



Access control

OPTIMA®

ONE Safe



ONE **SAFE**

Copyright: © Eden Innovations

No part of this publication may be reproduced, transmitted, transcribed or translated in any form or by any means without the consent of the copyright holder. Unauthorized copying can not only break the laws of copyright but also reduce the ability of Eden Innovations to provide accurate information.

Contents

1. Specifications	4
2. Compatibilities	4
3. Restrictions	4
4. One Safe module.....	4
1- Activate ONE Safe	4
2- Access to the module.....	4
5. Settings.....	5
5.1- Add an intrusion device	5
5.1.1 General settings	5
5.1.2 Network settings.....	5
5.1.3 Functional parameters.....	5
5.2- Configuration of inputs, outputs and groups	5
5.2.1 Input points.....	6
5.2.2 Output points.....	6
5.2.3 Groups.....	6
3 -Start/stop communication with intrusion device.....	7
6. Configuring intrusion systems.....	7
6.1- RISCO alarm configuration.....	7
6.2- GALAXY HONEYWELL alarm configuration	8
6.2.1 Configuration from the HONEYWELL keypad	8
6.2.2 Configuration of the intrusion device from the RSS software (GALAXY Flex).....	8
6.2-3 Set intrusion device in the OPTIMA interface.....	9
6.3- VANDERBILT SPC alarm configuration	10
6.3.1 Time out configuration	11
6.3.2 IP Address - Communication Port - Client Code	11
6.3.3 Encryption key.....	12
6.3.4 User names and password.....	13
6.3.5 Time to retrieve data from the unit.....	13
6.3.6 Vanderbilt software specifics.....	14
7. Operation	18
7.1-Dashboard.....	18
7.1.1 Input points.....	18
7.1.2 Output points.....	19
7.2-Intrusion event live	19
7.3-Events list.....	19
7.4- Actions record.....	20

- 7.5-User codes 21
- 7.6- Alerts..... 21
- 7.7- Adding a group, inputs, outputs in Supervision..... 22
- 7.8- Automation associated with Intrusion 22
 - 7.8.1 Possible conditions on intrusion groups 22
 - 7.8.2 Possible conditions on intrusion inputs 22
 - 7.8.3 Possible conditions on the intrusion outputs 22
 - 7.8.4 Possible actions on the intrusion ouputs points..... 22
 - 7.8.5 Possible actions on the intrusion groups 22
- 8- Use case 23
 - 8.1 Scenario 1..... 23
 - 8.2 Scenario 2..... 24

1. Specifications

The *ONE Safe* module allows you to interface your access control with compatible intrusion devices in order to manage alarm groups, trigger alerts and process them.

Features:

- Control the groups of your alarm intrusion systems to activate arming/partial arming/delayed arming/disarming, remote acknowledgment.
- Monitor the alarms of your groups to carry out the desired actions.
- Check the status of your alarm inputs and take the desired actions, with the possibility of excluding/including at the level of Intrusion monitoring.
- Check the status of your Intrusion outputs and take the desired actions, with the ability to change their status.

The different elements can be consulted/activated on the Supervision plans (see OPTIMA 360 module).

2. Compatibilities

The ONE Safe module is compatible with

- **RISCO** intrusion devices including **LightSYS™2**, **ProSYS Plus**, **LightSYS+**
- **HONEYWELL** intrusion devices including **GD-96**, **GD-520**, **GD-48**, **GD-264**, **Galaxy Flex**
- **VanderBilt** including **SPC4**, **SPC5** and **SP6**

3. Restrictions



The establishment of communication between the OPTIMA and the intrusion devices does not allow simultaneous connection with their administration software.

A poor data link between the OPTIMA and the intrusion devices affects the control, monitoring and verification of alarm states.

4. One Safe module

1- Activate ONE Safe

It is necessary to activate this additional module from the Configuration menu/Installation administration/Additional modules. You will be asked for an activation code.



Fig. 1: One Safe activation.

2- Access to the module

The ONE Safe module is available from the operation menu.



Fig. 2: Access to the One Safe additional module.

5. Settings

5.1- Add an intrusion device

Units list / Add unit:

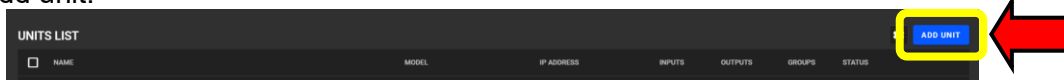


Fig. 3: Add unit.

5.1.1 General settings

- **Brand** : select the brand of the intrusion device
- **Model** : select the model
- **Name** : name the device

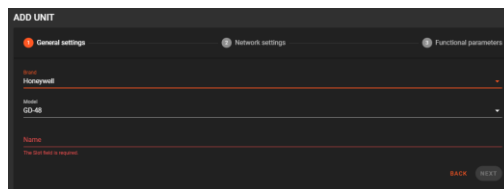


Fig. 4: General settings.

5.1.2 Network settings

- **IP address**: enter the intrusion device's IP address
- **Communication port** : enter the communication port
- **Client code** : enter the client code
- **Remote code**: enter the remonte code

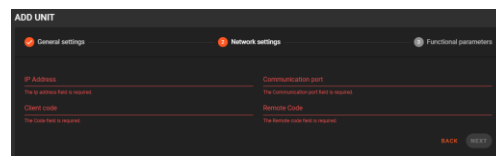


Fig. 5: Network settings.

5.1.3 Functional parameters

- **Company** : select the company to which the device is attached
- **Time to retrieve data from the unit**: choose the delay between 5s and 600s
- **Switch 8 disabled**: only available for HONEYWELL device

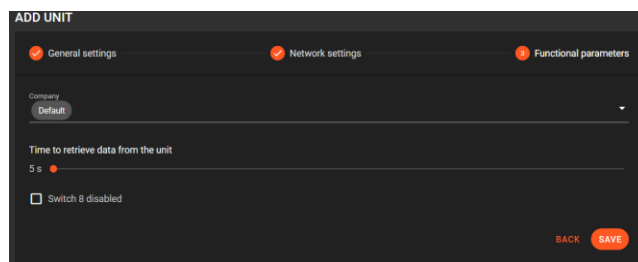




Fig. 6: Functional parameters.


5.2- Configuration of inputs, outputs and groups

From the control panel, select the device and press the button  to configure the elements of the control panel.

Press  to save settings.

To directly access the elements, you can search directly in the search box .

GROUP PROCESSING allows you to enable or disable supervision on all selected items.

It is possible to synchronize the labels of the intrusion device  in the ONE Safe interface.

5.2.1 Input points

You can rename the labels of the entry points and activate for each of them the possibility of managing supervision, acknowledgment, report, priority level, and setpoint display (if existing).

INDEX	NAME	SUPERVISED	ACKNOWLEDGMENT	REPORT	PRIORITY LEVEL	INSTRUCTION
01	porte 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10	No instruction
02	porte 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10	No instruction
03	porte 3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10	No instruction
04	Zone 04	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10	No instruction
05	Zone 05	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10	No instruction
06	Zone 06	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10	No instruction
07	Zone 07	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10	No instruction
08	Zone 08	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10	No instruction
09	Punto d'entree 09	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10	No instruction
10	Punto d'entree 10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10	No instruction
11	Punto d'entree 11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10	No instruction

Fig. 7: Input points.

It is possible to synchronize the labels of the intrusion device  in the ONE Safe interface.

5.2.2 Output points

You can also rename the output points and choose whether they are supervised or not (single or group selection).

INDEX	NAME	SUPERVISED
01	Sortie 1	<input checked="" type="checkbox"/>
02	Sortie 2	<input checked="" type="checkbox"/>
03	Sortie 3	<input checked="" type="checkbox"/>
04	Sortie 4	<input checked="" type="checkbox"/>
05	Sortie 5	<input checked="" type="checkbox"/>
06	Sortie 6	<input checked="" type="checkbox"/>
07	Punto de salida 07	<input checked="" type="checkbox"/>
08	Punto de salida 08	<input checked="" type="checkbox"/>
09	Punto de salida 09	<input checked="" type="checkbox"/>
10	Punto de salida 10	<input checked="" type="checkbox"/>
11	Punto de salida 11	<input checked="" type="checkbox"/>

Fig. 8 : Output points.

It is possible to synchronize the labels of the intrusion device  in the ONE Safe interface.

5.2.3 Groups

The available groups can be renamed, with the choice of the pooling tempo (10 sec by default) and choose whether they are supervised or not.

