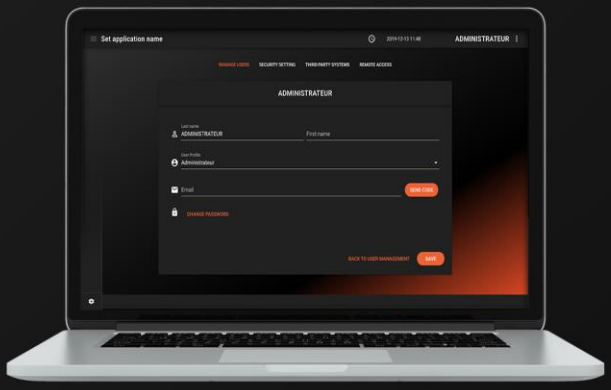
GUIDE



CONTRÔLE D'ACCÈS

OPTIMA

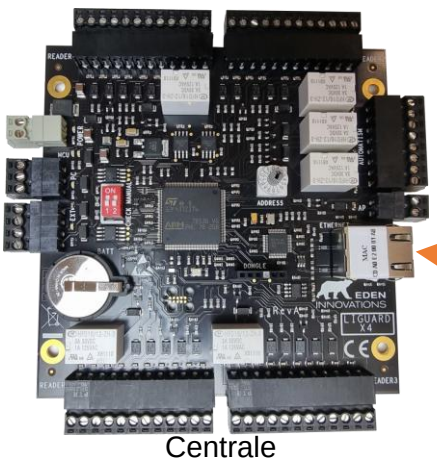
EDEN INNOVATIONS

INSTALLATEUR

Important : une fois que l'OPTIMA Box a été mise sous tension, si vous souhaitez la mettre hors tension, il faudra obligatoirement l'arrêter « proprement », en passant par le logiciel (depuis le Menu Exploitation / Maintenance technique / Marche/Arrêt de la box). Sans cela, le produit peut subir des dommages irrémédiables.

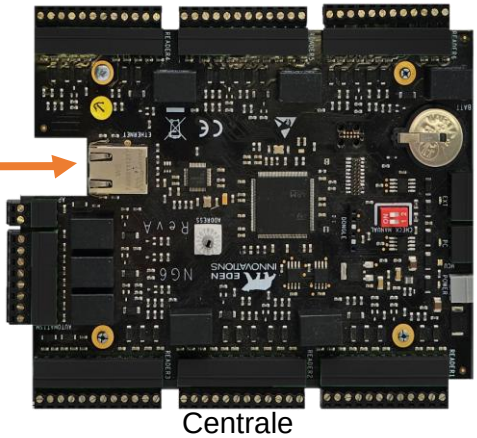
Table des matières

Schéma de principe



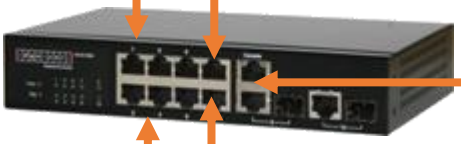
Centrale

(LDMV2, C1P2FX, C4PLUSFX, LIGUARD LIGUARDX)



Centrale

(LDMV2, C1P2FX, C4PLUSFX, LIGUARD LIGUARDX)



SWITCH ou ROUTEUR

OPTIMA Box®

OPTIMA Wi®

PC, MAC, tablette, ou n'importe quel appareil avec un navigateur internet.

REMARQUES :

- Lorsque vous utilisez un appareil mobile comme un smartphone, vous êtes directement redirigé vers le kiosque OPTIMA® donnant accès à OPTIMA Time, OPTIMA Access, OPTIMA Pass et OPTIMA Mobile
- Pour un accès distant à OPTIMA®, il faut ouvrir le port **80** en TCP (modifiable), ou le port **443** en sécurisation HTTPs (non modifiable).

OPTIMA Box®:

- Veuillez utiliser un câble RJ45 Cat5e FTP blindé (ou F/UTP blindé).
- La connexion de l'OPTIMA Box® en PPOE n'est pas compatible.
- La longueur maximale du câble entre l'appareil et le switch ne doit pas dépasser 100 m.

Connection à OPTIMA®

Pour accéder à l'OPTIMA®, il vous suffit de la brancher sur votre réseau Ethernet, d'ouvrir un navigateur Internet (Firefox, Chrome, Opera recommandés), puis de saisir l'adresse IP de l'appareil.

Nous vous recommandons d'utiliser le navigateur Mozilla Firefox pour une meilleure expérience utilisateur.

- L'adresse IP par défaut de l'OPTIMA Box® est 192.168.3.130.
- L'adresse IP par défaut de l'OPTIMA Wi® est l'adresse IP du PC qui héberge le logiciel OPTIMA Wi®.

Pour configurer l'adresse de l'OPTIMA Box®, vous devez vous connecter à l'OPTIMA Box® avec un ordinateur qui possède la même plage d'adresses.

Vous pouvez également utiliser OPTIMA Detect® inclus dans le pack Optima Tools depuis cette page : https://optimabox.fr/

OPTIMA® est livrée par défaut avec le nom d'utilisateur "ADMINISTRATEUR" sans mot de passe.

Modification des paramètres réseau

OPTIMA® comporte deux types d'interfaces :

- Une interface pour PC et MAC
- Une interface pour les smartphones, tablettes, et autres appareils mobiles

Vous pouvez configurer les paramètres réseau depuis l'interface :

" ***Menu configuration*** " → " ***Administration du logiciel »*** → ***« Paramètres réseau*** ".

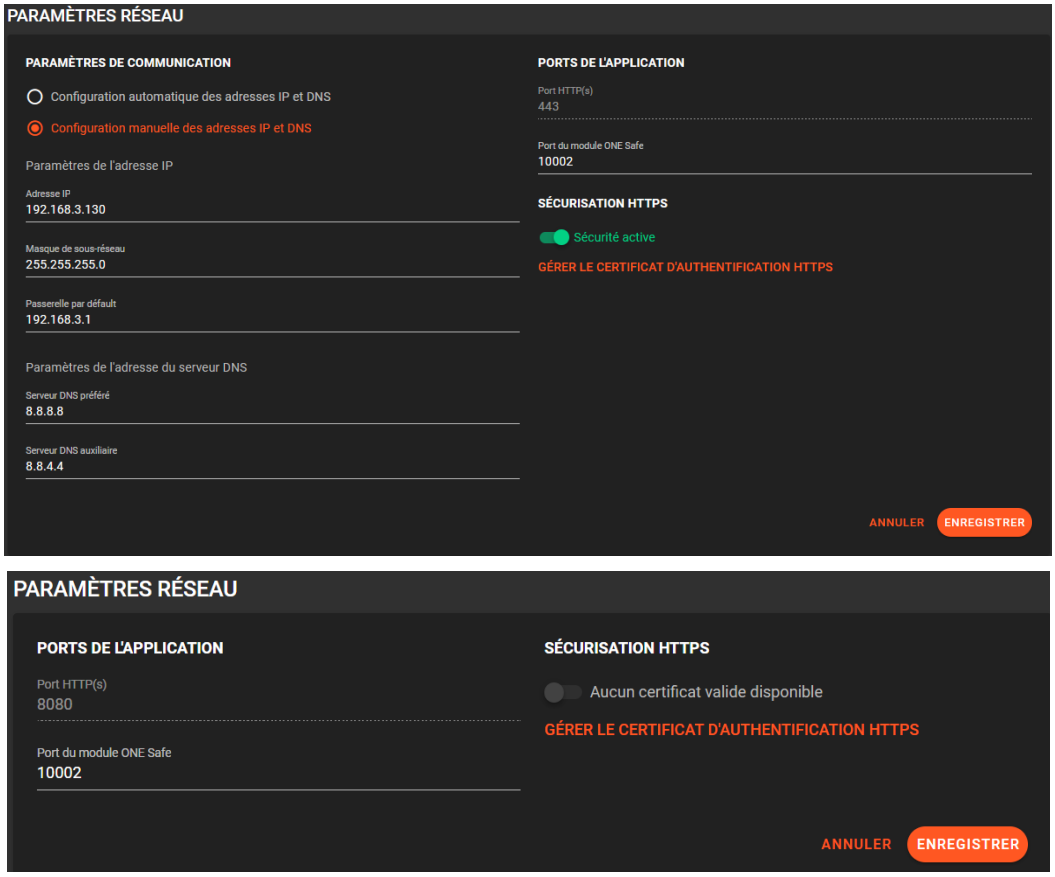


Fig. 1 : Paramètres réseau OPTIMA® / Optima Wi®

Certains ports de communication sont déjà réservés pour des services tiers.
L'utilisation de ces ports peut engendrer des conflits entre les services

La connexion à l'OPTIMA® est possible en connexion avec authentification HTTPS. De cette manière les communications sont cryptées entre le PC client et OPTIMA® (serveur).

Pour de plus de détails, veuillez consulter ce document.

Modification de la langue du logiciel

La sélection de la langue depuis la page d'accueil change la langue de l'interface graphique mais ne modifie pas la langue de la base de données.

Pour modifier la langue de l'interface graphique **et** de la base de données, il faut restaurer la box OPTIMA® à l'origine (reset) et sélectionner la langue de l'interface graphique souhaitée

Pour restaurer OPTIMA® à l'origine, allez dans le Menu **Configuration → "*Administration de l'installation*" → "*Restaurer*" → sélectionner "*Restaurer à l'origine* ».**

Accès rapides

Ce menu disponible au démarrage permet d'accéder plus rapidement aux différentes fonctionnalités pour gérer l'exploitation du site, et donne un accès rapide aux modules additionnels déjà activés.

(Voir *Administration de l'installation*)

Le menu est accessible à tout moment en cliquant sur l'icône situé en haut à gauche de l'écran, ou bien en cliquant sur le nom de l'installation (ici « OPTIMA »).

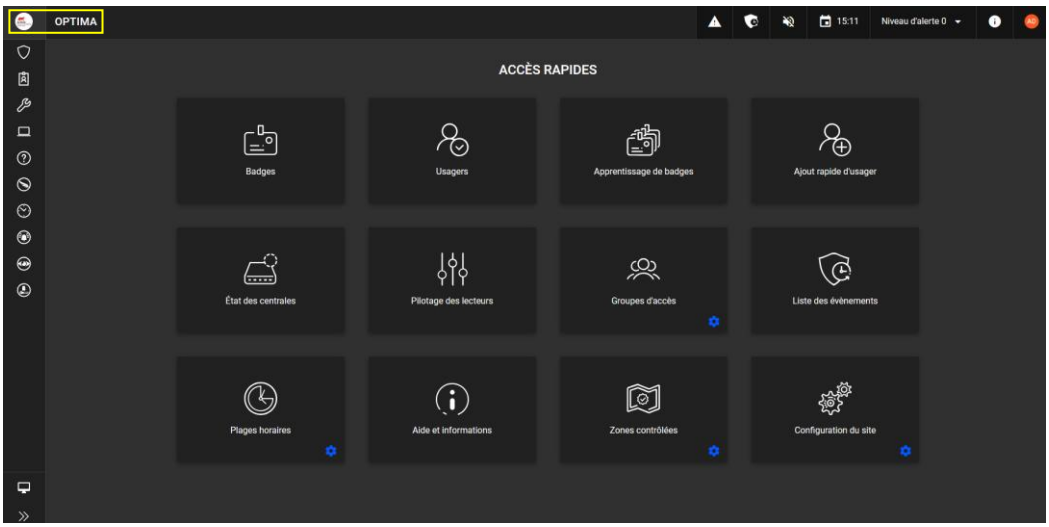


Fig. 2 : Menu Accès rapides

Vous pouvez disposer les accès rapides selon vos préférences (Utilisation du logiciel – *Edition des accès rapides*).

Les raccourcis associés à un engrenage font partie du ***Menu Configuration***.

Barre d’état

La barre horizontale indique en un coup d’œil les informations sur votre contrôle d’accès, votre version OPTIMA® et vos systèmes d’alarme.

