GUIDE ADMINISTRATEUR

SECRETMANAGER V1.X

Résumé :	Ce guide explique comment paramétrer et administrer l'outil « SECRETMANAGER » et son serveur interne le « SECRETSERVER ».

HISTORIQUE DU DOCUMENT		
Version	**Date**	**Modifications**
1.0-0	19/09/2015	Création

DOCUMENTS DE REFERENCE		
Index	**Titre**	**Référence**
DR01	Guide d'Installation de SecretManager	FR - Guide Installation - SecretManager v1.x – v1.0-0.pdf

TABLE DES MATIERES

1. AVANT PROPOS

Attention, malgré l'attention portée à cet outil, vous utilisez cet outil à vos risques et périls.

2. PRE-REQUIS

Le mode opératoire décrit ci-dessous ne vaut que si l'outil « SecretManager » a été installé conformément au « Guide d'Installation » () fournit dans le package d'installation.

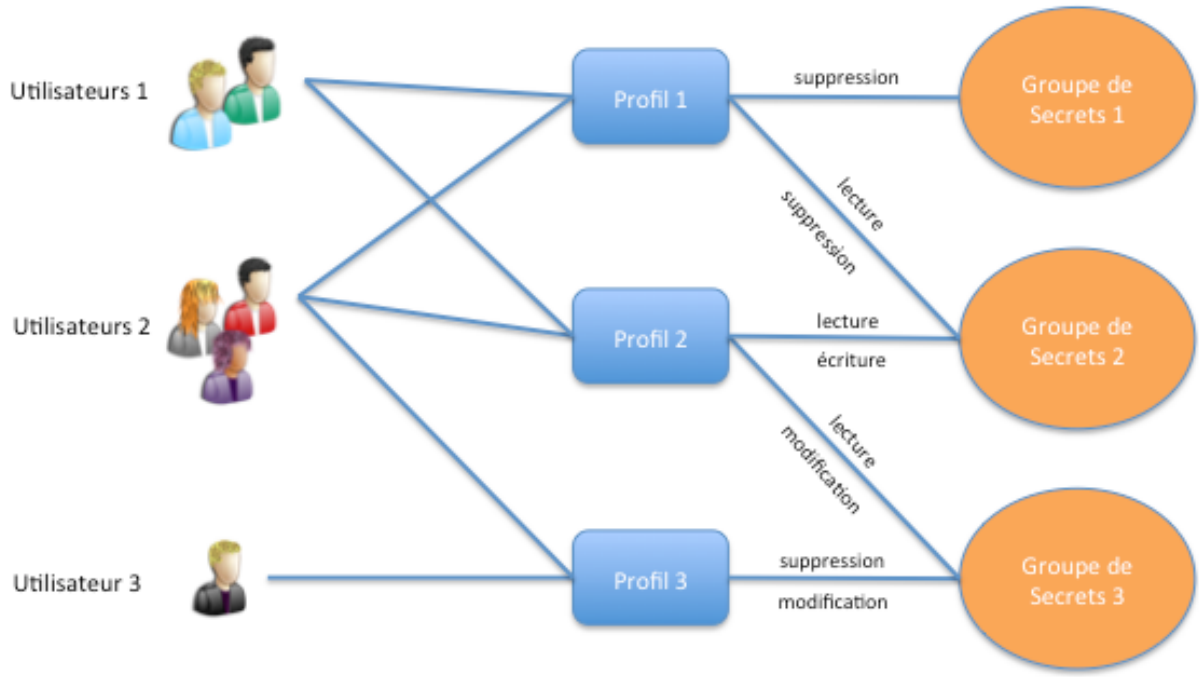
3. FONCTIONNEMENT GLOBAL

Pour partager un « Secret » l'utilisateur de « **SecretManager** » doit le placer dans un « Groupe de Secret ». C'est au travers ce dernier qu'il pourra le partager. Effectivement, un « Groupe de Secret » est attaché à un ou plusieurs de « Profils ». C'est en créant le lien entre le « Profil » et le « Groupe de Secrets » que l'on définit des droits d'accès aux « secrets » contenu dans un « Groupe de Secrets ».

Enfin, on associe des « Utilisateurs » à des « Profils ».

Attention, par défaut, un « Utilisateur » n'est rattaché à aucun « Profil ».

Quand un « Utilisateur » dispose de plusieurs « Profils » (droits d'accès) sur un même « Groupe de Secrets », les droits d'accès sont additionnés et seuls les droits les plus forts sont conservés.



4. PREMIERE CONNEXION A L'OUTIL « SECRETMANAGER »

Commencez par une connexion locale à votre serveur. Pour ce faire, utilisez votre navigateur et tapez l'adresse IP où a été installé le SecretManager. Par exemple :

```
https://ihm.secretmanager.fr/
```

Attention : « ihm.secretmanager.fr » est une entrée DNS d'exemple. Voir ce qui a été paramétré lors de l'installation du « SecretManager ».

Vous devriez obtenir l'écran ci-dessous :

Si vous venez d'installer l'outil, il n'existe qu'un seul utilisateur par défaut.

