EDEN INNOVATIONS

Contrôle d'accès

OPTIMA Box®

ONE Pass

ONE **PASS**

Table des matières

1- Compatibilités

- OPTIMA Box en version 4.12.0 minimum avec le module additionnel « ONE Pass » activé
- Au moins une interface C485-IP-SSCP connecté au même réseau IP que l'OPTIMA Box
- Au moins un lecteur d'actualisation STID ARC-W33 SSCP connecté en Bus à l'interface C485-IP-SSCP
- Lecteurs compatibles Offline pour standard OSS « standard Offline ».
  Configuration et mise à jour : logiciel et/ou badges de configuration nécessaires par le fabricant
- Tablette ONE Pass constitué par un écran d'affichage et un lecteur d'actualisation connecté à l'interface C485-IP-SSCP (en option)
- Badges MIFARE DESFire® 2K minimum

2- Module ONE Pass

2.1 Activation du module

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

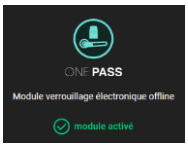


Fig. 1: Module additionnel ONE Pass.

2.2 Accès au module

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

Fig. 2: Accès au module additionnel ONE Pass.

3- Présentation

3.1 Principe de fonctionnement

L'installation en mode Hors ligne (offline) avec ONE Pass de OPTIMA requiert des lecteurs compatibles offline, des badges et un ou plusieurs lecteurs d'actualisation connecté(s) à l'OPTIMA Box.

Les badges sont directement utilisés sur les poignées de porte ou sur les cylindres compatibles en mode offline avec le standard OSS « standard Offline », selon les droits d'accès, les dates validité et les plages horaires autorisées.
Nul besoin de câblage, ni de centrale de contrôle d'accès.

Etant donné que les lecteurs ne se paramètrent pas en ligne afin de délivrer ou non les droits, une fréquence de réactualisation est configurable pour chacun des badges afin d'inciter les détenteurs de badges à mettre à jour leurs droits d'accès.

Lorsque la date d'actualisation est dépassée, les badges ne sont plus autorisés sur tous les lecteurs : il est nécessaire de mettre à jour la date butoir, ainsi que les droits utilisateurs en passant le badge sur un des lecteurs d'actualisation mis à disposition.

En plus de l'actualisation de la date butoir au passage sur le lecteur d'actualisation, les actions suivantes sont réalisées :

- Mise à jour de tous les droits s'ils ont été modifiés entre temps par l'Administrateur
- Récupération des évènements de passage sur les lecteurs
- Effacement des événements enregistrés dans le badge

Le module ONE Pass vous permet de configurer les règles d'actualisation des badges et offre la possibilité de créer ou d'éditer les badges par encodage sur le lecteur d'actualisation.

La technologie choisie pour les badges est MIFARE DESFire®.

3.2 Règle d'actualisations

La fréquence minimum de réactualisation des badges est de 24h.

- Un compromis concernant la fréquence d'actualisation doit être configurée : plus elle est réduite, plus les utilisateurs doivent se réactualiser régulièrement : plus les droits et les évènements sont actualisés fréquemment.
- Les plages horaires permettent de restreindre les accès à des horaires spécifiques pendant la période définie avant la prochaine actualisation.
- Les dates de validités sont configurables pour bloquer l'accès des badges jusqu'à une date donnée.

3.3 Lecteur d'actualisation

Rôle du lecteur d'actualisation

Le lecteur d'actualisation est requis :

- Pour l'administrateur du site afin de créer chaque nouveau badge par encodage avec des droits spécifiques.
- Pour la récupération des évènements de passage du badge.
- Pour le détenteur du badge afin de réactualiser ses droits et la date butoir.
- Pour la récupération des évènements de passage du badge.

Disposition du lecteur d'actualisation

Plusieurs lecteurs d'actualisation peuvent être connectés à l'OPTIMA Box.
Si un seul lecteur d'actualisation est disponible, il faut vous assurer que le lecteur d'actualisation soit toujours physiquement accessible pour mettre à jour les droits et pour récupérer les évènements :

- Le lecteur d'actualisation est situé à l'intérieur d'un bâtiment : l'accès à ce bâtiment doit se faire par un contrôle d'accès standard (online).
- Le lecteur d'actualisation est à l'extérieur d'un bâtiment : les lecteurs donnant accès au bâtiment doivent être proches du lecteur d'actualisation.

Le protocole choisi pour la communication avec le lecteur est SSCP® pour un maximum de sécurisation.

3.4 Badges interdits

Si vous désirez rapidement bloquer l'accès à un badge, et ceci avant la prochaine date d'actualisation (badge volé/perdu, ou autre…), vous pouvez l'inscrire sur liste des badges interdits depuis le logiciel Optima.

Un badge spécifique contenant la liste des badges à interdire l'accès doit être encodé depuis l'interface ONE Pass à l'aide du lecteur d'actualisation.

Ce badge **doit être ensuite passé sur les portes concernées** pour bloquer le ou les badges souhaités pendant une durée d'interdiction à spécifier (jusqu'à 256 badges).

4- Configuration générale

4.1 Configuration des clés du lecteur d'actualisation et des paramètres des cartes

Menu ONE Pass / Configuration générale 

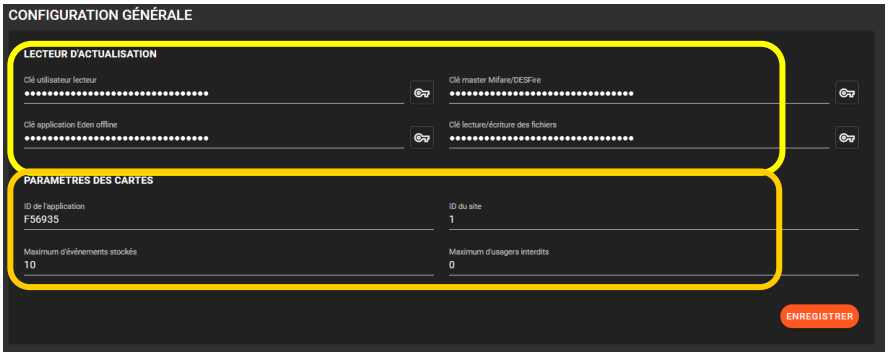


Fig. 3: Configuration générale des lecteurs d'actualisation.