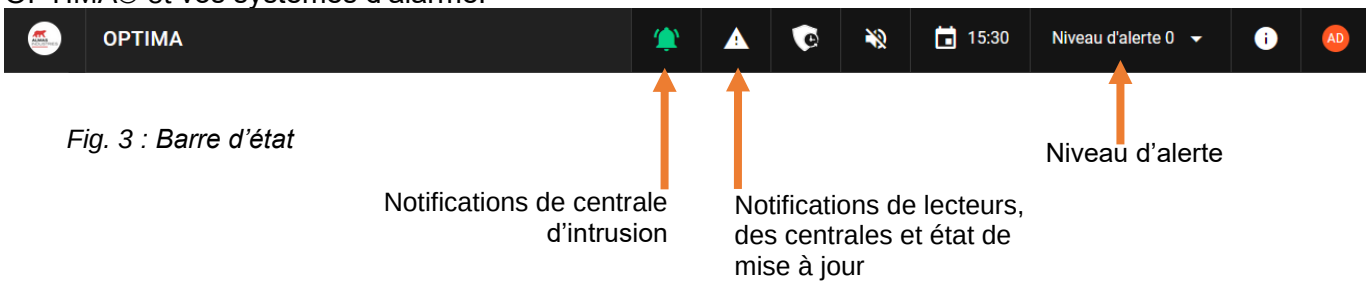


Fig. 3 : Barre d’état

Ouverture page courante / ouverture dans un nouvel onglet

Chaque fonctionnalité s’ouvre par défaut dans la page courante.

Si vous souhaitez ouvrir un nouvel onglet, cliquez sur l’icône à droite de la fonctionnalité à ouvrir.

Exploitation/Configuration

Vous pouvez basculer à tout moment entre le **Menu Exploitation** et le **Menu Configuration** (pour réaliser la configuration du contrôle d’accès) en cliquant sur le bouton correspondant situé en bas à droite de l’interface.

Le mode **Configuration** est aisément indentifiable par sa couleur bleue dans la partie inférieure gauche.

Le menu de gauche peut être déployé pour afficher tous les noms des fonctionnalités en cliquant sur la double flèche

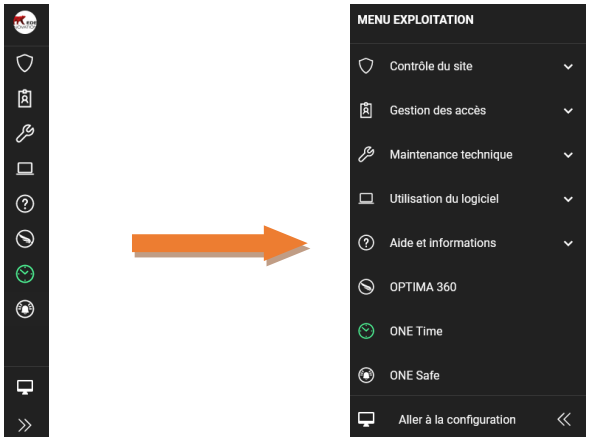


Fig. 4 : Menu déployé.

I- Menu Configuration

01- Configuration technique

1) Configuration du site

Présentation

La configuration du site affiche l'ensemble des éléments de votre site, constitué par les réseaux de centrale, les interfaces IP-BUS, les centrales associées, les lecteurs, ainsi que les cartes d'entrées et de sortie (si existantes).

Vous avez également la possibilité de réinitialiser l'ensemble des centrales du contrôle d'accès en cliquant sur le bouton « *Initialisation de toutes les centrales* »  .

(attention le contrôle d'accès est opérationnel seulement à la fin de cette opération).

Les lecteurs, cartes d'entrée et cartes de sortie peuvent être associées à des zones pour regrouper les éléments dans une même **zone** géographique. Cela vous permet d'atteindre rapidement les éléments d'une zone donnée.

Fig.5 : Menu configuration du site (par défaut).

La partie à gauche vous permet de filtrer les centrales/lecteurs/cartes d'entrées/cartes de sortie par nom de **réseau** ou par **zone** (voir *Configuration des lecteurs*).

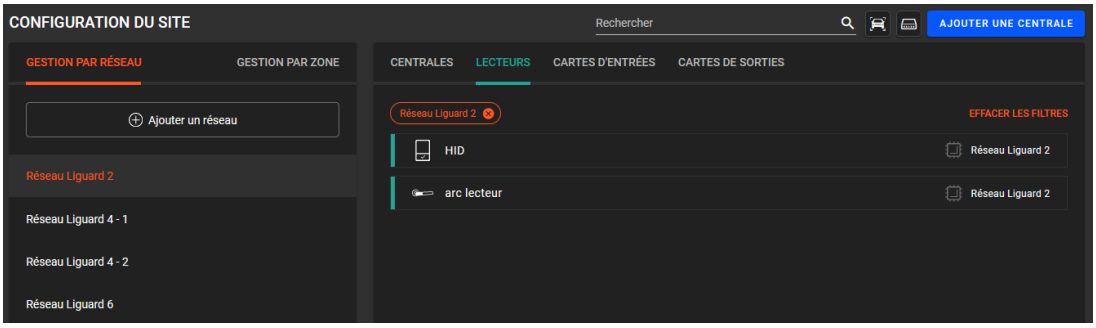


Fig.6 : Affichage des lecteurs appartenant au réseau « Réseau Liguard 2 ».

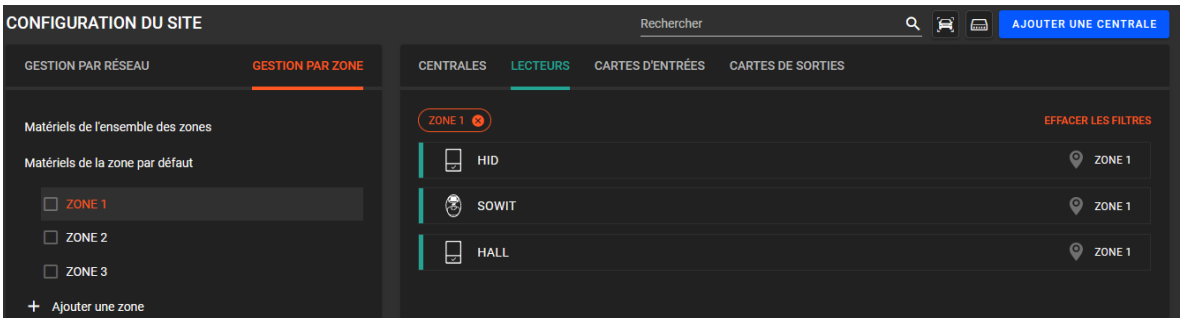
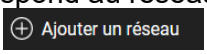


Fig.7 : Affichage des lecteurs appartenant à la zone « ZONE 1 ».

La configuration du site se fait en 3 étapes :

a. Création d'un réseau.
b. Création d'une centrale dans ce réseau.
c. Configuration des lecteurs de la centrale.

a) Création d'un réseau

Veuillez ajouter un réseau correspond au réseau de la centrale ou de l'interface IP-BUS en cliquant sur le bouton « *Ajouter un réseau* »  depuis le menu *Gestion par réseau*.

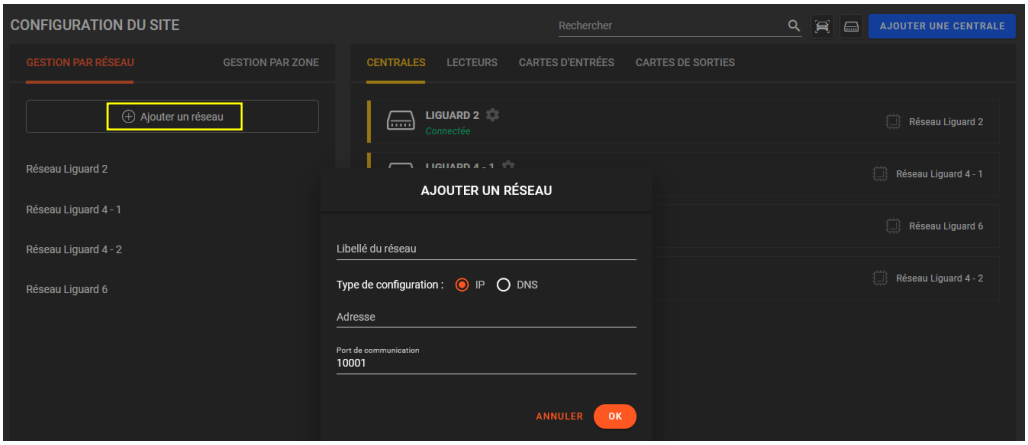


Fig.8 : Ajout de réseau.

Donner un nom au réseau, choisir ensuite entre IP ou DNS de la centrale ou interface IP-BUS (disponible depuis le logiciel CONFIG-IP).

Le port par défaut d'une centrale est ***10001***.

Le même principe s'applique dans le cas d'un DNS.

Fig. 9 : Création d'un réseau nommé 'Réseau 1'.

b) *Création d'une centrale*

Une fois que vous avez créé un réseau, vous pouvez ajouter une centrale à ce réseau en cliquant sur « *Ajouter une centrale* » AJOUTER UNE CENTRALE.

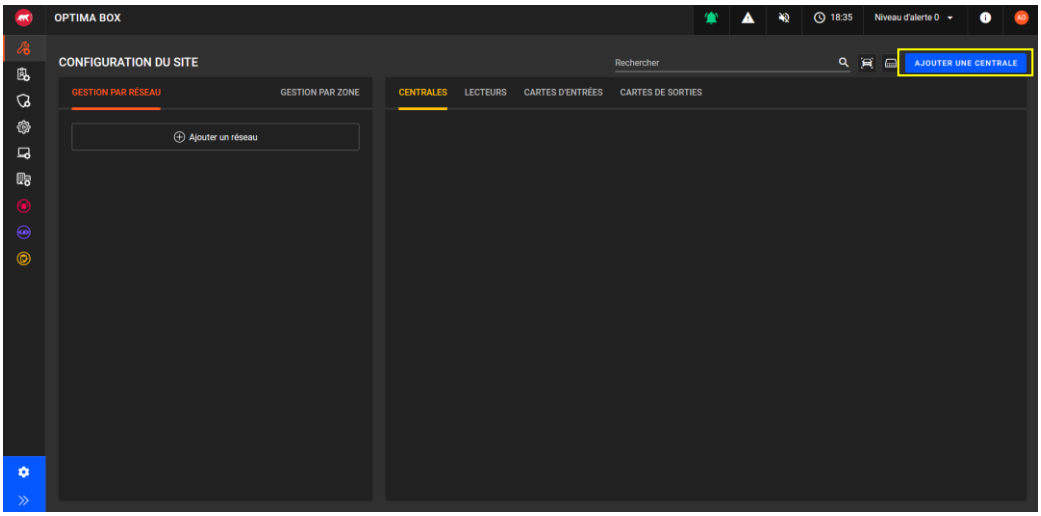


Fig. 10 : Ajout de centrale.

Sélectionnez le réseau existant ou bien ajouter un nouveau réseau si nécessaire.

Fig. 11 : Choix du réseau pour la centrale.

Sélectionnez la *catégorie* de centrale.

Entrez un *nom* pour cette centrale.

Sélectionner l'*adresse bus*.

- L'adresse bus est '1' pour les centrales ayant nativement un module IP (LDMV2®, LIGUARD, C4PlusFX®-IP).
- L'adresse bus est entre 1 et 10 pour les centrales en 'version bus' (voir le manuel de ces centrales pour savoir comment paramétrer l'adresse bus).

