

**OPTIMA®**

**ONE Safe**

---



ONE **SAFE**

*Droits d'auteur : © Eden Innovations*

*Aucune partie de cette publication ne peut être reproduite, transmise, transcrite ni traduite sous une forme quelconque ou par un moyen quelconque sans le consentement du détenteur des droits d'auteur. La copie non autorisée peut non seulement enfreindre les lois de copyrights mais peut également réduire la capacité d'Eden Innovations à fournir des informations exactes.*

# Table des matières

1. Présentation.....	4
2. Compatibilités.....	4
3. Restrictions.....	4
4. Module ONE Safe .....	4
4.1 Activation de ONE Safe .....	4
4.2 Accès au module .....	5
5 - Paramétrage.....	5
5.1 Ajouter une centrale d'alarme.....	5
5.1.1 Configuration du profil.....	5
5.1.2 Paramètres réseau .....	5
5.1.3 Paramètres fonctionnels.....	5
5.2- Configuration des points d'entrées, de sorties et des groupes.....	6
5.2.1 Points d'entrée.....	6
5.2.2 Points de sortie .....	6
5.2.3 Groupes.....	7
5.3 -Démarrer/stopper la communication avec une centrale d'alarme.....	7
6 – Configuration des centrales d'alarme.....	8
6.1- Configuration alarme RISCO .....	8
6.2 - Configuration alarme GALAXY HONEYWELL.....	9
6.2.1 Paramétrage de la centrale d'alarme depuis le clavier de la centrale (GALAXY Dimension) .....	9
6.2.2 Paramétrage de la centrale d'alarme depuis le logiciel RSS (GALAXY Flex).....	9
6.2-3 Paramétrage de la centrale d'alarme dans l'interface OPTIMA .....	10
6.3- Configuration alarme VANDERBILT SPC.....	11
6.3.1 Configuration des Timeout .....	12
6.3.2 Adresse IP - Port de communication - Code client .....	12
6.3.3 Clé de cryptage.....	13
6.3.4 Noms et mot de passe utilisateur .....	15
6.3.5 Délai pour forcer la récupération des données de la centrale .....	15
6.3.6 Spécificités logiciel Vanderbilt .....	15
7- Exploitation.....	18
7.1-Tableau de bord.....	18
7.1.1 Point d'entrées.....	18
7.1.2 Points de sortie .....	19
7.2-Evénements live.....	19
7.3-Historique des évènements.....	20

7.4-Journal de bord..... 20

7.5-Codes utilisateur..... 21

7.6- Alertes..... 21

7.7-Ajout d'un groupe, d'une entrée ou d'une sortie dans la Supervision..... 22

7.8- Automatismes associés à l'Intrusion ..... 22

    7.8.1 Conditions possibles sur les groupes ..... 22

    7.8.2 Conditions possibles sur les entrées ..... 23

    7.8.3 Actions possibles sur les sorties..... 23

8- Cas d'utilisation..... 24

    8.1 Scénario 1..... 24

    8.1 Scénario 2..... 25

# 1. Présentation

---

Le module *ONE Safe* vous propose d'interfacer votre contrôle d'accès avec les centrales d'intrusion compatibles afin de piloter les groupes d'alarme, de recueillir les alertes et de les traiter.

## Fonctionnalités :

- Pilotage des groupes de vos centrales d'alarme pour activer la Mise en service/Mise en service partiel/Mise en service temporisée/Mise hors service/Acquittement distant.
- Surveillance des mises en alarme de vos groupes afin de mener les actions désirées.
- Vérification de l'état de vos entrées d'alarme et mener les actions désirées, avec la possibilité d'exclure/inclure au niveau de la surveillance Intrusion.
- Vérification de l'état de vos sorties d'Intrusion et mener les actions désirées, avec la possibilité de changer leurs états.
- Gestion des codes utilisateurs pour les centrales de marque RISCO

Les différents éléments peuvent être consultés/activés sur les plans de Supervision (*voir module OPTIMA 360*).

# 2. Compatibilités

---

La fonction intrusion de **ONE Safe** est compatible avec :

- Les centrales **RISCO** avec les modèles **LightSYS™2**, **ProSYS Plus**, **LightSYS+**
- Les centrales **HONEYWELL** avec les modèles **GD-96 GD-520**, **GD-48**, **GD-264** et **Galaxy Flex**
- Les centrales **VANDERBILT** avec les modèles **SPC4**, **SPC5** et **SP6**.

# 3. Restrictions

---



L'établissement de la communication entre l'OPTIMA et les centrales d'intrusion ne permet pas la connexion simultanée avec leurs logiciels d'administration.

Une bonne qualité de liaison de données IP entre l'OPTIMA et les centrales d'intrusion est nécessaire (**ping < 100ms**) pour assurer le pilotage, la surveillance et la vérification des états des alarmes.

# 4. Module ONE Safe

---

## 4.1 Activation de ONE Safe

Pour activer ce module, appuyer sur 'Activer' dans le menu Configuration/Administration de l'installation/Modules additionnels. Un code d'activation vous sera demandé.



Fig. 1 : Module additionnel ONE Safe.

## 4.2 Accès au module

Le module **ONE Safe** est disponible depuis le menu contextuel de gauche de l'interface OPTIMA.



Fig. 2 : Accès au module additionnel ONE Safe.

# 5 - Paramétrage

## 5.1 Ajouter une centrale d'alarme

Menu Configuration des centrales  / Ajouter une centrale :

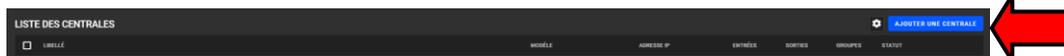


Fig. 3 : Ajouter une nouvelle centrale d'intrusion.

### 5.1.1 Configuration du profil

- **Marque** : choisir la marque de la centrale
- **Modèle** : sélectionner le modèle
- **Libellé** : nommer la centrale



Fig. 4 : Configuration du profil.

### 5.1.2 Paramètres réseau

- **Adresse IP** : saisir l'adresse IP de la centrale
- **Port de communication** : saisir le port de communication
- **Code client** : entrer le code client
- **Code distant** : saisir le code distant



Fig. 5 : Paramètres réseau.

### 5.1.3 Paramètres fonctionnels

- **Société** : sélectionner la société à laquelle la centrale est rattachée.
- **Délais pour forcer la récupération des données de la centrale** : choisir le délai entre 5 et 600s
- **Switch 8 désactivé** : uniquement disponible pour centrale HONEYWELL



Fig. 6 : Paramètres fonctionnels.

## 5.2- Configuration des points d'entrées, de sorties et des groupes

Depuis la configuration des centrales, sélectionnez la centrale, et appuyez sur les boutons  afin de paramétrer les éléments de la centrale.

Appuyez sur  afin de conserver les paramètres.

Pour accéder directement aux éléments vous pouvez rechercher directement dans la zone de recherche .

Le bouton  **TRAITEMENT GROUPE** active ou désactive la supervision sur l'ensemble des éléments sélectionnés.

Il est possible de synchroniser les libellés de la centrale d'intrusion  vers l'interface ONE Safe.

### 5.2.1 Points d'entrée

On peut renommer les libellés des points d'entrée, et activer pour chacun d'entre eux la possibilité de gérer la supervision, l'acquiescement, le rapport, le niveau de priorité, et l'affichage de consigne (si existantes).



Fig. 7 : Points d'entrée.

Appuyez sur la fonction  « Synchroniser les libellés » afin de récupérer les noms depuis votre centrale d'intrusion.

### 5.2.2 Points de sortie

On peut également renommer les points de sortie et choisir s'ils sont supervisés ou non (sélection unitaire ou groupée).

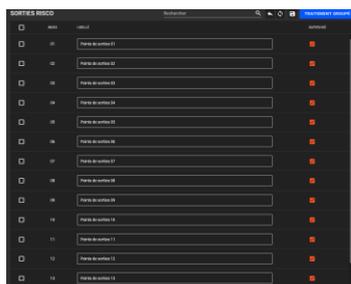


Fig. 8 : Points de sortie.