Clés du lecteur d'actualisation
Pour l'ensemble de vos lecteurs d'actualisation, définissez les clés en terme de :

- Clé utilisateur lecteur
- Clé application Eden offline
- Clé master Mifare/DESFire
- Clé lecture/écriture des fichiers

Ces clés doivent être composées de 32 caractères en format hexadécimal.
Les clés assurent l'authentification du lecteur.
Toute perte de celles-ci conduit le retour du lecteur au fabricant pour le réinitialiser en mode usine.

Paramètres des cartes
Pour l'ensemble de vos lecteurs d'actualisation, définissez les paramètres en terme de :

- ID de l'application
- ID du site
- Maximum d'évènements stockés
- Maximum d'usagers interdits (256 maximum)

Notice technique pour le lecteur d'actualisation :
https://www.optimabox.fr/doc/produits/notices/spinel/fr_FR/modules/C485-IP-SSCP.pdf

L'utilisateur ou l'Administrateur doit conserver les valeurs de chaque clé dans un fichier indépendant qui demeure sous sa responsabilité.
EDEN Innovations n'est pas tenu pour responsable en cas de perte.

4.2 Configuration des paramètres des lecteurs d'actualisation

Configurez ici l'adresse IP de chaque interface C485-IP-SSCP (par défaut: 192.168.3.140 / port 10001).
Renseignez également la(les) société(s) associé(s) et les paramètres liés à la gestion de l'arrachement.
Sélectionnez au moins un lecteur en tant que lecteur d'encodage.

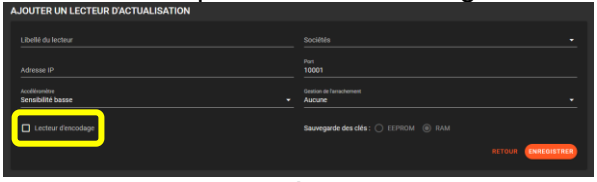


Fig. 4: Configuration des paramètres d'un lecteur d'actualisation.

Gestion de l'arrachement
En fonction des mouvements détectés par l'accéléromètre du lecteur, réglez le niveau de sensibilité pour effectuer les opérations suivantes :

- Aucune (action)
- Réinitialisation du lecteur
- Effacement des clés
- Réinitialisation et effacement des clés

Le réglage de la gestion de l'arrachement est conseillé sur « *Réinitialisation et effacement des clés* » afin d'assurer un maximum de sécurité.
La prochaine connexion au lecteur enregistre les clés nécessaires à sa connexion.

Il faut tenir compte du type de cartes DESfire (1K, 2K, 8K, etc.) en fonction du nombre d'évènements souhaités à enregistrer en considérant le nombre de lecteurs dans votre installation et la fréquence de rafraîchissement.

L'accès aux portes est toujours autorisé mais l'évènement ne sera pas enregistré dans le badge si la taille est insuffisante.

4.3 Etablissement de la connexion avec le lecteur d'actualisation

Après avoir configuré les paramètres du lecteur et des cartes, vous pouvez appuyer sur le bouton TESTER LA CONNEXION afin de vérifier la connexion de chaque lecteur.

La communication avec le lecteur d'actualisation est établie : les diodes « **Receive** » et «**Transmit** » de l'interface C485-IP-SSCP clignotent en permanence.

En cas de défaut de connexion, une notification de déconnexion est affichée dans la barre de menu d'information OPTIMA.

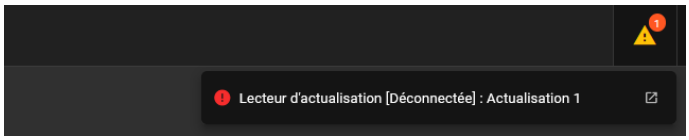


Fig. 5: Notification de déconnexion du lecteur d'actualisation.

5- Configuration des lecteurs et des groupes Offline

L'autorisation sur une porte se fait en donnant l'accès au lecteur **ou** au groupe appartenant à la porte.
La configuration des lecteurs et des groupes offline est uniquement disponible e se connectant à OPTIMA avec le profil utilisateur en mode Administrateur.

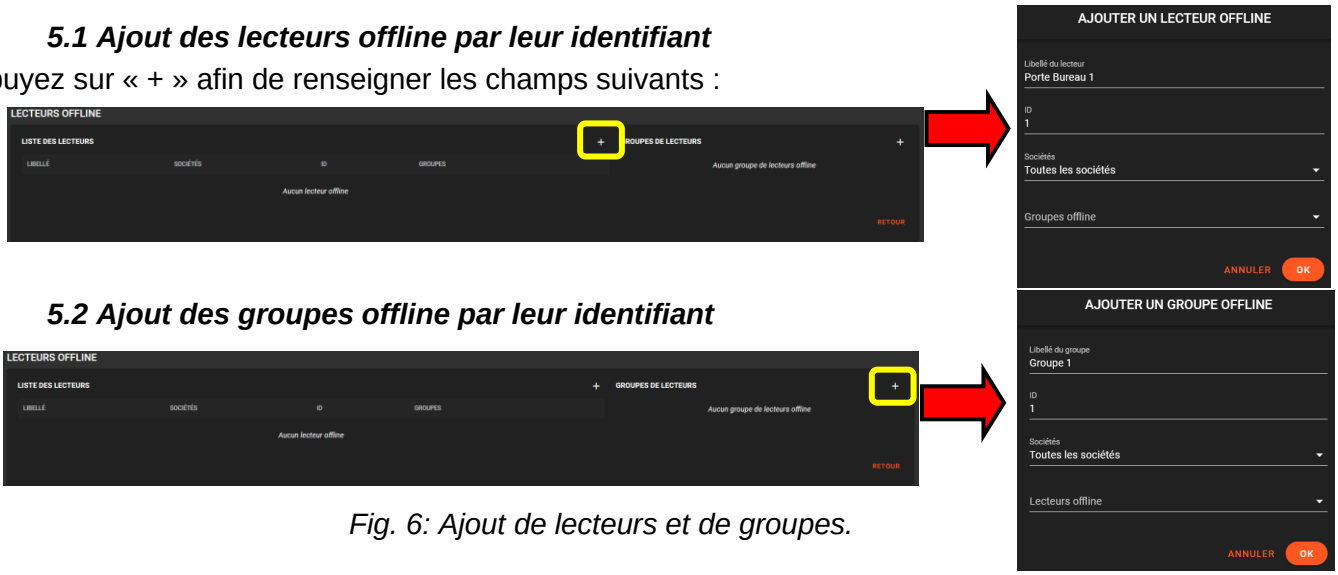
Depuis le menu lecteurs Offline  , ajoutez :

- Les lecteurs correspondants à votre installation en paramétrant leur identifiant.
- Les groupes correspondants à votre installation en paramétrant leur identifiant.