INDEX	NAME	POOLING TIME	SUPERVISED
1	Partition 1	10	<input checked="" type="checkbox"/>
2	Partition 2	10	<input checked="" type="checkbox"/>
3	Partition 3	10	<input checked="" type="checkbox"/>
4	Partition 4	10	<input checked="" type="checkbox"/>

Fig. 9: Groups.

It is possible to synchronize the labels of the intrusion device  in the ONE Safe interface.

3 -Start/stop communication with intrusion device

From the units list, select the device and press Connect / Disconnect depending on the situation:

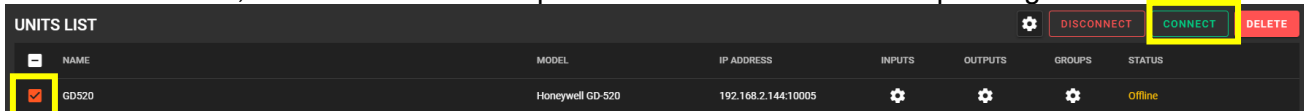



Fig. 10: Connecting the devices

 Connection to the intrusion device is unavailable if another interface is already connected. It appears in "Disconnected" status (automatic connection when the third-party interface is disconnected).

6. Configuring intrusion systems

6.1- RISCO alarm configuration



Connection to the intrusion device is unavailable if another interface is already connected. It appears in "Disconnected" status

- Select the RISCO brand, model, and enter the name:

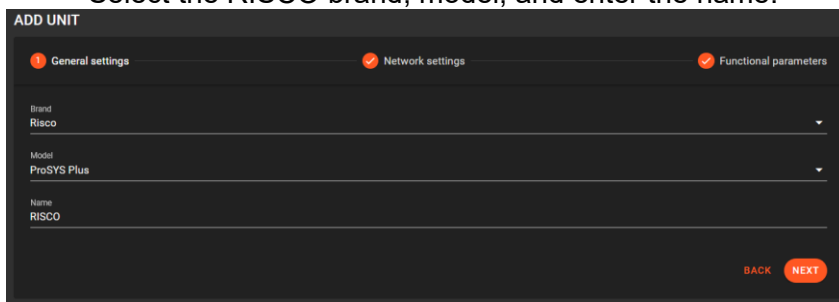
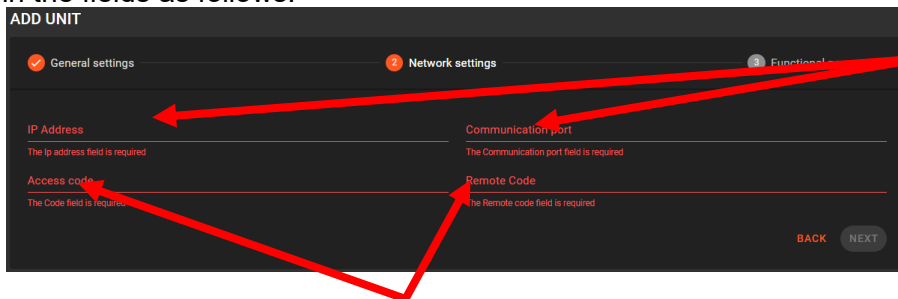
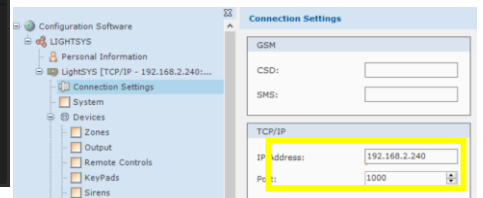


Fig. 11: RISCO intrusion device settings.

- Fill in the fields as follows:



IP and Port de communication from Connection Settings



Access code and Remote code from Communication/Communication Software

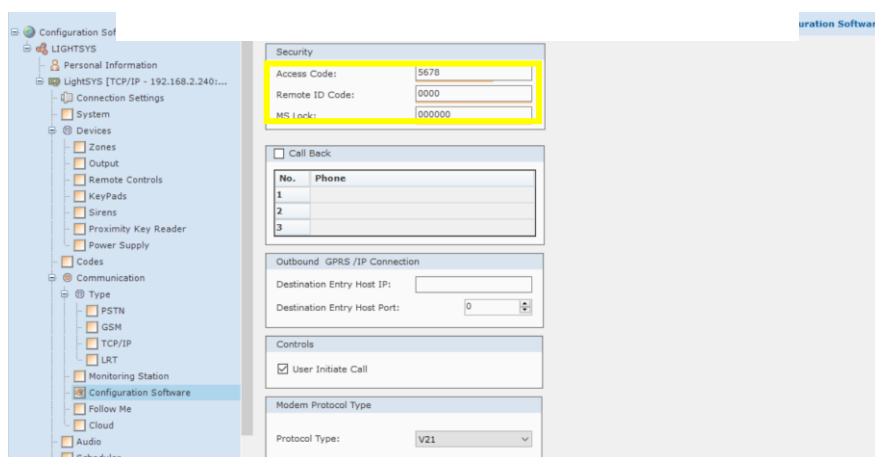


Fig. 12 : RISCO device configuration.

6.2- GALAXY HONEYWELL alarm configuration

6.2.1 Configuration from the HONEYWELL keypad

1: Give the right to the installer

- Compose the Manager code « 12345 » + ent
- Go to menu 48.1 and activate the installer rights.

2: Enter installer mode to perform the following operations

- Compose the code Manager « 112233 » + ent.

3: Configure the Ethernet module

- Go to menu 56.4.1.1: Indicate the IP address of the device.
- Go to menu 56.4.1.4: Indicate the subnet mask.

4: Alarm report

- Go to menu 56.4.2.1: Select "SIA" level 4.
- Set all the events to be managed to "ON".
- Go to menu 56.4.2.2.1: Indicate the **IP address of the OPTIMA** which communicates with the intrusion device.
- Go to menu 56.4.2.2.2: Indicate the communication port "10002"
- Go to menu 56.4.2.4: Indicate the customer code "1234".
- Go to menu 56.4.2.8: Indicate the TCP protocol: "1".

5: Remote access

- Go to menu 56.4.3.1: Select "Always" for the access period
- Go to menu 56.4.3.2: Select "Direct access" for the mode.

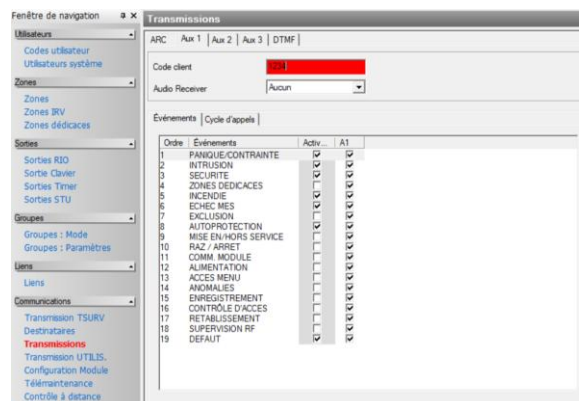
6: SIA Command

- Go to menu 56.4.8: Indicate the **IP address of the OPTIMA** which communicates with the intrusion device.

6.2.2 Configuration of the intrusion device from the RSS software (GALAXY Flex)

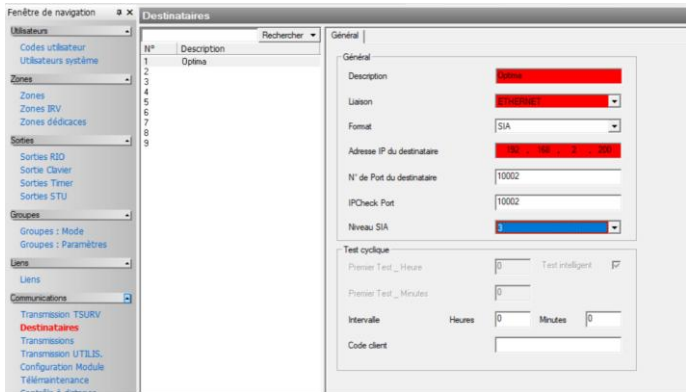
Give the right to the installer and rights of alarm reports

Give the client code and check the following boxes from the *Communications/Transmissions menu*:



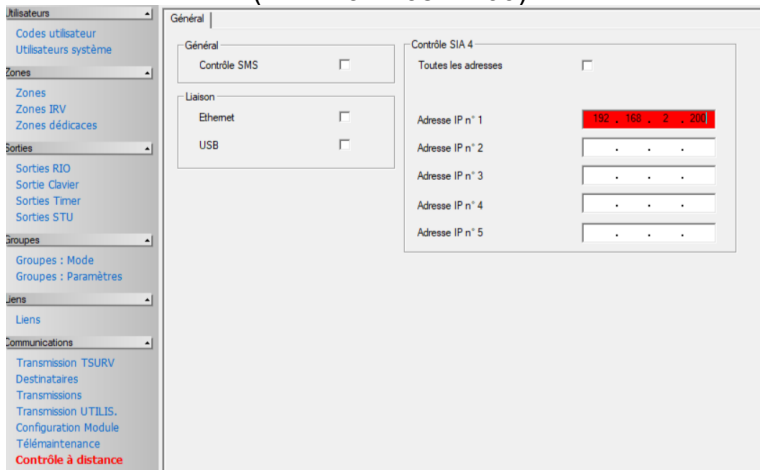
Configure Ethernet Module and SIA Command

From the *Communications/Recipients* menu: indicate the **IP address of the OPTIMA** which communicates with the intrusion device (here **192.198.2.200**) and the communication port (here **10002**).