Appuyez sur la fonction  « Synchroniser les libellés » afin de récupérer les noms depuis votre centrale d'intrusion.

### 5.2.3 Groupes

Les groupes disponibles peuvent être renommés, avec le choix de la tempo pooling (10 sec par défaut) et choisir s'ils sont supervisés ou non.

<input type="checkbox"/>	INDEX	LIBELLÉ	TEMPO POOLING	SUPERVISÉ
<input type="checkbox"/>	1	Groupes01	10	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2	Groupes02	10	<input checked="" type="checkbox"/>
<input type="checkbox"/>	3	Groupes03	10	<input checked="" type="checkbox"/>
<input type="checkbox"/>	4	Groupes04	10	<input checked="" type="checkbox"/>

Fig. 9 : Groupes.

Appuyez sur la fonction  « Synchroniser les libellés » afin de récupérer les noms depuis votre centrale d'intrusion.

### 5.3 -Démarrer/stopper la communication avec une centrale d'alarme

Depuis la configuration des centrales, sélectionner la centrale et appuyer sur Connecter/Déconnecter selon la situation :

<input checked="" type="checkbox"/>	LIBELLÉ	MODÈLE	ADRESSE IP	ENTRÉES	SORTIES	GROUPES	STATUT
<input checked="" type="checkbox"/>	GD520	Honeywell GD-520	112.111.222.3:33				Déconnectée

Fig. 10 : Communication des centrales.



La connexion à la centrale est indisponible si une autre interface est déjà connectée. Elle apparaît en statut « Déconnecté » (connexion automatique quand l'interface tierce est déconnectée).

## 6 – Configuration des centrales d'alarme

### 6.1- Configuration alarme RISCO



La connexion à la centrale est indisponible si une autre interface est déjà connectée. Elle apparaît en statut « Déconnecté »

- Sélectionner la marque RISCO, le modèle, est saisir le nom :

Fig. 11 : Configuration alarme RISCO.

- Remplir les champs de connexion comme suit :

IP et Port de communication dans Connection Settings

Code d'accès et Code distant dans Communication/Communication Software

Fig. 12 : Configuration réseau alarme RISCO.

## 6.2 - Configuration alarme GALAXY HONEYWELL

### 6.2.1 Paramétrage de la centrale d'alarme depuis le clavier de la centrale (GALAXY Dimension)

#### 1 : Donner le droit à l'installateur.

- Composer le code Manager « 12345 » + ent
- Aller dans le menu 48.1 et activer le droit de l'installateur.

#### 2 : Entrer en mode installateur pour effectuer les opérations suivantes

- Composer le code Manager « 112233 » + ent

#### 3 : Configurer le module Ethernet

- Aller dans le menu 56.4.1.1 : Indiquer l'adresse IP de la centrale.
- Aller dans le menu 56.4.1.4 : Indiquer le masque de sous-réseau.

#### 4 : Report alarme

- Aller dans le menu 56.4.2.1 : Sélectionner « SIA » niveau 4.
- Mettre à « ON » tous les événements à gérer.
- Aller dans le menu 56.4.2.2.1 : Indiquer l'adresse IP de l'OPTIMA qui communique avec la centrale d'intrusion.
- Aller dans le menu 56.4.2.2.2 : Indiquer le port de communication « 10002 »
- Aller dans le menu 56.4.2.4 : Indiquer le code client « 1234 ».
- Aller dans le menu 56.4.2.8 : Indiquer le protocole TCP : « 1 ».

#### 5 : Accès distant

- Aller dans le menu 56.4.3.1 : Sélectionner « Toujours » pour la période d'accès
- Aller dans le menu 56.4.3.2 : Sélectionner « Accès direct » pour le mode.

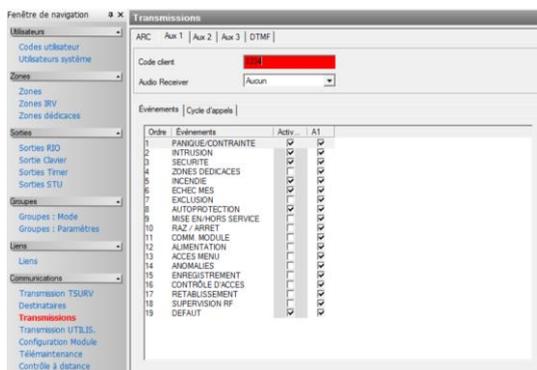
#### 6 : Commande SIA

- Aller dans le menu 56.4.8 : Indiquer l'adresse IP de l'OPTIMA qui communique avec la centrale d'intrusion.

### 6.2.2 Paramétrage de la centrale d'alarme depuis le logiciel RSS (GALAXY Flex)

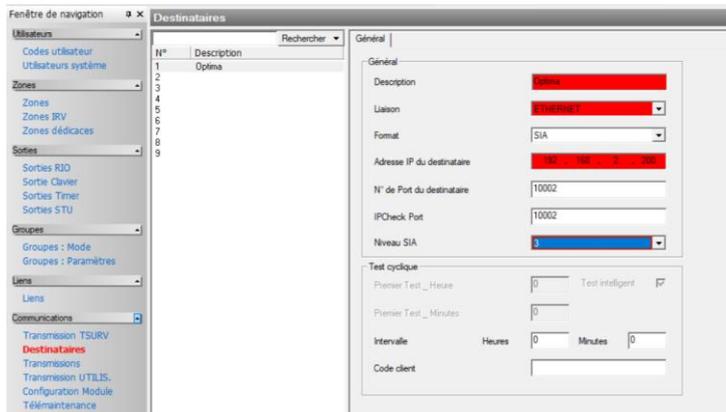
#### 1 : Donner le droit à l'installateur et droits des reports d'alarme

Indiquez le code client et cochez les cases suivantes depuis le menu Communications/Transmissions :



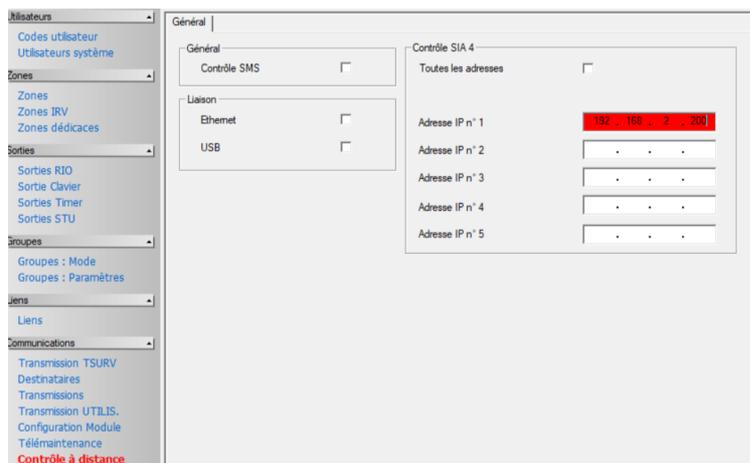
## 2 : Configurer le module Ethernet et la commande SIA

Depuis le menu *Communications/Destinataires* : indiquez **l'adresse IP de l'OPTIMA** qui communique avec la centrale d'intrusion (ici *192.198.2.200*) et le port de communication (ici *10002*).



## 3 : Accès distant

Indiquez dans *Communications/Contrôle à distance* **l'adresse IP de l'OPTIMA** qui communique avec la centrale d'intrusion (ici *192.168.2.200*).