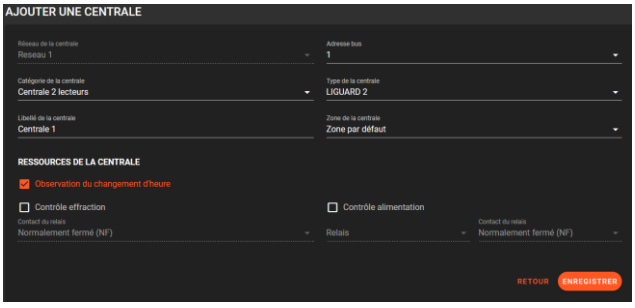


Fig. 12 : Entrez les paramètres de la centrale.

La centrale communique avec OPTIMA® lorsqu'elle est sous tension et si elle déjà connectée au réseau..

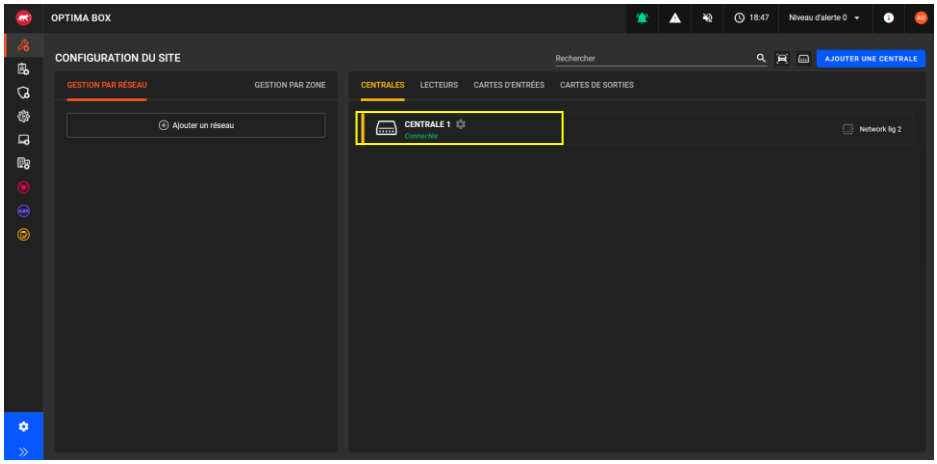


Fig. 13 : Vérification la communication de la centrale.

c) *Configuration des lecteurs*

Lorsqu'une centrale est créée, ses lecteurs le sont aussi automatiquement.

Par défaut, les lecteurs sont paramétrés en mode Wiegand/Wiegand automatique.

Pour modifier le type d'un lecteur, cliquez sur la centrale pour déployer les lecteurs, puis un clic gauche pour choisir '*Configuration du lecteur*'.

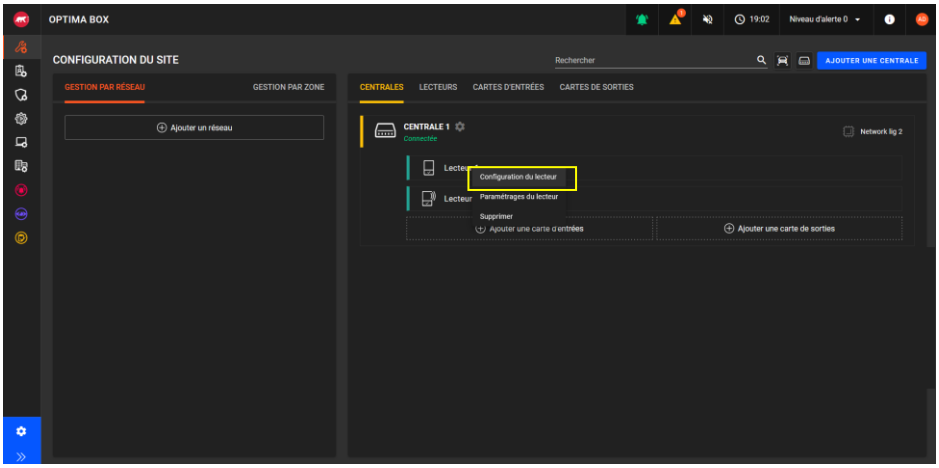


Fig. 14 : Configuration du lecteur « Lecteur 1 ».

Sélectionnez ensuite le type de lecteur dans la liste déroulante (ici lecteur en Wiegand automatique).

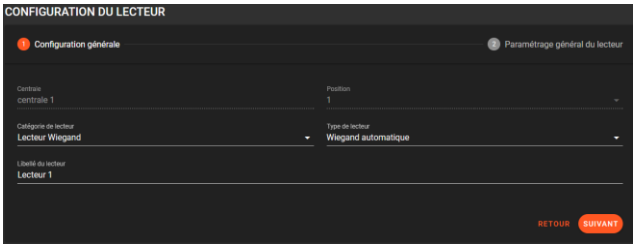


Fig. 15 : Configuration générale du Lecteur 1.

Sélectionner le type de lecteur (décimal).

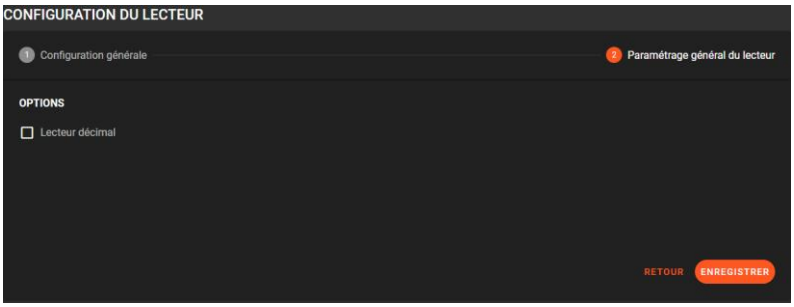


Fig. 16 : Paramétrage général du lecteur.

Pour un lecteur biométrique, choisissez le type ‘Lecteur d’empreintes » et saisissez le numéro de série figurant au dos du lecteur (ou appui simultané sur les 2 touches autour de l’écran pour un lecteur SOWIT).

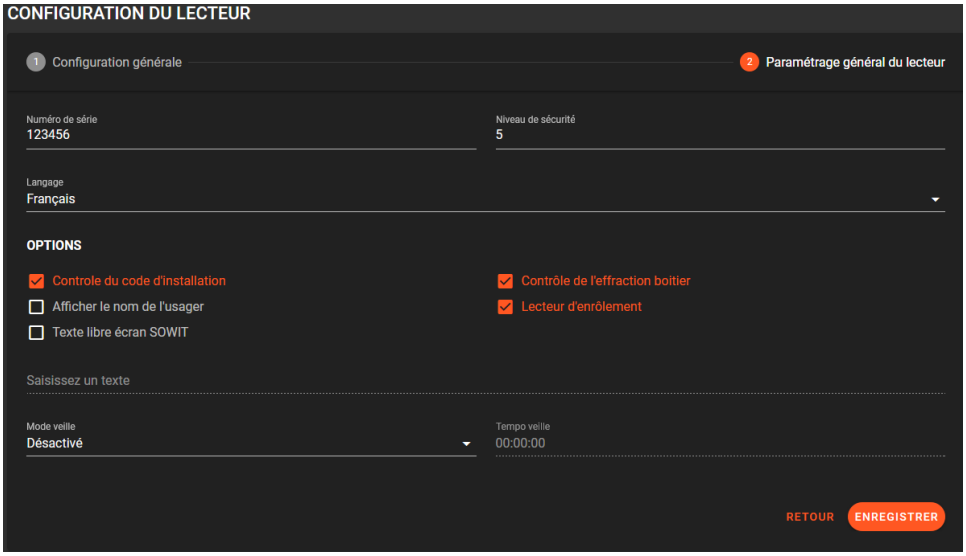


Fig. 17 : Paramétrage lecteur biométrique.

A la suite du paramétrage du lecteur s’ouvre la configuration de celui-ci :

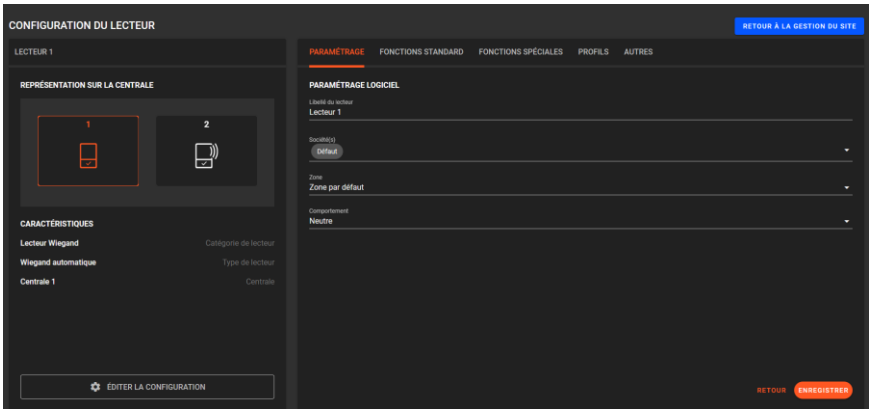


Fig. 18 : Paramétrage lecteur.

Voici le détail de toutes les fonctionnalités associés aux lecteurs :

1- Paramétrage

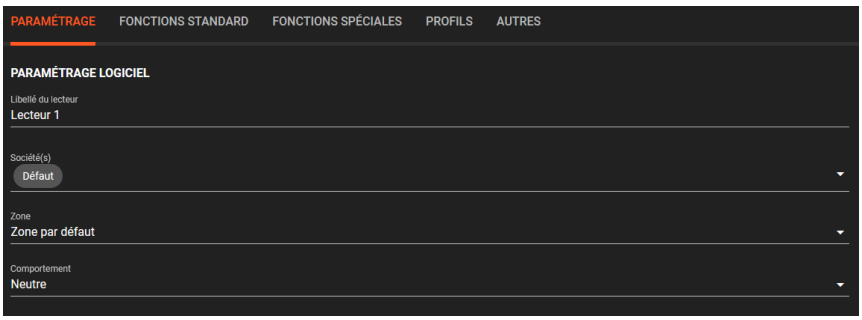


Fig. 19 : Paramétrage logiciel du lecteur.

Ici vous pouvez :

- Saisir le nom de votre lecteur
- Choisir la société associée à celui-ci.
- Sélectionner la zone correspondante au lecteur.
- Configurer son comportement: Neutre/Entrée/Sortie (nécessaire pour l'occupation de zone et la fonction Anti-Passback).

2- Fonctions standard

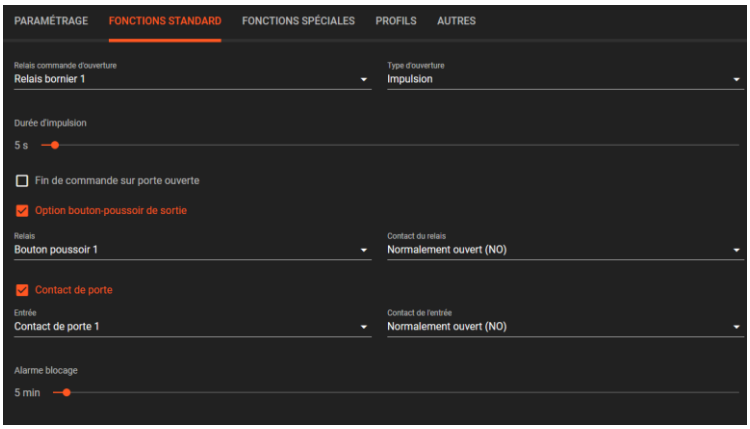


Fig. 20 : Fonctions standard du lecteur.

Vous pouvez configurer les fonctions générales du lecteur en terme de :

- Choix du relais commandé par le lecteur
- Type d'ouverture (impulsion ou alternée)
- Le délai d'ouverture d'impulsion

L'option « **Fin de commande sur porte ouverte** » provoque la fin de l'impulsion à la détection de la fermeture de porte à travers le contact de porte (si connecté).

L'option « **Bouton poussoir de sortie** déclenche l'impulsion sur détection d'une entrée à choisir (en NF ou NO)

L'option « **Contact de porte »** permet de surveiller une effraction de porte si l'entrée choisie est activé sans autorisation sur la porte (en NF ou NO). En général on choisira l'entrée Contact de porte correspondante au lecteur concerné.

