ[BBOX_X2]}}, {{::OBJ[BBOX_Y2]}}], }{{LIST OBJECTS[PARAM=COMMA]}}]
Message Example	<pre>[{ "event_name": "My Event Name" "class": "person", "bbox": [0.145877, 0.56192, 0.158819, 0.63], },{ "event_name": "My Event Name" "class": "person", "bbox": [0.093212, 0.512331, 0.121459, 0.585929], }]</pre>

If you use the {{LIST OBJECTS[PARAM=COMMA]}} token to enclose the phrases of the list of object information, it will add a comma (,) between each phrase if there is more than one event object. You can use this to build JSON strings, even if you use repeating object information sentences.

2.4 Event Metadata Token List

This section describes each of the supported event metadata tokens. The event metadata tokens are categorized into four groups: event source, event information, object information, and time information about the object that generated the event.

1. Event sources and information

It is a list of tokens for basic information about the event, such as where it happened on what equipment.

- {{CH}}
- The channel number where the event occurred (1-8) {{CH NAME}}
- Channel name where the event occurred
- Video Source the channel name specified in the video stream setup

Channel Name Channel Name Video Source (MAC) Device MAC address ({RULE NO}) The action rule ID containing the event Intrusion Detection (1) No Name Activa ({RULE NAME}) (RULE NAME) Intrusion Detection (1) Intrusion Detecti	Attribute			
 Video Source {{MAC}} Device MAC address {{RULE NO}} The action rule ID containing the event Intrusion Detection (1) No Name Activation {{RULE NAME}} The action rule name containing the event {{RULE NAME}} The action rule name containing the event Intrusion Detection (1) No Name Activation Activation My Rule #nfmW 		Channel Name	Channel Name	
<pre>{{MAC}} Device MAC address {{RULE NO}} The action rule ID containing the event Intrusion Detection (1) No Name Activa 1 My Rule #nfmW {{RULE NAME}} The action rule name containing the event Intrusion Detection (1) No Name Activa 1 My Rule #nfmW () </pre>	Video Source			
Intrusion Detection (1) No Name Active 1 My Rule #nfmW • {{RULE NAME}} • • The action rule name containing the event • Intrusion Detection (1) • • No Name Active 1 My Rule #nfmW •	 {{MAC}} Device MAC add {{RULE NO}} The action rule 	dress ID containing the e	vent	
No Name Active 1 My Rule #nfmW Image: Comparison of the second sec	Intrusion Detec	ction (1)		
1 My Rule #nfmW {{RULE NAME}} The action rule name containing the event Intrusion Detection (1) No Name 1 My Rule #nfmW	No	Name		Activat
{{RULE NAME}} The action rule name containing the event Intrusion Detection (1) No Name Actival 1 My Rule #nfmW	1	My Rule #nfmW		C
Intrusion Detection (1) No Name 1 My Rule #nfmW	{RULE NAME}} The action rule	name containing th	ie event	
No Name Activa 1 My Rule #nfmW O	Intrusion Detec	:tion (1)		
1 My Rule #nfmW	No	Name		Activati
	1	My Rule #nfmW		O

	Rule Name	My Ru	le #nfmW		
	Ø UUID	78a2bb00	d-113b-4d38-9da9-cfd184	407e747	
	Activation	O			
	Event Setting	Add			
		Video	Event Type	Event Name	UUID
		CH 1	Intrusion Detection	Front Door Intrusion	e971dee5-
	Action Setting	A -1 -1			
{{EVENT TYPE}} Event type Intrusion Detection	n Basic Setting	Add			
{{EVENT TYPE}} Event type Intrusion Detection	Basic Setting Rule Name	Add My R	Rule #nfmW		
{{EVENT TYPE}} Event type Intrusion Detection	Basic Setting Rule Name	My R 78a2bb	Rule #nfmW 0d-113b-4d38-9da9-cfd	18407e747	
{{EVENT TYPE}} Event type Intrusion Detection	Rule Name UUID	My R 78a2bb	lule #nfmW 0d-113b-4d38-9da9-cfd	18407e747	
{{EVENT TYPE}} Event type Intrusion Detection	Basic Setting Rule Name UUID Activation Event Setting	My R 78a2bb	Rule #nfmW 0d-113b-4d38-9da9-cfd	18407e747	
{{EVENT TYPE}} Event type Intrusion Detection	Basic Setting Rule Name UUID Activation Event Setting	My R 78a2bb Add Video	Rule #nfmW 0d-113b-4d38-9da9-cfd Event Type	18407e747 Event Name	UUID
{{EVENT TYPE}} Event type Intrusion Detection	Basic Setting Rule Name UUID Activation Event Setting	Add My R 78a2bb Add Video CH 1	tule #nfmW 0d-113b-4d38-9da9-cfd Event Type Intrusion Detection	18407e747 Event Name Front Door Intrusion	UUID e971da

Number of event objects

2. Event time-related tokens

For example, if the event was at 18:43:9.739 on 7 March 2023 in the GMT+9:00 time zone, each time token would be replaced as follows.

- {{TIME YYYY-MM-DD}}
 - Event date ex) 2023-03-07
- {{TIME YYYYMMDD}}
- Event date ex) 20230307
- {{TIME DD/MM/YYYY}}
- Event date ex) 07/03/2023
- {{TIME YYY}}
- Event year with 4-digit ex) 2023
 {{TIME YY}}
- Event year with 2-digit ex) 23
- {{TIME mm}}

- Event month with 2-digit ex) 03
- {{TIME dd}}
- Event date with 2-digit ex) 07
- {{TIME HH}}
- Event occurrence hour on a 24-hour basis ex) 18
- {{TIME MM}}
- Event occurrence minute with 2-digit ex) 43
- {{TIME SS}}
- Event occurrence second with 2-digit ex) 09
- {{TIME MS}}
- Event occurrence millisecond ex) 739
- {{TIMESTAMP}}
- Timestamp of the event occurrence time ex) 1678182189.739000
- {{TIME ISO8601}}
 - ISO8601 standard format for the event occurrence time ex) 2023-03-
 - 07T18:43:09.739000+09:00
- {{UTC ISO8601}}
 - UTC time in ISO 8601 standard format for the event occurrence time ex) 2023-03-
 - 07T09:43.09.739000+00:00
- {{TIME}}
 - Event time format as designated ex) 07 March 2023 18:43:09
- 3. Token for object information
 - {{LIST OBJECTS}} ~ {{LIST OBJECTS}}
 - Repeat as many times as objects to output the internal syntax.
 - {{LIST OBJECTS[PARAM=COMMA]}} ~ {{LIST OBJECTS[PARAM=COMMA]}}
 - Use commas (,) to separate repeated statements, and repeat the internal syntax as many times as there are objects
 - {{::OBJ[INDEX]}}
 - The event object's index, starting from 0
 - {{::OBJ[TRACK ID]}}
 - Object tracking ID
 - {{::OBJ[CLASS]}}
 - Object class. Different apps and event types detect different objects.
 - person / car / bike / violence / fire / abandoned / animal / man / woman / helmet / nohelmet / vest / no-vest / fallen / lp / ...
 - {{::OBJ[SCORE]}}
 - Object confidence score value
 - The value is for reference and is not appropriate to make a general judgment.
 - {{::OBJ[BBOX_X1]}}
 - The X coordinate of the top left point of the object's bounding box.
 - The coordinate system is normalized to 0-1. The left end is 0, the right end is 1.
 {{::OBJ[BBOX Y1]}}
 - The Y coordinate of the top left point of the object's bounding box
 - The coordinate system is normalized to 0-1. The top end is 0, the bottom end is 1.
 - {{::OBJ[BBOX_X2}}
 - The X coordinate of the right bottom point of the object's bounding box.
 - {{::OBJ[BBOX_Y2}}
 - The Y coordinate of the right bottom point of the object's bounding box.
- 4. Token for displaying LPR object information

When using LPR object information, you must use {{LIST OBJECTS}} or {{LIST OBJECTS[PARAM=COMMA]}} to enclose the object display syntax, as with normal object information.

- {{::OBJ[LP_TEXT_DETECTED}}
- The plate number by License plate recognition
- {{::OBJ[LP_TEXT_DB}}
- The plate number registered to DB by the user

• LP_TEXT_DETECTED and LP_TEXT_DB are usually the same. However, if you are using a loose matching policy, they may be matched even if they are not exact matches.

Matching Policy	Normal	~

Allow similar characters

- {{::OBJ[LP_GROUP_NAME]}}
 - Group name containing the user's registered plate number in DB.
 - If the number is in several groups at the same time, it is replaced by a comma (,) separated list of group names.
 - ex) Group 1, Group 2
- {{::OBJ[LP_ID]}}
- Index number registered in DB
- {{::OBJ[LP_NOTE]}}

.

- The note on the plate number the user has registered in DB.
- {{::OBJ[LP_COUNTRY_CODE]}}
 - Country code of the recognized vehicle number
 - 2-digit alphabetic country code for LPR-EU. Replaced by EU if not detected.
 - 2-digit alphabetic state code for LPR-US. Replaced by US if not detected.
 - Replaced by JP for LPR-JP.
 - Replaced by KR for LPR-KR.
 - {{::OBJ[MOVEMENT_DIR]}}
 - The direction of movement of the recognized vehicle number (indicated by A or B).
 - {{::OBJ[MOVEMENT_DIR_NAME]}}
 - The event name you set for the direction of movement of the recognized vehicle number.

Object Movement Direction 🔞

Direction Discrimination	Vertical 🗸
A-Direction Recognition 🛧	
A-Direction Name	Direction A
B-Direction Recognition 🖊	
B-Direction Name	Direction B

6. Object attributes information token

When you activate the Basic Attributes app or the Advanced Attributes app, additional analysis of detected person's attribute information is performed.

If you want to include object attribute information in an action message, the object display syntax should be start and end with {{LIST OBJECTS}} or {{LIST OBJECTS[PARAM=COMMA]}}. Please refer to the token information for representing the attributes below.

- {{::OBJ[ATTR_TOP_COLOR]}}
 - Top clothes color
 - When top clothes color is analyzed, it will be replaced with one of black, white, red, purple, yellow, gray, blue, green.
- If the estimated top clothes color is unclear, it is replaced with an empty string.
- {{::OBJ[ATTR_BOTTOM_COLOR]}}
 - Bottom clothes color
 - When bottom clothes color is analyzed, it will be replaced with one of black, white, red, purple, yellow, gray, blue, green.
 - If the estimated bottom clothes color is unclear, it is replaced with an empty string.
- {{::OBJ[ATTR_GENDER]}}
 - Gender
 - When gender is analyzed, it will be replaced with one of man, woman.
 - If the estimated gender is unclear, it is replaced with an empty string.
- {{::OBJ[ATTR_AGE]}}
 - Age group
 - If age group is analyzed, it will be replaced with one of young, teenager, adult, old.
 - If the estimated age group is unclear, it is replaced with an empty string.
- {{::OBJ[ATTR_BACKPACK]}}
 - Presence of backpack
 - If presence of backpack is analyzed, it will be replaced with one of yes, no.
- {{::OBJ[ATTR_BAG]}}
 - Presence of bag
 - If presence of bag is analyzed, it will be replaced with one of yes, no.
- {{::OBJ[ATTR_HANDBAG]}}
 - Presence of handbag
 - If presence of handbag is analyzed, it will be replaced with one of yes, no.
- {{::OBJ[ATTR_CLOTHES]}}
 - Clothes type
 - If clothes type is analyzed, it will be replaced with one of dress, pants.
- {{::OBJ[ATTR_HAIR]}}
 - Hair length
 - If hair length is analyzed, it will be replaced with one of short, long.
- {{::OBJ[ATTR_HAT]}}
 - Presence of hat
 - If Hat on is analyzed, it will be replaced with one of yes, no.
- {{::OBJ[ATTR_SLEEVE_LENGTH]}}
 - Top sleeve length
 - If the top sleeve wear length is analyzed, it will be replaced with one of short, long.
- {{::OBJ[ATTR_DOWN_LENGTH]}}
 - Bottom wear length
 - If the bottom wear length is analyzed, it will be replaced with one of short, long.