## 6.2-3 Paramétrage de la centrale d'alarme dans l'interface OPTIMA

### Profil :



## Paramètres réseau : saisir 10005 concernant le port de communication



## Paramètres fonctionnels :

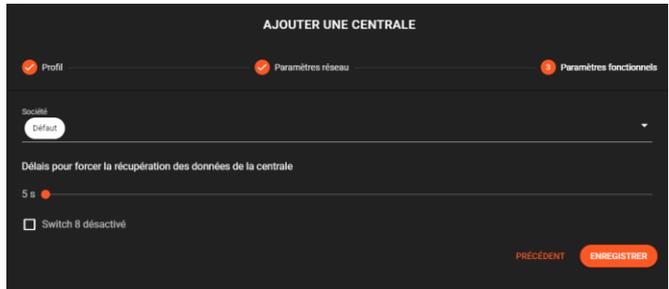
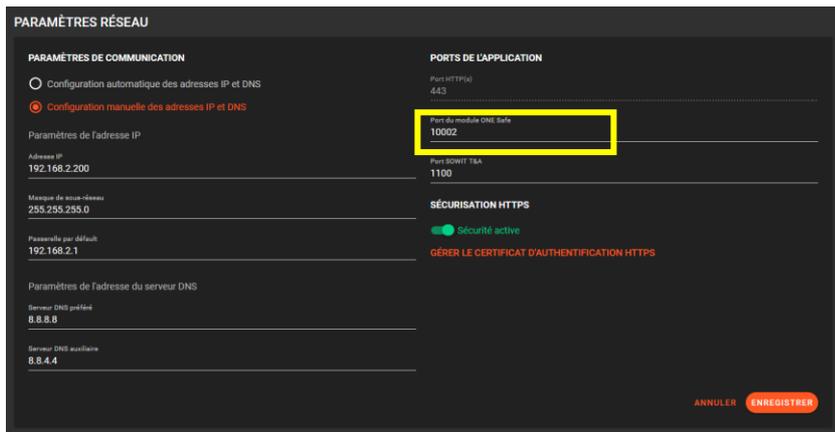


Fig. 13 : Configuration réseau alarme GALAXY.

## Port de dialogue :

Configurez le port de dialogue avec la centrale depuis Administration du logiciel / Paramètres réseau.



## 6.3- Configuration alarme VANDERBILT SPC

Les paramètres de configuration à saisir pour établir la connexion avec une centrale *Vanderbilt* dans le module Intrusion sont les suivants :

- ✓ Adresse IP
- ✓ Port de communication
- ✓ Code client
- ✓ Clé de cryptage
- ✓ Nom de l'utilisateur
- ✓ Mot de passe de l'utilisateur
- ✓ Délais pour forcer la récupération des données de la centrale

Les paramètres doivent correspondre avec ceux configurés au niveau du logiciel Vanderbilt.

**Note:** après la configuration complète, le processus d'établissement de la connexion est possible en sauvegardant la configuration sur l'interface Vanderbilt depuis le Menu **Users/Users** et appuyer sur le bouton **Save** en bas à gauche de la page (attendre environ 1 min pour obtenir « Connectée »).



Fig. 14 : Etablissement de la connexion.

### 6.3.1 Configuration des Timeout

Le délai conseillé du Timeout Polling ATS et Timeout évènement ATS est de 60 sec  
**Menu Communications > Onglet FlexC > Editer ATS > Défaut de l'ATS**

**Défauts de l'ATS**

Timeout Polling ATS	<input type="text" value="60"/>	Secondes
Timeout évènement ATS	<input type="text" value="60"/>	Secondes
Génère un Défaut de Transmission	<input type="checkbox"/>	
Transmet les défauts ATS/ATP	<input type="checkbox"/>	
Evénements remis en file attente	<input checked="" type="checkbox"/>	
Délai de remise en file d'attente	<input type="text" value="300"/>	Secondes
JDB Défauts de l'ATS	<input type="checkbox"/>	
Temps maxi de remise en file	<input type="text" value="86400"/>	Secondes

**Détails de l'installation**

Détails de l'installation

### 6.3.2 Adresse IP - Port de communication - Code client

La configuration de l'adresse IP, du port de communication et du code client dans le logiciel *Vanderbilt* s'effectue au niveau de l'interface d'édition du chemin de transmission d'alarme (ATP).  
**Menu Communications > Onglet FlexC > Editer ATS > Editer**

- ✓ Code Client – Identifiant = Code d'accès
- ✓ Adresse IP ou URL Récepteur = Adresse IP de l'OPTIMA
- ✓ Port IP Récep. = port de communication (voir plus bas)

**Configuration du Chemin - FlexC - Récepteur**

**Identification Centrale**

N° Séquence ATP: 1  
 ID Unique Chemin: 230  
 Nom du Chemin: Primary ATP 1 for AT  
 Code Client-Identifiant: 1234

**Identifiant du Récepteur RCT**

ID Récepteur: 1  
 Adresse IP ou URL Récepteur: 192.168.2.215  
 Port IP Récep.: 52000

**Interface du Chemin**

Interface de communication: Ethernet  
 Catégories du Chemin: Cat 1 [Ethernet]

**Avancé**

Paramètres avancés du Chemin ATP: Paramètres avancés du Chemin ATP

Le port de communication (port IP Récep) est modifiable dans le menu Configuration technique /Administration du logiciel / Paramètres réseau:

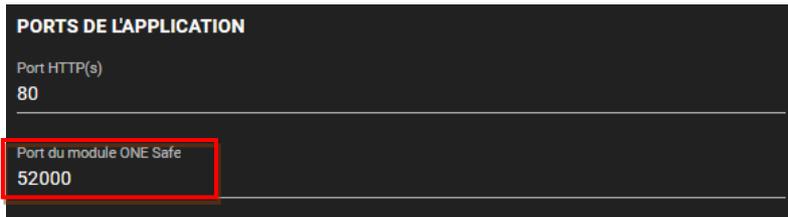


Fig. 15 : Port de communication.



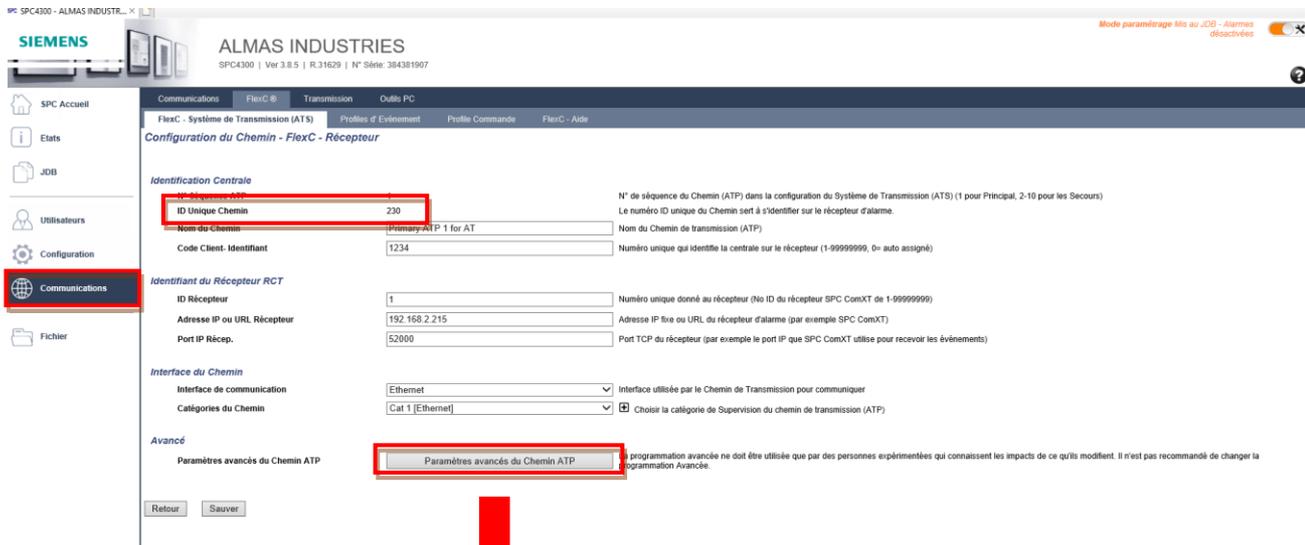
Le port 52000 étant utilisé par l'application Vanderbilt, nous recommandons de configurer un autre port.