L'option **« Alarme blocage »** détecte la présence d'un blocage de porte si le délai est supérieur au délai indiqué (entre 1 et 255 min)

3- Fonctions spéciales

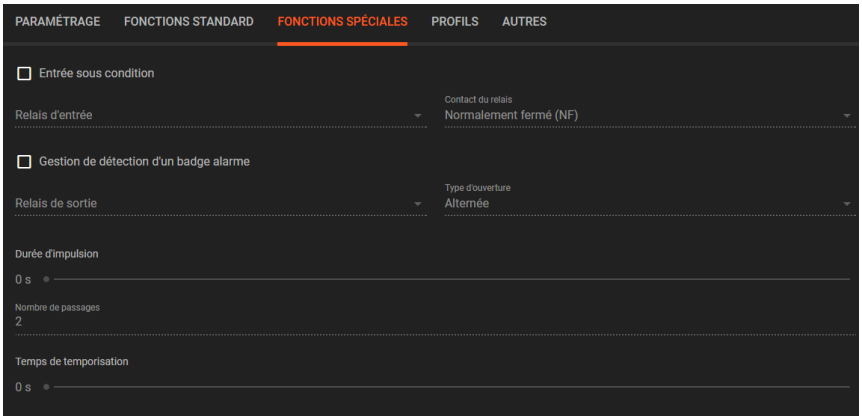


Fig. 21 : Fonctions spéciales du lecteur.

Il est possible ici d'activer l'option **« Entrée sous condition »** qui rajoute une condition d'accès au lecteur sur activation d'une entrée à choisir (en NO ou NF). En général on choisira l'entrée sous condition correspondant au bornier du lecteur utilisé.

L'option « *Gestion de détection d'un badge alarme* » permet de déclencher un évènement d'alarme au passage successif d'au moins deux passages d'un badge alarme sur le lecteur. On peut également sélectionner la sortie à activer (en alterné ou en impulsion).

4- Profils

On choisit le comportement du lecteur pour chaque niveau d'alerte.

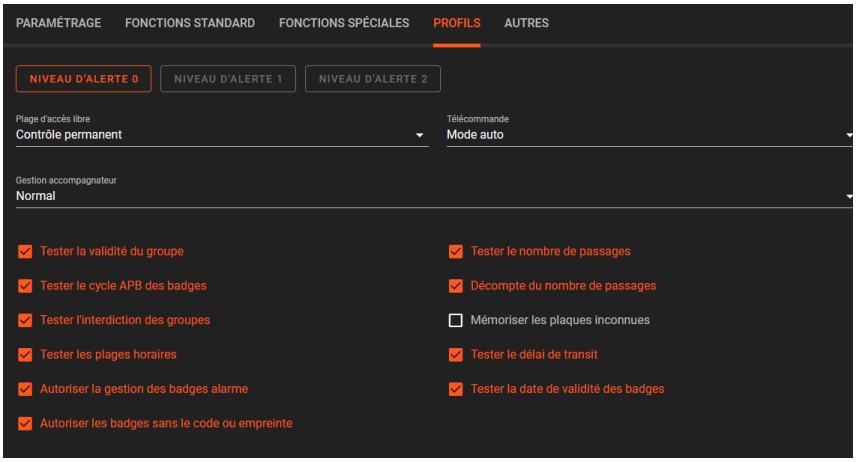


Fig. 22 : Profils du lecteur.

- La **Plage d'accès libre** pour laquelle le lecteur autorise les accès (accès permanent par défaut).
- La commande d'ouverture (**Télécommande**) est en Mode auto par défaut. Il est possible de sélectionner en ouverture maintenue ou en fermeture maintenue afin de commander le relais selon le niveau d'alerte en cours.
- Option **« Gestion accompagnateur »** permet de sélectionner le mode d'accompagnement (normal, accompagnateur toujours refusé ou accompagnateur toujours accepté).
- Les autres options concernent le comportement du lecteur au passage des badges :
    - Tester la validité du groupe
    - Tester le cycle APB des badges
    - Tester l'interdiction des groupes
    - Tester les plages horaires
    - Autoriser la gestion des badges alarme
    - Autoriser les badges sans le code ou empreinte
    - Tester le nombre de passages
    - Décompte du nombre de passages
    - Mémoriser les plaques inconnues
    - Tester le délai de transit
    - Tester la date de validté des badges

5- Autres

Gérez la fonction accompagnateur et le raccordement du lecteur.

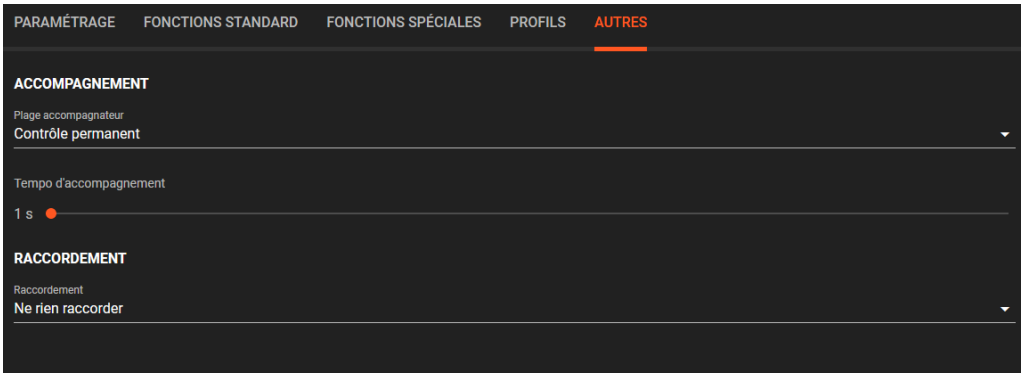


Fig. 23 : Fonction accompagnateur et raccordement clavier.

- **Accompagnement**

Sélectionner la plage horaire pendant laquelle l'acccompagnateur est accepté, ainsi que le temporisation pour passer le badge de l'accompagnateur (de 1 à 255 sec)

- **Raccordement**

Définissez ici la gestion du clavier intégré au lecteur.

2) Mise à jour du matériel

Il est possible de mettre à jour les lecteurs et centrales en choisissant le fichier contenu dans l'OPTIMA® ou bien depuis un fichier à importer.

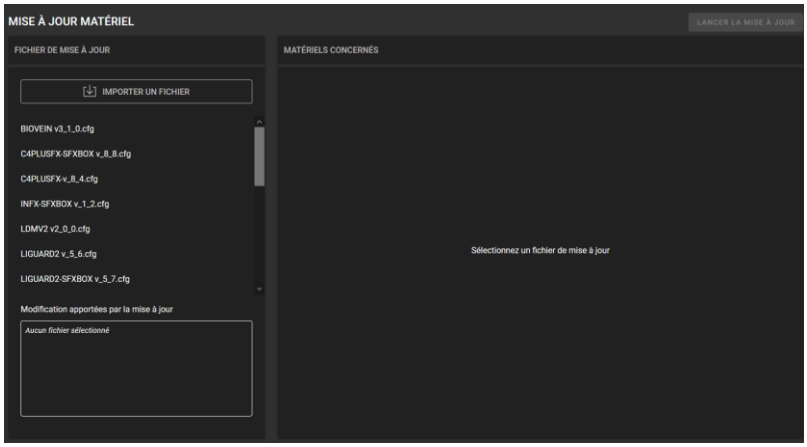


Fig. 24 : Mise à jour du matériel.

Le choix d'un fichier propose automatiquement la liste des matériels afin de lancer la mise à jour.

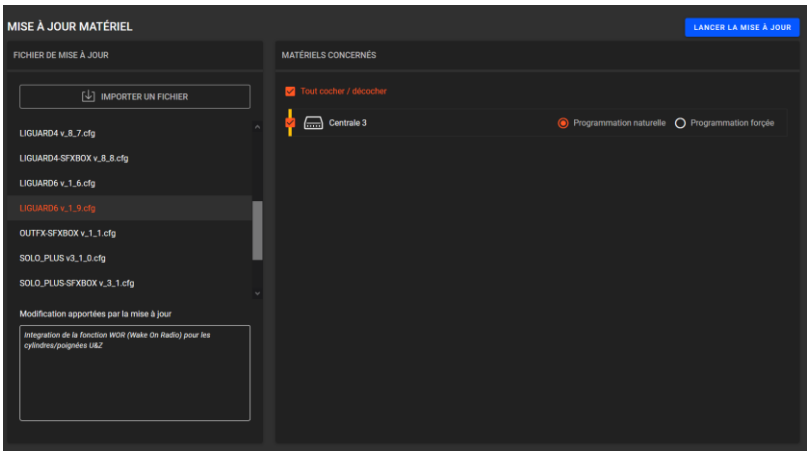


Fig. 25 : Liste du matériel à mettre à jour.

Voici un exemple de mise à jour de la centrale LIGUARD 6 :

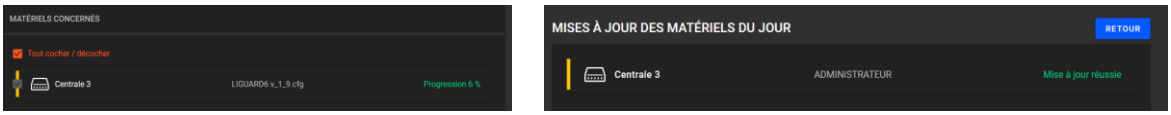


Fig. 26 : Mise à jour de centrale.

REMARQUE : Il est possible de lancer plusieurs mises à jour en simultané pour les LIGUARDX.

3) Code site

Les codes site fournissent un niveau supplémentaire de sécurité par rapport à un site n'utilisant que le numéro du badge pour identifier les usagers.

Lorsqu'une installation utilise les codes site, le système vérifie d'abord le code site du badge pour s'assurer que le badge appartient bien à ce site. Il vérifie ensuite le numéro du badge pour identifier la personne.

Le code site peut être configuré pour chaque centrale. Ainsi, un code site différent peut être paramétré pour chaque société lors de la gestion multi-société.

Plusieurs codes site peuvent être paramétrés sur chaque centrale. Dans le cas d'une gestion multi-sociétés, les points d'accès communs auront les codes sites de toutes les sociétés créées.

Pour ajouter un code site, vous pouvez ajouter un code site individuellement, ou bien pour l'ensemble des centrales selon la sélection située à gauche de chaque centrale en appuyant sur le bouton « *Ajouter un code site* » AJOUTER UN CODE SITE.

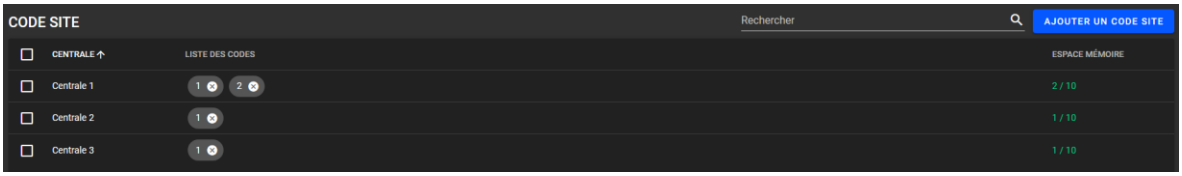


Fig. 27 : Le code site '1' a été ajouté à toutes les centrales, « 2 » pour Centrale 1 uniquement.

4) Codes distributeur

Les codes distributeur fournissent un niveau de sécurité supplémentaire pour l'identification d'un badge.

Lorsqu'un code distributeur est utilisé, le système vérifie le code distributeur, puis le code site (si activé) et enfin le numéro du badge.

02- Droits d’accès

Ce menu est essentiel pour attribuer les droits des utilisateurs sur chaque lecteur, en fonction d’une plage horaire si nécessaire.

1) Plages horaires

Il y deux sortes de plages horaires, « utilisateurs » et « automatismes ».