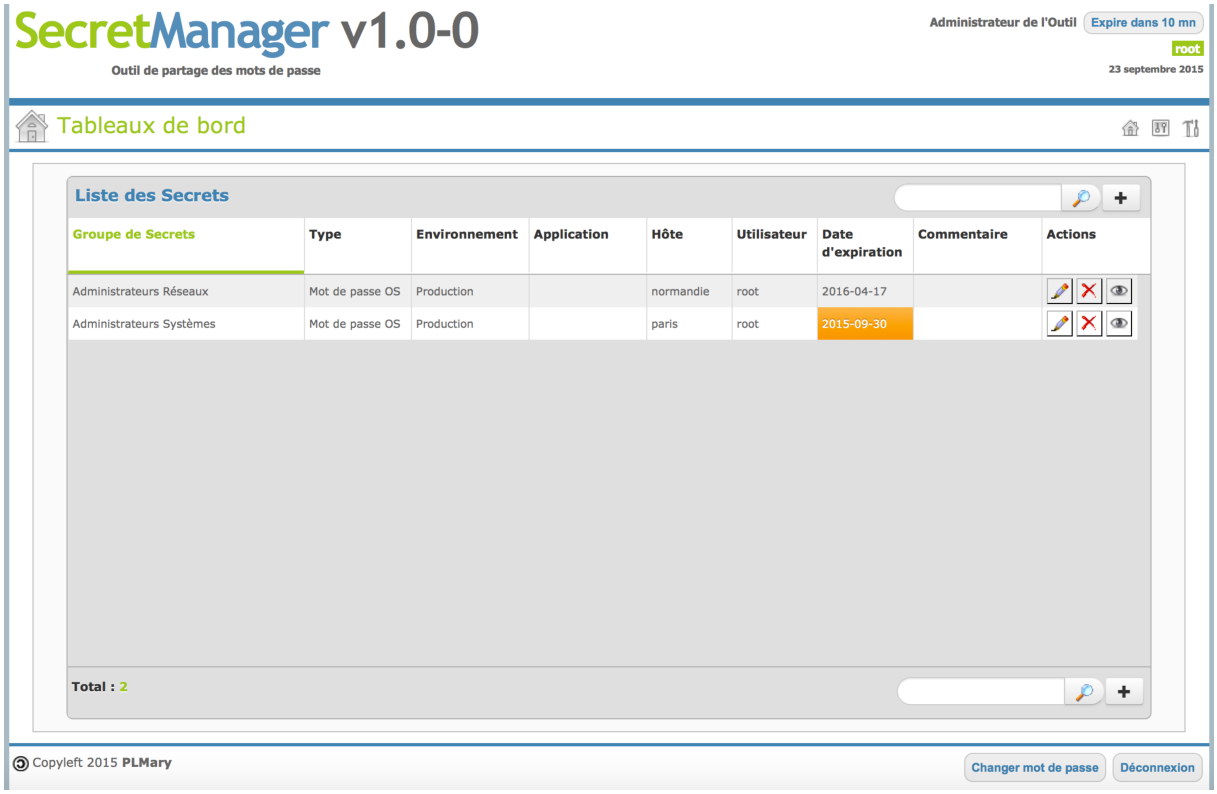
Cet utilisateur est l'utilisateur « `root` », son mot de passe par défaut est « `Welcome !` » (l'espace est important entre le « `e` » et le « `!` »).

Attention : nous vous conseillons de changer ce mot de passe avant de passer l'outil « SecretManager » en « Production ».

Remarque 1 : *« SecretManager » est multilingue, pour utiliser une des langues gérées, il suffit de cliquer sur l'un des drapeaux présents en haut à droite de l'écran.*

Remarque 2 : *Je dis que « SecretManager » est multilingue, mais les traductions sont largement perfectibles (toute contribution est la bienvenue).*

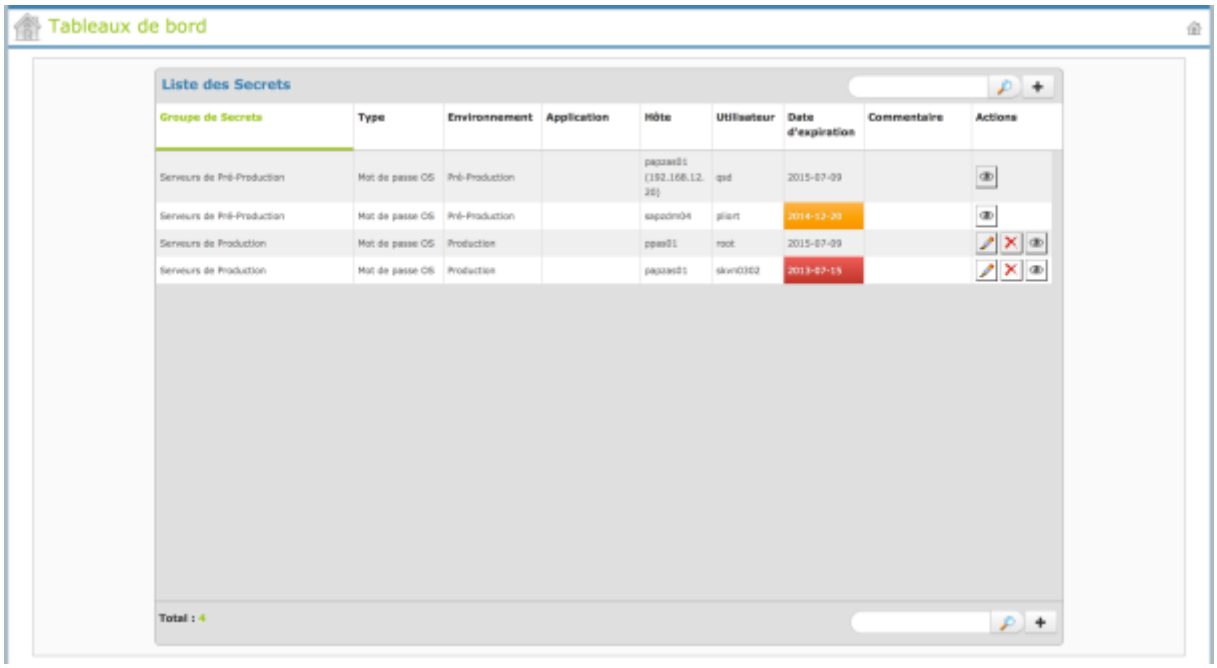
Après vous êtes identifié, vous devriez arriver sur l'écran ci-dessous :



Cet écran est votre tableau de bord, il vous donne accès à tous les secrets auxquels vous avez droit.