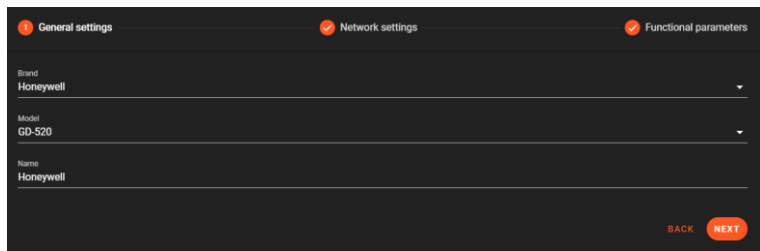
Remote access

From the *Communications/Remote control* menu, give the **IP address of the OPTIMA** which communicates with the intrusion device (here **192.168.2.200**).

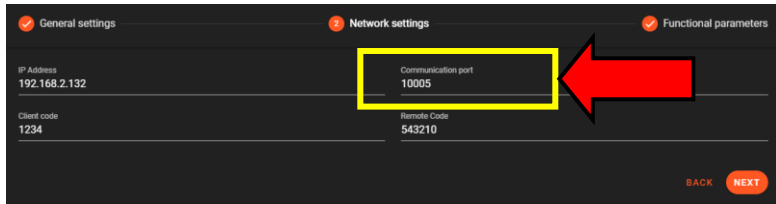


6.2-3 Set intrusion device in the OPTIMA interface

Profile :



Network settings:



Enter **10005** for the communication port.

Functional parameters:

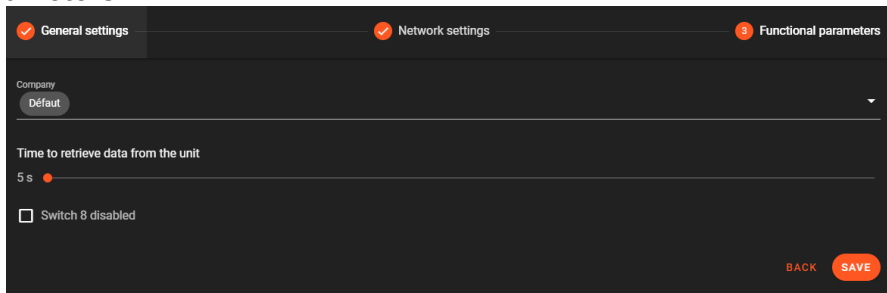
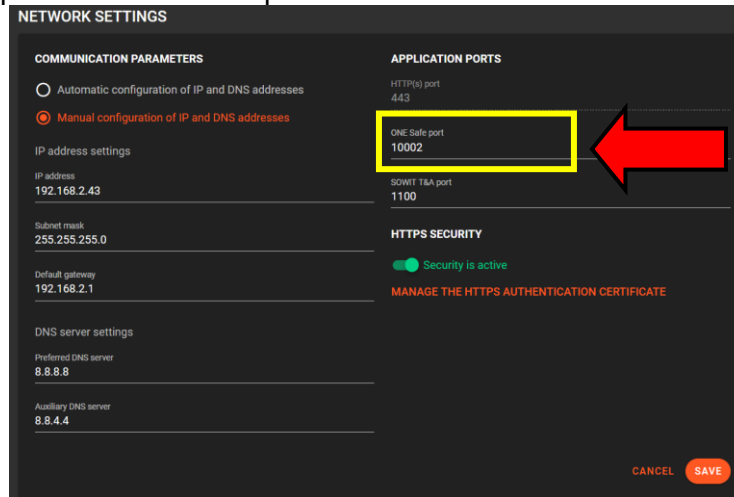


Fig. 13: Network settings for GALAXY intrusion device.

Dialog port:

Configure the dialog port with the control panel from Software administration / Network parameters.



6.3- VANDERBILT SPC alarm configuration

The configuration parameters to enter to establish the connection with a Vanderbilt control panel in the Intrusion module are as follows:

- IP address
- Communication Port
- Client code
- Encryption key
- Username
- Username password
- Time to retrieve data from the unit

The settings must match those configured in the Vanderbilt software.

Note: after the complete configuration, the connection establishment process is accelerated by saving the configuration on the Vanderbilt interface from the Users / Users Menu and pressing the Save button at the bottom left of the page (wait 1 min to obtain " Connected ").



Fig. 14: Connecting the intrusion device.

6.3.1 Time out configuration

The recommended time for ATS Polling Timeout and ATS Event Timeout is 60 sec
Communications Menu > FlexC Tab > Edit ATS > ATS faults

ATS Faults	
ATS Polling Timeout	60 Seconds
ATS Event Timeout	60 Seconds
Generate FTC	<input type="checkbox"/>
ATS/ATP Fault Events	<input type="checkbox"/>
Re-queue Events	<input checked="" type="checkbox"/>
Re-queue Event Delay	300 Seconds
Log ATS Faults	<input type="checkbox"/>
Re-queue Event Duration	86400 Seconds

6.3.2 IP Address - Communication Port - Client Code

The configuration of the IP address, communication port, and client code in Vanderbilt software is done at the Alarm Transmission Path (ATP) edit interface.

Communications menu > FlexC tab > Edit ATS AT > Edit

- ✓ Client Code – Identifiant
- ✓ IP address or URL Récepteur = OPTIMABOX IP address
- ✓ Port IP Récep. = communication port (see below)

The screenshot shows the 'ATP Configuration' page for 'FlexC RCT'. The 'RCT Identification' section contains the following fields:

- RCT ID: 1
- RCT URL or IP Address: 192.168.2.43
- RCT TCP Port: 10002

The 'SPT Account Code' field is set to 1234. The 'Communications' menu item in the left sidebar is highlighted with a red box. Red arrows point from the list above to the 'SPT Account Code', 'RCT URL or IP Address', and 'RCT TCP Port' fields.

The communication port (Receiver IP port) can be modified in the configuration menu / Software administration / Network settings:

The screenshot shows the 'APPLICATION PORTS' configuration window. The 'ONE Safe port' field is highlighted with a red box and contains the value 10004.

Fig. 15 : Communication port.



Since port 52000 is used by the Vanderbilt application, we recommend configuring another port.

6.3.3 Encryption key

Editing of the encryption key in Vanderbilt software is done in the advanced settings of the alarm transmission path (ATP)

(Use Google Chrome or Mozilla Firefox)

- ✓ **Communications menu > FlexC ATS tab > Edit ATS configuration > Edit > Edit the ATP configuration > Advanced ATP Settings Button**