### 6.3.3 Clé de cryptage

L'édition de la clé de cryptage dans le logiciel *Vanderbilt* s'effectue dans les paramètres avancés du chemin de transmission d'alarme (ATP)

(Utiliser Google Chrome ou Mozilla Firefox)

- ✓ **Menu Communications > Onglet FlexC > Editer ATS > Editer > Bouton Paramètres avancés du Chemin ATP**



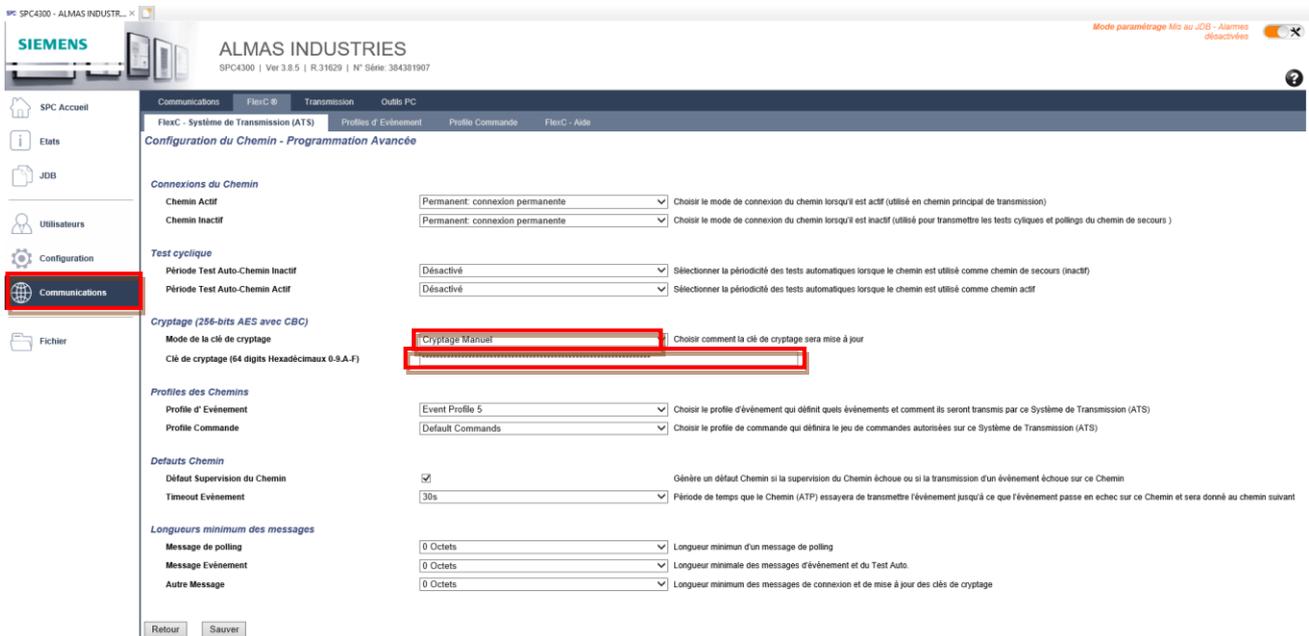
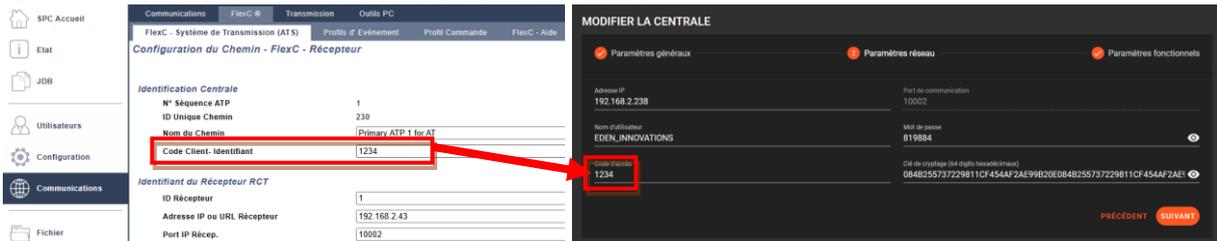


Fig. 16: Clé de cryptage SPC.

Le mode de la clé de cryptage à sélectionner est le Cryptage Manuel.  
 La clé de cryptage à saisir doit être une clé de 64 digits hexadécimaux (0-9.A-F)

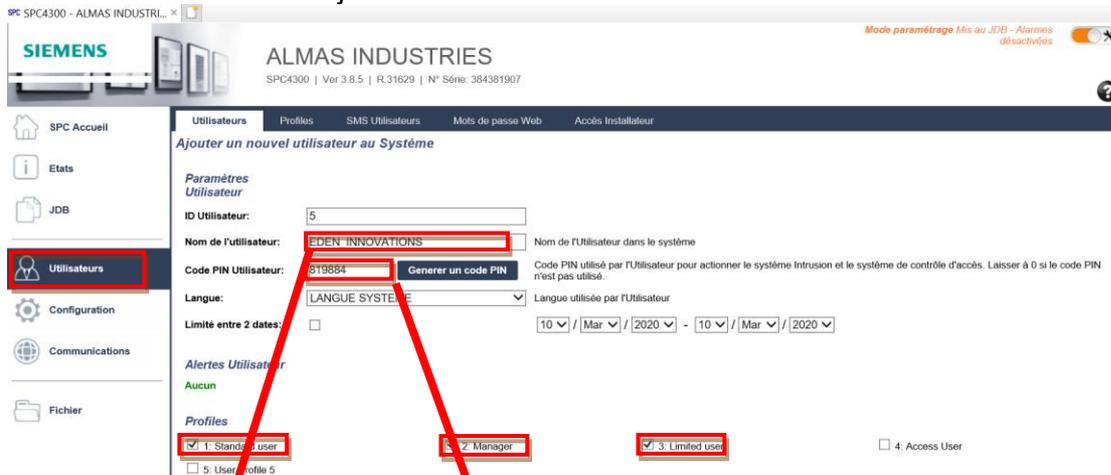
Code client identifiant = Code d'accès dans OPTIMA



### 6.3.4 Noms et mot de passe utilisateur

Les identifiants utilisateur à saisir correspondent à ceux d'un utilisateur enregistré dans le logiciel *Vanderbilt* au niveau du menu Utilisateurs.

L'édition du nom d'utilisateur et du mot de passe s'effectue en cliquant sur le bouton icône "éditer" de l'utilisateur ciblé ou lors de l'ajout d'un nouvel utilisateur.



Le profil doit être de type « Standard », « Manager » et « Limited user ».

Informations à saisir dans le profil de la centrale dans l'interface ONE Safe :

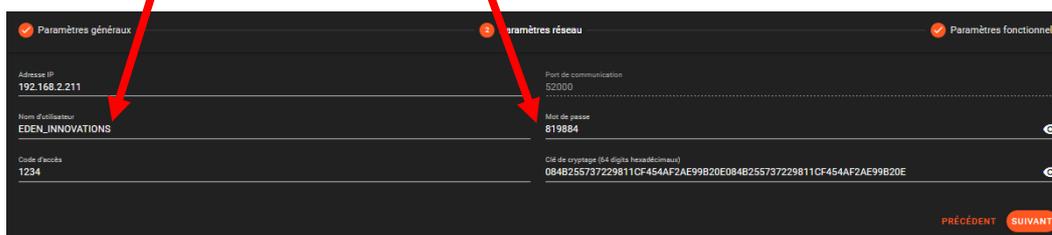


Fig. 17 : Clé de cryptage OPTIMA.

Code d'accès = Code Client – Identifiant (voir plus haut)

Mot de passe = Code PIN Utilisateur

Ex de clé de cryptage : 084B255737229811CF454AF2AE99B20E084B255737229811CF454AF2AE99B20E

### 6.3.5 Délai pour forcer la récupération des données de la centrale

Le paramètre est par défaut configuré à 30 sec. Parfois ce temps est insuffisant pour établir une bonne communication entre OPTIMA et la centrale d'intrusion et peut conduire à l'apparition de fréquentes déconnexion/connexion de centrale.