Veuillez-vous reporter à la notice « **Configuration_offline_U&Z** » pour la configuration des lecteurs offline de la marque U&Z disponible ici :
https://www.optimabox.fr/doc/produits/notices/spinel/fr_FR/logiciels/Configuration_offline_U&Z.pdf
La notice « ***Configuration_offline_APERIO*** » pour la configuration des lecteurs offline de la marque APERIO disponible ici :
https://www.optimabox.fr/doc/produits/notices/spinel/fr_FR/logiciels/Configuration_offline_APERIO.pdf
La notice « ***Configuration_offline_domarkaba*** » pour la configuration des lecteurs offline de la marque dormakaba disponible ici :
https://www.optimabox.fr/doc/produits/notices/spinel/fr_FR/logiciels/Configuration_offline_dormakaba.pdf

5.1 Ajout des lecteurs offline par leur identifiant

Appuyez sur « + » afin de renseigner les champs suivants :



5.2 Ajout des groupes offline par leur identifiant

Fig. 6: Ajout de lecteurs et de groupes.

La liste des lecteurs dans le Groupe offline est purement **informative**.
Cette liste est à remplir selon la configuration initiale des lecteurs à un groupe donné.
<u>Les lecteurs appartenant à cette liste ne sont pas autorisés par défaut.</u>

Fig. 7: Configuration du groupe offline 1 avec l'ID de lecteur 1 et 2.

5.3 Suppression des lecteurs

Supprimez les lecteurs en cliquant sur 

La suppression d'un lecteur conduit à la suppression des libellés de lecteurs dans l'historique des évènements. L'accès aux lecteur supprimé n'est plus autorisé après actualisation des droits.

6- Configuration des badges

Ce menu permet d'établir une configuration « type » à appliquer à vos badges, en termes de :

- Droit d'accès
- Type d'évènement à écrire dans le badge
- Règle d'actualisations

6.1 Droits d'accès

Sélectionnez les lecteurs et/ou les groupes autorisés avec les plages horaires offline.
Il est possible d'affecter jusqu'à 4 plages horaires offline par lecteur.

Par défaut, ou bien si aucune plage horaire n'est sélectionnée, l'accès est permanent.

Choisissez pour chacun d'entre eux l'option Mode alterné et/ou Ouverture prolongée.
Pour fonctionner, les options « Modes alterné » (= mode Passage libre permanent) (Toggle mode) et « Ouverture prolongée » (Extended Unlock time) doivent être activées sur les lecteurs concernés.

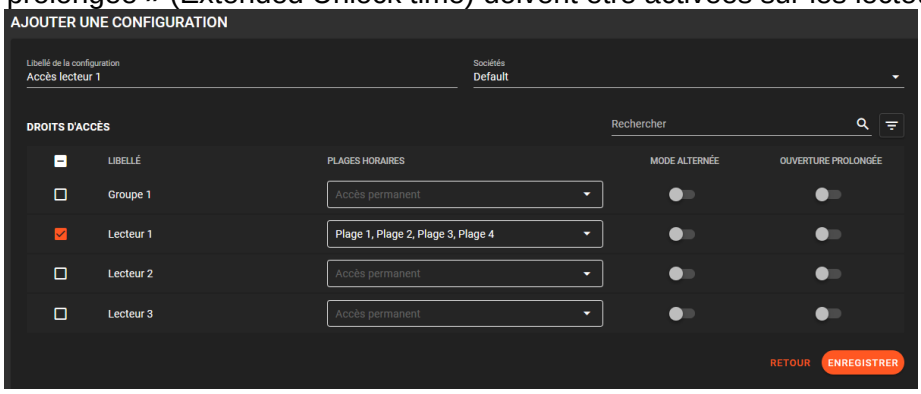


Fig. 8: Configuration des droits d'accès.

6.2 Type d'évènement

Créez des configuration « type » à appliquer à vos badges pour enregistrer ou non certains types d'évènements au passage sur les lecteurs.

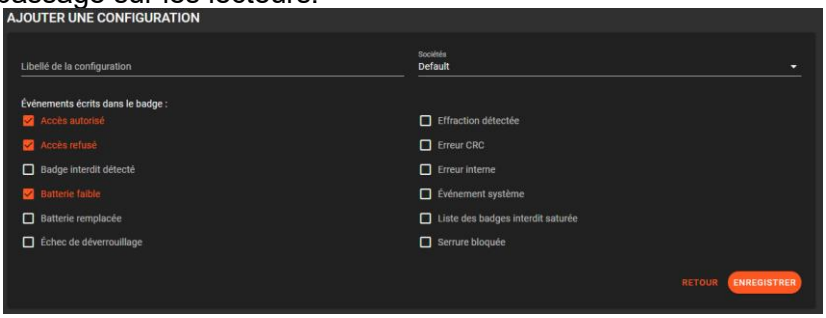


Fig. 9: Types d'évènements à enregistrer dans les badges.

6.3 Règle d'actualisations

La date d'actualisation est le seul moyen de contraindre les utilisateurs de passer leur badge sur le lecteur d'actualisation.
Passée cette date, les badges ne sont plus autorisés sur **tous les lecteurs**.

La fréquence d'actualisation conditionne donc la fréquence de passage des badges sur le lecteur d'actualisation pour renouveler les droits et pour procéder à la récupération des évènements.

- La fréquence la plus réduite possible est de 24h.
- La date est réactualisée en additionnant le nombre de jours/semaines/mois par rapport à la dernière date d'actualisation du badge.

- La récupération des évènements transfère les évènements dans la base de données OPTIMA, puis vide la carte de tous les événements enregistrés.

- Il est recommandé de configurer des règles d'actualisation pour **tous** les badges, y compris concernant les badges des invités, employés, administrateurs, ou personnes de confiance. En effet en cas de perte ou de vol, ou de départ du titulaire du badge de l'entreprise, le badge sera automatiquement bloqué sur tous les lecteurs dès lors que la date d'actualisation sera passée.

- Choisissez les jours du samedi et/ou du dimanche à exclure si vous ne souhaitez pas les compatibiliser dans la fréquence d'actualisation (fonctionnalité disponible en fréquence « Jour » uniquement).

- A minima il est recommandé de configurer une date de validité afin de bloquer les badges après une date donnée.

Il est vivement conseillé d'activer la règle d'actualisation.
Dans ce cas, le détenteur du badge aura accès aux lecteurs compris dans ses droits d'accès de façon illimité.
Sauf passage du « Badge interdit » sur les lecteurs dont il faut bloquer l'accès.