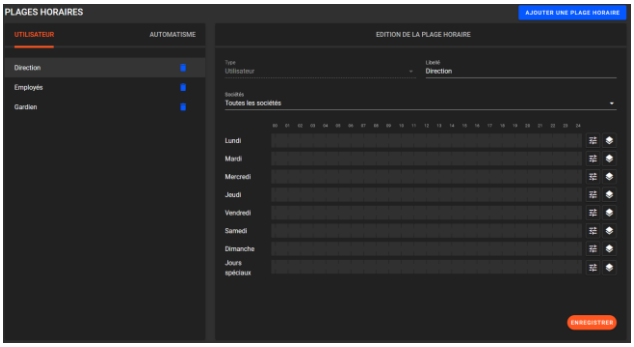


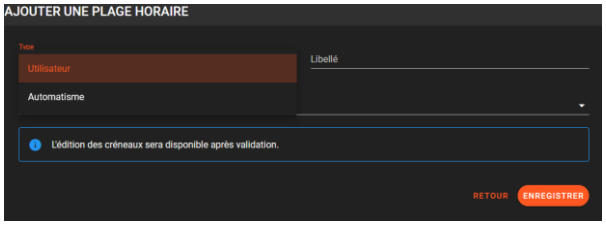
Fig. 28 : Liste de plage horaires.

Plage horaire utilisateurs

Une plage horaire utilisateurs est utilisée pour définir des périodes pendant lesquelles des utilisateurs ou groupes d’accès sont autorisés ou interdits.

Vous pouvez créer jusqu’à 64 plages horaires et 10 périodes par jour de minimum 5 min par période.

Pour ajouter une nouvelle plage horaire cliquez sur AJOUTER UNE PLAGE HORAIRE.



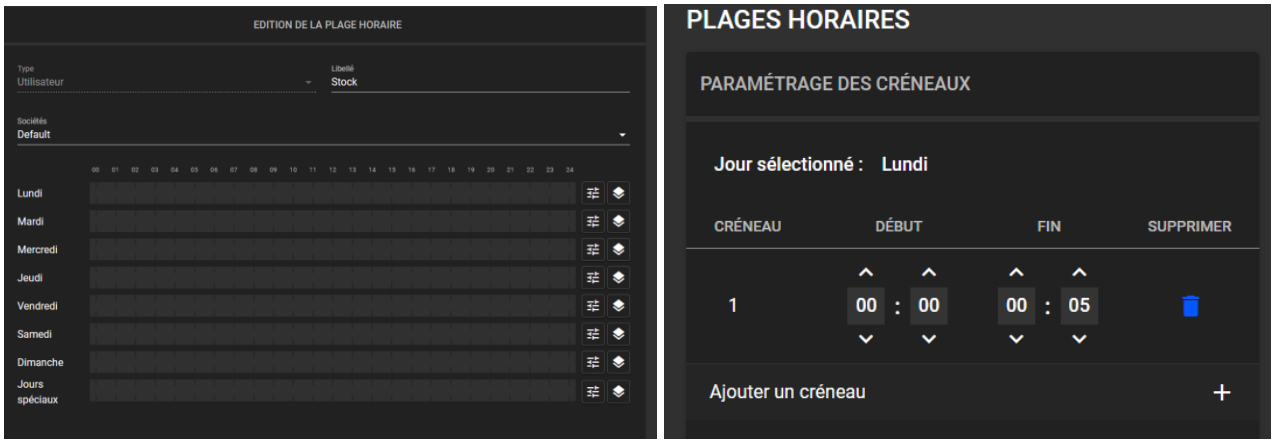


Fig. 29 : Ajout de plage horaire utilisateur.

Les créneaux de chaque journée peuvent être recopiées grâce à l'outil  permettant de Couper/Copier/Coller/Appliquer à tous les jours/ Appliquer à tous les jours ouvrés/ Appliquer au week-end ou Appliquer aux jours spéciaux.

Plage horaire automatismes

Le principe est le même que pour les plages horaires utilisateurs.

La différence est qu'elle s'applique aux automatismes ou aux lecteurs.

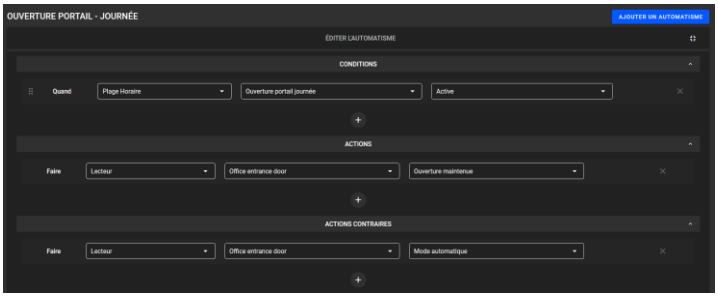


Fig. 30 : Exemple d'association de plage horaire dans un automatisme.

L'onglet *Profil* de chaque lecteur permet de piloter le relais associé en sélectionnant la plage horaire automatisme dans le champ « Plage d'accès libre ».

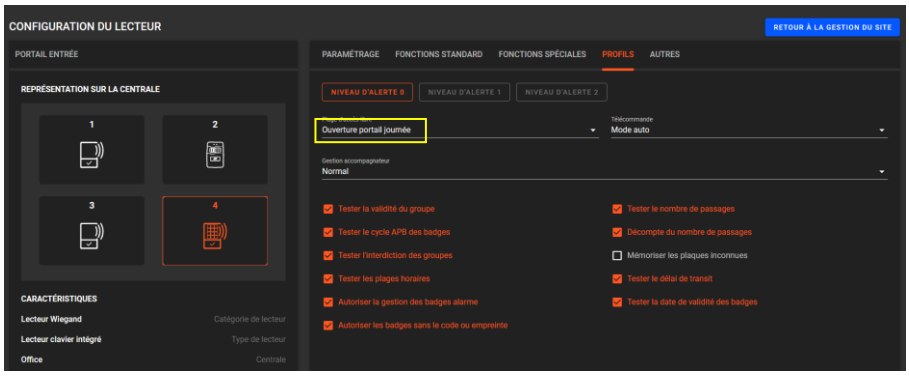


Fig. 31 : Ex d'association de plage horaire dans un lecteur.

Les créneaux de chaque journée peuvent être recopiées grâce à l'outil « *Recopier la plage* »  permettant de Couper/Copier/Coller/Appliquer à tous les jours/ Appliquer à tous les jours ouvrés/ Appliquer au week-end ou Appliquer aux jours spéciaux.

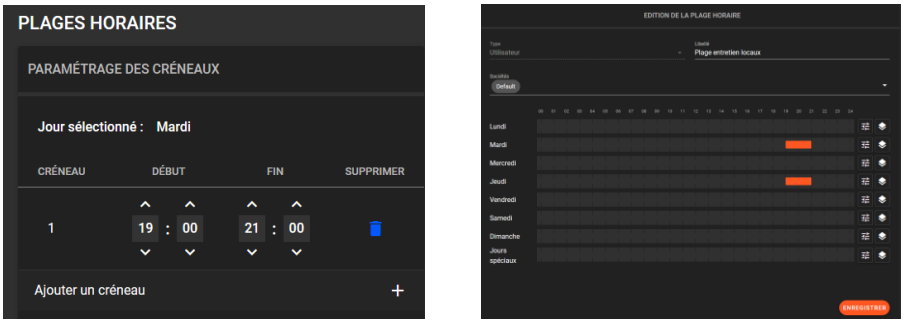


Fig. 32 : Paramétrage des créneaux horaires.

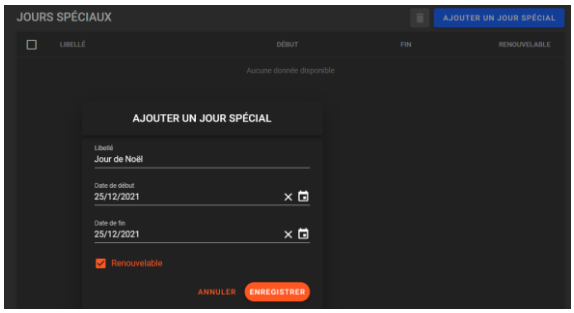
Dans les 2 exemples ci-dessus, le portail va s'ouvrir pendant la période de la plage horaire d'automatisme, et va se refermer automatiquement hors période. L'accès reste disponible hors période par l'autorisation d'un usager sur ce lecteur.

2) Jours spéciaux

Les jours spéciaux doivent être définis au préalable afin de restreindre/autoriser les accès sur un jour ou une période entière. (ex : accès non autorisé pour les jours de fête, ou accès autorisé pour journées porte ouverte).

Vous pouvez créer jusqu'à 32 périodes de jours spéciaux sans limite sur le nombre de jours par période.

Cliquer sur le bouton « *Ajouter un jour spécial* » AJOUTER UN JOUR SPÉCIAL et saisir la période (de 1 à plusieurs jours).



Le jour spécial est renouvelable en cochant l'option adéquate.

Fig. 33 : Ajout d'un jour spécial (renouvelable) pour la journée de Noël.

3) Groupes d'accès

Les groupes d'accès sont essentiels pour définir les droits d'accès aux lecteurs à une liste de personnes.

Vous pouvez créer jusqu'à 1024 groupes d'accès.

Pour rajouter un groupe d'accès, cliquez sur le bouton « Ajouter un groupe d'accès » AJOUTER UN GROUPE D'ACCÈS afin de lui associer les lecteurs correspondants.

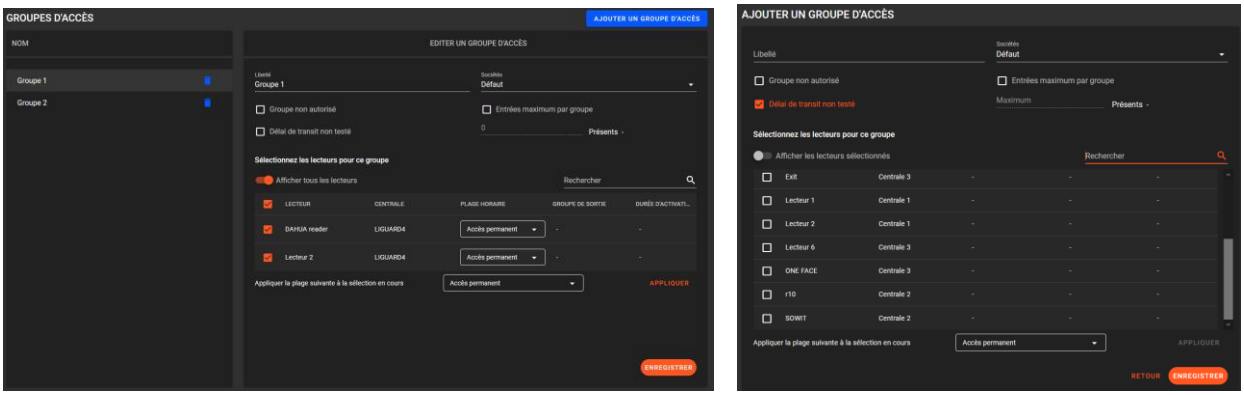


Fig. 34 : Edition de groupe d'accès-Sélection des lecteurs.

Agrandissez la fenêtre d'édition des groupes d'accès en appuyant sur « Agrandir » .

4) Groupes d'entrées/sorties

Constituez des groupes d'entrées et des groupes de sortie en rapport avec les cartes d'entrées et de sorties connectées à votre installation.

Ce menu vous permet d'afficher/éditer vos groupes d'entrées et de sorties.