Nous recommandons donc de configurer un délai de minimum de **120** secondes.

### 6.3.6 Spécificités logiciel Vanderbilt

**Profil d'événements :**

Le module Intrusion de l'OPTIMA intègre des fonctionnalités limitées des centrales d'alarmes.

Pour les centrales Vanderbilt, de nombreux événements envoyés par la centrale ne sont ainsi pas traités par le serveur.

Afin de réduire le travail de filtrage du serveur sur les événements traités, un **profil d'événement** spécifique peut être créé dans le logiciel Vanderbilt pour le système de transmission d'alarme (ATS) configuré pour le module Intrusion.

Dans ce profil d'événement, seuls les événements nécessaires pour le bon fonctionnement du module Intrusion peuvent être sélectionnés ce qui limitera l'envoi d'événements inutiles à filtrer par le serveur.

Accès au menu de gestion des profils événements : **Menu Communications > Onglet FlexC > Sous-onglet Profiles d'Evénement**

Liste des événements à cocher obligatoirement :

The screenshot displays the 'Profiles d'Evénement' configuration window. The 'Communications' menu is highlighted in the sidebar. The main window shows the configuration for 'Event Profile 5'. The 'Identification' section has 'Event Profile 5' entered in the 'Nom' field. The 'Filtrer' section is divided into three sub-sections: 'Intrusion / Incendie / Médical', 'Supervision Système', and 'Porte et Utilisateur'. Each sub-section lists various event types with 'Transmettre l'événement' and 'Compteur d'exception d'événement' columns. Several checkboxes are checked, including 'Alarmes confirmées', 'Alarme Intrusion', 'Amnement', 'Inhibe et isole', 'Changement état Zone', and 'Changement état Zone en Alarme'. At the bottom, the 'Filtre sur Secteur' section has four buttons: '1: Area 1', '2: Area 2', '3: Area 3', and '4: Area 4', all of which are checked.

L'attribution du profil spécifique se fait au niveau de l'édition du système de transmission d'alarme (ATS) dans la section **Profils ATS > Modifier Profils d'Évènement**.

Editer	Effacer	ID	Nom Profil Utilisateur
		1	Standard user
		2	Manager
		3	Limited user
		4	Access User
		5	User Profile 5

### Optimisation de la communication

Pour encore améliorer la réactivité entre la centrale et OPTIMA, désactivez le « Changement état zone » dans votre profil d'Evènements.

Ce paramétrage a pour effet d'actualiser uniquement les changements d'état des groupes d'alarme dans le tableau de bord à chaque récupération forcée des données.

Le délai pour forcer la récupération des données de la centrale est à minimiser dans les Paramètres fonctionnels de la configuration de centrale.

Les évènements liés à la centrale sont toujours gérés en temps réel, **avec une réactivité accrue**.

# 7- Exploitation

## 7.1-Tableau de bord

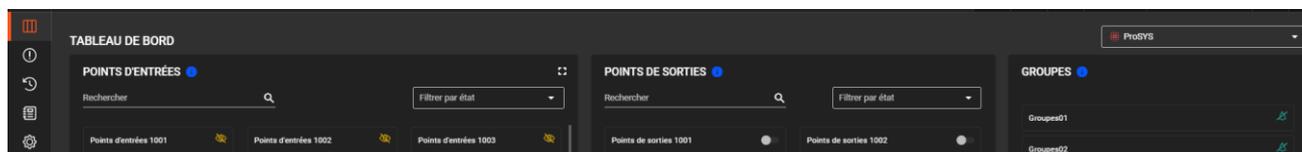


Fig. 18 : Tableau de bord.

Ce menu permet de voir d'un seul coup d'œil l'état des centrales, avec un visuel sur les points d'entrées, de sorties et l'état des groupes.

L'état de connexion de chaque centrale est visible à gauche du libellé :

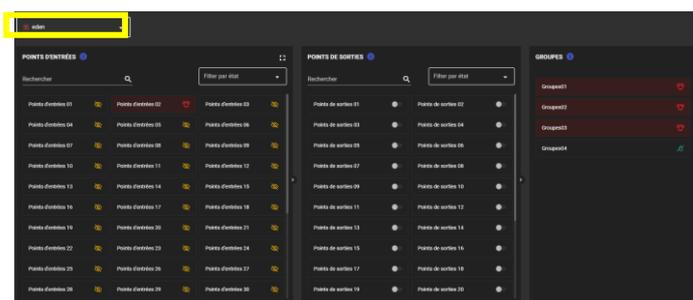
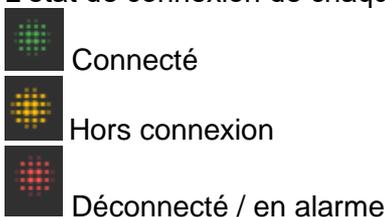


Fig. 19: Tableau de bord complet.

### 7.1.1 Point d'entrées

- Les points d'entrée peuvent être agrandis sur la page principale grâce à l'icône zoom

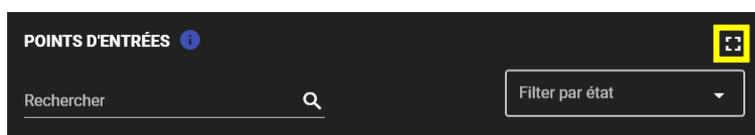
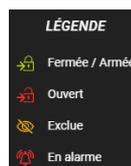


Fig. 20 : Agrandir page.



L'état des entrées est symbolisé par la légende suivante :

Il est possible de spécifier directement une entrée dans le champ de recherche, ou de les filtrer selon leur état :

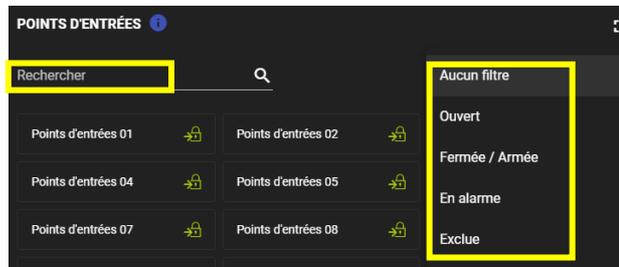


Fig. 21: Recherche d'une entrée.

- Les entrées peuvent être exclues/inclues par un clic gauche :

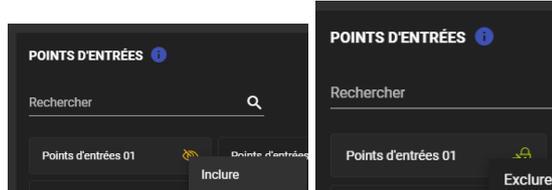
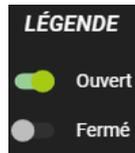


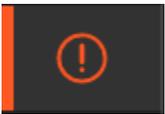
Fig. 22: Exclusion d'une entrée.

### 7.1.2 Points de sortie

Ils renseignent l'état de sortie selon les deux états « Ouvert » ou « Fermé ».



## 7.2-Événements live



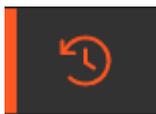
Ce menu affiche en direct les 100 derniers événements liés aux centrales d'intrusion.