Tip!

Une actualisation quotidienne est recommandée si vous souhaitez une gestion plus fine des droits d'accès et si vous voulez obtenir les évènements les plus à jour.

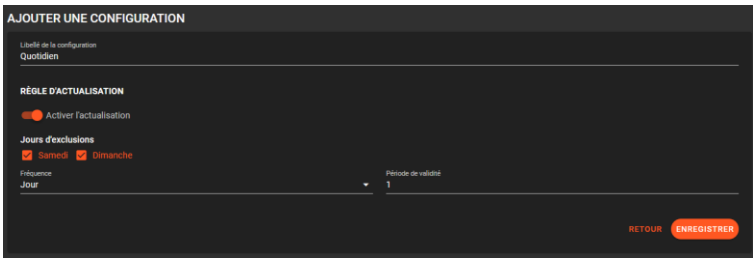


Fig. 10: Règle d'actualisation quotidienne sans compter le Week end.

Cas pratiques de réactualisation:

- L'utilisateur passe son badge sur le lecteur d'actualisation à 13h00 pour une fréquence d'actualisation de 1 jour.
  L'accès est autorisé jusqu'au lendemain à 13h00. Passé cet horaire, l'usager doit passer son badge sur le lecteur d'actualisation pour délivrer à nouveau les accès pour 24h supplémentaires.

- Samedi exclu : si le badge a une fréquence d'actualisation de 3 jours avec la dernière actualisation le vendredi à 8h00, l'usager devra s'actualiser après le mardi suivant à partir de 8h00 pour obtenir à nouveau les accès.

7- Paramétrage des évènements

Modifiez ici les évènements en termes de :

- Libellé dans la liste des évènements
- Couleur du libellé dans la liste des évènements
- Récurrence de la purge (90 jours par défaut)

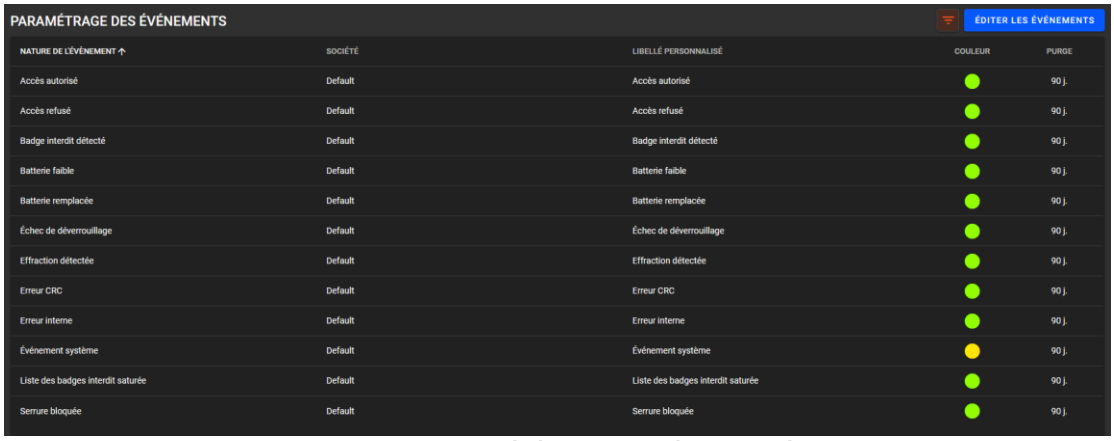


Fig. 11: Liste des évènements à paramétrer.

8- Droits d'accès des badges

Donnez à vos badges les droits de façon détaillée ou bien appliquez des configurations existantes. La configuration doit être détaillée si aucune configuration n'a été sélectionnée en ce qui concerne les droits d'accès, la configuration des évènements et la configuration de l'actualisation.

8.1 Plages horaires

Les plages horaires offline des usagers sont disponibles depuis le menu Droits d'accès / Plages horaires du menu Configuration de l''interface OPTIMA avec l'option cochée « *Plage horaire utilisé dans le module ONE Pass* ».

Celles-ci sont identifiées par le symbole  .

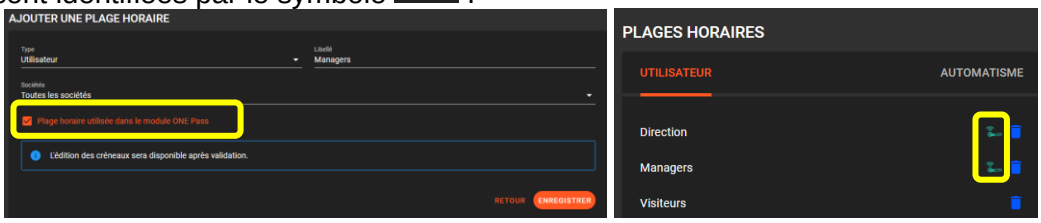


Fig. 12: Configuration des plages horaires offline des usagers.

Il est possible d'associer jusqu'à 4 créneaux de plage horaire par jour.
Les plages horaires existantes du contrôle d'accès (online) ne sont pas compatibles avec les plages horaires offline.

8.2 Validité

La période de validité de l'usager est disponible dans l'onglet « *Droits d'accès* » de la fiche Usager depuis l'interface principale OPTIMA.

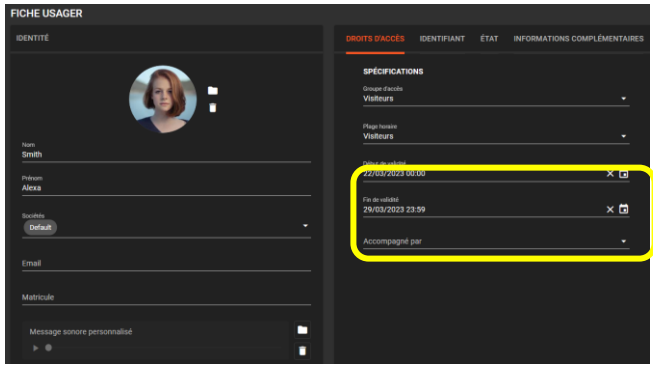


Fig. 13: Configuration des dates de validité depuis interface principale OPTIMA.

9- Création des badges par encodage

Pour affecter les badges aux utilisateurs il est nécessaire de les encoder.

La liste des usagers offline correspond à la liste des Usagers du contrôle d'accès.
Seuls les droits en termes de plages horaires (offline) et en terme les dates de validité sont appliquées depuis le contrôle d'accès.
L'encodage d'un badge nécessite au préalable de le configurer : cliquez sur le badge afin de choisir sa configuration de droits d'accès, d'événements et de règles d'actualisation.