Comme vous êtes « Administrateur », il est normal que vous ayez accès à tout.

Un autre utilisateur pourrait avoir une vue différente sur ces données comme ci-dessous :



On constate que selon les droits, on peut réaliser plus ou moins d'action sur un Secret (de boutons accessibles).

5. ERGONOMIE DES ECRANS

5.1. Entête des écrans

Sur la partie gauche de l'entête, il est rappelé la version actuelle de l'outil « **SecretManager** ».

Sur la partie de droite, on affiche la « Civilité » de l'utilisateur connecté (prénom et nom), dans notre exemple : **Pierre-Luc Mary**

Un bouton affiche le nombre de minutes restant avant l'expiration de la session de l'utilisateur. Le nombre de minutes se décrémente toutes les minutes. En arrivant à 0, l'utilisateur est automatiquement déconnecté. En réalisant des actions, comme rafraîchir l'écran, l'utilisateur réinitialise son nombre de minutes. L'utilisateur peut également directement cliquer sur le bouton pour réinitialiser son nombre de minutes.

> ***Remarque** : le nombre de minutes avant expiration est paramétrable (voir le chapitre « 7.2.1 » pour plus d'information).*

On affiche également le « nom d'utilisateur » utilisé pour la connexion, dans notre exemple : **plm**

Remarque : *une civilité peut-être rattachée à plusieurs utilisateurs, c'est pour cela que cette information peut-être importante.*

Enfin, on affiche la date du jour.

5.2. Zone titre

Sur la gauche de cette zone, on affiche le titre de la page courante.

Sur la droite de cette zone on trouve les boutons. Ces boutons permettent d'avoir accès en permanence aux différents modules auxquels un utilisateur à accès.

Un administrateur dispose de tous les boutons :

Le premier bouton permet d'avoir accès au « Tableau de bord », tous les utilisateurs y ont accès.

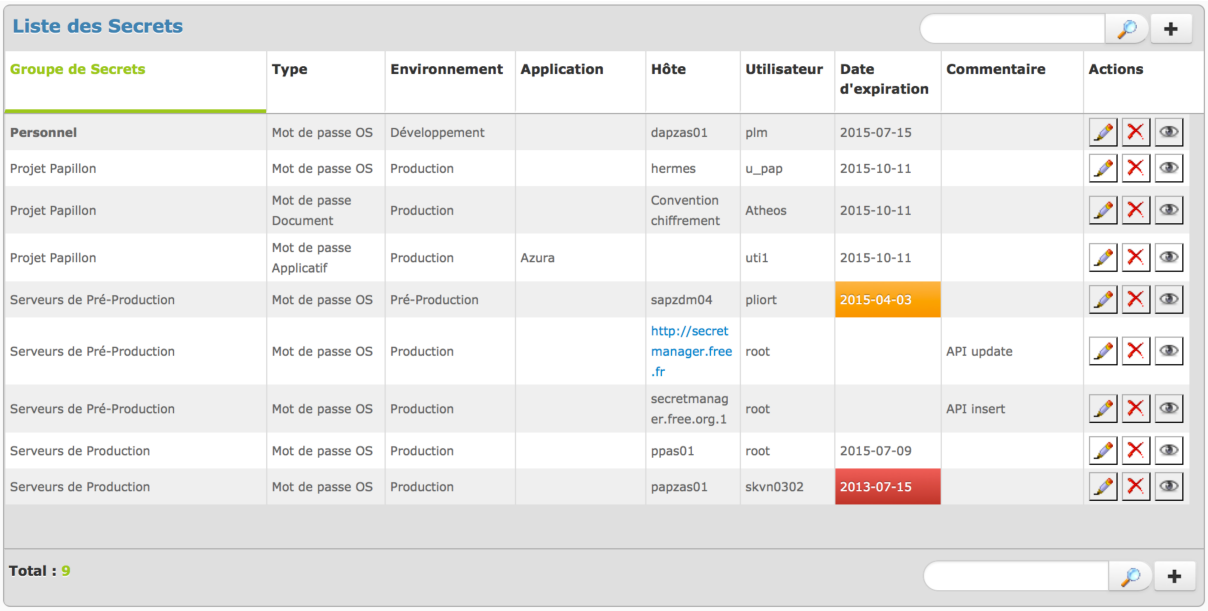
Le deuxième bouton permet d'avoir accès à la « Gestion des Préférences » (seuls les administrateurs y ont accès).

Le troisième bouton permet d'avoir accès à « l'Interface d'Administration » (seuls les administrateurs et les opérateurs y ont accès).

En fonction de ses droits, un utilisateur aura plus ou moins de boutons (d'actions possibles) sur un Secret (une occurrence).

Rappel : les droits sont donnés au « Groupe de Secrets » et non pas unitairement à un Secret.

5.3. Zone corps



On trouve toutes les informations propres à chaque écran.