DATE P	NATURE DE L'ÉVÉNEMENT	CENTRALE	POINT / CONTACT	STATUT
8/7/2019 14:21	Entrée inactive	vidéo	Points d'entrées 03	
8/7/2019 14:21	Alarme acquiescée	vidéo	Points d'entrées 01	
8/7/2019 14:22	Acquisition d'état du groupe	vidéo	Groupe01	
8/7/2019 14:22	Entrée inactive	vidéo	Points d'entrées 01	
8/7/2019 14:23	Acquisition d'état du groupe	vidéo	Groupe02	
8/7/2019 14:23	Acquisition d'état du groupe	vidéo	Groupe01	
8/7/2019 14:23	Dispositif alarme	vidéo	Points d'entrées 01	
8/7/2019 14:23	Entrée inactive	vidéo	Points d'entrées 01	
8/7/2019 14:23	Sortie inactive	vidéo	Points de sorties 01	
8/7/2019 14:23	Badge accepté	vidéo	Points d'entrées 01	
8/7/2019 14:23	Entrée inactive	vidéo	Points d'entrées 01	
8/7/2019 14:24	Entrée inactive	vidéo	Points d'entrées 01	
8/7/2019 14:25	Entrée inactive	vidéo	Points d'entrées 01	
8/7/2019 14:25	Entrée inactive	vidéo	Points d'entrées 01	

Fig. 23 : Évènement en temps réel.

Il est possible d'effectuer une recherche pour les trier selon leurs natures, leurs centrales, ou leurs points/groupes.

### 7.3-Historique des évènements



Cette page affiche la liste complète des évènements avec la possibilité de filtrer les données dans une période donnée et/ou la nature d'évènement.

DATE ↓	NATURE DE L'ÉVÉNEMENT	CENTRALE	POINT / GROUPE	RAPPORT
30/10/2019 10:08	Alarme acquittée	Logitech	Pointu d'entrée 01	
30/10/2019 10:08	Sortie en alarme d'acquiescement	Logitech	Pointu d'entrée 01	
30/10/2019 10:08	Sortie en alarme	Logitech	Pointu d'entrée 01	
30/10/2019 10:08	Sortie alarme	Logitech	Pointu de sortie 02	
30/10/2019 10:08	Groupe en alarme	Logitech	Groupe01	
30/10/2019 10:07	Terrain connecté	Logitech		
30/10/2019 10:07	Mise en service du groupe	Logitech	Groupe01	
30/10/2019 09:56	Groupe acquitté	Logitech	Groupe01	
30/10/2019 09:56	Groupe hors service	Logitech	Groupe01	
30/10/2019 09:56	Sortie alarme	Logitech	Pointu de sortie 02	
30/10/2019 09:56	Acquiescement distant du groupe	Logitech	Groupe01	
30/10/2019 09:56	Terrain connecté	Logitech		

Fig. 24 : Historique des évènements.

Les résultats de recherche peuvent être exportés en format tableur en cliquant sur [EXPORTER](#).

Si des caméras sont liées aux points d'intrusion ou aux zones, la colonne Visualiser fait apparaître une icône caméra

Celle-ci donne directement accès à la séquence vidéo à l'instant de l'évènement (le module **ONE View** activé et configuré, voir documentation).

DATE ↓	NATURE DE L'ÉVÉNEMENT	CENTRALE	POINT / GROUPE	RAPPORT	VISUALISER
15/3/2022 14:50:26	Disparition alarme	RISCO LIGHTSYS	Zone 01		
15/3/2022 14:50:22	Acquiescement distant du groupe	RISCO LIGHTSYS	Partition 1		
15/3/2022 14:49:49	Alarme acquittée	RISCO LIGHTSYS	Partition 1		
15/3/2022 14:49:47	Groupe en alarme	RISCO LIGHTSYS	Partition 1		
15/3/2022 14:49:47	Entrée en alarme	RISCO LIGHTSYS	Zone 01		
15/3/2022 13:57:16	Groupe en service	RISCO LIGHTSYS	Partition 1		
15/3/2022 13:57:15	Mise en service du groupe	RISCO LIGHTSYS	Partition 1		
	hors service	EDEN	COMMUNS		
	hors service	EDEN	COMPTA		
	hors service	EDEN	DIRECTION		
	hors service	EDEN	BE HOTLINE		

Fig.25: Affichage flux vidéo lié à une entrée en alarme.

### 7.4-Journal de bord

Ce menu affiche la liste des actions menées par les utilisateurs.



Se rajoute la possibilité de rechercher par points/groupe ou de rechercher par les actions effectuées.

Les résultats de recherche peuvent être exportés en format tableur en cliquant sur [EXPORTER](#).

JOURNAL DE BORD		Rechercher	EXPORTER
DATE	UTILISATEUR	POINT / GROUPE	ACTION EFFECTUÉE
4/12/2020 17:23:39	ADMINISTRATEUR		Connexion centrale (ONE Safe)
4/12/2020 17:23:35	ADMINISTRATEUR		Déconnexion centrale (ONE Safe)

Fig. 26 : Journal de bord.

## 7.5-Codes utilisateur

Ce menu affiche la liste des usagers associés à des codes clavier (centrales RISCO uniquement).



CODES UTILISATEUR RISCO					Rechercher
USAGER ↑	GROUPE D'ACCÈS	BADGE	CODE UTILISATEUR	CENTRALES	
GOMEZ Diego	Office	1300123501	⊗		
PADILLA Adam	Office	4100619136	⊗		
VELPO Brian	Ménage	612903066	⊗		

Fig. 27 : Liste des usagers associés à des codes clavier.

Sélectionnez un utilisateur afin d'ajouter/éditer/supprimer un code clavier associé à l'armement/désarmement de zone(s) avec les droits correspondants (Master/Armer...).

**AJOUTER UN CODE UTILISATEUR RISCO**

**INFORMATIONS**

NOM PRÉNOM  
Padilla Adam

NUMÉRO DE BADGE  
4100619136

**CODE UTILISATEUR**

Centrale intrusion  
LightSYS Plus

Code PIN  
••••

Partitions  
Toutes les partitions

Code PIN Authority  
Armer

RETOUR ENREGISTRER

Fig. 28 : Ajout code clavier.

Le code PIN établi à « 0 » supprime le code et les droits existants associé à l'utilisateur.

**Note :** Un usager supprimé depuis le contrôle d'accès ne supprime pas son code associé et ses droits d'armement/désarmement.

## 7.6- Alertes



Fig. 29 : Alerte dans le bandeau horizontal.

La notification d'alerte s'affiche aussi bien dans l'interface dans le bandeau horizontal du module Intrusion que dans l'interface principale.

Un clic sur la notification affiche la liste des acquittements en attente.

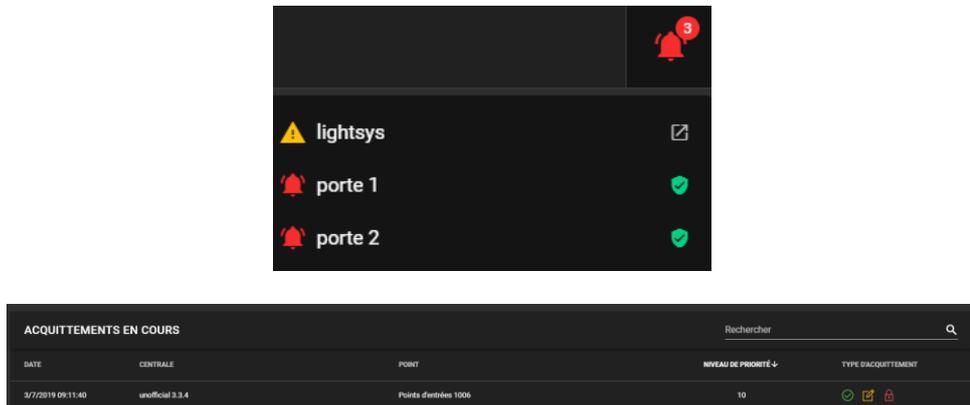


Fig. 30 : Acquitement.

Le détail de l'acquitement se fait en cliquant sur la ligne concernée, avec la possibilité d'acquitter en renseignant le motif de l'alerte.