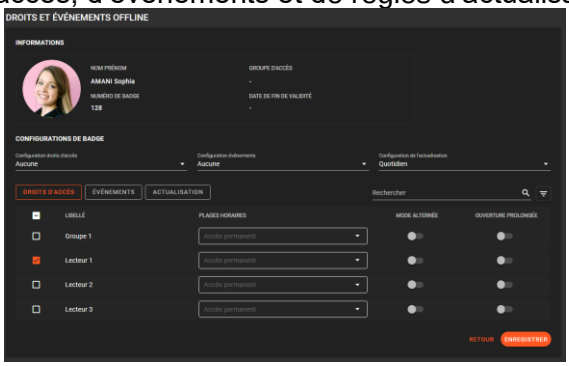


Fig. 14: Configuration des droits et évènements.

Depuis le menu Droits des usagers  choisissez l'usager dont le badge n'a pas encore été encodé : ils sont identifiés par le symbole  .

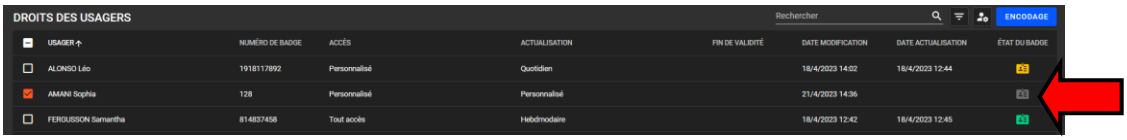


Fig. 15: Sélection d'un usager pour encodage.

Cliquez ensuite sur le bouton ENCODAGE et présentez le badge Mifare®/DESFire® sur le lecteur d'actualisation jusqu'à ce que les diodes du lecteur s'allument en vert et apparition du message « Encodage terminé avec succès ».

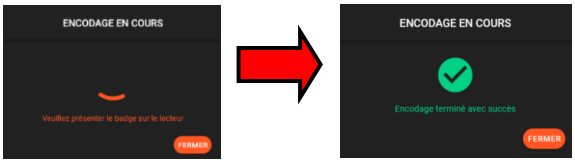


Fig. 16: Encodage réussi.

Un lecteur d'encodage doit être sélectionné si plusieurs lecteurs d'actualisation avec l'option « *Lecteur d'encodage* » sont disponibles.

Note : Il est impossible d'associer un usager à un badge déjà encodé à un autre usager existant. Si vous souhaitez encoder un badge déjà associé à un usager existant :

- Identifiez au prélable celui-ci au passage du badge sur le lecteur d'actualisation dans le Journal de bord (voir section Journal de bord).
- Selon l'usager identifié dans le Journal de bord, supprimez le depuis l'interface OPTIMA.

10- Droits des usagers

Consultez les propriétés des usagers depuis le menu 

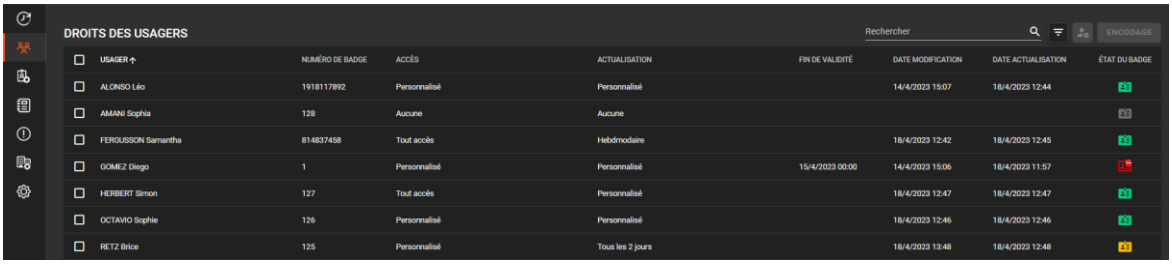


Fig. 17: Droits des usagers.

10.1 Etat du badge

A la date de consultation des badges, vérifiez l'état de l'ensemble des badges. Il peuvent avoir le statut :

- Badge non encodé  : aucune association de l'usager avec un badge encodé.
- Badge en cours de validité  : le badge utilisateur valide au moment de la consultation.
- Badge avec configuration différente  : la configuration du badge a été changée après la dernière actualisation.
- Badge interdit  : le badge appartient à la liste des badges interdits.

   Il est effectivement interdit après encodage du badge interdit et passage de celui-ci sur les lecteurs concernés (voir Section « *Badges interdits* »).

- Badge hors validité  : la date de fin de validité du badge est dépassée.
- Badge hors cycle d'actualisation  : le badge a dépassé sa date d'actualisation : il est refusé sur tous les lecteurs.

  Il doit nécessairement être réactualisé en passant sur le lecteur d'actualisation (mise à jour de la date butoir).

10.2 Filtre

Cliquez sur l'icône filtre  pour faire appaittre le menu de filtrage des données afin de sélectionner le ou les usagers selon les critères souhaités.
Critères de filtres :

- Date de fin de validité
- Configuration de de droits
- Configuration d’actualisation
- Etat du badge

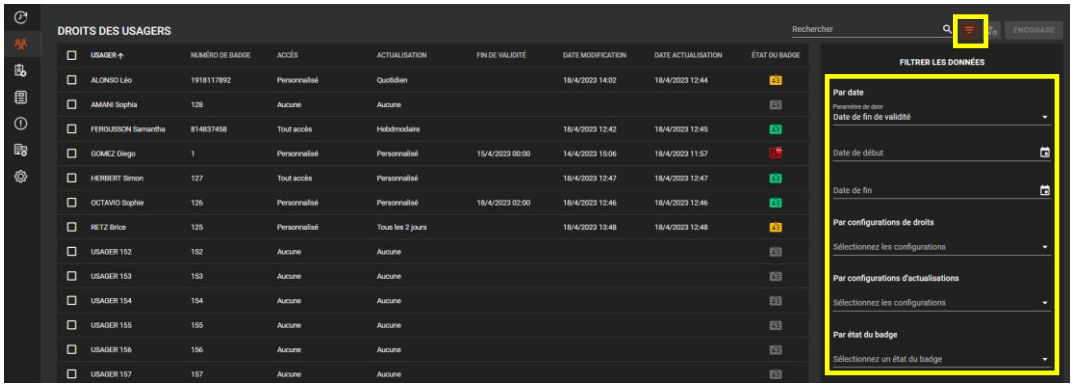


Fig. 18: Filtrer les données.