Le cadre bleu apparaît une seule fois, juste après l'écran de connexion. Il permet de rappeler des informations importantes à l'usager.

5.4. Zone pied de page

Dans la partie gauche de cette zone, on rappelle que cet outil est sous licence GPL 3.0 et qu'il est maintenu par moi même et tous ceux qui voudront y participer.

Dans la partie droite de cette zone, deux boutons sont accessibles :

Le premier bouton permet à l'utilisateur connecté de pouvoir changer son mot de passe.

Le deuxième bouton permet à l'utilisateur de se déconnecter de l'outil.

6. FONCTIONNEMENT GLOBAL DE L'OUTIL « SECRETMANAGER »

L'outil « **SecretManager** » permet de partager des « Secrets » entre les « Utilisateurs ».

Toutefois, l'outil ne permet à proprement parler de partager des « Secrets », il permet plutôt de partage des « Groupes de Secrets ».

Comment faire si un Secret est extrêmement sensible et qu'il doit donc être partagé avec très peu de monde ?

Il faudra simplement créer un Groupe de Secrets dans lequel, peut-être, il n'y aura que ce Secret.

Comprenez bien que quand un Utilisateur à accès à un « Groupe de Secrets », il accède à tous les Secrets de ce Groupe de la même façon (en fonction des droits mis sur le Groupe, toutefois).

Afin de ne pas avoir trop de rattachement à faire par Utilisateur, l'outil « **SecretManager** » embarque une notion de « Profil ».

Ainsi, nous obtenons la représentation suivante :

Utilisateurs ⇔ Profils ⇔ Groupes de Secrets ⇔ Secrets

Soit un « Utilisateur » peut être associé à un ou plusieurs « Profils ».

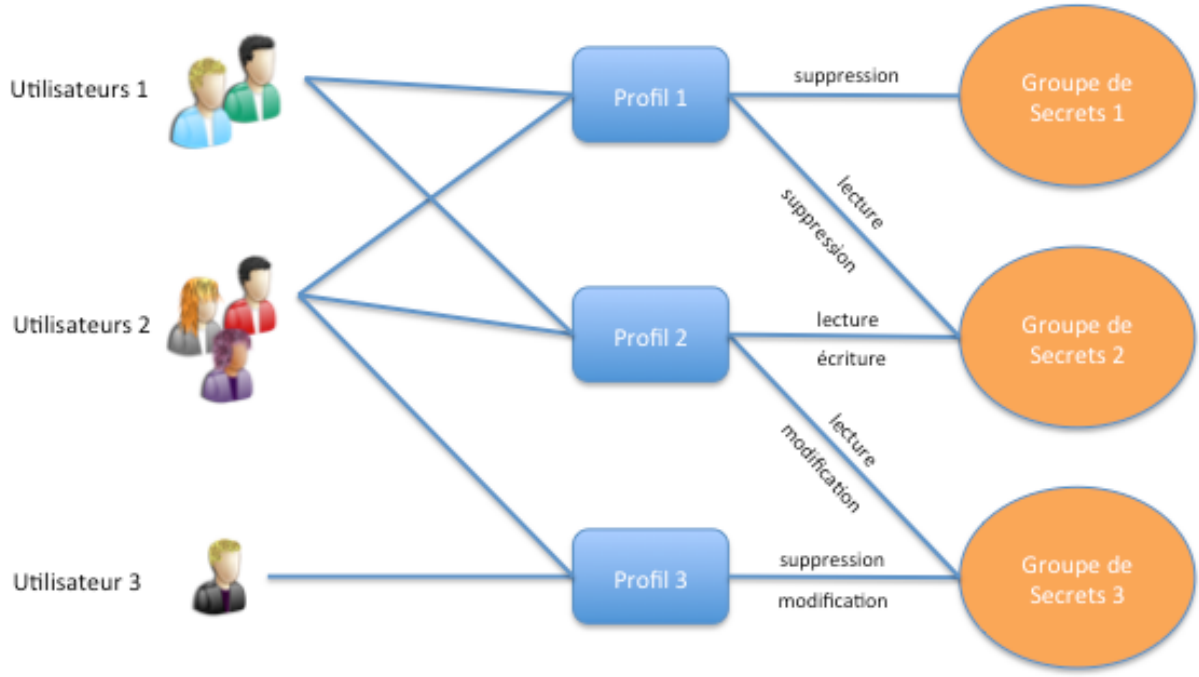
Les « Profils » donnent des accès à des « Groupes de Secrets ». La notion d'accès est importante. Effectivement, on définit un « droit d'accès » entre un « Profil » et un « Groupe de Secrets ». Il existe **4** droits dans l'outil :

1. *Lecture* : l'utilisateur peut lire les « Secrets » contenus dans le « Groupe de Secrets » ;
2. *Ecriture* : l'utilisateur peut créer des « Secrets » dans le « Groupe de Secrets » (on parle bien de création. Le Secret ne doit donc pas exister dans la base) ;

3. *Modification* : l'utilisateur peut modifier les « Secrets » dans le « Groupe de Secrets » (le Secret existe déjà dans la base, s'il n'existe pas il y aura une erreur et il ne sera donc pas créé) ;
4. *Suppression* : l'utilisateur peut supprimer les « Secrets » dans le « Groupe de Secrets ».

Les « Groupes de Secrets », quant à eux, sont des conteneurs de « Secrets ».