1. System

1. Relay

Relays are functions that output digital signals through device I/O terminals. Relays can be used to control a warning light or to operate with a door lock as a door control signal. Relay actions can be added from the Action Settings.

Action Type	Relay	\sim
-------------	-------	--------

Select the action type to **Relay**, you'll see the relevant settings at the bottom.

Output

Туре	On for Duration	^
	On for Duration	High Priority
	Off for Duration	High Priority
	ON	Normal Priority
	OFF	Normal Priority

The relay's output type is actually two settings, ON/OFF, but the settings screen is configured to allow you to select four different items. The definitions for each output type are as follows.

Output type	Description	Priority
On for Duration	ON output maintains during the duration time	High
Off for Duration	ON output maintains during the duration time	High
ON	Changes alarm output status to ON	Normal
OFF	Changes alarm output status to OFF	Normal

You'll notice that the right side of each output type describes its priority. Since there are a limited number of relays, and many event action items can be assigned to them, this creates an issue of control over the relay device.

X Relay type control policy

If multiple relay actions are the same priority, the last one to occur takes control
 If a higher and lower priority actions are competing, the higher relay type takes control. Higher priority alarms have a duration, so the last lower priority action takes control after the time elapses.
 Low-priority items have no duration, so they permanently change the default state of the output until a new request is made by another event action.

2. Camera speaker Output

If IP camera connected to the AI AIBOX supports audio output through speakers, you can drive an event action to emit audio output.

Camera speaker output operates based on the protocols defined by the ONVIF Audio Backchannel standard.

※ Preconditions

To run the Camera Speaker Output action, you must set the video stream to connect an additional audio session for sound transmission.

Make sure the following settings are checked for the camera you want to use in the **Video stream – Etc** settings.

Use Cam Speaker 🔽 Connect additional audio session for transmitting sound sources.

2.1 Action Settings

The camera speaker output action can be added from the Action Settings.

1. Select the Action Type to **Camera Speaker**, then, the relevant settings at the bottom.

Action Setting		
Action Type	Camera Speaker	~
Target Camera Sel	lect the camera to send the audio	~
Sound Test	est	
Audio File(mp3/wav)	New Recently Added	
Name		
Audio File	Select	
	Upload	
	Cancel	Apply

2. Select a camera connected to the AI AIBOX to output speaker sound

Target Camera	Video 1	\sim
---------------	---------	--------

3. Select a sound source to send to the camera. Sound files can be uploaded on the **New** menu. MP3 and WAV formats are available.

Audio File(mp3/wav)	New	Recently Added	
Name			
Audio File			Select
	Upload		

Alternatively, select the audio file on the existing list to send to the camera.

Audio File(mp3/wav)	New	Recently Added	
	 Intru 	ision Warning	Edit Delete

3. RS485(RS232)

You can send messages through the RS485 or RS232 interface when an application event occurs. (RS232 is not supported on some models.)

3.1 Basic Interface Wiring

- Rear View



RS-232 (DB-9) Connector Pinout

Below is the pinout of a typical 9 pin RS-232 connector, this connector type is also referred to as a DB-9 connector. A computer's COM port (DTE) is usually male, and any peripheral devices you connect to this port usually have a female connector (DCE).



Pin	Signal	DTE Signal Direction	Description
1	-	-	-
2	RXD	IN	Receive Data : Pin 2 (RXD) is connected to Pin 3 (TXD) of another device.
3	TXD	OUT	Transmit Data : Pin 3 (TXD) is connected to Pin 2 (RXD) of another device.
4	-	÷	·
5	GND	-	Signal Ground : Pin 5 (GND) is commonly connected across all devices.
6	-	-	·
7	-	-	•
8	-	-	-
9	-	1-	-

RS-485 Connector Pinout

Pin	Signal	Signal Direction	Description
1	TX+	Transmit Data+	Device A's TX+ is connected to Device B's RX+
2	TX-	Transmit Data-	Device A's TX- is connected to Device B's RX-
3	RX+	Receive Data+	Device A's RX+ is connected to Device B's TX+
4	RX-	Receive Data-	Device A's RX- is connected to Device B's TX-

RS-485 Topologies

Connecting RS485 4-wire to 4-wire (Full Duplex)

This is an example of a standard 4-wire RS485 device to RS485 device configuration.



Connecting RS485 4-wire to 2-wire (Half Duplex)

For 2-wire transmission, you will need to short the transmit (TXD) and receive (RXD) signals together on the RS-485 port. Wire the 2-wire device's send pin (TXD) to both TXD- and RXD-. Wire the device's receive pin (RXD) to both TXD+ and RXD+.



3.2 Action Setup

The setup procedures for RS485 and RS232 are the same, with the only difference being the output interface.

You can add an RS485 or RS232 action from the action settings screen.

Action Type	RS485	~
-------------	-------	---

When you set the Action Type to RS485, the related settings will be displayed below.

3.3 Message Type

Message Type	Hex Codes	^
	Hex Codes	3
	UTF-8 Characters	

You can set the message type to either Hex Codes or UTF-8 formats. The default setting is Hex Codes.

Hex Codes

When you select the Hex Codes format, you can transmit binary data using hexadecimal values. Event metadata tokens cannot be used when transmitting binary data; instead, you must use fixed binary data. Please refer to the setup example provided.

Setup Example

Message Type	Hex Codes	~
	48 65 6c 6c 6f 0a	

UTF-8

The UTF-8 format allows settings to be configured using Tokens and templates. Please refer to the setup example provided.

Setup Example

Message Type	UTF-8 Characters	
String Construction	Use template \sim	Use
	Select to add tokens \sim	Add
Editable Box	{{DEVICE NAME}} {{MAC}} {{CH}} {{CH NAME}} {{CH NAME}} {{EVENT TYPE[EN]}} {{EVENT NAME}} {{TIME YYYY-MM-DD}} {{TIME HH:MM:SS}} {{TIMESTAMP}}	
Message Example	Device 00116F0003FD 3 Front Door Intrusion Detection My Event Name 2022-09-02 15:37:02 1561961100.123456	

3.4 RS485 (RS232) Setting

Configure Baudrate, DataBits, Parity, and StopBits. These settings are shared across all items of the same action type. Therefore, if you change settings in a specific action handler, it will apply to all action handlers.

RS485 Setting		
Baudrate	115200 bps	~
Data Bits	8 bits	~
Parity	None	~
Stop Bits	1	~
** This setting is the init	tialization setting for $\lceil RS485 floor$	and is shared by all action handlers of the $\ensuremath{\sc {rRS485}}\xspace_1$ type.

Submit

Cancel

2. NETWORK

1. HTTP

When an event occurs, the device can upload event information and snapshot images to an external HTTP server. Messages to be uploaded can be easily edited using token variables.

Action Type HTTP 🗸 🗸

Select the Action Type to HTTP API, then the relevant settings at the bottom

1.1 URL Settings

1. Select the HTTP API URL and Method.

Method	GET ^	
URL	GET	https://edgedx.ai/api
2nd URL	POST	Request here on failure(optional)
Validate Server Certificate	PUT	

Method	GET	\sim	
URL	HTTPS	~	https:// Ganz.it /api
2nd URL	HTTPS	~	Request here on failure(optional)

2nd URL : If you configure a 2nd URL, the request to the 2nd URL is automatically retried only if the request to the primary URL fails.
 However, if the request to the primary URL is successful, the request to the secondary URL will not be made. The 2nd URL is not a required value, so you do not have to set it

2. If you input **Https** protocols, the Validate Server Certificate is activated.

	URL	GET	~	https:// Ganz.it /api
Validate Server Certificate		On	~	
2nd URL	HTTPS	\sim	Requ	est here on failure(optional)

1.2 Authentication

Authentication	None 🔿	
Username	None	
Password	Basic	
	Digest	

Authentication methods are available None, Basic, and Digest.

1.3 Action Delay

Action Dolay	0	^
Action Delay	0	×

After the event occurs, the message is sent after a delay of the amount of time specified in Action Delay. Normally, you can leave it at the default value of 0.

1.4 Show event data

API request data can contain event information.

Select to add tokens	^	Add	
СН			Channel
CH NAME			Channel Name
MAC			MAC Address
TIMESTAMP			timestamp(UTC)
TIME ISO8601			time(UTC)
TIME			time
TIME %YYYY			4 digit year of the time

1. Enter event data values using predefined tokens.

	Select to add tokens	~	Add
Editable Box	{{MAC}}		

- 2. Select the desired token value from the combo box.
 - The selected token value will be added as {{token}} in the form of {{token}}.
 - When sending actual data, this part is replaced by event data.
 - Tokens can only be used where they can be input via the combo box.

1.5 Custom Header Settings

Set



button to set the header

Custom Header	Set
---------------	-----

2. You can use event data tokens on the Custom Header settings page. To use a token, select the text field and add the token. It is only available for Value.

	Custom Header				
	Select to add toke	ens		∨ Use	
	mac		{{mac}}		Delete
	Кеу		Value		Delete
					Cancel Submit
1.6 Que	ery Settings				
Qı	uery String	Set	?ch=3&event_nam	ne=My%20Event%	20Name

The query string can be configured in the same way as the header. Once set, you will see a quick view of the query string.

1.7 Content-type

Selecting Content Type will display the Type settings page.

Content-type : multipart/form-data

From Field Settings

1. Click the

button to set the data.

Content-Type	multipart/form-da	ata				
Form Fields	event	=	CH{{ch}} -	{{event_name}} - {	{{utc	Set
	Key	=	Value			Set
Attach Snapshot						
Snapshot Time Range	From 3 s 🗸	To 1 sec:	/			
Snapshot files key	snapshots					

2. If you click the button, the settings window pop-upUse the event data token to set the value. There's also a simple template.

myEvent		×
String Construction	Use template V	
	Select to add tok V	
Editable Box	CH{{CH}} - {{EVENT NAME}} - {{TIMESTAMP}}	
Message Example	CH3 - My Event Name - 1561961100.123000	
		Cancel Submit

• There are also simple templates available.
ig Construction	Use template A Use
	Simple msg template
Editable Box	Simple msg template(Json) TIMESTAMP}}
	Basic msg template
	Basic msg template(Json)

Snapshot settings

multipart/form-data allows snapshots to be appended.

Attach Snapshot	✓	
Snapshot Time Range	From 3 s 🗸	To 1 sec: V
Snapshot files key	snapshots	

Content-type: Application/Json

Application/Json provides event data token functionality and template functionality. It also provides templates in the form of Json.

Content-Type	application/json	~		
String Construction	Use template	~	Use	
	Select to add tokens	~	Add	
Editable Box	{ "ch":"{{CH}}", "event_name":"{{EVENT NAME}}", "utc_timestamp":"{{TIMESTAMP}}" }			
Message Example	{ "ch":"3", "event_name":"My Event Name", "utc_timestamp":"1561961100.123456" }			

1.8 Message test

You can test your setup data using the Test button at the bottom. Success is displayed at the top.

HTTP Action Setting	Requested. Please check your server log.
Action	Туре НТТР 🗸
Action Preset 1	lame HTTP
Method URL 2nd URL Validate Server Certificate	GET ~ HTTP ~ http://192.168.101.11:8883/ HTTP ~ Request here on failure(optional) Off ~
Action Delay	0
Authentication Username Password	None V
Custom Header Query String	Set Set
Content-Type	application/json
String Construction	Use template V Use Select to add tokens V Add
Editable Box	{ "ch":"{{CH}}", "event_name":"{{EVENT NAME}}", "utc_timestamp":"{{TIMESTAMP}}" }
Message Example	{ "ch":"3", "event_name":"My Event Name", "utc_timestamp":"1561961100.123456" }
Send example message	Test

2. FTP Upload

FTP upload allows you to upload an event snapshot to an FTP server when an application event occurs. The directory and file name to store the snapshot file can be set variably using the event's metadata. The FTP Upload can be added from the Action settings. Select the Action Type to FTP, then, the relevant settings at the bottom.

\sim

2.1 Snapshot Time Range Settings

1. Set the time range for uploading snapshots based on the time of the event.



In the example set above, snapshots taken from 2 seconds before the event to 1 second after the event will be uploaded.

Periodic snapshots are taken at least once per second for each channel, in addition to event snapshots.