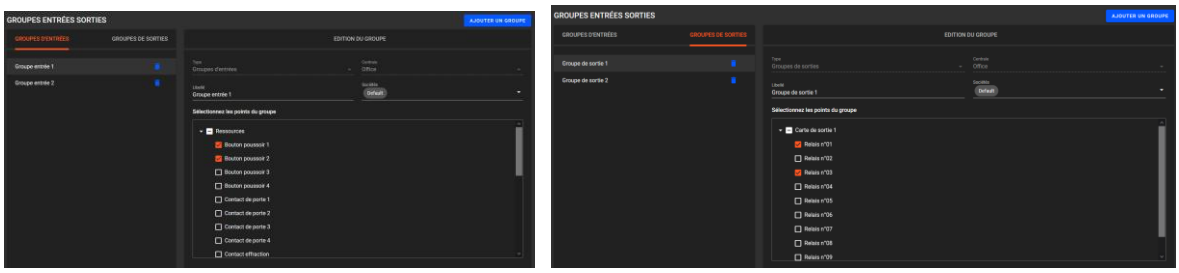


Fig. 35 : Edition de groupe d'entrées et des groupes de sorties.

5) Fonction complémentaire des zones

Configurez la fonction Anti-passback, Anti-timeback et le délai de transit pour chaque centrale individuellement ou bien pour l'ensemble des centrales du site.

Anti-passback :

Pour que la fonction Anti-passback (APB) fonctionne, il faut au moins qu'un lecteur soit défini en entrée et un lecteur défini en sortie.

Il est alors interdit à un même badge de passer deux fois sur une entrée sans être passé par une sortie entre les 2 entrées, ou, inversement de passer deux fois sur une sortie sans être passé sur une entrée.

Anti-Timeback :

La fonction « Anti-timeback » (ATB) permet de réaliser un anti-passback en fonction d'une durée de temps à définir. Un même badge ne peut pas accéder deux fois de suite sur un même accès, sans laisser s'écouler un certain temps, défini par la durée de reset APB.

Dans ce cas les lecteurs définis en entrée peuvent suffire.

Ce temps peut être réglé de 0 à 254 minutes. Lorsque le temps est paramétré à 0, l'anti-timeback est désactivé, et c'est l'anti-passback qui fonctionne.

Les fonctionnalités Anti-passback et Anti-timeback fonctionnent indépendamment sur chaque centrale si au moins une centrale n'a pas l'APB activée.

Pour activer l'APB global à toutes les centrales, il est nécessaire d'appliquer l'option d'Anti-passback à toutes les centrales depuis le menu « *Traitement groupé sur les centrales* »  .

Dans ce cas le logiciel OPTIMA traite les fonctionalités APB et ATB.

Délai de transit :

La fonction « Délai de transit » permet de limiter le temps dont les personnes disposent pour aller d'un accès à un autre. Au delà de ce temps, les utilisateurs sont refusés sur le second accès et sont contraints de retourner vers le premier.

6) Ajout rapide d'usagers

Configurez les méthodes d'ajout des identifiants et les profils des droits d'accès afin d'ajouter rapidement les usagers à votre contrôle d'accès.

03- Paramètres de contrôle

1) Zones contrôlées

Définissez vos zones contrôlées en choisissant les lecteurs d'entrée et de sortie.

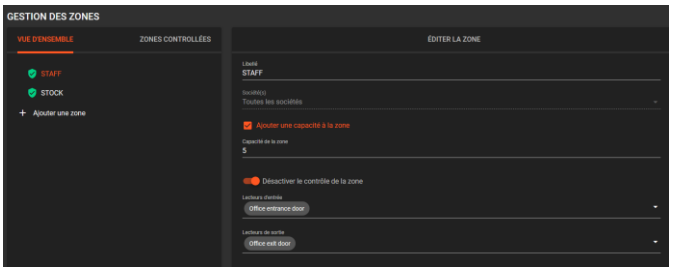


Fig. 36 : Edition de la zone « STAFF ».

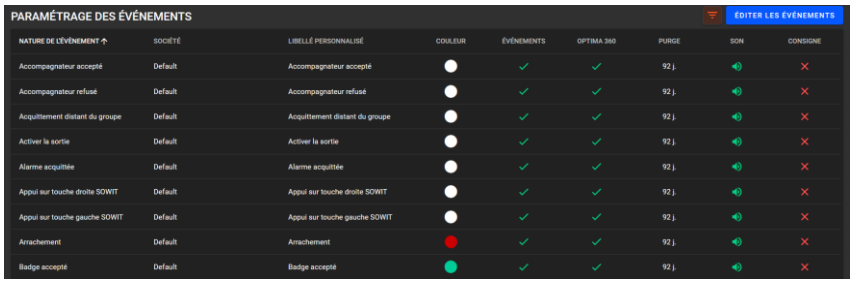
Définissez une capacité à la zone pour obtenir leurs taux d'occupation.

2) Paramètres des évènements

Paramétrez les évènements générés par le contrôle d'accès.

Chaque évènement peut être filtré dans la liste des évènements du contrôle d'accès et de la supervision OPTIMA 360. Il peut générer un son, afficher un « pop-up » et être affiché avec une couleur préétablie.

On peut également définir le temps pendant lequel chaque type d'événement est conservé dans la base de données (**92 jours par défaut**, configurable jusqu'à 366 jours).



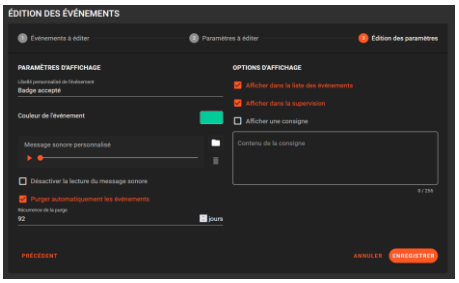


Fig. 37 : Liste de paramétrage des évènements, édition de l'évènement « Badge accepté ».

04- Automatismes

Les automatismes sont des scénarios utilisés pour déclencher des actions en fonction de conditions préétablies.

1) Automatismes de centrale

Ces automatismes s'exécutent directement par la centrale, autorisant un fonctionnement autonome.

Appuyez sur « *Ajouter un automatisme* » AJOUTER UN AUTOMATISME afin de choisir la condition (2 maximum) et l'action (2 maximum).

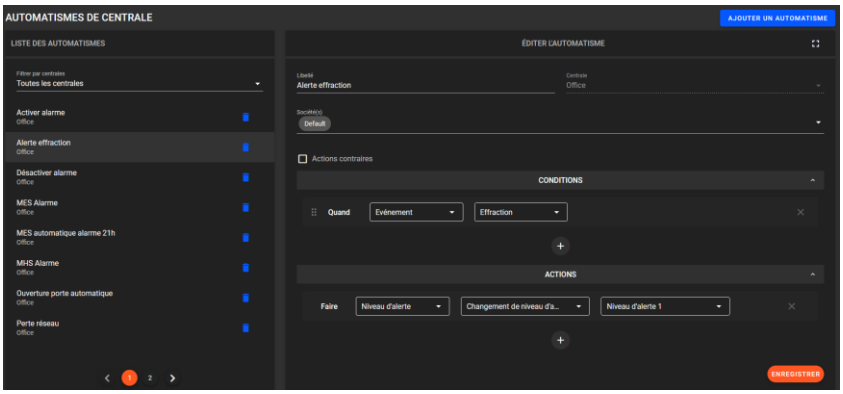


Fig. 38 : Ex. d'automatisme de centrale qui change le niveau d'alerte en cas d'effraction.

Agrandissez la fenêtre d'édition en appuyant sur « *Agrandir* » .

Vous pouvez configurer une action contraire en cochant la case correspondante.

Celle-ci est valable pour une condition avec plage horaire d'automatisme (plage horaire valide/hors plage horaire) ou selon le statut d'une entrée (actif/inactif).

2) Automatismes logiciel

Ces automatismes sont exécutés par l'OPTIMA® et proposent une plus grande richesse de fonctionnalités que les automatismes de centrale.

Appuyez sur « *Ajouter un automatisme* » AJOUTER UN AUTOMATISME afin de choisir la condition et l'action.

La temporisation des actions est disponible (désactivée par défaut). Durée de temporisation des actions 0 secondes

Vous pouvez configurer une action contraire en cochant la case correspondante.

Celle-ci est valable pour une condition avec plage horaire d'automatisme (plage horaire valide/hors plage horaire) ou selon le statut d'une entrée (actif/inactif).

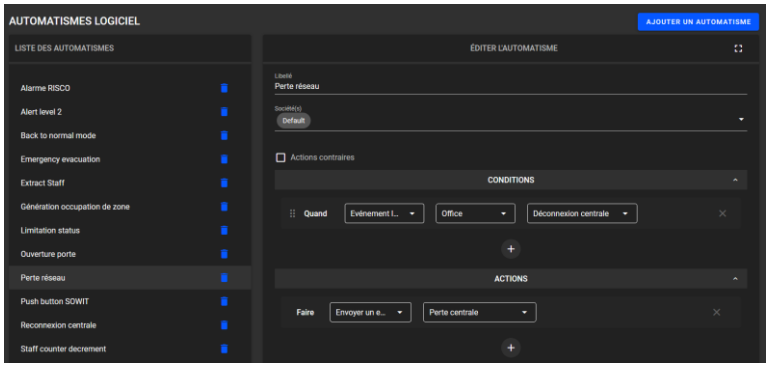


FIg.39 : Ex. d'automatisme logiciel qui envoie un email en cas de déconnexion de la centrale « Office ».

Agrandissez la fenêtre d'édition en appuyant sur .

3) Gestion des compteurs

Gérez des compteurs (de centrale ou logiciel) qui seront repris dans les automatismes de centrales ou logiciels, ou bien dans le cadre d'un affichage dans la supervision.

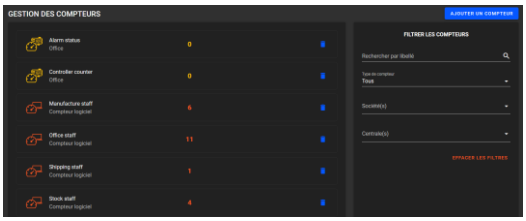


Fig. 40 : Liste des compteurs.

4) Emails

Créez un modèle d'email, en vue d'exploiter un automatisme logiciel pour expédier des données liées au contrôle d'accès.

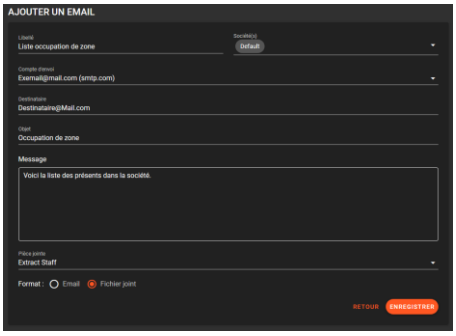


Fig. 41 : Modèle d'email pour recevoir la liste des occupants dans la zone.

5) Consignes

Créez des consignes (pop-up) en vue d'être exploitées par des automatismes.

Fig. 42 : Configuration et affichage de consigne en cas d'effraction.

6) Exports

Créez vos modèles d'exportation de fichier. Les fichiers peuvent contenir au choix :

- La présence des usagers dans les zones prédéfinies
- Les derniers évènements du contrôle d'accès
- Le résultat d'une requête de l'historique avancé dans le corps du mail ou en pièce jointe

Appuyez sur le bouton « *Ajouter un modèle d'exportation* » AJOUTER UN MODÈLE D'EXPORTATION afin d'éditer le modèle d'exportation.

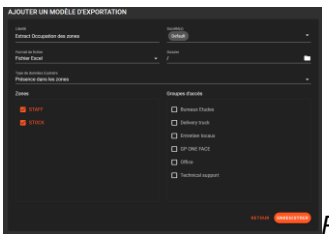


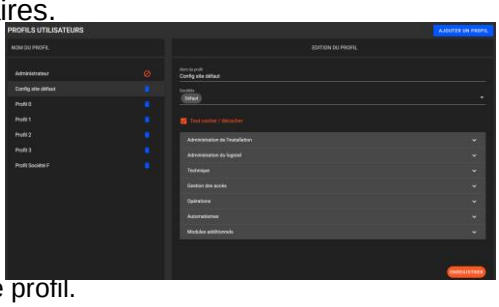
Fig. 43 : Edition du modèle d'exportation.