Le schéma ci-dessous, résume les concepts qui viennent d'être énoncés :



7. GESTION DES PREFERENCES

Cet ensemble d'écrans est réservé aux Administrateurs. Ils permettent de gérer le paramétrage interne de l'outil « **SecretManager** ».

Pour accéder à ces écrans, l'administrateur doit utiliser le bouton suivant «  ».

Il arrive ensuite sur l'écran ci-dessous :

7.1. Gestion des « Alertes »

Toutes les actions réalisées dans « **SecretManager** » sont tracées dans la base de suivi du « **SecretManager** » (voir chapitre « 8.8 » pour plus d'information).

Pour des raisons de sécurité, il peut-être important d'externaliser certains événements de la base interne du « **SecretManager** ». Pour cela, on générera des « alertes » vers d'autres dispositifs :

- Envoi au `Syslog` de la machine hébergeant le « **SecretManager** » (prochainement, on pourra dupliquer cette alerte sur le `Syslog` d'un autre serveur (en plus du `Syslog` local)).
- Envoi d'un `Courriel` (pour peu que la machine qui héberge le « **SecretManager** » dispose d'un serveur de courriel).

Les alertes peuvent être mises sur les événements suivants :

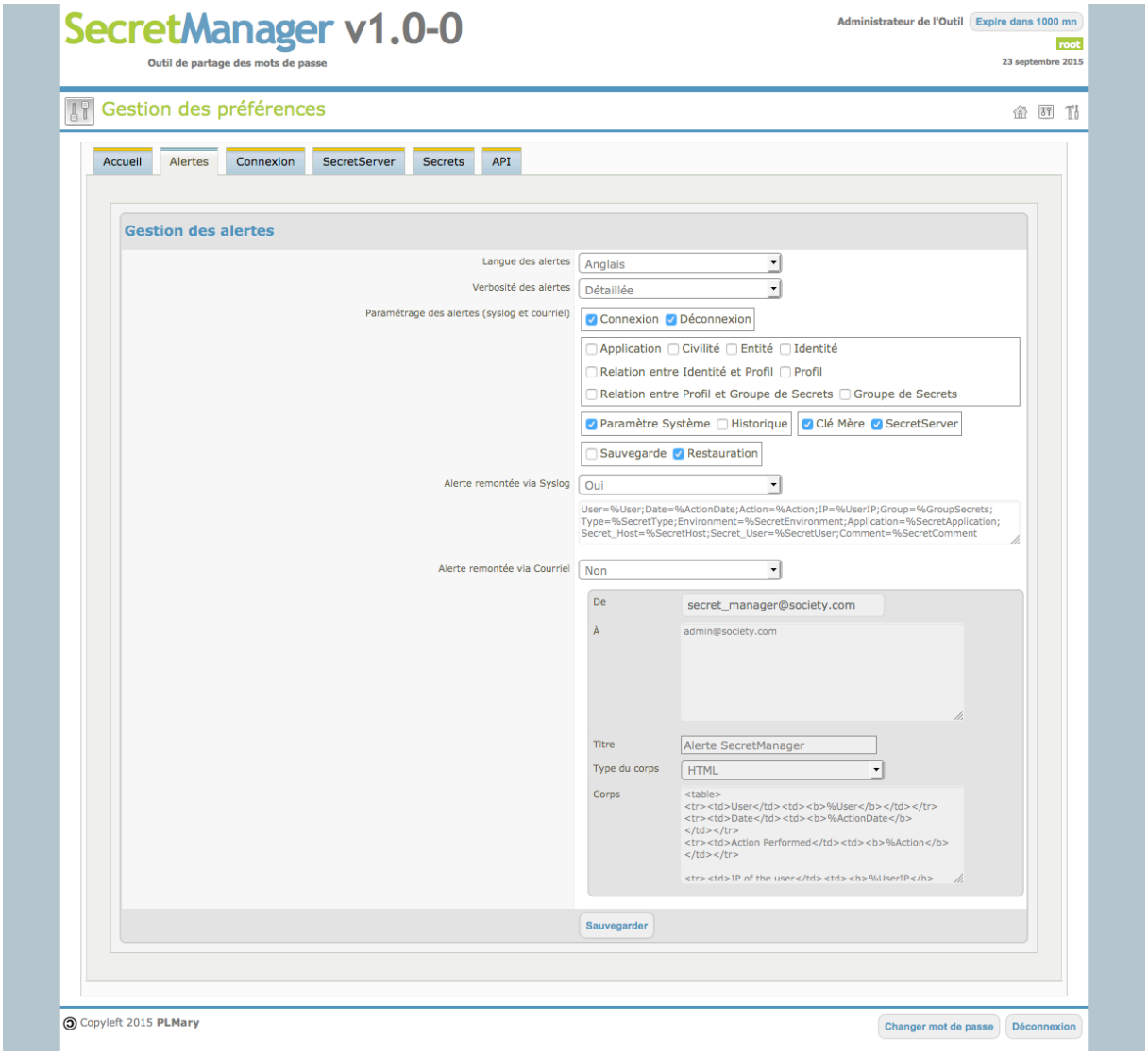
- Action de « Connexion » ;
- Action de « Déconnexion » ;
- Action sur une « Application » ;
- Action sur une « Civilité » ;
- Action sur une « Entité » ;
- Action sur une « Identité » ;
- Action sur une « Relation entre Identité et Profil » ;
- Action sur une « Profil » ;
- Action sur une « Relation entre Profil et Groupe de Secrets » ;
- Action sur une « Groupe de Secrets » ;
- Action sur une « Paramètre Système » ;
- Action sur une « Historique » ;
- Action sur une « Clé Mère » ;

- Action sur une « SecretServer » ;
- Action sur une « Sauvegarde » ;
- Action sur une « Restauration » .