10.3 Traitement groupé

Appliquez une modification de configuration sur la sélection des badges en termes de :

- Configuration des droits d’accès
- Configuration d’évènements
- Configuration de règle d’actualisation

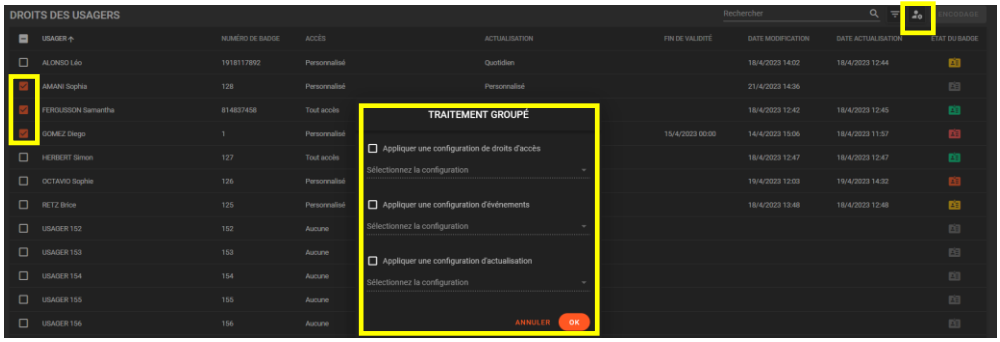


Fig. 19: Traitement groupé.

11- Badges interdits

Si vous souhaitez restreindre rapidement l'accès d'un usager dans les cas suivants :

- La date butoir n'est pas dépassée
- La fin de de validité n'est pas dépassée
- La plage horaire offline est valide

Il est possible de créer un badge contenant le ou les badges pour lesquels il faut interdire l'accès. Tous les lecteurs doivent être mis à jour en présentant le badge encodé avec la liste des usagers interdits.

11.1 Changement des droits d'accès

Il est conseillé de changer les droits d'accès afin de restreindre l'accès ultérieur aux lecteurs des badges.
Cliquez sur la fiche usager afin de désélectionner les lecteurs/groupe dans les droits d'accès.

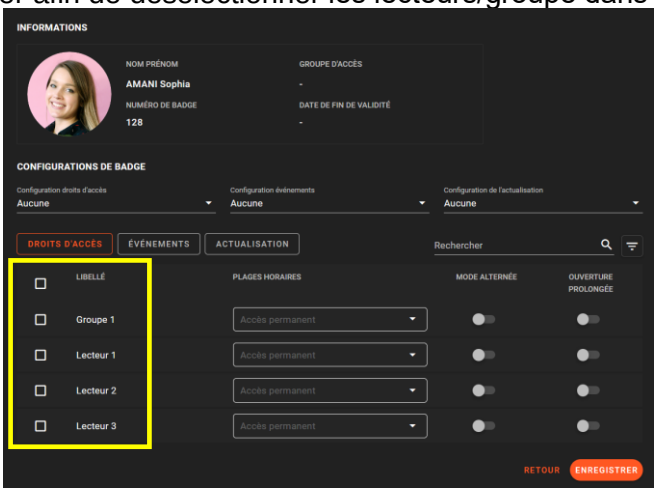


Fig. 20: Les lecteurs et groupes sont désactivés.

11.2 Création du badge interdit

Cliquez sur AJOUTER depuis le menu « Badges interdits » afin de sélectionner l'usager (saisir les lettres de l'utilisateur à rechercher) et sélectionnez une date d'expiration.
La date d'expiration doit correspondre à une date ulterieure à la prochaine date d'actualisation du badge (si existante).

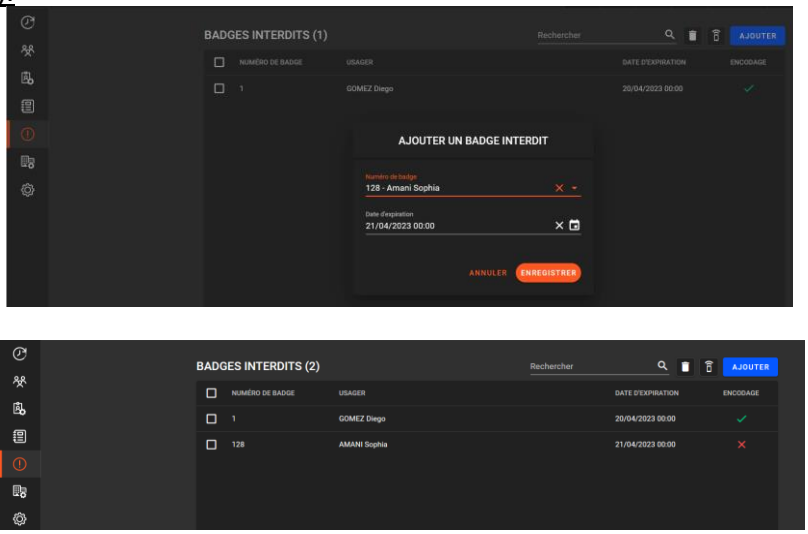


Fig. 21: Ajout de l'utilisateur à interdire.

11.3 Encodage du badge interdit

Cliquez ensuite sur le bouton « Encoder »  et présentez un badge Mifare®/DESFire® sur lecteur d'actualisation.

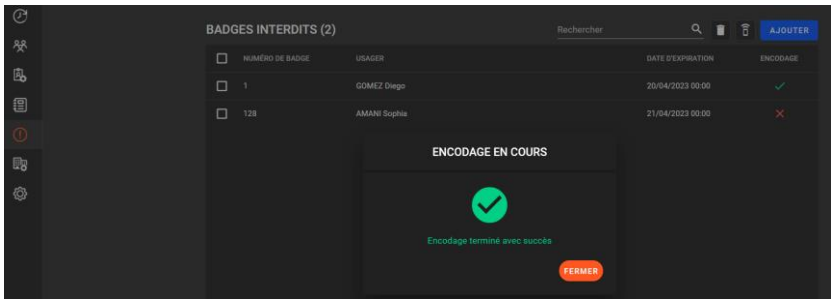


Fig. 22:Encodage du badge de liste interdit.

11.3 Mise à jour des lecteurs

Présentez ensuite le badge précédemment encodé sur les lecteurs dont vous souhaitez interdire le passage du (des) badge(s).

Note : Il est possible de configurer jusqu'à 256 usagers interdits. Il est important de réduire au maximum la date d''expiration afin de libérer de l'espace mémoire pour un rajout ultérieur de badges à interdire.