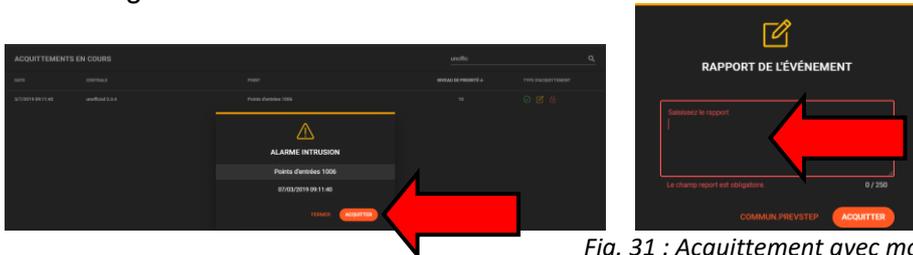


Fig. 31 : Acquitement avec motif alerte.

## 7.7-Ajout d'un groupe, d'une entrée ou d'une sortie dans la Supervision

Voir la notice d'utilisation **OPTIMA 360**.

## 7.8- Automatismes associés à l'Intrusion

Menu « Configuration technique » / « Automatismes » / Automatismes centralisés » :

Renseigner les paramètres de l'automatisme :

- **Libellé**
- **Conditions**
- **Actions**

### 7.8.1 Conditions possibles sur les groupes

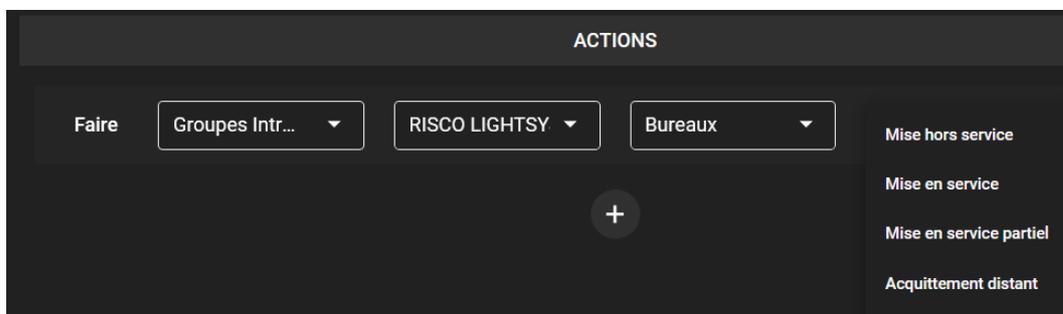


Fig. 32 : Conditions sur les groupes.

## 7.8.2 Conditions possibles sur les entrées

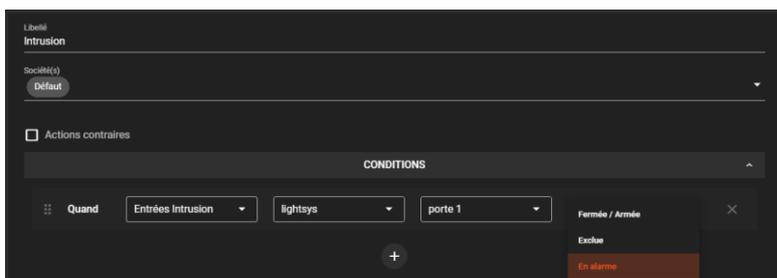


Fig. 32 : Conditions sur les entrées.

## 7.8.3 Actions possibles sur les sorties

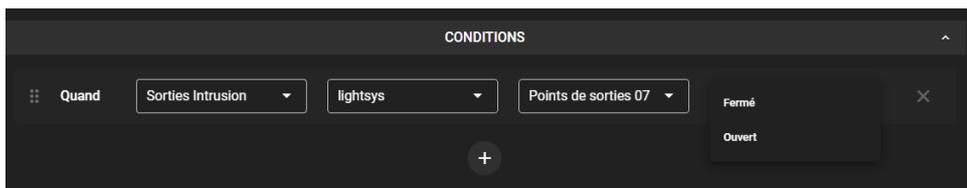


Fig. 33 : Actions sur les sorties.

## Exemple d'automatisme : incrémentation du niveau d'alerte si la partition 1 est en alarme



Fig. 34 : Incrémentation niveau d'alerte si partition 1 en alarme.

## 8- Cas d'utilisation

### 8.1 Scénario 1

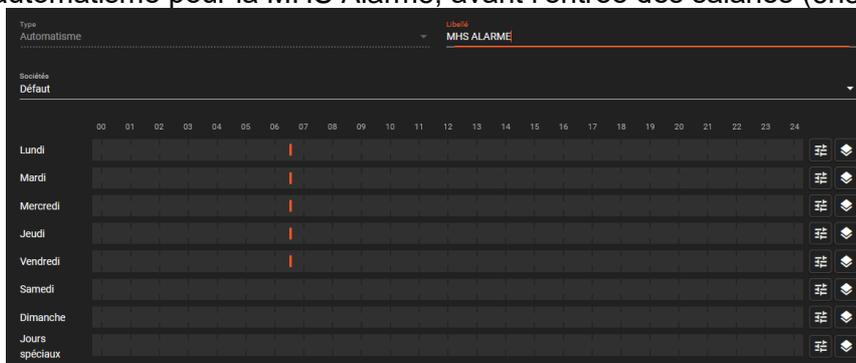
La mise en service du groupe d'alarme se fait en fin de journée à heure fixe (plage horaire), la mise hors service en début de journée.

### Configuration

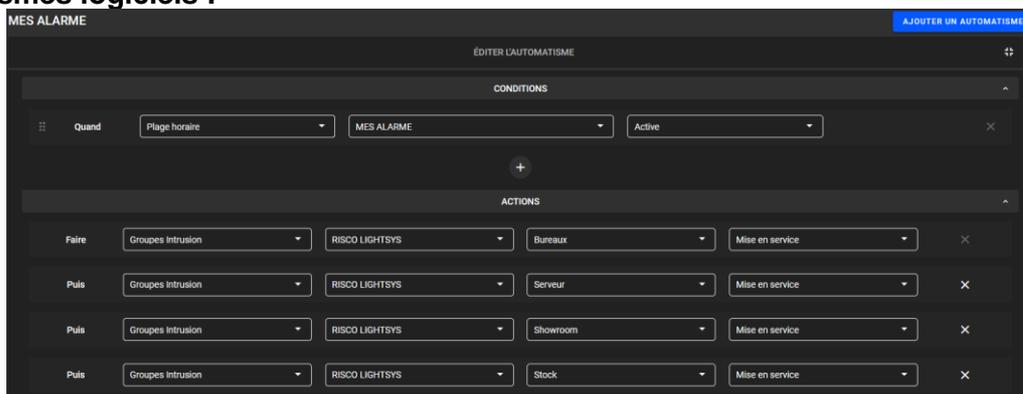
Plage horaire d'automatisme pour la MES Alarme, après la sortie de tous les salariés (23h30) :

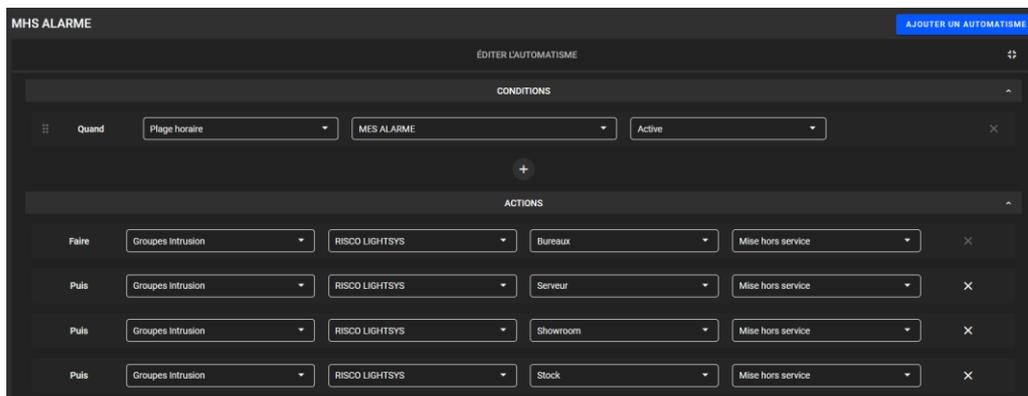


Plage horaire d'automatisme pour la MHS Alarme, avant l'entrée des salariés (6h30) :



### Automatismes logiciels :





## 8.1 Scénario 2

Le double badgeage en fin de journée par le dernier salarié sur un lecteur spécifique (ici lecteur Portail) réalise :

- La mise en service (MES) du groupe d'alarme
- La LED du lecteur change de couleur pour informer de l'état actif de l'alarme
- Le niveau d'alerte bascule au niveau 1

Le simple badgeage en début de journée sur un lecteur spécifique (ici lecteur Portail) réalise :

- La mise hors service (MHS) du groupe d'alarme se fait au 1er badgeage de la journée en tenant compte de l'état du groupe d'alarme (action si groupe d'alarme en service ou en alarme ou en en service partiel)
- La LED du lecteur se remet en couleur d'origine pour informer de l'état inactif de l'alarme.
- Le niveau d'alerte bascule au niveau 0

### Connectiques :

Les lecteurs de marque STid sont équipés d'une entrée LED2 pilotable pour indiquer à l'utilisateur l'état de l'alarme (en Service/Hors Service) avec une couleur particulière.