05- Administration du logiciel

1) Profils utilisateurs

Ce menu sert à la création des droits des utilisateurs du logiciel.

Cliquez sur « *Ajouter un profil* » AJOUTER UN PROFIL pour créer un nouveau profil. Cochez les cases nécessaires.



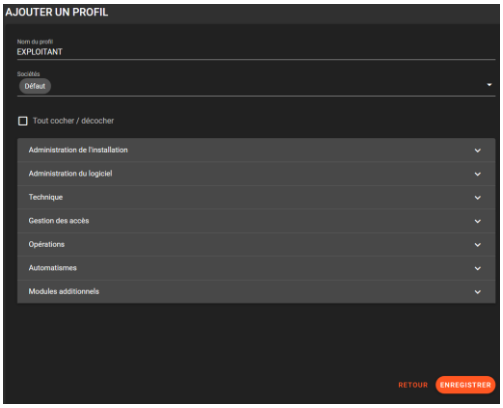


Fig. 44 : Edition de profil.

2) Gérer les utilisateurs

Une fois que vous avez créé les profils, vous pouvez créer les comptes utilisateurs.

Saisissez un nom (obligatoire), un prénom, sélectionnez le profil, puis définissez un mot de passe :

il doit contenir au moins : 1 lettre majuscule, 1 lettre minuscule, 1 chiffre et un caractère spécial [! @ # $% ^ & *]

Note : Un seul utilisateur peut se connecter à l'OPTIMA® à la fois.

Si un utilisateur se connecte après une session déjà ouverte, la session précédemment ouverte sera déconnectée.

Fig. 45 Gestion des utilisateurs.

REMARQUE : Un profil peut être attribué à un ou plusieurs utilisateurs du logiciel.

Vous pouvez créer autant de profils que vous le souhaitez.

Pour utiliser la fonction « Double authentification par email », il est nécessaire de valider la vérification du compte d'envoi email « Double authentification ».

3) Compte d'envoi d'emails

Ajoutez et configurez un compte d'envoi d'emails afin d'exploiter les fonctionnalités telles que :

- Automatisme : envoi d'emails depuis les automatismes logiciels

- Vérification des emails : nécessaire pour les fonctionnalités Mot de passe oublié et Double authentification (A2F)
- Mot de passe oublié : nécessaire pour les fonctionnalités Mot de passe oublié et Double authentification (A2F)
- Double authentification : accès à l'interface OPTIMA® avec saisie obligatoire du mot de passe de connexion et du code de vérification fournie par email
- Envoi des QR codes : envoi des QR codes des usagers par email

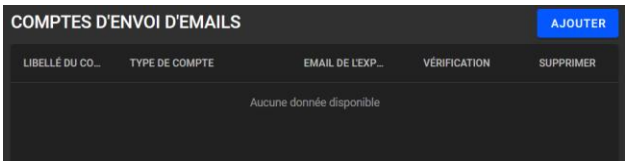


Fig. 46 Gestion/Edition des comptes d'envoi d'emails.

4) Configuration SSO Azure AD

Complétez les données pour assurer la synchronisation avec votre compte Azure AD.

Plus d'informations .

5) Sécurité de l'application

Activer la fonction du mot de passe oublié seulement si un compte d'envoi d'emails « Mot de passe oublié » a été ajouté et validé.

6) Système tiers

Configurez les accès pour les systèmes tiers tels que :

- API : interface de programmation d'application avec le système OPTIMA®
- Optima Access : interface d'affichage de données lecteur
- Optima Time : interface d'affichage de données de pointage (module additionnel One Time)
- ONE Pass Tablet : interface d'affichage de données d'actualisation (module additionnel One Pass)

7) Paramètres réseau

Paramétrez les propriétés réseau de votre OPTIMA®.

Le port HTTP(s) vous permet la redirection de l'accès à l'OPTIMA®.

8) Sécurisation HTTPS

Deux méthodes s'offrent à vous :

- Importation d'un certificat auto-signé généré par OPTIMA®.

  Dans ce cas le 1er accès à la page OPTIMA® vous prévient que la page n'est pas certifiée avec une autorité valide : appuyez sur Avancés/ Continuer sur cette page.

- Importation d'un certificat signé : merci de vous rapprocher de votre administrateur réseau pour configurer et obtenir le certificat.

Veuillez suivre les instructions disponibles dans ce document.

Le port d'accès à la page OPTIMA® devient nécessairement le port 443.

Celui-ci est non modifiable.

9) Paramètres Date/heure

Réglez la date et l'heure manuellement ou en fonction de la date et de l'heure de votre région. Vous avez également la possibilité de configurer un serveur NTP si l'OPTIMA est connectée à Internet.

L'horloge OPTIMA est synchronisée avec l'horloge du PC Windows ou est installé OPTIMA Wi ®.

10) Mise à jour

Si l'OPTIMA® est connectée au réseau Internet, une notification de mise à disposition d'une nouvelle mise à jour va apparaitre.

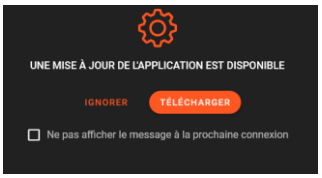


Fig. 47 : Proposition de mise à jour.

Le bouton « *Télécharger* » TÉLÉCHARGER vous dirigera vers la page de téléchargement www.optimabox.fr

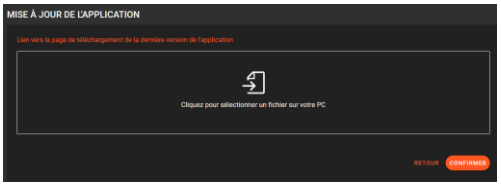


Fig. 48 : Sélection de la mise à jour.

On peut ainsi charger le fichier de mise à jour afin de profiter des dernières fonctionnalités.

06- Administration de l’installation

1) Sociétés

L’OPTIMA® inclut une gestion multi-sociétés.

Il est possible de gérer l'accès aux locaux de plusieurs sociétés ainsi que des accès en communs à travers l’affectation des lecteurs, des badges, etc, aux sociétés.

Par défaut, il n'existe qu'une seule société nommée "Default".

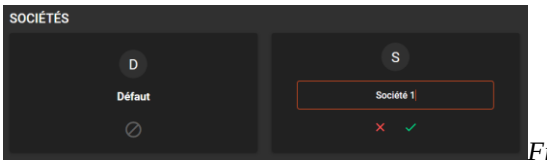


Fig. 49 : Ajout de la Société 1.

Note : Il est possible de la renommer et d'en créer autant que nécessaire.

On retrouve la notion de société dans les menus appropriés, tels que les lecteurs et les badges :

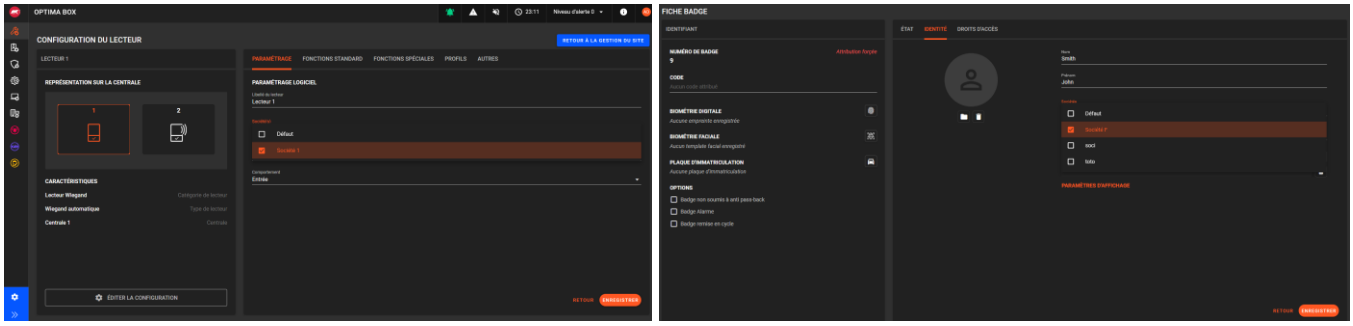


Fig. 50 : Lecteur 1 et badge 9 associés à la Société 1.

Le champ « Société » permet de définir un paramètre supplémentaire et d’indiquer à quelle société appartient l’élément. Certains éléments peuvent appartenir à plusieurs sociétés, comme c’est le cas pour un lecteur d’entrée en commun par exemple.

Le filtrage par société peut s'appliquer aux éléments suivants :

- Automatisme : peut être affecté à une ou plusieurs sociétés.
- Badges : peut être affecté à une ou plusieurs sociétés.
- Carte entrées/Carte sorties : peut être affecté à une ou plusieurs sociétés.
- Compteurs globaux : peut être affecté à une ou plusieurs sociétés.
- Consigne : peut être affecté à une ou plusieurs sociétés.
- Email : peut être affecté à une ou plusieurs sociétés.
- Groupe : ne peut être affecté qu'à une seule société.
- Groupe d’entrées/Groupe de sorties : peut être affecté à une ou plusieurs sociétés.
- Lecteur : peut être affecté à une ou plusieurs sociétés.

- Liste : peut être affecté à une ou plusieurs sociétés.
- Paramétrage des événements : peut être affecté à une ou plusieurs sociétés.
- Plages horaires : peut être affecté à une ou plusieurs sociétés.
- Profil d'utilisateurs : peut être affecté à une ou plusieurs sociétés.
- Zone contrôlée : peut être affecté à une ou plusieurs sociétés.

Répartition des usagers par sociétés

L'activation de la fonction « Répartition des usagers par sociétés »  vous permet de distribuer les usagers uniquement sur les lecteurs correspondants à leur société(s). voir *Guide utilisateur du contrôle d'accès.*

2) Préférences

Ce menu est constitué de 2 onglets.

Le 1er onglet vous permet de gérer votre installation avec les paramètres suivants :

- Le nom de l'installation. Ce paramètre sert à nommer les sauvegardes de votre installation
- Le fond d'écran
- L'icône qui apparait dans le navigateur (favicon)
- Le code installation : celui-ci différencie une installation d'une autre concernant la lecture de badges sur les lecteurs biométriques EDEN INNOVATIONS
- Le nombre d'événements affichés à l'ouverture de la liste des évènements
- L'activation de l'affichage du numéro de badge en Hexadécimal
- L'activation de l'affichage de statistiques de l'installation pour dénombrer les usagers par centrale ou par centrale/lecteur si la fonction « Répartition des usagers par sociétés » est activée
- L'activation du filtrage des événements par sociétés des badges
- Masquer le raccourci vers la liste des évènements
- La désactivation de l'initialisation automatique des centrales
- Désactivation de la gestion du son

Pour les sites dont la connexion aux centrales n'est pas stabilisée, nous préconisons de désactiver l'initialisation automatique des centrales.

Le 2ème onglet « Contacts et liens » vous permet de configurer la carte de contact et les liens utiles disponibles dans la rubrique « Aide logiciel » du menu Aide et information de la partie Exploitation.

3) Modules additionnels

Ce menu liste tous les menus additionnels et permet de les activer.

L'activation des modules additionnels requiert de contacter Eden Innovations par téléphone au (+33) 4 42 24 70 40 ou par mail à contact@eden-innovations.com. Transmettez une copie d'écran avec le nom du module et du code pour obtenir votre clé d'activation.

4) Sauvegarde automatique

Par défaut l'OPTIMA® sauvegarde automatiquement et quotidiennement les 20 dernières configurations du contrôle d'accès dans sa mémoire interne.

Configurez la fréquence de sauvegarde en choisissant l'heure de sauvegarde, la fréquence (jour/semaine/mois) et le nombre de sauvegardes maximum.

En plus de la sauvegarde en interne, Il est possible de sauvegarder sur un support USB connecté à la Box (non disponible pour OPTIMA Wi®) ou de copier les fichiers sur un serveur distant.