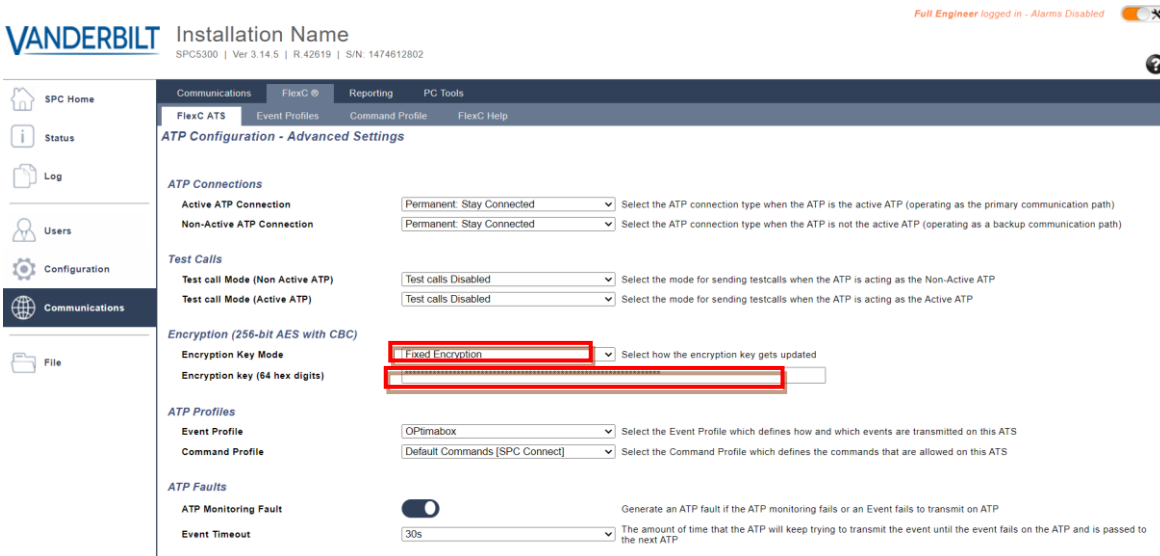
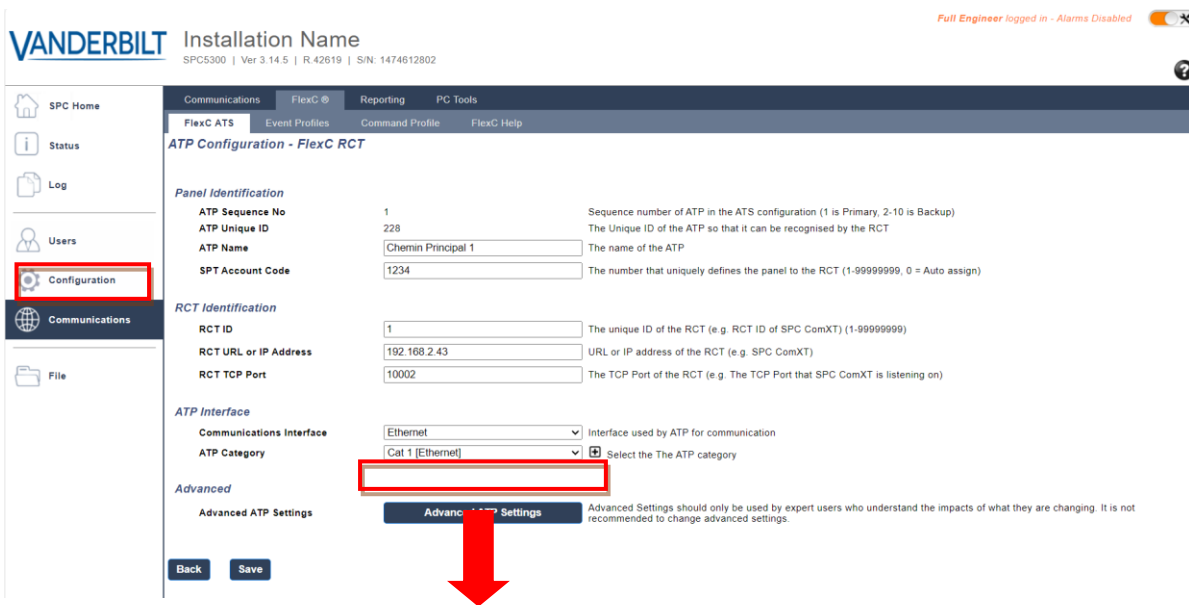
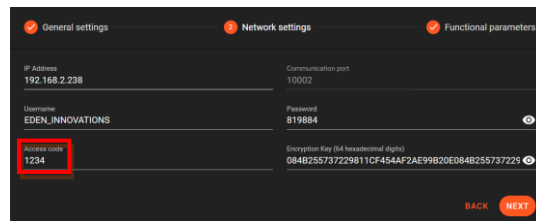
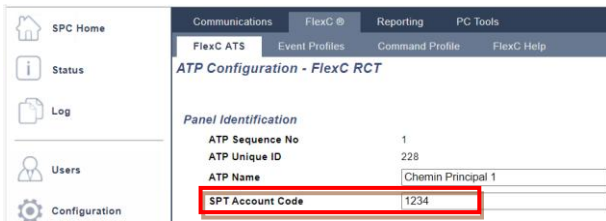


Fig. 16 : OPTIMA Encryption key.

The mode of the encryption key to select is Manual Encryption.
The encryption key to enter must be a key of 64 hexadecimal digits (0-9.A-F)

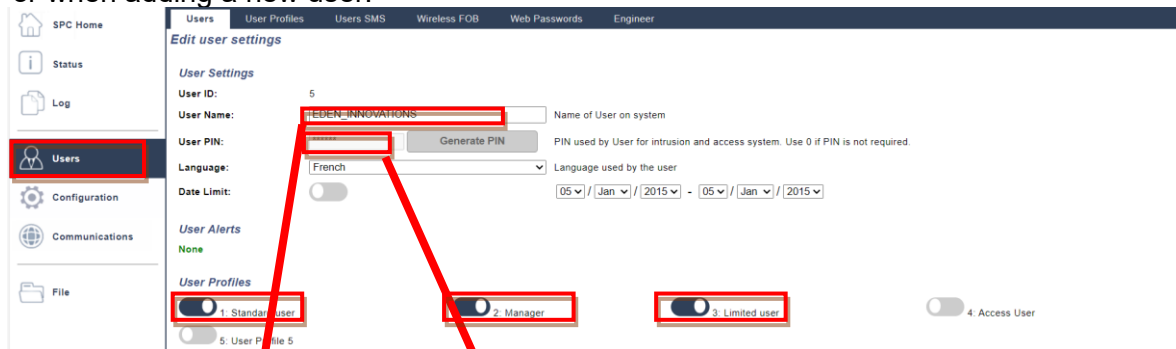
STP account code = Access code in OPTIMA



6.3.4 User names and password

The user IDs to be entered correspond to those of a user registered in the Vanderbilt software under the Users menu.

Editing of the username and password is done by clicking on the “edit” icon button of the targeted user or when adding a new user.



The profile must be of type "Standard", "Manager" and "Limited user".

Information to be entered in the control unit profile in the ONE Safe interface:

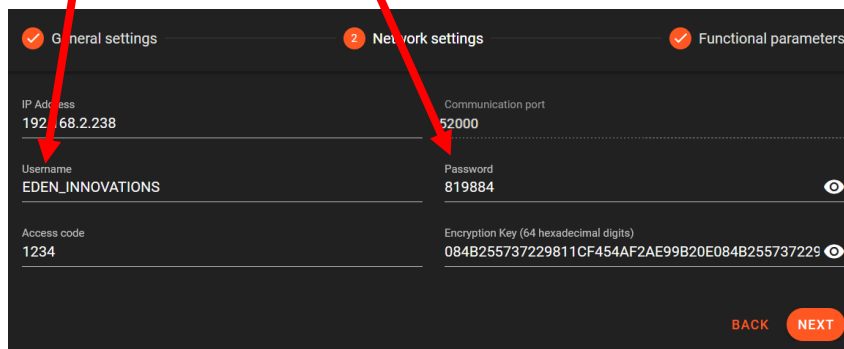


Fig. 17: Identification by name (Username) and password (User PIN code).

Access code = SMTP account code

User PIN = Password

Encryption key: here= 084B255737229811CF454AF2AE99B20E084B255737229811CF454AF2AE99B20E

6.3.5 Time to retrieve data from the unit

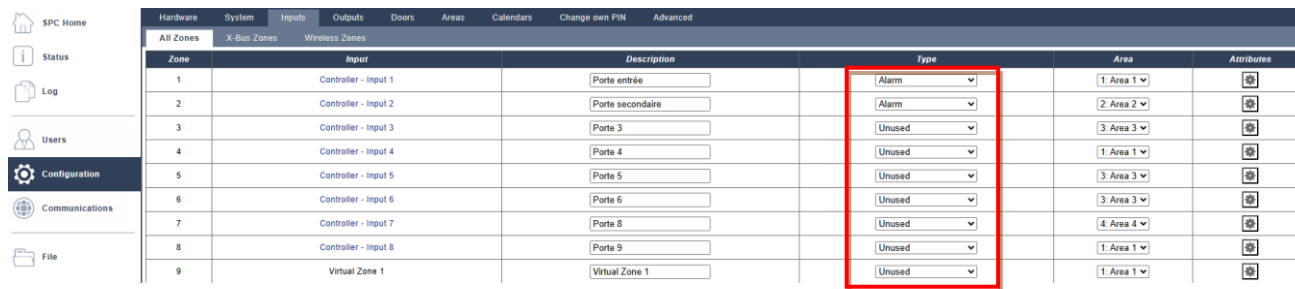
The parameter is by default set to 30 sec. Sometimes this time is insufficient to establish good communication between OPTIMA and the intrusion device and can lead to the appearance of frequent disconnection/connection from the intrusion device.