Par défaut les événements suivants sont sous alerte :

- Action de « Connexion » ;
- Action de « Déconnexion » ;
- Action sur une « Paramètre Système » ;
- Action sur une « Clé Mère » ;
- Action sur une « SecretServer » ;
- Action sur une « Restauration » .

Pour gérer les remontées d'alertes externes à l'outil, l'Administrateur doit cliquer sur l'onglet « Alertes ». Il arrivera dans l'écran ci-dessous :



7.1.1. Langue des alertes

Ce champ permet de sélectionner la langue dans laquelle seront générés les messages d'alerte. Par défaut, les messages sont en « Anglais ».

7.1.2. Champ « Verbosité des alertes »

L'outil gère 2 types de verbosité d'alerte :

1. Normale ;
2. Détaillée (par défaut).

La verbosité « normale » remonte seulement le libellé et l'identifiant de l'action réalisé sur un objet. En revanche, la verbosité « détaillée » donne tous les détails sur l'action réalisée sur l'objet.

7.1.3. Champ « Paramétrage des alertes (syslog et courriel) »

7.1.3.1. Champ « Connexion »

En cochant ce champ, des alertes seront remontées à chaque connexion d'un utilisateur.

7.1.3.2. Champ « Déconnexion »

En cochant ce champ, des alertes seront remontées à chaque déconnexion d'un utilisateur.

7.1.3.3. Champ « Application »

En cochant ce champ, des alertes seront remontées à chaque fois que des modifications sont réalisées sur les objets de type « Application ».

7.1.3.4. Champ « Civilité »

En cochant ce champ, des alertes seront remontées à chaque fois que des modifications sont réalisées sur les objets de type « Civilité ».

7.1.3.5. Champ « Entité »

En cochant ce champ, des alertes seront remontées à chaque fois que des modifications sont réalisées sur les objets de type « Entité ».

7.1.3.6. Champ « Identité »

En cochant ce champ, des alertes seront remontées à chaque fois que des modifications sont réalisées sur les objets de type « Identité ».

7.1.3.7. Champ « Relation entre Identité et Profil »

En cochant ce champ, des alertes seront remontées à chaque fois que des modifications sont réalisées sur les objets de type «Relation entre Identité et Profil ».

7.1.3.8. Champ « Profil »

En cochant ce champ, des alertes seront remontées à chaque fois que des modifications sont réalisées sur les objets de type « Profil ».

7.1.3.9. Champ « Relation entre Profil et Groupe de Secrets »

En cochant ce champ, des alertes seront remontées à chaque fois que des modifications sont réalisées sur les objets de type «Relation entre Profil et Groupe de Secrets ».

7.1.3.10. Champ « Groupe de Secrets »

En cochant ce champ, des alertes seront remontées à chaque fois que des modifications sont réalisées sur les objets de type «Groupe de Secrets ».

7.1.3.11. Champ « Paramètre Système »

En cochant ce champ, des alertes seront remontées à chaque fois que des modifications sont réalisées sur les « Paramètres de l'outil ».

7.1.3.12. Champ « Historique »

En cochant ce champ, des alertes seront remontées à chaque fois que des consultations sont réalisées sur « l'Historique ».

7.1.3.13. Champ « Clé Mère »

En cochant ce champ, des alertes seront remontées à chaque fois que la « Clé Mère » est modifiée.

7.1.3.14. Champ « SecretServer »

En cochant ce champ, des alertes seront remontées à chaque fois que le « SecretServer » est arrêté.

7.1.3.15. Champ « Sauvegarde »

En cochant ce champ, des alertes seront remontées à chaque fois qu'une « Sauvegarde » est lancée.

7.1.3.16. Champ « Restauration »

En cochant ce champ, des alertes seront remontées à chaque fois qu'une « Restauration » est lancée.

7.1.4. Champ « Alerte remontée via Syslog »

Si cette option est activée, les alertes émises sur l'accès aux Secrets sous surveillance ou les alertes cochées seront remontées via le flux « Syslog » du serveur hébergeant **SecretManager**.

Le champ situé en dessous permet de formater le message à inscrire dans le « syslog ». Chaque code est préfixé par un « % ». Ces codes sont remplacés au moment de la génération des messages. Voir le chapitre « 7.1.5.6 » pour plus d'information sur ces codes.

7.1.5. Champ « Alerte remontée via Courriel »

Si cette option est activée, les alertes émises seront remontées via le flux « Courriel ». Pour cela, il faut qu'un serveur de messagerie soit installé sur le même serveur que celui du **SecretManager**.

7.1.5.1. Le champ « De »

Ce champ permet de préciser un nom d'émetteur pour les courriels d'alertes.

7.1.5.2. Le champ « A »

Ce champ permet de préciser un ou plusieurs noms de destinataires pour les courriels d'alertes.

7.1.5.3. Le champ « Titre »

Ce champ permet de préciser un titre aux courriels qui seront envoyés par le **SecretManager**.

7.1.5.4. Le champ « Type du corps »

Ce champ permet de préciser le type « mime » du courriel qui sera généré.