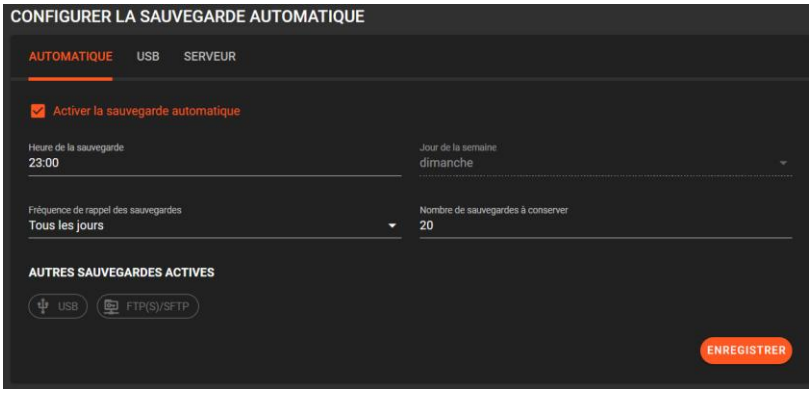


Fig. 51 : Configuration de la sauvegarde automatique FTP.

Il est conseillé de régulièrement sauvegarder manuellement la configuration.

Pour une automatisation des sauvegardes, l'activation de l'option « *Copier sur un serveur FTP distant* » est recommandée. Un serveur FTP est alors nécessaire.

5) Restaurer

Procédez à la restauration à l'origine ou au chargement d'une installation existante.

Fig. 52 : Restaurer à l'origine.

Vous pouvez restaurer une sauvegarde existante depuis la mémoire interne de la box ou d'un fichier contenu dans le poste client.

Fig. 53 : Restauration d'une sauvegarde.

Attention :

- La restauration va écraser la configuration existante.
- Une restauration à l'origine efface toutes les installations existantes.

II- Menu Exploitation

01- Contrôle du site

Ce menu vous propose de visualiser l'ensemble de votre site.

1) Liste des évènements

Affiche en temps réel la liste des évènements du contrôle d'accès.

Le nombre d'évènements affichés est configurable de 100 jusqu'à 1000 évènements.

2) Historique des évènements

Recherchez/exportez directement les événements du contrôle d'accès selon les critères de votre choix.

3) Occupation des zones

Une zone contrôlée est une zone délimitée par un ou plusieurs lecteurs d'entrée et ou plusieurs lecteurs de sortie.

Chaque zone dispose d'un système de comptage des présents et de leur date d'entrée, permettant à chaque instant de connaître le nombre d'occupants dans chaque zone.

Il est aussi possible de consulter le taux d'occupation si une capacité a été indiquée.

On peut également procéder à la remise en cycle des badges qui aura pour effet de vider la zone (le système change le statut du badge de « Entrée » ou de « Sortie » en « Indéterminé »).

Attention : la remise en cycle des badges est susceptible de bloquer temporairement les accès pendant la durée de remise en cycle.

4) Temps de présence

Cet utilitaire affiche les temps de présence des usagers sur la période et la zone choisie.

5) Pilotage des lecteurs

Le pilotage des lecteurs permet de contrôler tous les lecteurs d'un site :

- Ouverture impulsionnelle
- Ouverture maintenue
- Fermeture maintenue
- Mode automatique

6) Requêtes avancées

Cette fonctionnalité filtre les évènements du contrôle d'accès selon vos besoins.

7) Liste des absences

Ce menu vous propose de consulter pour une période donnée la liste des usagers qui ne se sont pas authentifiés sur le site.

02- Gestion des accès

Si vous utilisez des badges de proximité, vous devez créer un badge dont le numéro correspond à l'ID du badge de proximité.

Si vous utilisez la biométrie, vous pouvez utiliser n'importe quel numéro de badge.

OPTIMA® peut gérer jusqu'à 10 000 fiches badges.

Pour qu'un badge autorise un accès, il doit nécessairement être associé à un usager pour lequel on lui attribue un nom (obligatoire), une société, un groupe d'accès et une plage horaire.

Selon le mode d'approche que vous souhaitez, les utilisateurs sont accessibles par badge ou bien par usager :

- Les fiches badge pour ajouter/éditer/supprimer des badges
- Les fiches usagers pour ajouter/éditer/supprimer les utilisateurs

1) Badges

Ce menu permet d'accéder aux fiches badges, la recherche se faisant par leur numéro.

2) Usagers

Les usagers représentent les utilisateurs associés à des badges existants, la recherche se faisant sur le nom, le prenom, ou le groupe d'accès.

3) Profils additionnels

Ce menu vous donne accès à toutes les fiches usagers avec le rappel du profil actif, et de leurs conditions d'activation sur les profil additionnels 1 et 2.

4) *Apprentissage de badges*

Cette fonction permet d'ajouter des badges dans la base de données en les présentant devant un lecteur de l'installation. Cela est utile s'il n'y pas d'ID gravé sur le badge ou pour éviter les erreurs de saisie.

Sélectionner le lecteur à utiliser pour l'apprentissage, puis présentez les badges devant ce lecteur.

5) *Récupération rapide des données*

Cette fonctionnalité vous permet de créer des nouveaux usagers à partir d'un fichier csv ou bien à partir d'un copier-coller de données directement depuis un fichier.

Suivez les étapes d'importation de données, association des champs, et attribution.

Vous avez la possibilité de modifier les usagers s'ils sont déjà existants, d'ajouter les groupes d'accès et plages horaires si manquants. Un bilan des opérations effectués vous est fourni en fin de procédure.

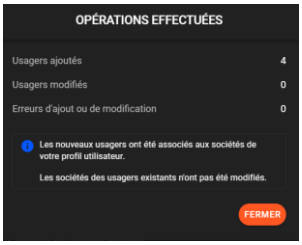


Fig. 54 : Bilan des opérations effectuées.

Remarque : La 1ère ligne du fichier sert de modèle et n'est pas prise en compte dans le cadre de l'importation.

6) *Droits d'accès*

Prenez connaissance des droits d'accès des usagers : il s'agit de l'association entre les usagers et les lecteurs.

7) *Ajout rapide d'usagers*

Cette fonctionnalité vous permet d'ajouter des usagers en quelques clic en sélectionnant la méthode d'ajout et en sélectionnant un droit d'accès parmi des profils prédéfinis.

03- Maintenance technique

1) *Etat des centrales*

Le menu *'Etat des centrales'* donne un aperçu de chacune des centrales du site.

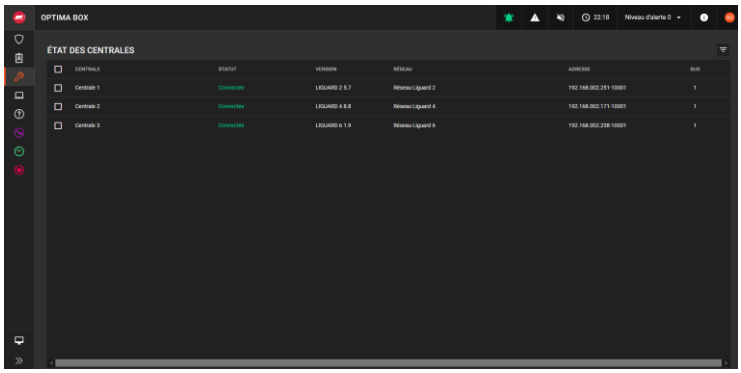


Fig. 55 : Etat des centrales.

- La première colonne affiche le nom de la centrale.
- La colonne *'Statut'* affiche le statut de la centrale.
- La colonne '*Version'* affiche le type de la centrale et sa version. Tant qu'aucune communication entre le logiciel et la centrale n'est établie, la version reste *v 0.0'*.
- La colonne '*Réseau'* affiche le nom du réseau auquel la centrale est attachée.
- La colonne *'Adresse'* affiche l'adresse IP du réseau auquel la centrale est connectée.
- La colonne *'Bus'* affiche l'adresse de la centrale sur le bus. Un bus peut avoir jusqu'à 16 centrales. Les centrales disposant nativement d'un module IP ne peuvent pas être connectés à un bus.

Une centrale peut avoir les statuts suivants :

Nominal : C'est le statut de la centrale lorsque la communication entre le logiciel et la centrale a été établie. *'Nominal'* est le statut dans lequel doit se trouver normalement la centrale.

Initialisation : Une centrale affiche ce statut lorsqu'elle communique pour la première fois avec le logiciel, lors d'un paramétrage, ou lorsque l'utilisateur initialise manuellement la centrale.

Mise à jour : Ce statut s'affiche lorsque le logiciel envoie des données à la centrale. Dans ce statut la centrale ne remonte aucun événement au logiciel.

Occupé : Ce statut s'affiche lorsque la centrale envoie des événements au logiciel.

Réseau indisponible : Ce statut s'affiche lorsque le logiciel ne parvient pas à établir de communication avec l'interface IP (module IP de la centrale ou C485FX-IP pour un bus de centrales).

Déconnectée : Ce statut apparaît lorsque la communication entre le logiciel et l'interface IP a été établie mais l'interface ne parvient pas à communiquer avec la centrale.

Hors connexion : L'utilisateur du logiciel a désactivé la communication entre la centrale et le logiciel. Le contrôle d'accès reste opérationnel.

Version incompatible : Ce statut s'affiche lorsque la version de la centrale est incompatible avec le logiciel. Dans ce cas, la centrale doit être mise à jour.

Type incompatible : Ce statut indique que le type de centrale a été mal déclaré.

Selon l'état de la centrale sélectionnée, on peut :

- Connecter la centrale
- Mettre hors connexion la centrale
- Initialiser la centrale

L'action ***'Mettre hors connexion'*** passe les centrales en mode ***'Hors connexion'***, alors que ***'Connecter'*** rétablit la communication avec les centrales.

Lorsqu'une centrale est ***'Hors connexion'*** la communication entre le logiciel et la centrale est désactivé mais le contrôle d'accès est opérationnel.

2) Marche/Arrêt de la box

Ce menu vous permet de redémarrer le service/redémarrer la Box/arrêter la Box

3) Rapport de configuration

Visualisez et télécharger tous les éléments de votre contrôle d'accès.

04- Utilisation du logiciel

1) Sauvegardes

Les sauvegardes sont réalisées quotidiennement (sauvegarde des 20 derniers jours par défaut).

Il est ici possible de déclencher une sauvegarde dans la mémoire de l'OPTIMA®, ou bien de télécharger sur le poste client.

Fig. 56 : Liste des sauvegardes/Sauvegarde en cours.

REMARQUE :

Nous conseillons vivement de télécharger régulièrement la sauvegarde et la conserver sur un support amovible afin de garder une copie de sécurité.

2) Téléchargement

Ce menu donne accès à l'espace de téléchargement dans lequel les résultats des requêtes d'exportation sont sauvegardées.

3) Journal de bord

Cet utilitaire est un historique des actions qui ont été appliquées sur le logiciel par les utilisateurs.

4) Edition des accès rapides

Organisez les accès rapides de la page principale selon vos préférences.

05- Aide et informations

Aide logiciel

Obtenez dans 4 fenêtres :

- La liste des guides utilisateur
- Les liens utiles
- Le fabricant
- La carte de visite

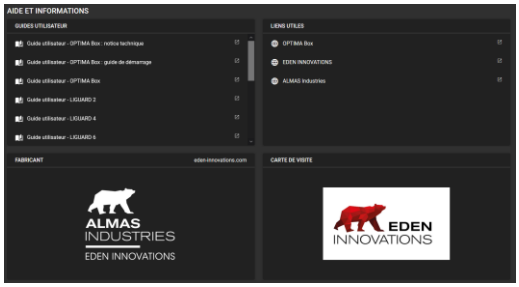


Fig. 57 : Aide et informations.

EDEN INNOVATIONS

Zone Commerciale et Artisanale

670, route de Berre

13510 EGUILLES

France

www.eden-innovations.com