Il existe deux manières de connecter :

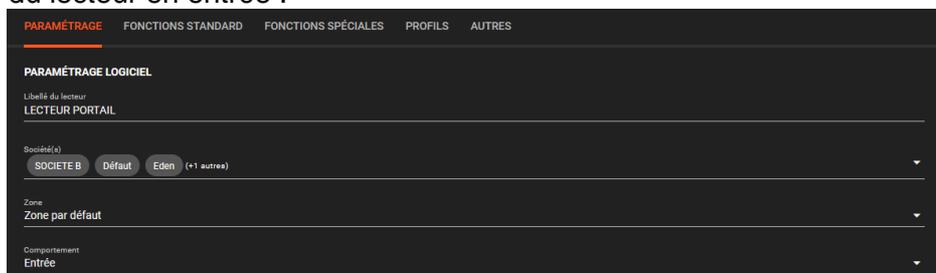
- Utilisation de la Sortie collecteur ouvert de la centrale EDEN branchée sur LED2 du lecteur STid (masse commune entre le lecteur et la sortie collecteur ouvert)

ou

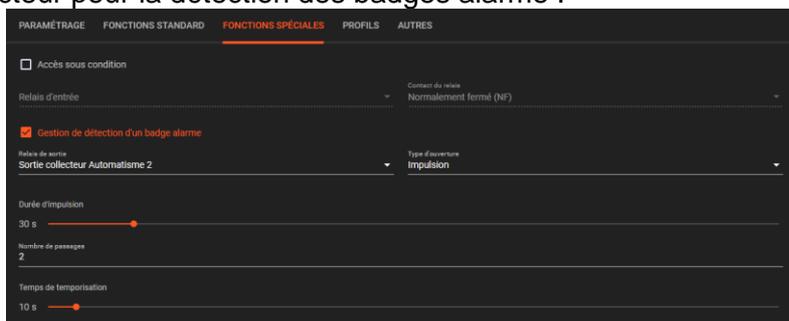
- Sortie relais d'automatisme de la centrale EDEN connectée à LED2 du lecteur STid (le connecteur du COMMUN -ici COM1) être branchée à la même masse que le lecteur.

### Configuration dans OPTIMA :

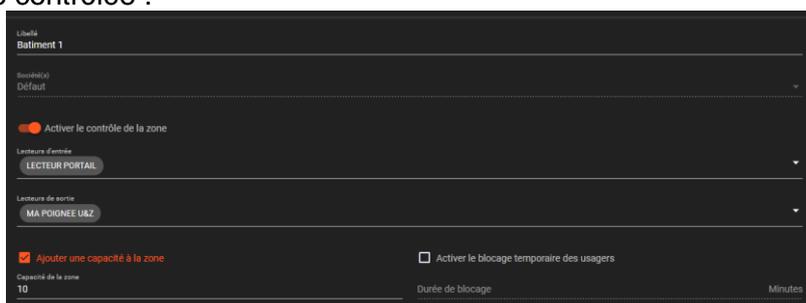
Configuration du lecteur en entrée :



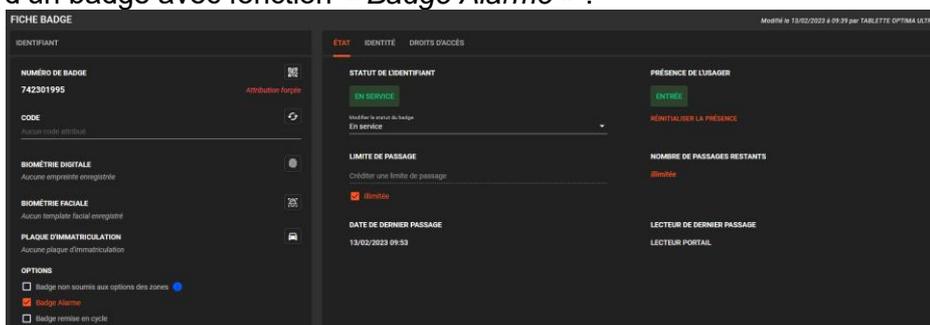
## Configuration du lecteur pour la détection des badges alarme :



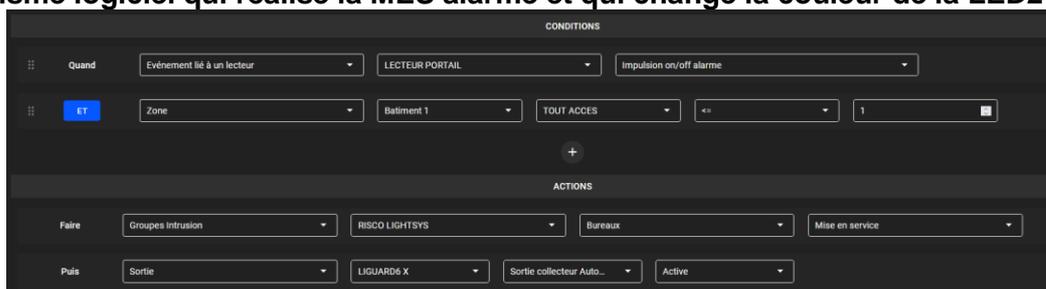
## Configuration zone contrôlée :



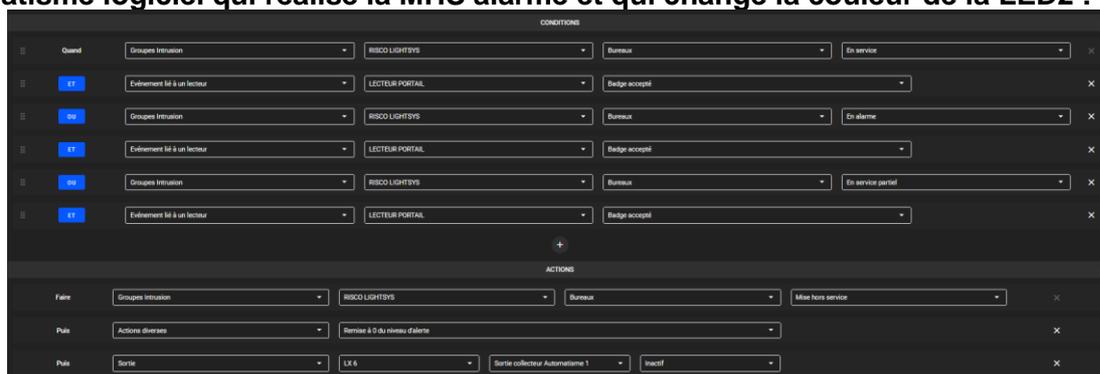
## Configuration d'un badge avec fonction « Badge Alarme » :



## Automatisme logiciel qui réalise la MES alarme et qui change la couleur de la LED2 :



## Automatisme logiciel qui réalise la MHS alarme et qui change la couleur de la LED2 :





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

[www.eden-innovations.com](http://www.eden-innovations.com)