We therefore recommend configuring a minimum delay of 120 seconds.

6.3.6 Vanderbilt software specifics

Input configuration:

Intrusion groups are managed by OPTIMA if the inputs are configured with the “Alarm” type.



Zone	Input	Description	Type	Area	Attributes
1	Controller - Input 1	Porte entrée	Alarm	1: Area 1	[Icon]
2	Controller - Input 2	Porte secondaire	Alarm	2: Area 2	[Icon]
3	Controller - Input 3	Porte 3	Unused	3: Area 3	[Icon]
4	Controller - Input 4	Porte 4	Unused	1: Area 1	[Icon]
5	Controller - Input 5	Porte 5	Unused	3: Area 3	[Icon]
6	Controller - Input 6	Porte 6	Unused	3: Area 3	[Icon]
7	Controller - Input 7	Porte 8	Unused	4: Area 4	[Icon]
8	Controller - Input 8	Porte 9	Unused	1: Area 1	[Icon]
9	Virtual Zone 1	Virtual Zone 1	Unused	1: Area 1	[Icon]

Events Profile:

The OPTIMA intrusion module incorporates limited functions of intrusion devices.

For Vanderbilt devices, many events sent are therefore not processed by the server.

To reduce the work of filtering the server on processed events, a specific event profile can be created in Vanderbilt software for the Alarm Transmission System (ATS) configured for the Intrusion module.

In this event profile, only the events necessary for the proper functioning of the Intrusion module can be selected, which will limit the sending of unnecessary events to be filtered by the server.

Access to the event profiles management menu : **Communications menu > FlexC tab > Event Profiles sub-tab.**

List of events to be checked:

SPC Home | Status | Log | Users | Configuration | **Communications** | File | Status | Log | Users | Configuration | **Communications** | File

Communications FlexC® Reporting PC Tools
FlexC ATS Event Profiles Command Profile FlexC Help

Event Profiles

Edit	Delete	ID	Event Profile Name	Event Exceptions
	-	1	Default Events	0
	-	2	Default Events (SPC Connect)	0
		3	Profile d' Evénement 3	0
		4	Profile d' Evénement 4	6
		5	Event Profile 5	0

Add

FlexC ATS Event Profiles Command Profile FlexC Help

Event Profiles

Identification
Name: Name of the Event Profile

Event Filter

Intruder / Fire / Medical

Filter Group	Report Event	Event Exception Count	Add Event Exception
Confirmed alarms	<input checked="" type="checkbox"/>	0	- Select Event to Add Exception -
Intruder Alarms	<input checked="" type="checkbox"/>	0	- Select Event to Add Exception -
Intruder alarm Restores	<input type="checkbox"/>	0	- Select Event to Add Exception -
Panic / Holdup / Duress	<input type="checkbox"/>	0	- Select Event to Add Exception -
Fire Alarms and Restores	<input type="checkbox"/>	0	- Select Event to Add Exception -
Medical Alarms and Restores	<input type="checkbox"/>	0	- Select Event to Add Exception -
Tampers	<input type="checkbox"/>	0	- Select Event to Add Exception -
Tamper Restores	<input checked="" type="checkbox"/>	0	- Select Event to Add Exception -
Setting	<input type="checkbox"/>	0	- Select Event to Add Exception -

System Monitoring

Filter Group	Report Event	Event Exception Count	Add Event Exception
Faults	<input type="checkbox"/>	0	- Select Event to Add Exception -
Fault Restores	<input type="checkbox"/>	0	- Select Event to Add Exception -
Network	<input type="checkbox"/>	0	- Select Event to Add Exception -
Test Calls	<input type="checkbox"/>	0	- Select Event to Add Exception -
Engineer accessing system	<input type="checkbox"/>	0	- Select Event to Add Exception -
System Information	<input type="checkbox"/>	0	- Select Event to Add Exception -
Inhibits and Isolates	<input checked="" type="checkbox"/>	3	- Select Event to Add Exception -
Zone Walk Test	<input type="checkbox"/>	0	- Select Event to Add Exception -
Zone State Change	<input checked="" type="checkbox"/>	3	- Select Event to Add Exception -
Zone State Change in Alarm	<input checked="" type="checkbox"/>	0	- Select Event to Add Exception -
Camera	<input type="checkbox"/>	0	- Select Event to Add Exception -
Mapping Gate Status	<input type="checkbox"/>	0	- Select Event to Add Exception -

Door and User

Filter Group	Report Event	Event Exception Count	Add Event Exception
Door Warnings	<input type="checkbox"/>	0	- Select Event to Add Exception -
Door Information	<input type="checkbox"/>	0	- Select Event to Add Exception -
User Information	<input type="checkbox"/>	0	- Select Event to Add Exception -

Area Filter

1: Area 1 2: Area 2 3: Area 3 4: Area 4

The assignment of the specific profile is done at the level of the alarm transmission system (ATS) edit in the section Communications > FlexC > **Command Profile**.

The image shows two screenshots of the SPC Home interface. The top screenshot displays the 'Command Profiles' table with three entries. A red box highlights the 'Edit' icon for the third entry, and a red arrow points down to the second screenshot. The second screenshot shows the configuration page for the selected profile, including fields for Name, Authentication Mode, Live Streaming Mode, and a list of commands with enable/disable toggles.

Edit	Delete	ID	Command Profile Name	Commands Enabled	Commands Logged
	-	1	Default Commands	79	65
	-	2	Default Commands [SPC Connect]	105	65
		3	Default Commands [SPC Connect]	99	60

Configuration Page: Command Profile

Identification
 Name: Name of the Command Profile

Command Profile Authentication
 Authentication Mode: Mode used to authenticate the rights of the user using the Command Profile

Live streaming
 Live Streaming Mode: Select Live Streaming privacy options

Command Filter

	Command Enable	Log Command
System Commands		
Get Panel Summary	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Set the System Time and Date	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Grant Engineer Access	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Grant Manufacturing Access	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Revoke Engineer Access	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Revoke Manufacturing Access	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enter Full Engineer Mode	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Exit Full Engineer Mode	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Intruder Commands		
Get the Area Status	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Get the Change Mode Status of an Area	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Change the mode (Set/Unset) of an Area	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Get Status of Panel Alerts	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Perform actions on Alerts	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Silence Bells	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Get Zone Status	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Control a Zone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Get the System Log	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Get the Log for a Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Get the Wireless Log	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Get Hold-up DATA	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Edit Hold-up DATA	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Communication improvement :

To further improve responsiveness between the control panel and OPTIMA, disable the "Zone State Change" in your Events profile.

The screenshot shows the 'Event Profiles' configuration page for 'FlexC ATS'. The 'Event Filter' section is expanded to show 'Intruder / Fire / Medical' and 'System Monitoring' categories. The 'Zone State Change' option is highlighted with a red box. The 'Report Event' column shows a toggle switch for 'Zone State Change' that is currently turned on. The 'Event Exception Count' column shows a value of 3 for 'Zone State Change'. The 'Add Event Exception' column shows a dropdown menu with the text '- Select Event to Add Exception -' and a green plus icon.