2.2 Snapshot Upload Directory and File Name Format Settings

Directory	{{TIME YYYYMMDD}}/{{TIME %HH}}		Select	^	Add
Filename	{{TIME YYYYMMDD}}_{{TIME HHMMSS}}	jpg	TIME YYYYMMDD	YYYYMMDD	d
Example 20220902/15/20220902_153702.jpg			TIME HHMMSS	HHMMSS	
			TIME %YYYY 4 digit	year of the time	ŧ
			TIME %mm Month	n of system time	£
			TIME %dd Date	e of system time	E .
			TIME %HH Hou	r of system time	
			TIME %MM Minute	e of system time	1

- **Directory** : Specify the location where the snapshot image is stored when the FTP Upload action is performed.
 - Event metadata can be included in this setting. Setting the path to include timestamps, as in the setting example above, specifies the upload directory based on the event time. The snapshot will be saved to the root directory of the FTP connection if this setting is not specified.
- Filename : Snapshot file names can be set similarly to directories.
 - The extension for snapshot file names is automatically set to .jpg, so there is no need to change it in the preferences.
- If you specify a snapshot file name, the Example shows an example path to the snapshot created by the directory and file name you specify.

2.3 FTP Server settings

In the Server item, add the FTP server settings you want to transmit. Once added, the FTP server settings can be used to set up other rules or FTP uploading actions in other applications.

Add

1. Click the

button to add new server settings.

	FTP Server	
	Protocol	• FTP O SFTP
	Name	My FTP Server
	Host	192.168.0.5
	2 Port	21 ^
	Username	myftpuser
	Password	mypassword
	Passive Mode	
		Cancel Apply
the destina	ation FTP server informatio	on and click the button.
Server Ac	dd	
	Name	Host

192.168.0.5:21

...

After adding an FTP server setting, a new entry is added to the FTP server list. Select the desired server in the FTP server list to complete setting up the server.

My FTP Server

3. AWS S3 Upload

 \checkmark

2. Enter the

AWS S3 Upload action uploads event snapshots to AWS S3 storage when an application event occurs. The passkey value for the storage storing the snapshot file can be set using event metadata. AWS S3 Upload Action can be added from the Action settings. Select the Action Type to **AWS S3**, then, the relevant settings at the bottom.

Action Type AWS S3 \vee	ction Type	ype AW	S3		\sim
---------------------------	------------	--------	----	--	--------

3.1 Snapshot Time Range Settings

1. Set the time range for uploading snapshots based on the time of the event.

Spanshot Timo Pango	2	^		1	^	second(s)
Shapshot nime kange	-2	~	~		second(s)	

In the example set above, snapshots taken from 2 seconds before the event to 1 second after the event will be uploaded. Periodic snapshots are taken at least once per second for each channel, in addition to event snapshots.

3.2 Snapshot Upload File Path Settings

File Path	{{TIME YYYYMMDD}}/{{TIME HHMMSS}}	.jpg	Select	^	Add
Example	20220902/153702.jpg		TIME YYYYMN	IDD YYYYMN	IDD
			TIME HHMMS	S HHM	MSS
			TIME %YYYY	4 digit year of the	time
			TIME %mm	Month of system	time
		В	TIME %dd	Date of system	time n
			TIME %HH	Hour of system	time
			TIME %MM	Minute of system	time
			TIME O/ CC	C	·

- **File Path** : Specify the path where the snapshot is stored.
 - Event metadata can be included in this setting. Setting the path to include time metadata, as in the example above, sets the upload file path based on the time the event occurred.
 - Set a file path excluding the Region and Bucket parts. You only need to set the path within the bucket where the file will be saved.
- After setting the file path, the Example section shows an example snapshot path.

3.3 AWS S3 Storage Settings

Add

Add AWS S3 storage settings to the Server item.

Once added, AWS S3 storage settings can be used to set other rules or to set AWS S3 upload actions in other applications.

1. Click the

button to add new server settings.

AWS S3	
Name	My Seoul Event Bucket
Region	Asia Pacific (Seoul) 🗸 🗸
Bucket	mycompany.event.seoul
Access Key	AKIA43J3I7YRCPWUX3HF
Secret Key	
	Cancel Apply

2. Enter your target AWS S3 store information.

- 3. Click the Apply button to save the settings.
- 4. Once your AWS S3 storage has been added, it will be listed.

Server	Add				
		Name	Region	Bucket	Operation
		My Seoul Event Bucket	ap-northeast-2	mycompany.event.seoul	

• Once you have ticked the destination box, the setup process for your AWS S3 storage is complete.

4. MQTT Publish

You can use the publish feature of \underline{MQTT} to integrate AI AIBOX with a variety of devices.



4.1 MQTT ?

MOTT(Message Queuing Telemetry Transport) is a lightweight messaging protocol that is ideal for efficient communication in low-bandwidth or unreliable network environments, particularly with IoT(Internet of Things) devices. Its lightweight nature makes it specifically designed for delivering messages between remotely connected devices.

4.1.1 MQTT Features

- Lightweight protocol :MQTT is an efficient protocol for low-bandwidth and resource-constrained environments.
- Asynchronous communication : Clients able to send first and receive messages at a later time.
- Quality of Service(QoS) Level: MQTT also offers various Quality of Service (QoS) levels to guarantee message delivery reliability.
- Last Will and Testament(LWT) messages: The messages is sent when a client experiences an unexpected disconnection.

4.1.2 Main components of MQTT

Broker

The MQTT broker is server as a relay between clients, transmitting messages. The broker receives messages from clients and forwards them to other clients subscribed to the topic. The broker typically functions as a centralized server, serving as the hub for all message exchange.

Client

MQTT clients are endpoints that send and receive messages. Clients can publish messages to the broker or subscribe to specific topics. Clients can take many forms, including IoT devices, mobile apps, and server applications. • Topic

Topics in MQTT define how messages are categorized. Topics are strings that can be hierarchical. (Ex: "home/livingroom/temperature") Clients subscribe to the topics they are interested in, and receive messages only about those topics. Message Payload The message payload is the data component of the MQTT message.

It can vary in form, including text or binary data, and its size is determined by the broker's implementation.

The message payload contains the information that the client wants to send to other clients.

4.2 How to set up the MQTT Publish action

Action Type	MQTT Publish	~
-------------	--------------	---

Select "MQTT Publish" as the action type and click "Add" to show the relevant settings.

4.2.1 Topic Setting

Topic Setting			
Торіс	{{DEVICE NAME}}-{{CH}}	Add Token	Add
Topic Example	Device-3	DEVICE NAME	Device Name including MAC address
		MAC	MAC Address
Jayload Setting		СН	Channel
ayload Setting		CH NAME	Channel Name
ng Construction	Use template	EVENT TYPE[EN]	Event Type English Notation
	Select to add tokens	EVENT TYPE	Event Type
		EVENT NAME	Event Name
Editable Box			

Set the Topic. You can input which can be a specific phrase or a predefined token.

4.2.2 Message Payload Setting

String Construction	Use template			√ Use	
	Select to add	tokens		Add	
Editable Box					
Message Example					
🕖 QoS	Level 0	Level 1	Level 2		

You can set the Message Payload and set the QoS level.

Please refer to "<u>Utilizing Event Meta Tokens & Creating Action Message Guide</u>" for how to set the Message Payload.

4.2.3 MQTT Broker Setting

Message Payload Setting

MQTT Broker	Add		
	Name	Host	Operation
		-	

You can add an MQTT Broker, or select a Broker to use from the added MQTT Brokers. Click the 'Add' button to display a menu to add an MQTT Broker.

MQTT Broker	
Name	MQTT Broker Name
Version	● v3.1.1 ○ v5
Host	broker.hivemq.com
Port	1883
Protocol	MQTT over TCP \checkmark
CA Certificate	Select
Username	
Password	
	Cancel Apply

You can set the name of the MQTT Broker and set the MQTT Broker access information. If you need help with access information, contact your MQTT Broker representative.

4.3 How to test the MQTT Publish action

Here show you how to test using the MQTT Broker and MQTT Web Client, both of which are available for free from <u>hivemq</u>.

4.3.1 MQTT Client : Subscribe Setting

Access to <u>hivemq's MQTT Web Client</u>. Click the Connect button, as the connection to the hivemq free broker is already established by default.

Connection		•			\approx
Host mqtt-dashboard.com	Port 8884	ClientID clientId-UtNuOzOWRf		Connect	
Username	Password	Keep Alive	SSL	Clean Session	
Last-Will Topic		Last-W 0	ïII QoS ▼	Last-Will Retain	
Last-Will Messsage				ĥ	8

Click the "Add New Topic Subscription" button after connecting, and then input the name of the Topic ("ACTION_TEST_MQTT_PUBLISH") you wish to configure in the MQTT Publish action.

Connection				connected	\approx
Publish			~	Subscriptions	~
Topic testtopic/1 Message	QoS 0 v	Retain	Publish	Add New Topic Subscriptio	n

Once set up, you will see a page below. Check the Message section of this page for the test result once you have set up the MQTT Publish action.

Connection		connected	\approx
Publish	*	Subscriptions	
Topic QoS testtopic/1 0	Retain Publish	Add New Topic Subscription	
Messages	*		

4.3.2 MQTT Publish Action Setting

Set up the MQTT Publish action as follows.

MQTT Publish Action Setting								
Action Preset	t Name	MQTT Publish						
Topic Setting								
Торіс	ACTION,	TEST_MQTT_PUBLISH		Ad	ld Token	×	Add	
Topic Example	ACTION_T	EST_MQTT_PUBLISH						
Message Payload Setting								
String Construction	Basic Infe	ormation (JSON)		~	Use			
	Select to	add tokens			Add			
Editable Box	{ "device, "MAC"; "ch":"{(("ch_nar "event_" "event_" "date_ti "timest: }	_name":"{[DEVICE NAME] "{[MAC]}", CH])", De":"{[ICH NAME]}", type":"{[EVENT TYPE[EN] name":"{[EVENT NAME]} ime":"{[EVENT NAME]} ime":"{[TIME YYYY-MM-C amp":"{[TIME YYYY-MM-C))",))", ", DDJ)) ((TIME HH:MM:S	5]]*.				
Message Example	("devic "NAC": "ch_na "event "date_ "times)	e_name":"Device", "00116f000370", me":"Front Door", _type":"Intrusion Dete _name":"Ay Event Name", time":"2022-00-02 15:3 tamp":"1561961100.1234	ction", , 7:02", 56"				0	
QoS	Leve	IO Level 1 😋	Level 2					
MQTT Broker	Add							
		Name	Host	1			Op	eration
	8	MQTT Broker Name	brok	er.hivemq.c	om:1883			
Test	Test							

Set up the MQTT Broker as follows.

MQTT Broker	
Name	MQTT Broker Name
Version	o v3.1.1 ○ v5
Host	broker.hivemq.com
Port	1883
Protocol	MQTT over TCP \sim
CA Certificate	Select
Username	
Password	
	Cancel Apply

After configuration, click the Test button to run the MQTT Publish Test Action. When you see the MQTT Web Client, the test result is displayed as shown below.

Connection			connected	\approx
Publish		*	Subscriptions	~
Topic testtopic/1 Message	QoS Retai	n Publish	Add New Topic Subsc Qos: 2 ACTION_TEST_M	ription X Q
Messages		\$		
2023-12-11 15:07:07 Topic: ACTION_TEST_M { "device_name":"Device", "MAC":"00 "ch_name":"Front Door", "event_type" "event_name":"My Event Name", "dat "timestamp":"1561961100.123456" }	IQTT_PUBLI Qos: 2 116F0003FD", "ch":"3 :"Intrusion Detection e_time":"2022-09-02	3", ", 15:37:02",		

5. Email Alarm

You can email event snapshots and event metadata information when an event occurs.

5.1 Email Action using an SMTP Server Settings

Email actions using an SMTP server can be added from the Action settings.

1. Select the Action Type to Email(SMTP), then, the relevant settings at the bottom. If you set up your own SMTP server and credentials, you can configure an email action using that SMTP server.