Le maximum d'usagers sur liste interdite est configurable depuis la configuration générale  .

12- Journal de bord

Accédez aux informations relatives au lecteur d'actualisation.
Il s'agit principalement du passage des badges et des éventuelles connexions/déconnexions des lecteurs d'actualisation.

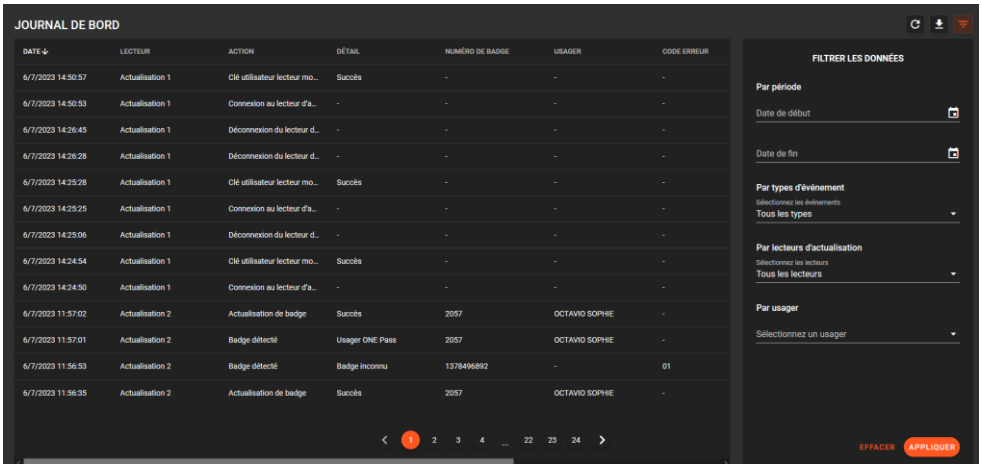


Fig. 23:Journal de bord.

La mise à jour de la liste se fait en cliquant sur le bouton 

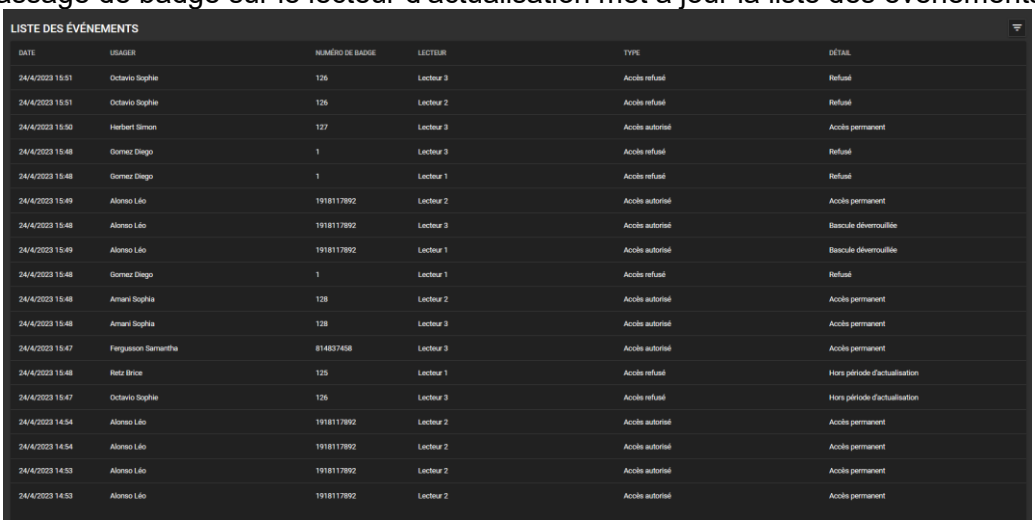
Vous pouvez filtrer  les données selon :

- Les dates de debut/fin
- Le type d'évènement
- Le lecteur d'actualisation
- L'usager

Exportez l'ensemble des données du journal dde bord en appuyant sur le bouton  .

13- Exploitation

Chaque passage de badge sur le lecteur d'actualisation met à jour la liste des évènements.



LISTE DES ÉVÉNEMENTS

DATE	USAGER	NUMÉRO DE BADGE	LECTEUR	TYPE	DÉTAIL
24/4/2023 15:51	Octavio Sophie	126	Lecteur 3	Accès refusé	Refusé
24/4/2023 15:51	Octavio Sophie	126	Lecteur 2	Accès refusé	Refusé
24/4/2023 15:50	Herbert Simon	127	Lecteur 3	Accès autorisé	Accès permanent
24/4/2023 15:48	Gomez Diego	1	Lecteur 3	Accès refusé	Refusé
24/4/2023 15:48	Gomez Diego	1	Lecteur 1	Accès refusé	Refusé
24/4/2023 15:49	Alonso Léo	1918117892	Lecteur 2	Accès autorisé	Accès permanent
24/4/2023 15:48	Alonso Léo	1918117892	Lecteur 3	Accès autorisé	Bascule déverrouillée
24/4/2023 15:49	Alonso Léo	1918117892	Lecteur 1	Accès autorisé	Bascule déverrouillée
24/4/2023 15:48	Gomez Diego	1	Lecteur 1	Accès refusé	Refusé
24/4/2023 15:48	Amani Sophia	128	Lecteur 2	Accès autorisé	Accès permanent
24/4/2023 15:48	Amani Sophia	128	Lecteur 3	Accès autorisé	Accès permanent
24/4/2023 15:47	Fergusson Samantha	814837458	Lecteur 3	Accès autorisé	Accès permanent
24/4/2023 15:48	Retz Brice	125	Lecteur 1	Accès refusé	Hors période d'actualisation
24/4/2023 15:47	Octavio Sophie	126	Lecteur 3	Accès refusé	Hors période d'actualisation
24/4/2023 14:54	Alonso Léo	1918117892	Lecteur 2	Accès autorisé	Accès permanent
24/4/2023 14:54	Alonso Léo	1918117892	Lecteur 2	Accès autorisé	Accès permanent
24/4/2023 14:53	Alonso Léo	1918117892	Lecteur 2	Accès autorisé	Accès permanent
24/4/2023 14:53	Alonso Léo	1918117892	Lecteur 2	Accès autorisé	Accès permanent

Fig. 24: Liste des évènements.

Les évènements passés sont disponibles en appliquant un filtre 

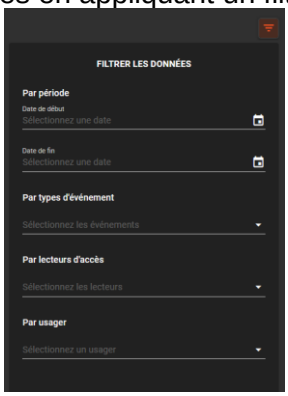


Fig. 25: Filtre des évènements.