Filter Group	Report Event	Event Exception Count	Add Event Exception
Confirmed alarms	<input checked="" type="checkbox"/>	0	- Select Event to Add Exception -
Intruder Alarms	<input checked="" type="checkbox"/>	0	- Select Event to Add Exception -
Intruder alarm Restores	<input type="checkbox"/>	0	- Select Event to Add Exception -
Panic / Holdup / Duress	<input type="checkbox"/>	0	- Select Event to Add Exception -
Fire Alarms and Restores	<input type="checkbox"/>	0	- Select Event to Add Exception -
Medical Alarms and Restores	<input type="checkbox"/>	0	- Select Event to Add Exception -
Tampers	<input type="checkbox"/>	0	- Select Event to Add Exception -
Tamper Restores	<input checked="" type="checkbox"/>	0	- Select Event to Add Exception -
Setting	<input checked="" type="checkbox"/>	0	- Select Event to Add Exception -
System Monitoring			
Faults	<input type="checkbox"/>	0	- Select Event to Add Exception -
Fault Restores	<input type="checkbox"/>	0	- Select Event to Add Exception -
Network	<input type="checkbox"/>	0	- Select Event to Add Exception -
Test Calls	<input type="checkbox"/>	0	- Select Event to Add Exception -
Engineer accessing system	<input type="checkbox"/>	0	- Select Event to Add Exception -
System Information	<input type="checkbox"/>	0	- Select Event to Add Exception -
Inhibits and isolates	<input checked="" type="checkbox"/>	3	- Select Event to Add Exception -
Zone Walk Test	<input type="checkbox"/>	0	- Select Event to Add Exception -
Zone State Change	<input checked="" type="checkbox"/>	3	- Select Event to Add Exception -
Zone State Change in Alarm	<input checked="" type="checkbox"/>	0	- Select Event to Add Exception -
Camera	<input type="checkbox"/>	0	- Select Event to Add Exception -
Mapping Gate Status	<input type="checkbox"/>	0	- Select Event to Add Exception -
Door and User			
Door Warnings	<input type="checkbox"/>	0	- Select Event to Add Exception -
Door Information	<input type="checkbox"/>	0	- Select Event to Add Exception -
User Information	<input type="checkbox"/>	0	- Select Event to Add Exception -

Area Filter: 1: Area 1 2: Area 2 3: Area 3 4: Area 4

This setting updates only alarm group status changes in the dashboard each time data is forced to be retrieved.

The time to retrieve data from the unit from the intrusion device should be minimized in the *Functional parameters* of the intrusion device configuration.

Intrusion device events are always managed in real time, with **increased responsiveness**.

7. Operation

7.1-Dashboard

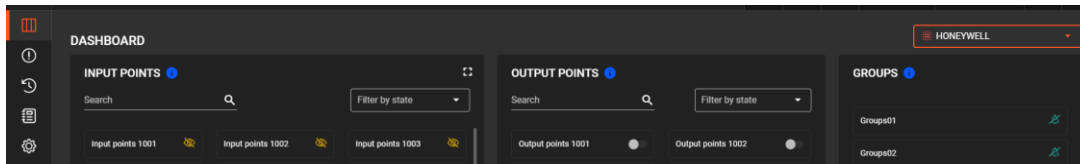


Fig. 18: Dashboard.

This menu allows you to see the status of the devices at a glance, with a visual on the input and output points and the status of the groups.

The connection status of each device is visible to the left of the label:

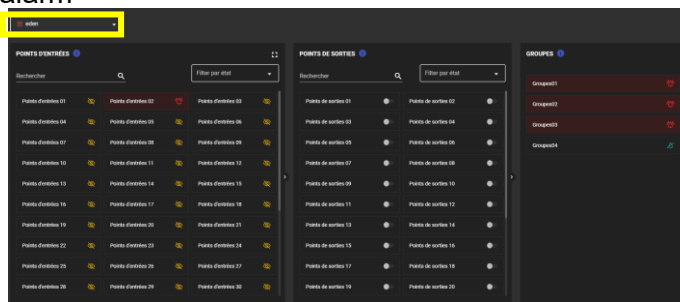
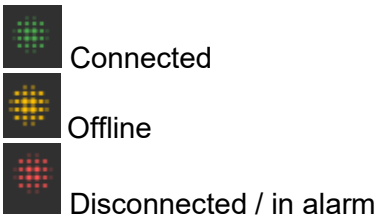


Fig. 19 : Dashboard.

7.1.1 Input points

- Input points can be enlarged on the main page using the zoom icon

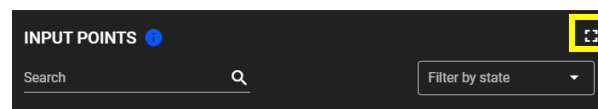
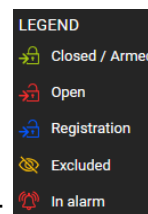


Fig. 20: Enlarge page.



The status of the inputs is symbolized by the following legend:

Note: The Recording status is only available for Honeywell alarm systems from version OPTIMA 5.3.0 onwards.

You can directly specify an input point in the search field, or filter them according to their status:

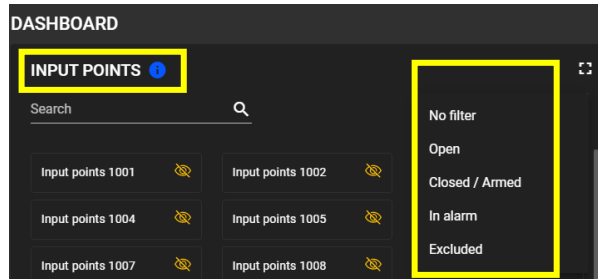


Fig. 21: Search input point.

- Input points can be excluded / included with a left click:

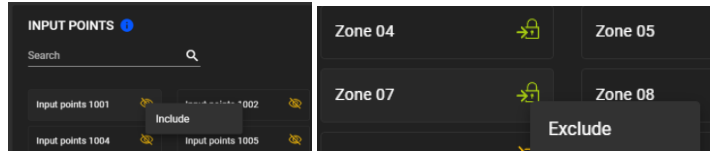
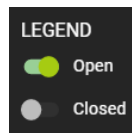


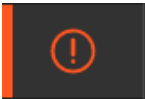
Fig.22: Exclusion.

7.1.2 Output points

They provide information on the output state according to the two status “Open” / “Closed”.



7.2-Intrusion event live



This menu displays live the last 100 events related to intrusion devices.

DATE	NATURE OF EVENT	CENTRAL UNIT	POINT / GROUP	REPORT
12/4/2020 5:30:06 PM	Inclure l'entrée	lightsys	Points d'entrées 10	
12/4/2020 10:14:24 AM	Sortie active	lightsys	Sortie 1	
12/4/2020 10:14:22 AM	Activer la sortie	lightsys	Sortie 1	
12/3/2020 3:32:10 PM	Groupe hors service	lightsys	Partition 1	
12/3/2020 3:32:09 PM	Groupe acquitté	lightsys	Partition 1	
12/3/2020 3:32:05 PM	Acquittement distant du groupe	lightsys	Partition 1	
12/3/2020 3:31:39 PM	Alarme acquittée	lightsys	porte 2	
12/3/2020 3:31:36 PM	Alarme acquittée	lightsys	porte 1	
12/3/2020 2:44:31 PM	Alarme acquittée	lightsys		
12/3/2020 2:44:30 PM	Terminal connecté	lightsys		

Fig. 23: Live events.

It is possible to carry out a search to sort them according to their nature, their power plants, or their points / groups

7.3-Events list



This page displays the complete list of events with the possibility of filtering the data in a given period and / or the nature of the event.

DATE	NATURE OF EVENT	CENTRAL UNIT	POINT / GROUP
12/4/2020 5:30:06 PM	Inclure l'entrée	lightsys	Points d'entrées 10
12/4/2020 10:14:22 AM	Sortie active	lightsys	Sortie 1
12/4/2020 10:14:22 AM	Activer la sortie	lightsys	Sortie 1
12/3/2020 3:32:05 PM	Groupe hors service	lightsys	Partition 1
12/3/2020 3:32:05 PM	Groupe acquitté	lightsys	Partition 1
12/3/2020 3:32:05 PM	Acquittement distant du groupe	lightsys	Partition 1
12/3/2020 3:31:39 PM	Alarme acquittée	lightsys	porte 2
12/3/2020 3:31:36 PM	Alarme acquittée	lightsys	porte 1
12/3/2020 2:44:31 PM	Alarme acquittée	lightsys	
12/3/2020 2:44:30 PM	Terminal connecté	lightsys	
12/3/2020 2:42:58 PM	Alarme acquittée	lightsys	
12/3/2020 2:42:57 PM	Terminal connecté	lightsys	
12/3/2020 2:33:07 PM	Alarme acquittée	lightsys	
12/3/2020 2:33:05 PM	Terminal connecté	lightsys	

Fig. 24: Events list.

Search results can be exported in spreadsheet format by clicking on **EXPORT**.

If cameras are associated with intrusion points or zones, the View column displays a camera icon.

This gives direct access to the video sequence at the time of the event (the **ONE View** module activated and configured, see documentation).

Fig. 25: Video stream display associated with an alarm input.

7.4- Actions record

This menu displays the list of actions carried out by users.



There is also the possibility of searching by points / group or by searching by the actions carried out.