Pour l'instant, seul deux types sont gérés :

1. TEXT ;
2. HTML (défaut).

7.1.5.5. Le champ « Corps »

Ce champ permet de formater l'information que l'on désire remonter dans le courriel. La forme du Corps dépend du choix qui a été fait au niveau du « Type du corps » et le corps devra donc suivre le formalisme spécifié. Le corps par défaut est en « HTML » et il est structuré de la façon suivante :

```
<table>
<tr><td>User</td><td><b>%User</b></td></tr>
<tr><td>Date</td><td><b>%ActionDate</b></td></tr>
<tr><td>Action Performed</td><td><b>%Action</b></td></tr>

<tr><td>IP of the user</td><td><b>%UserIP</b></td></tr>
<tr><td>Group of Secrets</td><td><b>%GroupSecrets</b></td></tr>
<tr><td>Type</td><td><b>%SecretType</b></td></tr>
<tr><td>Environment</td><td><b>%SecretEnvironment</b></td></tr>
<tr><td>Application</td><td><b>%SecretApplication</b></td></tr>
<tr><td>Host</td><td><b>%SecretHost</b></td></tr>
<tr><td>User</td><td><b>%SecretUser</b></td></tr>
<tr><td>Comment</td><td><b>%SecretComment</b></td></tr>
</table>
```

Dans cet exemple, on comprend que les informations seront formalisées dans un tableau.

On notera également que des mots clés sont disponibles. Les mots clés sont remplacés par l'information de contexte au moment de la création du courriel. Voici leur utilisation :

7.1.5.6. Codes possibles

Mot clé	Désignation
%User	Ce mot clé sera remplacé par le nom de connexion de l'utilisateur qui a réalisé l'action.
%ActionDate	Ce mot clé sera remplacé par la date et l'heure de la réalisation de l'action.
%Action	Ce mot clé sera remplacé par le libellé de l'action.
%UserIP	Ce mot clé sera remplacé par l'adresse IP de l'utilisateur qui a réalisé l'action.
%GroupeSecrets	Ce mot clé sera remplacé par le Groupe de Secrets auquel le Secret est rattaché.

%SecretType	Ce mot clé sera remplacé par le Type de Secret auquel le Secret est rattaché.
%SecretEnvironment	Ce mot clé sera remplacé par l'Environnement auquel le Secret est rattaché.
%SecretApplication	Ce mot clé sera remplacé par l'Application à laquelle le Secret est rattaché.
%SecretHost	Ce mot clé sera remplacé par le nom du Serveur ou l'URL auquel le Secret est rattaché.
%SecretUser	Ce mot clé sera remplacé par l'Utilisateur auquel le Secret est rattaché.
%SecretComment	Ce mot clé sera remplacé par le Commentaire auquel le Secret est rattaché

Ces mots clés peuvent être n'importe où dans le Corps du courriel et ils ne sont pas sensibles à la casse lors de leur recherche.

On pourrait également remonter les informations, comme un flux CSV. Par exemple sous la forme ci-dessous :

```
%User;%ActionDate;%Action;%UserIP;%GroupSecrets;%SecretType;%SecretEnvironment;%Sec
retApplication;%SecretHost;%SecretUser;%SecretComment
```

7.1.6. Bouton « Sauvegarder »

Ce bouton permet de sauvegarder l'ensemble des modifications effectuées dans cet onglet.

Important : si l'Administrateur change d'onglet sans avoir sauvegardé, il perd ses modifications.

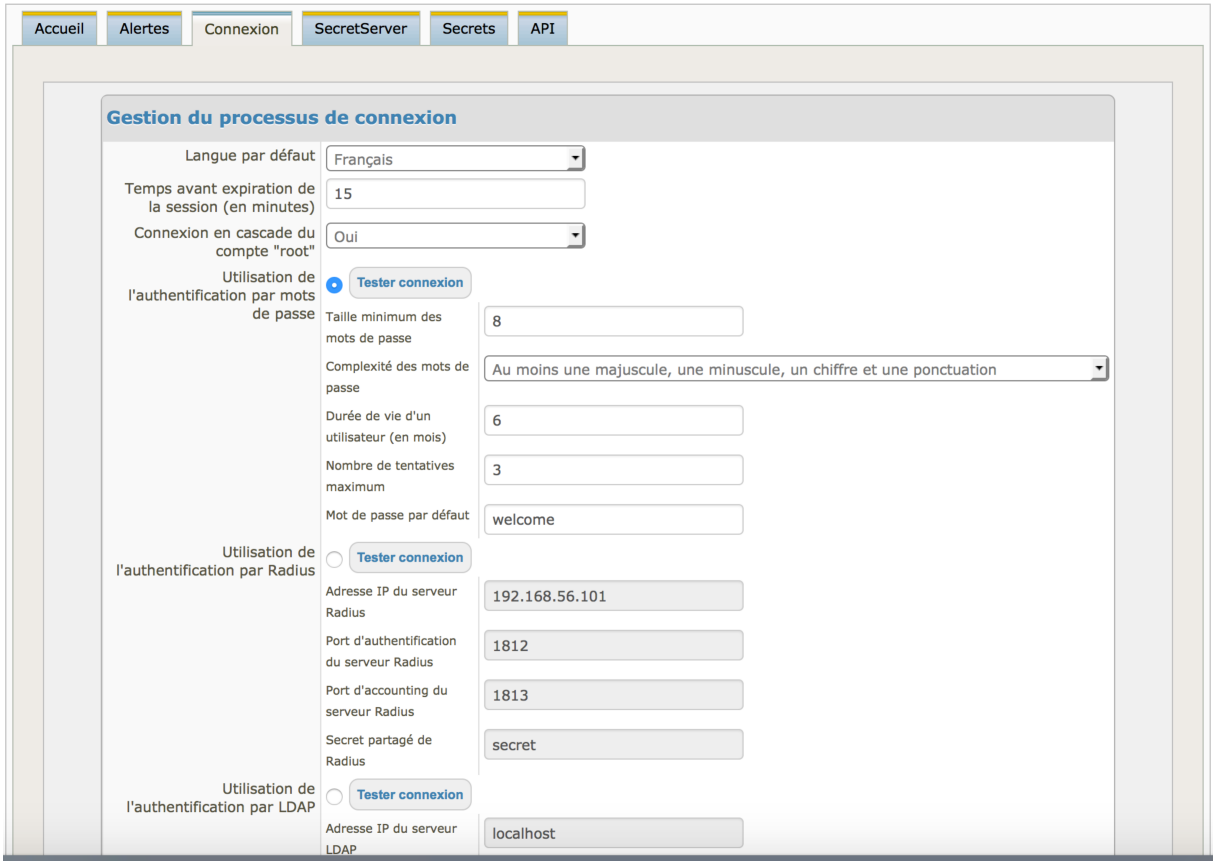
7.2. Gestion des « Connexions »