Action	/pe Email(SMTP)	~
То	Email recipient	Add
Sender Name	No recipient	
Token	Select to add tokens	
Email Title		
Email Message		
Attach Snapshot	-3 ^ ~ 2 ^ second(s)	
SMTP Server	lew	
[fallen	Edit Delete
	MTP Server smtp.gmail.com : 567 sername louiepark	
Send example message	fest	

2. Click the tap to add a new SMTP server configuration. Registered SMTP server configuration can be referenced to all event actions.

Name	Action preset name				
SMTP Server			25	^ ~	
Encryption	None	~			
Validate Server Certificate	Off	~			
From email					
SMTP Authentication	~				
Username					
Password					

- Name : Enter a SMTP name.
- **SMTP Server** : Enter the address and SMTP server port.
- Encryption: Select the encryption method used by the server, such as SSL/TLS.
- Validate Server Certificate : If you set the Validate server certificate item to ON, the server includes a procedure to verify the certificate presented by the server with a certificate authority. If you use a certificate that a certificate authority has not verified, the email will not be sent.
- From email : Enter the sender's email address if required by the SMTP server.
- SMTP Authentication: Enter the SMTP server authentication information.
- 1. If an SMTP server is added, it shows in the SMTP server list. Select one to configure the email alarm action.

SMTP Server	New			
	• My SMTP Server			
	SMTP Server smtp-mail.outlook.com : 587 Username MY_USERNAME			

3. VMS

1. Cortrol Plug-in Integration Guide

- **1.1 Introduction**
- **1.1.1 Prerequisites**
- AIAIBOX FW version 10124 or greater.
- Ganz Cortrol Premier VMS version 1.22 or greater.
- 1.1.2 Learn about integration architecture



- IP Camera transmits video stream to Cortrol VMS and AIAIBOX.
- AIAIBOX analyzes the received video stream by AI Apps and sends Metadata & Event to Cortrol VMS.
- AIAIBOX responds to Cortrol VMS's search requests.
- **1.2** Configuration
- **1.2.1 AIAIBOX Configuration**

Add AI app settings.

🕸 System <					
Q License Management	Application Info				
Cloud Service	In Use Period of Use Channels Available	• 2023-02-10 ~ 2024-02-10 2			
APP SETTINGS	Channels In Use Al Consumption per CH	1 Z 3 4 5 6 7 8 228			
III Applications	AI Total Consumption	456 / 4000			
4 Intrusion Detection					
⁰∱ Loitering Person	Intrusion Detection				≡ + (t <u>u</u> d
⊐. Virtual Fence	No Name	Activation		Channels In Use	Operation
👖 Tailgating					
Zone Counting			No items ⊘		
Suspicious Behavior					
Occupancy Counting					
*- People Counting					

Add Event Setting.

Rule Nan	me My Rule #i3h	5		
 Activation 	on 🜔			
Olor Lab	xel 🗿 None 📿		0	
Event Setti	ng Add			
	Video	Event Type	Event Nar	ne
Action Setti	ng Add			
	Action Type			
Intrusion Detection Basic Setting				
Intrusion Detection Basic Setting	ule #i3h5			
Intrusion Detection Basic Setting Rule Name My I	Rule #8h5			
Intrusion Detection Basic Setting Rule Name My I Activation C	Rute #i3h5			
Intrusion Detection Basic Setting Rule Name My I @ Activation (@ Color Label @ No	tute #BhS	a		
Intrusion Detection Basic Setting Rule Name My I Activation C Color Label No Event Setting Add	ne			
Intrusion Detection Basic Setting Rule Name My I Activation C Color Label No Event Setting Add	Rule #IDh5			
Intrusion Detection Basic Setting Rule Name My Activation Color Label No Event Setting Add Event Setting	Ruie #ID15		A VIDEO 1	- -
Intrusion Detection Basic Setting Rule Name My Activation Color Label No Event Setting Add Event Setting	Rule #I3h5		 VIDEO 1 Close 	o Appy

Zone or detailed setting of AI App.



Add Control Plug-in Action Setting.

Action Setting A	dip.		
Ac	tion Type		Operation
			-
Action Setting			
Action Type	Select	^	
	НТТР		
	FTP		
	Email(SMTP)		
	AWS S3		
	VMS		
	NX Plugin		
	Cortrol Plugin		
			Cancel Apply

Enter the **Cortrol VMS** information (Server Address, Port number, Username, Password) You can check if the **Cortrol VMS** settings are correct through the **"Login"** button.

Action Setting	
Cortrol Server Setup	
IP Address	192.168.103.199 Connected
Web Port	0308
Username	admin
Password	💿 Login
Metadata Enabled	
Channel Mapping	
Create Cortrol External Service	Create
	Cancel Submit
	Carrier Submit
	G

Note. When **"Metadata Enable"** is enabled, AIAIBOX transmits object **Metadata** detected by **AI** to **Cortrol VMS**. Please note that performance issues may occur if the AI app is installed in an environment where **many objects are detected**.

1.2.2 AIBOX Channel Mapping

Set up the relationship between the **AIAIBOX** channel and the channel of **Cortrol VMS**. Press the **"Mapping"** button to open the settings pop-up window.

Cortrol Server Setup				
	IP Address	192.168.103.199		Connected
	Web Port	8080		
	Username	admin		
	Password		۵	Login
Met	adata Enabled			
Cha	innel Mapping			
Create Cortrol E	xternal Service	Create		
Channel Mapping				
1 CH	Cortrol Channel ID		Cortrol Channel II	Disconnected
2 CH	Cortrol Channel ID		Cortrol Channel II	Disconnected
ЗСН	Cortrol Channel ID		Cortrol Channel II	Disconnected
4 CH	Cortrol Channel ID		Cortrol Channel II	Disconnected
5 CH	Cortrol Channel ID		Cortrol Channel II	Disconnected
6 CH	Cortrol Channel ID		Cortrol Channel II	Disconnected
7 CH	Cortrol Channel ID		Cortrol Channel II	Disconnected
8 CH	Cortrol Channel ID		Cortrol Channel II	Disconnected
Cam	ieras update			
				Close

Enter the **Recording identifier (UUID)** of the channel registered in **Control VMS** into **AIAIBOX**. **Recording identifier (UUID)** can be obtained from the **Details** menu of Channel in **Cortrol Management Console**.

Ganz CORTROL Management Console - 192.168.103.199 - Server					
Configur	ration > (Channels			
Configuration		Create channel group	Edit Assign mair		
Servers			2		
🛞 Networks *		door	■ 사무실		
🗠 External services		EU LPR	EU LPR		
Failover clusters *		G 3 3 3			
L Users					
■ Devices					
Channels					
Recording					
Maps					
- Lavout templates					
Channel	Details				
🖋 Details					
Wembers	Storage		Change		
Membership	Substream re	cording configuration			
Permissions	none		Change		
* Motion datastas	Substream record	ding configuration			
A Motor detector	Substream st	orage			
C Video analytics	Default	94	Change		
Audio	Edge recordu	ng contiguration			
→ Inputs	none		Change		
→ Outputs	Edge recording o	onfiguration			
E Channel configuration	Edge storage				
	Default		Change		
m video overlays	Edge storage				
IIII Dewarp	Video lost tin	ne			
Video configuration	Time Interval In s	econds			
Transport	Recording id	entifier			
Edge configuration	581E34D6-20 Unique recording	04A-44C3-84AB-BD1D2E65C3EA g identifier			
Related items *		l≥			

2 CH (3 CH (4 CH (Cortrol Channel ID Cortrol Channel ID	Cortrol Channel II Cortrol Channel II	Disconnected
3 CH 0	Cortrol Channel ID	Cortrol Channel II	Disconnected
4 CH			
	Cortrol Channel ID	Cortrol Channel II	Disconnected
5 CH	Cortrol Channel ID	Cortrol Channel II	Disconnected
6 CH	Cortrol Channel ID	Cortrol Channel II	Disconnected
7 CH	Cortrol Channel ID	Cortrol Channel II	Disconnected
8 CH	Cortrol Channel ID	Cortrol Channel II	Disconnected

Enter the **Recording identifier (UUID)** and press the **"Camera update"** button to check if it is entered correctly. If the channel is connected successfully, green Connected is displayed.

1.2.3 Create Cortrol External Service

Create an external service by clicking the "Create" button on AIAIBOX's "Cortrol VMS Setup page".

Cortrol Server Setup		
IP Address	192.168.103.199	Connected
Web Port	8080	
Username	admin	
Password	····· ©	Login
Metadata Enabled	8	
Channel Mapping	Mapping	
Create Cortrol External Service	Create	
		Cancel Subinit

Click the "Apply" button to save the Cortrol Server settings.

Action Setting		
Action Type	Cortrol Plugin	
Channel	door ~	
Event Type	detector 🗸	
Cortrol Server	• 192.168.103.199 Connected Edit	
	Web Port 8080 Username admin	
	Only one Cortrol server can be used.	
Test Event	Test	
		Cancel Apply
Setting Confirm		×
lame 🌔 Do you wa	ant to continue?	
	Cancel	
and the second se		

If you see the device registered in the format "AIAIBOX-MacAddress" in the External Service tab of the Cortrol Management Console, it's OK.

Next, Create an External Service Group.

Ganz CORTROL Management Conso	le - 192.168.103.199 - Server	
Configuration > I	External services	
Configuration	New external service grdvp	Edit 🕅 🗶
Servers	ΠΤLΕ	GROUP
Networks *	C Al Bridge-24:76:25:96:56:e1	none
🗠 External services		
E Failover clusters *		
L Users		
Devices		
Channels		

Enter the name of the new External Service Group as "AI AIBOX".

External service group AI Brid	lge*
External service group	Details
🖋 Details*	
Permissions	Title Al Bridge
	External services group name

Assign **AIAIBOX** to the new External Service Group.

	gernene cons	012 - 192.108.105.199 - 561Vei		
🗲 🖲 Configu	uration >	External services		
onfiguration		New external service group	Rdit	同
Servers				Lung
		TITLE		
Networks *		M Bridge-24:76:25:96:56:e1	none	
🖄 External services		🛃 Al Bridge		
Failover clusters *				
Users				
Devices				
Channels				
External service AI Bridge-24:7	6:25:96:56:e1			
xternal service	Details			
kternal service	Details			
xternal service	Details Title			
 Atternal service Details* Events and actions 	Details Title Al Bridge	-24:76:25:96:56:e1		
xternal service Details* Events and actions Related resources	Details Title Al Bridge External ser	-24:76:25:96:56:e1 vice title		
 kternal service Details* Events and actions Related resources 	Details Title Al Bridge External ser Server	-24:76:25:96:56:e1 vice title		
xternal service Details* Events and actions Related resources	Details Title Al Bridge External ser Server none	24:76:25:96:56:e1	Change	
xternal service Details* Events and actions Related resources	Details Title Al Bridge External ser Server none Server (if no	24:76:25:96:56:e1 vice title ne is selected the external service will run on central server)	Change	
xternal service Details* Events and actions Related resources	Details Title Al Bridge External ser Server none Server (if no Group	-24:76:25:96:56:e1 vice title ne is selected the external service will run on central server)	Change	
 Details* Events and actions Related resources 	Details Title Al Bridge External ser Server none Server (if no Group	24:76:25:96:56:e1 vice title ne is selected the external service will run on central server) dge	Change	

1.2.4 Create Cortrol Event & Rule

We need to configure the events, actions, and rules that will be sending notifications Click the **"+New Event"** button to add a new event.



Select Event Type as External Event – External Service.