En plus de la période, filtrez selon :

- Le type d'évènements
- Le lecteur d'accès
- L'usager

14- Application mobile OPTIMA Pass

14.1 Présentation

L'affichage de l'interface OPTIMA Pass est disponible sur un écran mural à travers les produits OPTIMA ULTRA OPassTablet :
https://www.optimabox.fr/doc/produits/notices/lecteurs/fr_FR/eden/OPTIMA_ULTRA_OPassTablet.pdf

Le produit est composé de :

- Lecteur de badge **STID ARC-W33 SSCP**

  https://www.optimabox.fr/doc/produits/notices/spinel/fr_FR/modules/C485-IP-SSCP.pdf

- Tablette tactile ANDROID nécessitant une connexion sans-fil (routeur wifi requis pour diffuser la connexion OPTIMA Box) et une alimentation électrique déjà précablée depuis la carte d'alimentation inclue (source d'alimentation 12V)

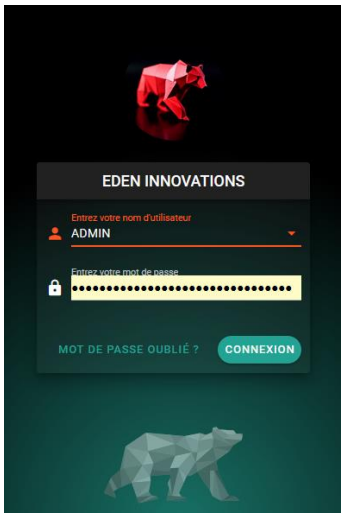
Entrez l'adresse IP de la box OPTIMA Box® dans un navigateur web de l'appareil mobile.
Si le lien ne fonctionne pas, saisissez l'adresse de l'OPTIMABOX suivie par '/mobile', exemple: *192.168.3.130/mobile*.
Sur la tablette OPTIMA ULTRA, l'accès direct à configurer dans l'application Kiosque dans le menu Genéral / « Kiosk URL », est : **url/mobile/app/opasstablet**
exemple : *192.168.3.330/mobile/app/opasstablet*

Sélection de la langue : le changement de la langue est disponible dans le paramétrage de la tablette Android : System / Language & input / Language : sélectionner la langue souhaitée, et la mettre en priorité.

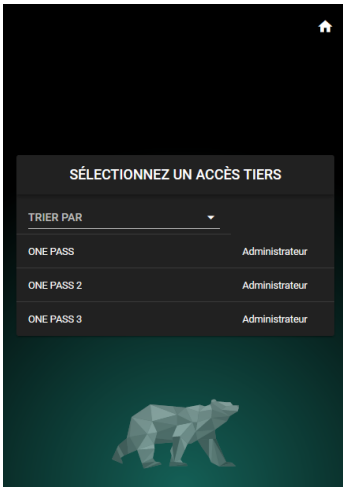
Note : Connexion internet requise.

Fig. 26: Applications OPTIMA : OPTIMA Time, OPTIMA Access, OPTIMA Pass et OPTIMA Mobile.

1. *Clic sur OPTIMA Pass.*



2. *Sélection du compte utilisateur associé au compte de système tiers Optima Pass.*



3. *Choix du système Tiers existant.*

Fig. 27 : Accès à Optima Pass.

Sélectionnez ensuite le lecteur (un seul lecteur à choisir).

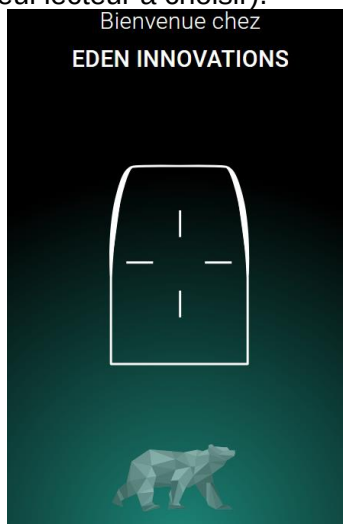
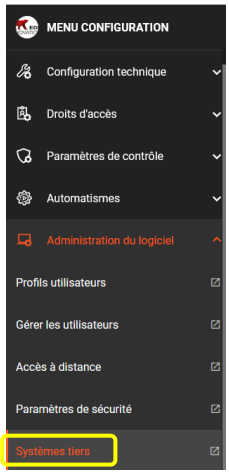


Fig. 28 : Affichage du lecteur.

14.2 Configuration

Il est nécessaire de disposer d'un compte d'accès à l'application OPTIMA Pass.



Celui-ci doit être créé depuis l'interface principale OPTIMA Box dans le menu Configuration / Administration du logiciel, pour ajouter un « Système tiers » de type « One Pass Tablet »

Fig. 29 : Système Tiers.

Cliquez sur le bouton « Ajouter un système Tiers » depuis l'onglet Système Tiers.

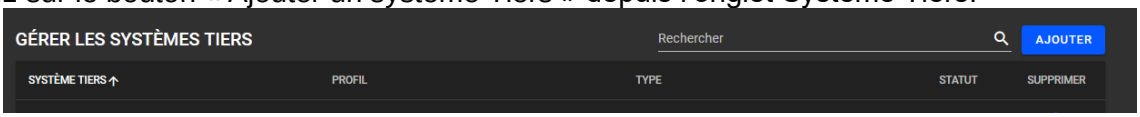


Fig. 30 : Ajouter un Système Tiers.

Saisir un nom de système tiers de type « **ONE Pass Tablet**» depuis la liste déroulante *« Type du système Tiers* » :

Fig. 31 : Ajout d'un Système Tiers de type ONE Pass tablet.

14.3 Ecran d'information

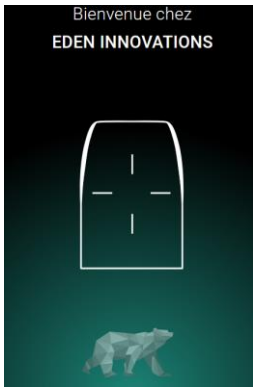


Fig. 32. Ecran principal.

Chaque fois qu'un badge passe sur le lecteur d'actualisation, l'écran d'information va indiquer :

Erreur de communication lecteur

Passage d'un badge inconnu

Encodage du badge

Actualisation en cours du badge

Actualisation terminée

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

www.eden-innovations.com