Search results can be exported in spreadsheet format by clicking on "Export" **EXPORT**.

DATE	USER	POINT / GROUP	ACTION DONE
12/4/2020 5:30:06 PM	RODRIGUEZZ Lionell	Points d'entrées 10	Inclure l'entrée
12/4/2020 10:14:22 AM	ADMINISTRATEUR	Sortie 1	Activer la sortie
12/3/2020 3:32:05 PM	RODRIGUEZZ Lionell	Partition 1	Acquittement distant du groupe

Fig. 26 : Action records.

7.5-User codes

This menu displays the list of users associated with keypad codes (RISCO intrusion devices only).



USER CODES (RISCO)				
OWNER ↑	ACCESS GROUP	BADGE	USER CODE	UNITS
GOMEZ Diego	Office	1300123501	✕	
PADILLA Adam	Office	4100619136	✕	
VELPO Brian	Maid	612903066	✕	

Fig. 27: List of users associated with keyboard codes.

Select a user to add/edit/delete a keypad code associated with arming/disarming zone(s) with the corresponding rights (Master/Armer...)

Fig. 28: Add RISCO user code.

The PIN code set to "0" deletes the existing code and rights associated with the user.

Note: A user deleted from access control does not delete his associated code and his arming/disarming rights.

7.6- Alerts

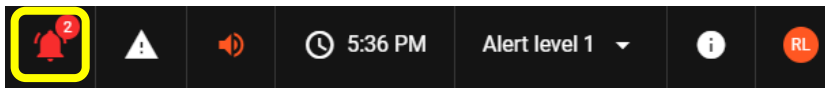
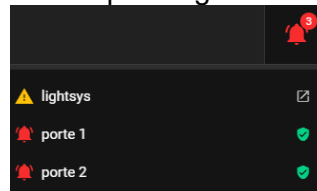


Fig. 29: Alerts in the header.

The alert notification is displayed both in the interface in the header of the Intrusion module and in the main interface.

Clicking on the notification displays the list of pending acknowledgments.



ONGOING ALERTS				
DATE ↓	CENTRAL UNIT	POINT	PRIORITY LEVEL ↑	ACKNOWLEDGMENT TYPE
12/4/2020 5:40:23 PM	lightsys	porte 1	10	✓
12/4/2020 5:40:24 PM	lightsys	porte 2	10	✓

Fig. 30: Acknowledgment.

The details of the acknowledgment are made by clicking on the line concerned, with the possibility of acknowledging by entering the reason for the alert.

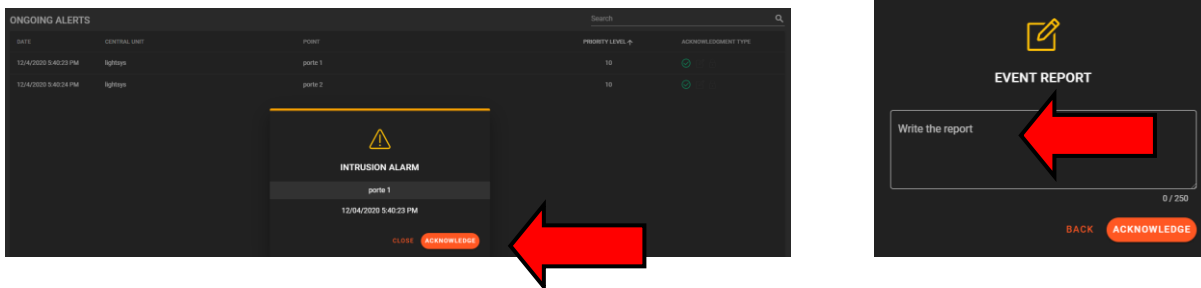


Fig. 31: Acknowledgment with reason of alert.

7.7- Adding a group, inputs, outputs in Supervision

See **OPTIMA 360** user guide.

7.8- Automation associated with Intrusion

"Configuration menu" / "Automation" / "Software automation ", enter the parameters of the automation:

- **Label**
- **Conditions**
- **Actions**

7.8.1 Possible conditions on intrusion groups

- Out of service
- In service
- In partial service
- In alarm

7.8.2 Possible conditions on intrusion inputs

- Closed / Armed
- Excluded
- In alarm
- Registration

7.8.3 Possible conditions on the intrusion outputs

- Open
- Closed

7.8.4 Possible actions on the intrusion outputs points

- Open
- Closed

7.8.5 Possible actions on the intrusion groups

- Deactivation
- Activation
- Partial activation
- Remote acknowledgement

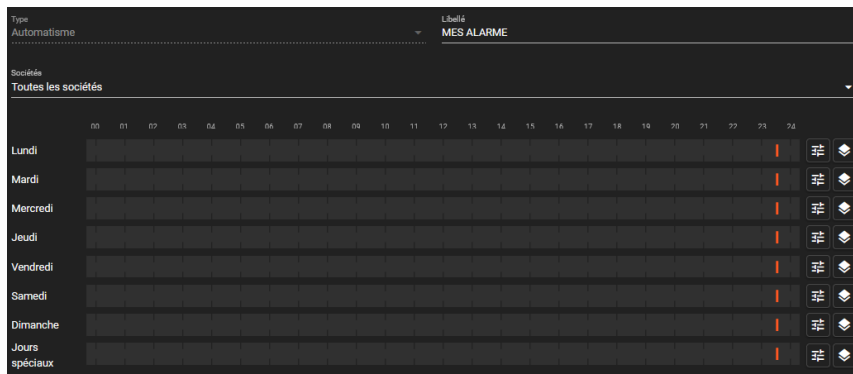
8- Use case

8.1 Scenario 1

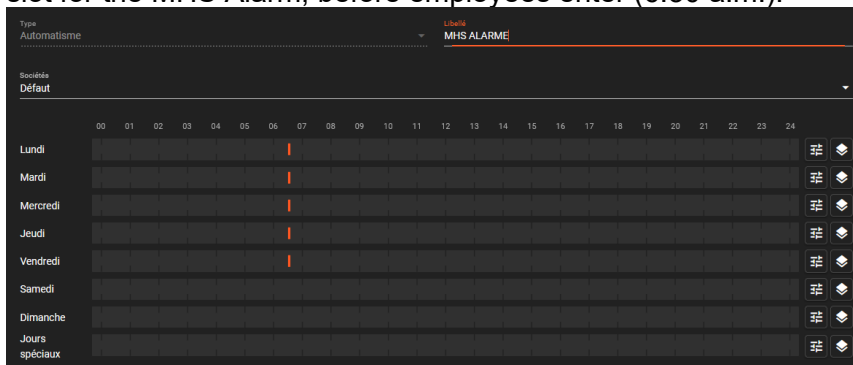
The activation of the alarm group is done at the end of the day at a fixed time (time slot), the decommissioning at the start of the day.

Configuration

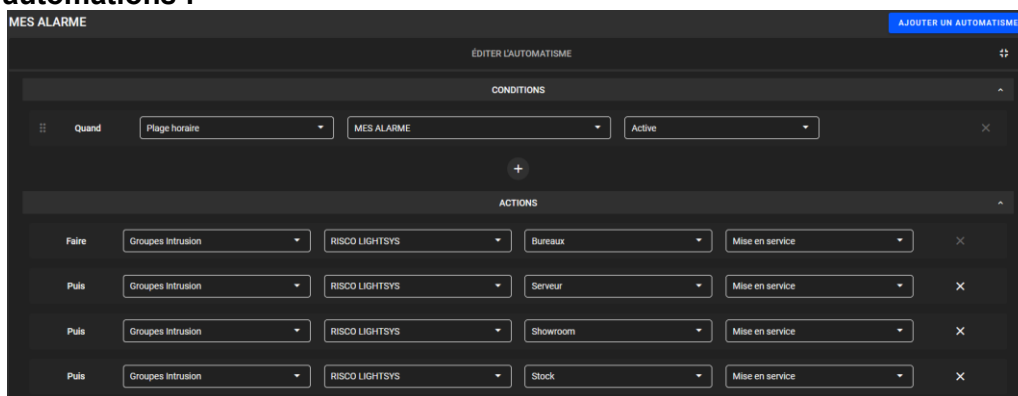
Automation time slot for Alarm activation, after all employees have left (11:30 p.m.):