	Details		
🖍 Details* 2	✤ Select event type		- 0
	Search		
	and the second se	Constant and a second s	
	Available event types		
	Access control (2)		
	Access control event		
	Generic or system event from access control software		
	Access control event related to door status		
	Channel related (2)		
	Digital input Event triggered by device digital input (DI) state change		
	VCA event		
	Event triggered by device-side analytics or Open VCA rule		
	- Contential entries		
	Event received from LPR, FR, or via HTTP API		
	External		
	Variables and counters (4)		
		[]	
		63	
		L3	
Front days Fritanella		13-11-13-110	
Event door External se	rvice*		
Event door External se vent	rvice* Details	La La	
Event door External se vent 🌶 Details*	rvice* Details	La La	
Event door External se vent Details*	Details Event type		
Event door External se vent Ø Details*	Trvice* Details Event type External service	Change	
Event door External se vent Details*	rvice* Details Event type External service Select event type from list of possible event types	Change	
Event door External se vent Details*	rvice* Details Event type External service Select event type from list of possible event types Title	Change	
Event door External se vent Details*	rvice* Details Event type External service Select event type from list of possible event types Title door External service	Change	
Event door External se vent Details*	rvice* Details Event type External service Select event type from list of possible event types Title door External service Event name	Change	
Event door External se vent Details*	rvice* Details Event type External service Select event type from list of possible event types Title door External service Event name Source	Change	
Event door External se vent Details*	rvice* Details Event type External service Select event type from list of possible event types Title door External service Event name Source I door	Change	
Event door External se vent Details*	rvice*	Change	
Event door External se vent Details*	rvice*	Change	
Event door External se vent Details*	rvice* Details Event type External service Select event type from list of possible event types Title door External service Event name Source Event source Service group A I Bridge	Change	
Event door External se vent Details*	rvice*	Change	
Event door External se vent Details*	rvice*	Change Change	
Event door External se vent ✔ Details*	rvice*	Change	
Event door External se vent Details*	rvice*	Change Change	
Event door External se vent ✔ Details*	rvice*	Change Change Change	

Create a rule by combining the created event type and action.

Server Server										
Events	Search	Q		Rules	Search	٩		Actions	Search	Q
CExpand / Collapse list				CExpand / Collapse list				CExpand / Collapse list		
	EVENT		>		RULE		+		ACTION	
4 🖶 door		^		≠ 🖶 door >>> door External ser	vice			4 🗗 door		
door External service			<	door >>> Pop-up on so	reen			Generate alert		
Motion							>	Generate alert substream		
Motion started								Pop-up on screen		
Motion stopped								Pop-up playback on screen		
Recording error								4 🖶 EU LPR		
Recording recovered								Generate alert		
Video lost								Generate alert substream		
Video restored								Pop-up on screen		
4 🖶 EU LPR								Pop-up playback on screen		
Motion										

1.2.5 AIAIBOX Rule Test

In AIBOX's Cortrol Setup page, use the event "Test" button to test whether the setting is successful.



Edit

Filter Setting(Optional)

Action Setting		
Action Type	Cortrol Plugin	
Channel	door 🗸	
Event Type	detector 🗸	
Cortrol Server	O 192.168.103.199 Connected	Edit
	Web Port 8080 Username admin	
	Only one Cortrol server can be used.	
Test Event	Tecthy	

1.3 Demo

1.3.1 Live

Set the **Cortrol Client** to display **Metadata** and **Alarms** to check if it works with **AIBOX**. (Click the icon at the bottom of the video)



1.3.2 Search



2. AIBOX Plugin Integration Guide for Network Optix VMS

1 Introduction

1.1 Prerequisites

- AIBOX FW version 10137 or greater.
- Network Optix Witness VMS version 4.2.0.32840 or greater.
- Network Optix Witness VMS version 5.0.0.35745 or greater.

1.2 Learn about integration architecture



- IP Camera transmits video stream to NX VMS and AIAIBOX.
- **AIBOX** analyzes the received video stream by AI Apps.
- AIBOX sends metadata & event to NX VMS with AIAIBOX NX Plugin.

2 AIBOX NX VMS Plugin Install & Configuration

2.1 Install Nx Witness VMS

Install the Nx Witness VMS v5.X or later. You will need both Server and Client, as the Client will be used in configuration.

2.2 Install AIBOX Plugin (On Windows)

1. Stop the Nx Witness server by right-clicking the tray icon and selecting Stop Server.



2. Download the AIAIBOX analytics plugin from our Customer Portal and unzip.

Copy the "**aibridge_analytics_plugin.dll**" file to {NxInstallPath}\plugins\ usually on "C:\Program Files\Network Optix\Nx Witness\MediaServer\plugins".

📕 🛃 📕 🖛 plu	ugins						
파일 홈 공	유 .	보기					
← → • ↑	→내	PC > SYSTEM (C:) > Program Files >	Network Optix > Nx Witness >	MediaServer > plugin	s	~	Ō
과 주거차기		이름	수정한 날짜	양유	크기		
이 비타 회 대		ibridge_analytics_plugin.dll	2023-03-14 오후 8:49	응용 프로그램 확장	303KB		
- 이상 외원	ж	axis_analytics_plugin.dll	2022-10-12 오후 6:01	응용 프로그램 확장	1,479KB		
◆ 다운로드	*	bosch_analytics_plugin.dll	2022-10-12 오후 6:01	응용 프로그램 확장	564KB		
🔮 문서	*	dahua_analytics_plugin.dll	2022-10-12 오후 5:57	응용 프로그램 확장	490KB		
📰 사진	*	dw_edge_analytics_plugin.dll	2021-05-13 오후 1:24	응용 프로그램 확장	1,389KB		
📕 동영상		dw_mtt_analytics_plugin.dll	2022-10-12 오후 6:06	응용 프로그램 확장	354KB		
h 음악		dw_mx9_analytics_plugin.dll	2022-10-12 오후 6:06	응용 프로그램 확장	395KB		
		generic_multicast_plugin.dll	2022-10-12 오후 6:02	응용 프로그램 확장	71KB		
OneDrive		generic_rtsp_plugin.dll	2022-10-12 오후 6:02	응용 프로그램 확장	30KB		
		hanwha_analytics_plugin.dll	2022-10-12 오후 6:50	응용 프로그램 확장	35,144KB		
3D 개체		hikvision_analytics_plugin.dll	2022-10-12 오후 6:01	응용 프로그램 확장	669KB		

3. Copy the **libzmq-mt-4_3_3.dll** file to {NxInstallPath}\ usually on "C:\Program Files\Network Optix\Nx Witness\MediaServer\".

	MediaServe	r					
파일 홈	공유 보	27					
$\leftarrow \rightarrow \land \uparrow$, > 내 P	C > SYSTEM (C:) > Program Files > Netwo	ork Optix > Nx Witness >	MediaServer		~	ū
🖈 즐겨찾기		이름 ^ 옛 Idap.dll	수정한 날짜 2022-10-12 오후 5:35	유형 응용 프로그램 확상	크기 257KB		
바탕 화면	A	ldap_r.dll	2022-10-12 오후 5:35	응용 프로그램 확장	279KB		
↓ 다운로드 값 문서	*	libssl-1_1-x64.dll	2022-10-12 오후 5:33 2022-10-12 오후 5:33	응용 프로그램 확장 응용 프로그램 확장	671KB		
▶ 사진	A	libzmq-mt-4_3_3.dll	2019-11-19 오후 3:18 2023-03-14 오후 9:01	응용 프로그램 확장 텍스트 문서	425KB 2,419KB		
📓 동영상		log_aibridge_1	2023-03-14 오후 8:49	텍스트 문서	1KB		
		log_aibridge_2 log_aibridge_3	2023-03-14 오후 8:49 2023-03-14 오후 8:49	텍스트 문서 텍스트 문서	47KB 168KB		
		log_aibridge_4	2023-03-14 오후 8:47	텍스트 문서	440KB		
3D 개체		msvcp140.dll	2022-10-12 오후 6:50 2022-10-12 오후 5:33	ㅎㅎ 프도그넘 응용 프로그램 확장	606KB		
🖊 다운로드		msvcp140_1.dll	2022-10-12 오후 5:33	응용 프로그램 확장	31KB		

4. Download & Install vc_redist.x64.exe (https://aka.ms/vs/16/release/vc_redist.x64.exe)

5. Start the Nx Witness server by right-clicking the tray icon and selecting Start Server.

	Server Web Page
ł	Start Server (stopped) Show Server Log
	Quit
흐림	^_@ ☜ Ლ ᡣ)⊗ ₂

6. Setup communication port & Setup Firewall

In the AIAIBOX analytics plugin engine setting menu, (Network Optix VMS System Administration > Plugins Menu) set a unique port (**9911**). This is a TCP port which is used for communication between the Nx Witness AIAIBOX analytics plugin and AIAIBOX.

W System Administration - Nx Wit	ness Client	×
General Users Updates Licenses	Email Security Nx Cloud Time Synchronization Routing Management	
aibridge analytics plugin	Engine settings	
	Service Port 9911 🗘	

7. If your Windows is using a firewall, add New Rule in Windows Firewall Setup > Advanced Settings > Inbound Rules > New Rule.

Note) How to Add a Rule or Port to a Windows 10 Firewall https://www.youtube.com/watch?v=JsEulhg5P8k

2.3 Add NX api Account

Add NX "api" account to be used by AIAIBOX. When creating an account, **enable digest authentication and set the administrator role.**

W System	Administration - N	x Witness Clie	ent					? ×
General L							Managemen	
Q Searc								
	Login 🖳 Name					Ro	ole	
	admin					Ov	vner	
	W User Settings	- api - Nx Wi	tness Clie	ent			×	
Enable								
		api						
		арі						
		•••••						
		•••••	••••					
		Administrator		Edit Roles				
	This user can use d	igest authentica	ition. <u>Learn</u>	More				
	Force Secure Au							
New User	C Enabled				ок Apply	Car	ncel	
								Cancol
					0			Cancel

2.4 Enable video channels to use AIBOX analytics plugin

In the NX client left panel, right-click the camera you want to process with AIBOX and select Camera Settings. In the Plugins tab, enable the AIBOX analytics plugin.

Q < Search ▲ NX50 ▲ admin C EN-IRSD2100 T EN-IRSD2100 Open in New Tab Open in New Window S st Open in New Window L Create Group Ctrl+G Delete Del Rename F2 Check Camera Issues Camera Settings	🔳 New L	.ayout × + ×		
 NX50 admin Server DESKTOP-A9TA3M1 EN-IRSD2100 PTZ Web Open in New Tab St Open in New Window Open in New Window Create Group Ctrl+G Delete Del Rename F2 Check Camera Issues Camera Settings 	Q, ✓ Search			
 Server DESKTOP-A9TA3M1 EN-IRSD2100 PT7 Web I Open in New Tab St Open in New Window Create Group Ctrl+G Delete Del Rename F2 Check Camera Issues Camera Settings 	▲ NX50 ▲ admin			
 ♥ PTZ ♥ Web i Open in New Tab ♥ St Open in New Window ♥ Users P ar Create Group Ctrl+G Delete Del Rename F2 Check Camera Issues Camera Rules Camera Settings 	✓ Image: Server Diagonal S	ESKTOP-A9TA3M1 SD2100		
ar Create Group Ctrl+G Delete Del Rename F2 Check Carnera Issues Carnera Rules Carnera Settings Carnera Settings	• ⑦ PT7 • ⑨ Web I · ⑤ Hí · ⑤ Si • ② Si	Open Open in New Tab Open in New Window		
DeleteDelRenameF2Check Carnera IssuesCarnera RulesCarnera Settings	▶ 💄 ar ि Local	Create Group	Ctrl+G	
Rename F2 Check Camera Issues Camera Rules Camera Settings		Delete	Del	
Check Camera Issues Camera Rules Camera Settings		Rename	F2	
Camera Settings		Check Camera Issues Camera Rules		
		Camera Settings		

Camera Settings - PTZ - Nx Witness Client	? ×
General Recording Motion Dewarping Plugins Expert	
albridge analytics plugin ROI version Uversion 1.0.1 Vendor albridge	
Engine settings □ Enable Metadata ☑ Ignore Metadata (unanalyzed face object ☑ Ignore Metadata (unanalyzed plate object ☑ Show Counter	s) (s)
Metadata Timestamp Correction (ms)	
Camera analytics will work only when camera is being viewed. Enable recording to make it work all the time.	
οκ	Apply Cancel

1. Enable Metadata : It is not recommended to use it except for installation or debugging purposes. Even if this option is disabled, the object on which the event occurred is automatically displayed (saved).

2. Ignore Metadata (unanalyzed face objects) : Face information that has not been analyzed is ignored.

3. Ignore Metadata (unanalyzed plate objects) : plate(LPR) information that has not been analyzed is ignored.

4. Show Counter : show number of Event Occurred.

5. Enable Debug Dump : It is not recommended to use it except for installation or debugging purposes.

A large size of log files can be stored in the {NxInstallPath}\ usually on "C:\Program Files\Network Optix\Nx Witness\MediaServer\". It should be disabled in a production environment.

📕 🛃 📕 🖛 1	MediaServe	er					
파일 홈	공유 브	보기					
\leftrightarrow \rightarrow \checkmark \uparrow	→ 내 P	C > SYSTEM (C:) > Program Files >	Network Optix > Nx Witness > N	MediaServer		~	Ō
📌 즐겨찾기		이름 (에 libzmq-mt-4_3_3.dll	수정한 날짜 2019-11-19 오루 3:18	유형 응용 프로그램 확상	크기 425KB		
📃 바탕 화면	*	log_aibridge_0	2023-03-14 오후 10:00	텍스트 문서	8,844KB		
➡ 다운로드	*	log_aibridge_1	2023-03-14 오후 9:39	텍스트 문서	22,734KB		
🔮 문서	*	log_aibridge_2	2023-03-14 오후 8:49	텍스트 문서	1KB		
문 사진		log_aibridge_3	2023-03-14 오후 8:49	텍스트 문서	47KB		
- 지원	7	log_aibridge_4	2023-03-14 오후 8:49	텍스트 문서	168KB		
📑 동영상		W mediaserver	2022-10-12 오후 6:50	응용 프로그램	50,476KB		
🎝 음악		msvcp140.dll	2022-10-12 오후 5:33	응용 프로그램 확장	606KB		
		msvcp140_1.dll	2022-10-12 오후 5:33	응용 프로그램 확장	31KB		
		msvcp140_2.dll	2022-10-12 오후 5:33	응용 프로그램 확장	199KB		
💻 내 PC		msvcp140_codecvt_ids.dll	2022-10-12 오후 5:33	응용 프로그램 확장	27KB		

6. Metadata Timestamp correction : Metadata (bounding box) is buffered for the set time. (Metadata is displayed delayed for the set time.)

2.5 Enable video channel recording

Non-recording analysis channels cannot use the EVENT and OBJECT panel in NX VMS.



3. AIBOX Configuration

Let's set up to integrate the Loitering Person app with the AIAIBOX $\ensuremath{\mathsf{Nx}}\xspace$ VMS Plugin.

3.1 Setting the video source

			СН 1		×
VIDEO		1	Attribute		
C2					
			Channel Name	Channel Name	
	Object Size Filter	N N	Video Source		
			URL	rtsp://root:~~QQww1122@192.168.103.229:554/cam0_0	
			Transport	TCP \lor	
SYSTE			HTTP(S) Port		
<>			Authentication		
\$			Username		
õ			Password		
	Cloud Service				

3.2 Setting up the Loitering Person app

3.2.1 Add Rule

VIDE		
C	Source	۰
□	Output	۲
SYST	EM SETTINGS	
<>	Network	
ŝ	System	
õ	License Management	
۵	Cloud Service	
APP S	SETTINGS	
0000	Applications	
*	Intrusion Detection	
3∦5	Loitering Person	
3.2.2 Adding event video source

To save the settings, click the "Submit" button before exiting.					
Loitering Person Detection B	asic Setting				
Rule Name	My Rule #PBXv		۲		
Activation	O				
Color Label	O None ○ ■	0 - 0 - 0 -			
Event Setting	Add				
	Video Event Ty	ype Event Name	UUID	Operation	
		7			

3.2.3 Setting Event Configuration

Event Setting				
	Event Type	Loitering Person Detection	~	VIDEO 1 \sim
		PRESE	71	
	Import Zone Settings	Select	~	٩
Event Name	street in front of building	Dwell T	me 5	second(s)
Event Count Label	Loitering	Same Object Repetit	ion 🗌 🛛	
Event Count Reset	Off ~ Rese	t Ignore Duplic	ate 🗌 🔘	
		Reminder Durat	ion 300	second(s)
		Ignoring Inte	val 3	second(s)
				Close Apply & View

AIBOX's Event Name field is displayed as Caption field in NX VMS. It is recommended to enter a name that can identify the event. It is tagged to the object as shown in the figure below. Also, when registering a rule, you can set a detailed rule through text comparison in the caption field.



3.3 Adding NX Plugin action handler

3.3.1 Add Action Setting

Event Setting	Add				
	Video	Event Type	Event Name	UUID	Operation
	CH 1	Loitering Person	street in front of building	3c4781f6-da0e-4d9d-8a94	
		Detection		201f64e08778	
Action Setting	Add				
	Action	Туре		Operation	
			-		

3.3.2 Select VMS / Nx Plugin

 Select	^
ТСР	
Onvif	
VMS	
NX Plugin	
Cortrol Plugin	
Milestone	

3.3.3 Editing VMS IP and Account

Action Setting						
Action	Type					
Nx Witness VMS	• 192.168.10	0.253 Disconnected		Edit		
	Vieb Port 700 Plugin Port 99 Username ap	יי 11 1				
Description	Only one NX ser	ver can be used.	Set			
					Cancel	Apply

Nx Server Setup		
IP Address	192.168.100.253	Disconnected
Web Port	7001	
Plugin Port	9911	
Username	api	
Password		Description Login
Metadata Enabled	V	
Channel Mapping	Mapping	
Test Event	Test	
		Cancel Submit

Enter the **"api"** (case sensitive) account information added in the previous step and test using the Login button. If the test is successful, you will see a connected green status indicator. Additional object information can be passed to NX VMS through the Description field. (For example, LPR app license plate recognition information, group information)

String Construction	Use template 🗸 🗸 🗸 Vse	
	Select to add tok Add	
Editable Box	СН	Channel
	CH NAME	Channel Name
	MAC	MAC Address
	RULE NO	Rule index
Message Example	RULE NAME	Rule Name
	EVENT NAME	Event Name
	EVENT TYPE	Event Type

3.3.4 Channel Mapping

Channel information connection between AIAIBOX and NX VMS is required. If the channel id is entered correctly, the green Connected status will be displayed when you click the Camera Update button.

1 CH	486fa489-a506-27	PTZ - rtsp	Connected
2 CH	NX Channel ID	NX Channel ID	Disconnected
3 CH	NX Channel ID	NX Channel ID	Disconnected
4 CH	NX Channel ID	NX Channel ID	Disconnected
5 CH	NX Channel ID	NX Channel ID	Disconnected
6 CH	NX Channel ID	NX Channel ID	Disconnected
7 CH	NX Channel ID	NX Channel ID	Disconnected
8 CH	NX Channel ID	NX Channel ID	Disconnected

Close

NX channel ID (Camera ID) information can be copied from the camera setup menu of NX VMS.



3.2.5 After completing all settings, click the Submit button at the bottom of the webpage. Your settings will not be saved unless you click the submit button.

Combined Rule	Add					
	UUID	NOT	Time Range	Operation		
			-			
					Cancel	Submit

3. Demo

3.1 Live

Objects with loitering person events are displayed in the NX VMS OBJECTS panel.



Saved objects can be searched through the Object "Advanced" menu of NX VMS.



When objects are not visible, activate Objects in "Show on Items" in the popup menu of the video window.



You can then manually specify the ROI area. It is automatically synchronized with the ROI(zone) information of AIAIBOX through AIAIBOX F/W upgrade in the future.

🛛 Camera Settings - PTZ - Nx Wi	tness Client		?	×
General Recording Motion Dewa	rping Plugins Expert			
aibridge analytics plugin ^ ROI	Polygons Polygon 1	Street ROI		
		+ Add		

3.2 Add Nx VMS Event Rules

If you set the desktop notification action by adding Camera Rules in NX VMS, you can see the event in the NX VMS EVENTS panel.

When registering camera rules, pay attention to the "Event Type" setting. If the APP set in AIBOX and the Event Type do not match, the event will not occur.

note) If the AIBOX Analytics plugin is not up-to-date, there may be no App Event Type supported by AIAIBOX FW. In that case, select "Event" as the Event Type.

Event			
When	Analytics Event		~
At	😈 PTZ		
Event Typ	e: 🔞	Event	^
Caption contains: 😧		Abandon Animal Detection	
Description contains: 😮		Crowd Detection	
🛗 Schedule		Event Fallen Person Detection	
		Fire Detection	
Comments:		Helmet Not Wearing	
		Illegal Parking	
Restore A	II Rules to Defau	Imminent Threat	
		Intrusion Detection	

3. AIBOX Integration Guide for Milestone XProtect VMS

- 1. Introduction
- **1.1 Prerequisites**
 - AIBOX FW version 102700 or greater.
 - Milestone XProtect 2023 R1 or greater.
- 1.2 Learn about integration architecture

There are two ways to integrate AIAIBOX with Milestone XProtect VMS:

1. Case 1

The AIAIBOX receives the RTSP video stream from the IPCAM and provides the annotated video and event data after AI analysis. The annotated video is transcoded to provide object recognition information, bounding boxes, zone information, and more from AIAIBOX's AI analysis.



2. Case 2

Both AIBOX and Milestone XProtect VMS simultaneously receive the RTSP video stream from the IPCAM, and the AIBOX sends the AI analysis events to XProtect VMS. It can also receive the RTSP stream from Milestone XProtect VMS instead of the IPCAM's RTSP video stream.



2. Configuration

2.1 Milestone xProtect VMS Configuration

We will explain how to integrate AIAIBOX with Milestone XProtect VMS using the Case1 method. Note:

For the Case2 integration type, you can skip step 1(Adding the AIAIBOX to Milestone XProtect VMS) and proceed from step 2(Enable the XProtect analytics events).

2.1.1 Adding the AIAIBOX to Milestone XProtect VMS.

In the XProtect Management Client, select "Add Hardware".

Milestone XProtect Management Client 2023 R2



If you know the IP address of the AIAIBOX device, choose "Manual".



Enter the **login** information for the AIBOX.

Add Hard	lware					_	×
Optie	onelly, specify additional user credentials to connect with if the	hardware is not using t	he factory defaults.		n	hilestor	ie
Include	User name	Password				Add	
	(Factory default)	•••••					
	admin	•••••					
	ADMIN	•••••					
	ADMIN	•••••					
	Help		< Back	Next >		Cancel	

Select "ONVIF" from the device driver options.



Select which drivers to use when scanning for hardware. The more drivers selected, the slower the scanning.

Arecont
AXIS
AXIS
Canon
Hanwha
HikVision
HikVision
Infinova
Infinova
JVC
Milestone
Mobotix
ONVIF
Samsung
Sony

Enter the IP address information of the AIBOX. If you haven't changed the onvif service port settings of AIBOX, the Port is 80. HTTPS is not used.

 Address
 Port
 Use HTTPS
 HTTPS port
 Hardware model

 192.168.103.233
 80
 443
 (Auto-detect)

Add the detected AIAIBOX hardware and change the name as desired. If this fails, recheck the setup and try again.

Milestone XProtect Management Client 2023 R2



2.1.2 Enable the XProtect analytics events

Click on the **Tools > Options** menu in the XProtect Management Client.

Milestone XProtect Management Client 2023 R2							
File View Action Tools Help							
Site Navigation	ig Server 👻	ņ					
DESKTOP-CH D	 cording Servers DESKTOP-CBJG4GL AlBridge (192,168,103,233) AlBridge (192,168,103,233) - Camera 1 AlBridge (192,168,103,233) - Camera 2 AlBridge (192,168,103,233) - Camera 3 AlBridge (192,168,103,233) - Camera 4 AlBridge (192,168,103,233) - Camera 4 AlBridge (192,168,103,233) - Camera 5 AlBridge (192,168,103,233) - Camera 6 	•					

In the Analytics Event tab, check the Enabled checkbox. The service port must be open in the firewall. If you change the service port, you must enter the same port number when registering the AIBOX's Milestone action handler.

Options					×
External II	P Audio Messages	Privacy settings	Access Control Settings	Analytics Events	Customer Dashboe < 🔸
Analytics	events				
Events	allowed from:				
● All n	etwork addresses				
⊖ Spe	cified network addresse	s:			
	Address				
•					
	Import				
	Help		C	OK	Cancel

2.1.3 Add analytics events and alarm definitions.

In the XProtect Management Client, select "Analytics events" from the left panel, right-click, and choose "Add New".



Enter the event name as "**AIBOX Event**". This value is an essential key for distinguishing events between AIAIBOX and XProtect. It must be entered in the "**Message key**" property in the Milestone Action handler settings of AIAIBOX.