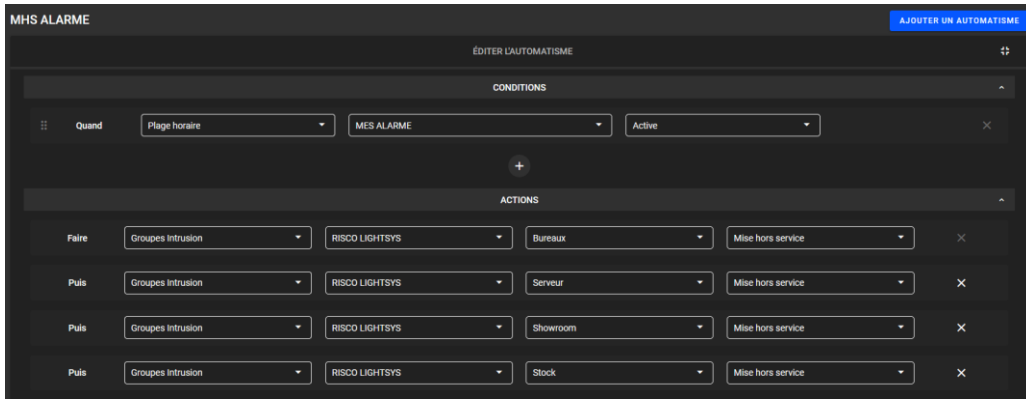


Automation time slot for the MHS Alarm, before employees enter (6:30 a.m.):



Software automations :





8.2 Scenario 2

Double clocking in at the end of the day by the last employee achieves:

- Commissioning of the alarm group
- Reader LED changes color to indicate active alarm status
- The alert level switches to level 1

Simply clocking in at the start of the day by the 1st employee achieves:

- The decommissioning of the alarm group takes place on the 1st clocking of the day.
- The reader's LED returns to its original color to indicate the inactive state of the alarm.
- The alert level switches to level 0

Connectors

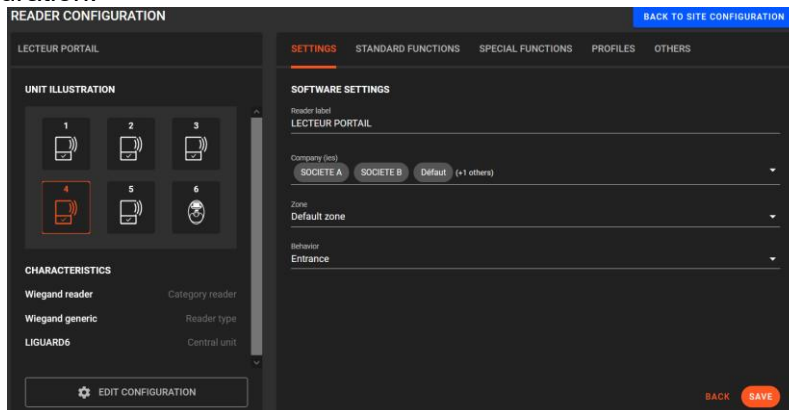
STid brand readers are equipped with a controllable LED2 input to indicate to the user the state of the alarm (In Service/Out of Service) with a specific color.

There are two ways to connect:

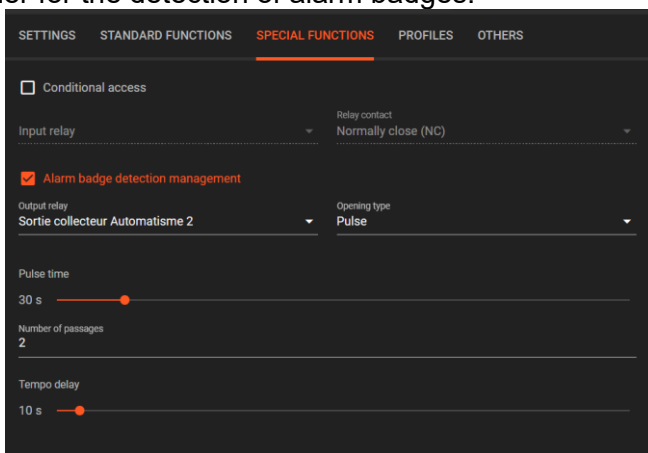
- Use of the open collector output of the EDEN control unit connected to LED2 of the STid reader
- Or**
- Automation relay output of the EDEN control unit connected to LED2 of the STid reader (the COMMON connector - here COM1) be connected to the same ground as the reader.

Configuration in OPTIMA

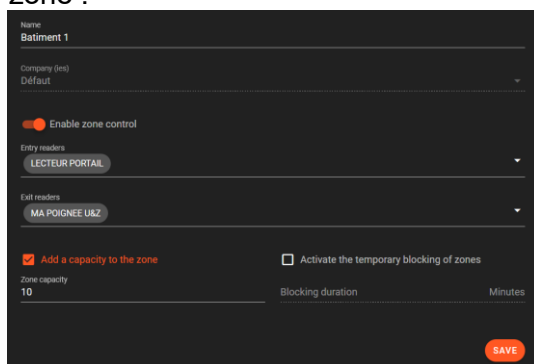
Input reader configuration:



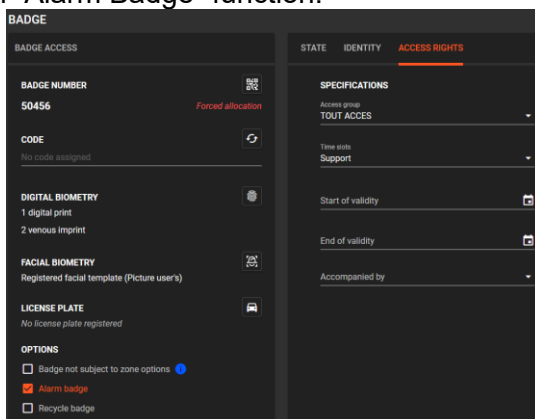
Configuration of the reader for the detection of alarm badges:



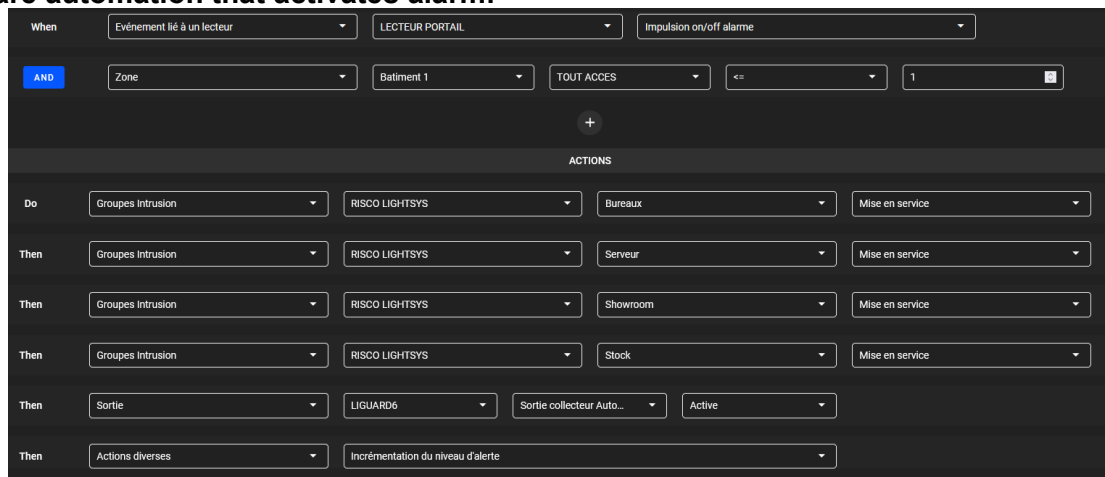
Controlled area configuration zone :



Configuration of a badge with “Alarm Badge” function:



Software automation that activates alarm:



Software automation that deactivates alarm:

When	Événement lié à un lecteur	LECTEUR PORTAIL	Badge accepté	
AND	Groupes Intrusion	RISCO LIGHTSYS	Bureaux	En service
+				
ACTIONS				
Do	Groupes Intrusion	RISCO LIGHTSYS	Bureaux	Mise hors service
Then	Groupes Intrusion	RISCO LIGHTSYS	Showroom	Mise hors service
Then	Groupes Intrusion	RISCO LIGHTSYS	Serveur	Mise hors service
Then	Groupes Intrusion	RISCO LIGHTSYS	Stock	Mise hors service
Then	Actions diverses	Remise à 0 du niveau d'alerte		
Then	Sortie	LIGUARD6	Sortie collecteur Auto...	Inactif



Zone Commerciale et Artisanale
670, route de Berre
13510 EGUILLES
France

www.eden-innovations.com