In the XProtect Management Client, add "Alarm definitions".

Select "Analytics Events" for the Trigger Event item, and choose the "AIBOX Event" you added earlier. For the Trigger Source item, add the channel of the AIAIBOX.

Note: When registering the Trigger Source, if you add the IPCAM channel instead of the AIAIBOX camera channel, it operates as the Case2 integration type.

Alarm Definitions 🛛 🗸 🕈	Alarm Definition Information					
B 🛃 Alarm Definitions	Alarm definition					
- JEridge Alarm	Enable:					
	Name:	AlBridge Alarm				
	Instructions:		~			
			~			
	Trigger					
	Triggering event:	Analytics Events	~			
		AlBridge Event	~			
	Sources:	8 items selected	Select			
	Activation period					
	Time profile:	Always	~			
	O Event bas Select Sources		× Select Select			
	Map Iype filter: All	~				
	Alarm manage Groups Servers	Selected:				
	Belated man:	 AlBridge (192.16 AlBridge (192.16 	8.103.233) - Camera 1 8.103.233) - Camera 2			
	Operator actic	8.103.233) - Camera State (192.16	8.103.233) - Camera 3			
	Time limit:	8.103.233) - Camer: AlBridge (192.16	8.103.233) - Camera 4 8.103.233) - Camera 5			
	Events trigger	Add AlBridge (192.16	8.103.233) - Camera 6 Select			
	Other AlBridge (192.16	8.103.233) - Camera 8.103.233) - Camera 8.103.233) - Camera	8.103.233) - Camera 7 8.103.233) - Camera 8			
	Related came AlBridge (192.16	8.103.233) - Camera	Select			
	Initial alarm or <	5.103.233) - Galilen	~			
	lablet shows as					

2.2 AIBOX Configuration

2.2.1 Add Video Stream

Set (add) the video stream. You can add it either by using an Onvif device search or by directly adding the IPCAM

RTSP stream address.

		CH 3		
VIDEO		Attribute		
🕞 Video Input	~	Characteria		Office Millerbore
Video Stream		Channel N	ame	Office-Milestone
False Alarm Reduction		Video Source		
💷 Display	- C			rten //102 168 102 222/live/main
ೆ Event Action List				nsp.//192.100.103.222/live/main
		Trans	port	TCP
SYSTEM SETTINGS		HTTP(S)	Port	
<> Network	с. С	Authentica	tion 🗌	
බි System	<	Usern	ame	
☐ License Management		Passw	ord	
APP SETTINGS		Video 1	ype	Normal (Min.1280x720, M $ \smallsetminus $
Explore Al Apps				

2.2.2 Set up the AI App

Select the desired AI App and set the AI event for the channel. In the Actions Setting, click the Add button to add the Milestone action handler.

VIDEO			Intrusion Detectio	Intrusion Detection - Rule Setting				
	Video Input	<	Rule Name	Rule #6434				
□	Display	<	🕼 UUID	d10a2533-8227-455	54-8f30-c61be95dab11	D		
	Event Action List							
SYSTE	M SETTINGS		Active	\bigcirc				
	Network	< .	Event Setting	Add				
	System	<		Video Event Type	e Event Name	UUID	Operation	
õ	License Management			CH 3 Intrusion	Intrusion Detection	Ø	54 . eb	
APP S	ETTINGS			Detection				
	Explore AI Apps		Action Setting	Add				
	Active AI Apps	~		Action Type	Action Name		Operation	
*	Intrusion Detection				-			
	Loitering Person							
ħ≈	People Counting							

2.2.3 Enter the Milestone XProtect VMS Server Information

Enter the IP address of the Milestone XProtect VMS and the Analytic Event service port number. Then click the channel "**Mapping**" button.

Milestone Action Setting				
Action Preset Name	Milestone			
Milestone XProtect 0 15	2.168.103.199			
Milestone Server Setup				
IP	Address 192.168.103.199			
· · · · · · · · · · · · · · · · · · ·	Veb Port 9090			
Channel I	Mapping			
		Cancel	Submit	
Vendor AlBri	dge]		
Test Event Test				
				Cancel Apply

Enter the Camera Channel ID of Milestone XProtect VMS.

Note: If you enter the IPCAM channel ID information instead of the AIAIBOX camera channel ID in the camera mapping information, it operates as the Case2 integration type.

1 CH	747dbad9-8bf7-4f47-b91e-6066e0c27d16
2 CH	Milestone Source
3 CH	7be85d10-b99c-43cd-84b4-dfbd96f0bab3
4 CH	Milestone Source
5 CH	Milestone Source
6 CH	Milestone Source
7 CH	Milestone Source
8 CH	Milestone Source

You can find the UUID for the Camera Channel ID by selecting the channel with the mouse while holding down the CTRL key and then looking at the bottom of the info tab.

Site Navigation 🗸 👎 🗙	Devices 🗸 🧸	Properties
DESKTOP-CBJG4GL - (23,2a)	Cameras	Device information
🖶 💷 Basics	😂 Camera Group 1	Manad
- 🔚 License Information	- 🔐 AlBridge (192,168,103,233) - C	Name:
Site Information	Sa AlRridge (192 168 103 233) - C	AlBridge (192,168,103,233) - Camera 3
Servers	- 🌱 AlBridge (192,168,103,233) - C	Short name:
Recording Servers	Albridge (192, 166, 103, 233) - C	
Mobile Servers	- AlBridge (192,168,103,233) - C	
Devices	AlBridge (192,168,103,233) - C	Description:
Cameras	AlBridge (192,168,103,233) - C	
- Microphones		
Votedata		
- Output		
□ I Client		Hardware exercit
View Groups		Hardware name.
Matrix		AlBridge (192,168,103,233)
Rules and Events		Port number:
- 📋 Rules		
Time Profiles		3
Notification Profiles		
- Vser-defined Events		Positioning information
Analytics Events		GPS coordinates: Illustration:
Generic Events		Non
Security		(Example: -33.856900, 151.215100)
- Roles		
- Rasic Users		Direction (a):
System Dashboard		0 Degrees
Current Tasks		Field of view (b):
Configuration Reports		0 Degrees
Matadata Lice		C
- Metadata Search		Depth (c):
Access Control		0 Meters v
🖃 🖾 Transact		
Transaction sources		Preview position in browser
Transaction definitions		
🖻 🛃 Alarms	1	
- 🧏 Alarm Definitions	1	ID and primary table = 7be85d10-b99c-43cd-84b4-dfbd96f0bab3
- Alarm Data Settings	1	Edge table = e457f3da-f4f6-49b2-8f40-241977b81cb0
-19 Sound Settings	1	

For the "Message Key" property, input the name of the "Analytic Event" that you added in Milestone XProtect. In this guide, we have entered it as **"AIBOX Event"**.

N

filestone Action Setting		
Action Preset I	Name Milestone	
Milestone XProtect	0 192.168.103.199	
	Web Port 9090	
	Only one Milestone server can be used.	
Message key	AlBridge Event	
Object	CH{{ch}} - {{event_name}} - {{utc_timesta	Set
Location	office	
Vendor	AlBridge	
Test Event	Test	

The Object field can be utilized in various ways. You can enter event texts, LPR information, etc., so you can send additional information in the Milestone XProtect Alarm Manager.

String Construction	Use template	Use
	Simple msg template	Add
Editable Box	Simple msg template(Json)	1P}}
	Basic Object msg template	
	Object msg template(Json)	
	Simple LPR msg template	
Message Example	Basic LPR msg template	456
	LPR msg template(Json)	
String Construction	Simple LPR msg template	√ Use
String Construction	Simple LPR msg template Select to add tokens	✓ Use ✓ Add
String Construction Editable Box	Simple LPR msg template Select to add tokens {{UST OBJECTS[PARAM=COMM/ {{::OBJ[LP_TEXT_DETECTED]}}{{US OBJECTS[PARAM=COMMA]]}	VUse Add

Note: If you want to set the Object property differently for each AI App, you can create a separate Milestone Action handler for each AI App.

By pressing the "Test" button, you can check the Test Event in the Milestone XProtect Client.

1 오후 3:55:20 Cannot show boun	ding boxes. Check if your compu	ater's system time is correct. If the	he system time is n	ot the issue, contact yo	ur system administrator.					
AlBridge (192.168.103.233	3) - Camera 3			- AI	Bridge (192.168.103.23	3) - Camera	a 1 - 2023-1	0-03 오후 3	:55:21.859	
Intrusion: 10			FQ		allen Person: 174		-10-03	2# 3:55:22.4	432	
Quick Filters	Alarms New (filter applied	d) 💙 Clear filter							Report	s 1-
T New (14)	! Time 👻	Priority Level State Level	State Name	Message	Source		Vendor	Location	Туре	Object
Y In progress (0)	요후 3:54:58 2023-10	1 1	New	AlBridge Event	AlBridge (192.168.103.233)	53786	AlBridge	office		CH1 1696
Y On hold (6)							Colorado			
T Closed (6)										

If the event test is successful, check the "Activate Milestone action handler" checkbox and press the "Apply" button to save the handler settings.

Action Setting					
	Action Type	Milestone	~		
•	Check the target acti You need to choose	on you want to apply to this rule. one action.			
	Milestone Action A	dd			
	Na	me	Operation		
	Mil	estone	o c i		
				Cancel	Apply

Finally, press the "Submit" button located at the bottom of the AI App settings to save all configurations.

ŝ	System <				
õ	License Management	Combined	Add		
APP S	ETTINGS	Rule			
	Explore AI Apps		Reference Rule / Event	NOT Time Range	Operation
	Active AI Apps ~			-	
*	Intrusion Detection				
² %	Loitering Person				
ħ =	People Counting				Cancel

3. Demo

3.1 Live

In the Live screen of the XProtect Smart Client, the analytics events will be listed within the Alarms panel as well as the annotated video.



3.2 Search

In the search menu, click on the "Search for.." button and select Alarms to search for AI Events.



3.3 Alarm Manager

1. In the Alarm Manager, by clicking on an individual alarm, you can check detailed event occurrence information with recorded video.

Milestone XProtect Smart													×
Views Expo	orts Search	Alarm Manag	ger 🧔						(A Not secure	오후 3:59:5	5 🛃	
												Setup	\checkmark
(i) 오草 3:55:20 Cannot sho	w bounding boxes. Check if y	our computer's system time is	correct. If the system time	e is not the issue,	contact your system	n administrator.							×
A <>	been selected				12	AlBridge (192.168.103.233) - Camera 1 -	2023-10-03 오후 24	12:45:577					-
						Fallen Person: 166			m				
	10 53774 AlBridge Ev	vent - AlBridge (192.168.10	3.233) - Camera 1			- 0 X			~				
	ABrage 192, De 1012	23) - Camera 1	mera 1		2023-10-03	2.#2.960 VS 2.223,827 ► Q.# 2.4238,837 ► Go to Alam Time						ACC DING	
	Instructions												
Owick Eiltern	Description				State:	1: New 👻					Reports	1-12	
					Priority:	1: High 👻					response		
T New (12)					Category:		D	Vendor 🔺	Location	Туре	Object		
T In progress (0)						53774	53774	AlBridge	office	Fallen	CH1 - Fallen	n Person D	stection
Y On hold (6)					Source:	AlBridge (192,168,103,233	53775	AlBridge	office	Fallen	CH1 - Fallen	Person D	tection
Y Closed (9)					Alarm:	AlBridge Alarm	53776	AlBridge	office	Fallen	CHI - Fallen	Person D	tection
	Activities				Message:	AlBridge Event	53778	AlBridge	office	Fallen	CH1 - Faller	Person D	dection
	Time Activity	of 1: Now			Туре:	Fallen	53779	AlBridge	office	Intrusion	CH3 - Intrusi	ion Detecti	on - 169
2	오후 2:42 Initial state	rity: 1: High			Rule:	Alarm Definition	53780	AlBridge	office	Fallen	CH1 - Faller	Person D	etection
Servers			6			office	53781	AlBridge	office	Fallen	CH1 - Fallen	Person D	atection
- DESKTOP-CBJG4GL							53782	AlBridge	office	Fallen	CH1 - Fallen	Person D	atection
						AlBridge	53783	AlBridge	office	Fallen	CH1 - Fallen	Person D	etection
				bbA		CH1 - Fallen Person Detec	53786	AlBridge	office		CH1 169	6316098.2	17266
							53788	AlBridge	office	Fallen	CH1 - Fallen	Person D	stection
	Help Prir	nt				ок							

Note: The Alarm Manager is supported in Milestone XProtect Express+ and higher versions.

2. To display analytic event properties in the Smart Client, you might need to adjust settings in the Management Client. First, navigate to "Alarms" and then to "Alarm Data Settings". From there, choose the event properties you want and transfer them from the left panel to the right.



3.To display the event properties in the Smart Client, right clicking on the event header and select the fields to display

	A P	2		-		x	-
- 3:30		◄ ◀ 2023-10-03		오후 3:59:4	8.027 II	•	2
					Reports		1-12
lame	Message	Source		Alarm	Vondor	L	ocation
	AlBridge Event	AlBridge (192.168		Category Level			office
	AlBridge Event	AlBridge (192.168		Cotoroo Nor			office
	AlBridge Event	AlBridge (192.168		Category Name	e		office
	AlBridge Event	AlBridge (192.168	~	ID			office
	AlBridge Event	AlBridge (192.168	~	Image		(office
	AlBridge Event	AlBridge (192.168	~	Location		1	office
	AlBridge Event	AlBridge (192.168	7	Message			office
	AlBridge Event	AlBridge (192.168	٠,	Object			office
	AlBridge Event	AlBridge (192.168	۲	Object			office
	AlBridge Event	AlBridge (192.168		Owner			office
	AlBridge Event	AlBridge (192.168	4	Priority Level			office
	AlBridge Event	AlBridge (192.168		Priority Name			office
				Rule			
				Server Name			÷
	-		1	Source			
ж	LIVE		٠.	Jource			

7. Schedule Setting Guide

A schedule can be set in all event action settings to trigger actions when events occur.



1. Schedule Overview

The schedule operates over a period of time to set the time for sending the notification whenever an event occurs. Depending on **weekly, monthly,** and **yearly** schedules can be set.

Additionally, specific dates can be designated as **exclusion schedules**. Actions will not be triggered during the exclusion schedule. Exclusion schedules are prior to regular schedules. This means that the action will not be triggered if an event occurs during a period that is included in both the exclusion and the regular schedule.

The schedule for event action settings operates according to the following policy.

X Schedule Application Policy

1. If no schedule is set in event actions, all events will always trigger the set action.

2. If multiple schedules are registered in event actions, the action will be triggered if one of them is true at least.

3. If an exclusion schedule is included, the action will not be triggered even if another schedule is true.

4. Schedules are set for each event action, but once created, they can be added in all event actions.

2. Create a New Schedule

1. Click the Setting butto	on to add a schedule.	
Schedule Setting S	etting	
Na	ime	Operation
	-	
2. Click the Add New bu	tton to create a new schedule at the bottom.	
Name	Schedule preset name	
Schedule Cycle	Weekly	~
Schedule Designation	Day-based	~
Schedule	Day	~
Time Range	© 00:00 ~ © 00:00	
Exclusion Schedule	Set this as exclusion schedule	

Name : Enter a schedule name on "Name" (e.g. working hours, holidays).

Schedule Cycle : Set the "schedule cycle" for how often the schedule should repeat as weekly, monthly, or yearly.

Schedule Designation : Select whether the schedule is based on days of the week or specific dates. **Schedule & Time range :** Set the days/dates/Time.

Exclusion Schedule : Check the box to set the schedule as an exclusion schedule.

3. Weekly Schedule

1. Since weekly schedules cannot specify dates, the schedule Designation is fixed to Day-based of the week. You can set the target days and specify the time range to create a schedule. For example, you can set a schedule for **every Monday to Friday**.

Schedule Cycle	Weekly	~
Schedule Designation	Day-based	~
Schedule	Day	^
Time Range	Mon	
Furthering Colored de	Tue	
Exclusion Schedule	Wed	
	Thu	
	Fri	
	Sat	
	Sun	

4. Monthly Schedule

1. For monthly schedules that use the Day-based option, you can specify by a week of the month. For example, you can set a schedule for **every second week of the month, Monday to Friday**.

Schedule Cycle	Monthly	~
Schedule Designation	Day-based	~
Schedule	Mon 🛞 Tue 🛞 Wed 🛞 Thu 🛞 Fri 🛞	~
	1st week 🛞 2nd week 🛞 4th week 🛞	~
Time Range	© 09:00 ~ © 18:00	
Exclusion Schedule	Set this as exclusion schedule	

2. For monthly schedules that use the Date-based option, you can specify the dates of the month for the schedule. For example, you can set a schedule for the **1st**, **15th**, **and the last day of the month**.

Schedule Cycle	Monthly	~
Schedule Designation	Date-based	~
Schedule	1 🛞 15 🛞 The last day 🛞	~
Time Range	© 09:00 ~ © 18:00	
Exclusion Schedule	Set this as exclusion schedule	

5. Yearly Schedule

1. For yearly schedules that use the Day-based option, you can specify the target month, week, and day. For example, you can set a schedule for **the second Monday to Friday of January to March every year**.

Schedule Cycle	Yearly	~
Schedule Designation	Day-based	~
Schedule	Mon 🛞 Tue 🛞 Wed 🛞 Thu 🛞 Fri 🛞	~
	1st week 🛞 2nd week 🛞 4th week 🛞	~
	Jan 🛞 Feb 🛞 Mar 🛞	~
Time Range	© 09:00 ~ © 18:00	
Exclusion Schedule	Set this as exclusion schedule	

2. For yearly schedules that use the Date-based option, you can specify the dates for each target month. For example, you can set up a schedule on **the 1st, 15th, and the last day of January to March.**

Schedule Cycle	Yearly	\sim
Schedule Designation	Date-based	\sim
Schedule	1 🛞 15 🛞 The last day 🛞	\sim
	Jan 🛞 Feb 🛞 Mar 🛞	\sim
Time Range	© 09:00 ~ © 18:00	
Exclusion Schedule	Set this as exclusion schedule	

6. Time Schedule Setting

The time schedule sets to run on the specified date. The time schedule follows the policy below.

1. If the start time is faster then the end time, the schedule will be applied according to the specified time in the day. (e.g. 09:00~18:00)

2. If the start and end time are the same, the schedule will be applied for the entire 24 hours of that day. (e.g. 00:00~00:00)

3. If the start time is later than the end time, the schedule will be applied from the start time of that day until the end time of the next day. (e.g. 21:00~09:00)

7. Exclusion Schedule

You can set a schedule as an exclusion schedule, which takes priority over the regular schedule. If any of the exclusion schedules are active during the scheduled time of an event action, the action will not be triggered.

Exclusion Schedule **Version Schedule**

8. Combined Rule Setting Guide

You can set compound rule conditions to trigger actions when events occur in event action settings.



1. Overview of Compound Rule Conditions

When setting up event action rules for each application, you can set conditions for triggering actions. In addition to setting scheduling conditions, you can also set conditions based on various system conditions to determine whether event actions should be triggered.

By utilizing the state of basic system resources such as alarm inputs or virtual alarm inputs, you can automatically control rules. If there are other event action settings that have been previously set up, you can also set conditions based on whether or not the event has occurred.

For example, if you want to turn on a warning light and broadcast a warning message to the camera through an alarm output for a residential intrusion event, you can reduce false alarms by setting the following conditions.

- Schedule (20:00~07:00)
- If even one person is detected outside the perimeter of the residential area within the last 10 seconds before the residential intrusion event occurs
- If alarm input signal 1 is being triggered

2. Combined Rule Conditions Setting

The following are the items that can be set as compound rule conditions

- Rules set up in the application
- Events specified by the application's rules.
- System I/O devices such as alarm inputs or virtual alarm inputs

Add

1. Click the

button to add a new condition on the event action setup screen.

Combined Rule	Add						
	UUID	NOT	Time Range	Operation			
			-				
Apply							

2. Click the button to save after set the each options.

Combined Rule
UUID
UUID
Search
NOT
Time Range(In Secs)
-5
~
0
Apply
Cancel
Apply

UUID : Ender the UUID value assigned to a target event, rule, or system device. When setting up an event action in the application, both the event and rule receive a unique UUID. You can input the UUID of the event

or rule that you want to set up as a condition. Alternatively, Click button next to the UUID field allows you to search for and input a previously set-up item.

DUUD	
Rules	
 System & I/O (5) I/O Devices Alarm In (4) Virtual Alarm In (20) 	
	Cancel

NOT : If NOT is checked, the condition will be true if the UUID event or rule is false. For example, if you specify the UUID of "Event A" and check the NOT checkbox, the condition will be true if "Event A" did not occur.

Time Range(In Secs) : Time Range field is used to set the valid time range for UUID events or rules. When an event for the rule occurs, if a UUID condition event occurs within the Time Range set based on the event occurrence time, the condition is considered true.

3. System I/O Combined Condition Settings

All rules and their events in currently used applications can be set as compound rule conditions. Additionally, **alarm** and **virtual alarm inputs** can always be set as conditions for composite rules, even without setting up a separate event action rule.

These inputs have a unique resource UUID assigned to them in their initial state, and can be selected as a separate item in the UUID search UI.

Ev	Event/Action Alarm In Virtual Alarm In Disarm								
,	Alarm in (4)								
	Device	Name 🖉	State	Normal State	UUID				
Ŀ									
	Alarm In 1	Front Door Relay	OFF	N/O	72a34355-e39c-4deb-a5b5-a6075ffd7318				
	Alarm In 2	Alarm IN 2	OFF	N/0	b5e081f6-e299-434d-8499-34acf7265d0f				
	Alarm In 3	Alarm IN 3	OFF	N/0	269333e8-d421-494f-a450-44beeb0b5a19				
	Alarm In 4	Alarm IN 4	OFF	N/0	0d778767-fb06-4c66-88b5-86900e07141f				

UUID

Rules

- Crowd Detection (1)
- Virtual Fence (2)
- Intrusion Detection (1)
- Loitering Person (1)
- System & I/O (5)

I/O Devices

- Alarm In (4)
- Virtual Alarm In (20)
 - Virtual Alarm IN 1 (8f3e8a1a-a85a-40dd-b27e-5f2820be5cdf) Virtual Alarm IN 2 (890a91de-53e4-4143-af0c-66f8efd7fb11) Virtual Alarm IN 3 (a63dd6c6-0e12-4cc1-8e8b-28dd556b6f26) Virtual Alarm IN 4 (c655b350-0828-4bc8-a8d1-fb9b0a0b6430) Virtual Alarm IN 5 (efbb8495-361d-4939-8f1f-a5720a27b406) Virtual Alarm IN 6 (8c773e5e-6d66-4849-8c7d-e96364add288) Virtual Alarm IN 7 (2241f66a-e853-48bf-8fd2-f97774e2049c) Virtual Alarm IN 8 (689f44a1-ce78-4bc7-80c3-cefa82aa5a6b) Virtual Alarm IN 9 (42bf1faa-2624-440f-841f-cd017d09ba75) Virtual Alarm IN 10 (b5d91997-e0b3-419e-a4c8-935933ee7bc2) Virtual Alarm IN 11 (8db0bd1f-86af-4e59-98e3-16979ef885e3) Virtual Alarm IN 12 (e500c982-eb95-47d5-ae6a-8ecf8f647082) Virtual Alarm IN 13 (66052861-7fae-4a7a-9142-ac9385110c86) Virtual Alarm IN 14 (84d51822-1864-49e1-8d5c-a2a1943c0882) Virtual Alarm IN 15 (d1481319-d693-4423-aba5-b1bd3ec27af3) Virtual Alarm IN 16 (b96a2c0e-08f5-4c2c-8667-058597b81c8d) Virtual Alarm IN 17 (495f0f77-f98c-432d-9142-1ed4c85c23ba) Virtual Alarm IN 18 (a05020a4-93ef-4c7f-a51d-f679e13d3477) Virtual Alarm IN 19 (71323411-6bac-40ff-a0ca-e04d7379d355) Virtual Alarm IN 20 (e8d2dad0-0c88-42e6-a951-88a387ed4cab)

Cancel