Par défaut, l'authentification des utilisateurs se fait par mot de passe et ces mots de passe sont stockés dans la base de données du **SecretManager**. Toutefois, afin de faciliter l'intégration de **SecretManager**, il est possible de décentraliser l'authentification :

- Sur un serveur Radius ;
- Sur un serveur LDAP.

Le fait d'utiliser une authentification décentralisée n'exonère pas l'Administrateur de créer et de maintenir les utilisateurs dans le SecretManager. On ne parle ici que du moyen d'authentification afin de limiter la profusion des mots de passe dans votre Système d'Information. Pour autant, les droits spécifiques des « Utilisateurs » et leurs rattachements à des « Groupes de Secret » ne sont gérés qu'à l'intérieur du SecretManager.

Pour gérer les authentifications des utilisateurs, l'Administrateur doit cliquer sur l'onglet « Connexion ». Il arrivera dans l'écran ci-dessous :



L'outil gère **3** types d'authentification pour les utilisateurs :

1. Authentification par mot de passe (interne à l'outil) ;
2. Authentification par Radius ;
3. Authentification par LDAP.

Pour passer d'un type d'authentification à l'autre, il faut utiliser le bouton radio en fasse du type choisi.

En sélectionnant un type d'authentification, les champs des autres types d'authentification se grisent.

7.2.1. Temps avant expiration de la session

Le temps avant expiration d'une session s'exprime en minute. Ce temps correspond au temps d'inactivité de l'utilisateur dans l'outil « SecretManager ». Par exemple, si le champ est valorisé à « 10 », l'utilisateur devra se reconnecter après 10 minutes d'inactivité.

7.2.2. Langue par défaut

La langue par défaut est la langue proposée avant que l'utilisateur n'ait fait son choix.

La notion de langue permet de changer les libellés de l'interface.

Par la suite, c'est la langue que l'utilisateur aura retenu dans sa session qui sera prioritaire (mais uniquement le temps de la session).

7.2.3. Connexion en cascade du compte « root »

Jusqu'à la version v0.9-1, quand on basculait le mode de « connexion », cette bascule s'appliquait à tous les utilisateurs, même au compte « root ».

Ce qui posait un problème, car suite à un changement hasardeux, par exemple suite à une bascule sur Radius, si vous aviez fait une erreur de saisie lors du paramétrage, vous ne pouviez plus vous connecter au « SecretManager ».

Désormais, en autorisant la connexion en cascade du compte « root », vous pouvez, si les OTP Radius ne fonctionnent pas taper le mot de passe interne du compte « root » et ainsi pouvoir malgré tout vous connecter.

Attention : ceci n'est valable qu'avec et seulement pour le compte « root ». Les comptes « superadmin » ne bénéficient pas de ce mode de connexion.

Par défaut, ce mode de connexion est activé. Toutefois, vous pouvez le désactiver ici.

7.2.4. Authentification par mot de passe

Attention : ces paramètres seront stockés dans le fichier :

`DIR_LIBRARIE/Config_Authentication.inc.php` (`DIR_LIBRARIE` est une constante définie dans le fichier « `Constants.inc.php` »). Assurez-vous que le serveur « Apache » exécutant « SecretManager » est les droits d'écriture sur ce fichier.

Les mots de passe sont stockés chiffrés en local dans la base de « SecretManager ».

7.2.4.1. Le champ « Taille minimum des mots de passe »

Cette information fixe la taille minimum des mots de passe que les utilisateurs devront saisir dans le système. Cette information n'est évaluée qu'au moment de la création ou de la modification d'un mot de passe. Elle n'a pas d'incidence sur un mot de passe qui a déjà été créé.

7.2.4.2. Le champ « Complexité des mots de passe »

Cette liste permet de choisir le niveau de complexité des mots de passe. Une fois encore, cette valeur n'est prise en compte qu'au moment de la saisie du mot de passe et n'influence pas les mots de passe déjà saisis.

7.2.4.3. Le champ « Durée de vie d'un utilisateur (en mois) »

Ce chiffre précise le nombre de mois avant l'expiration d'un utilisateur après sa création.

7.2.4.4. Le champ « Nombre de tentative maximum »

Cette information permet de désactiver un compte au-delà de ce nombre de tentative. Effectivement, quand un utilisateur saisi un mauvais de passe, on incrémente en base son nombre de tentative. Ce nombre en base ne doit pas excéder ce nombre de tentative maximum, sinon le compte est désactivé.

7.2.4.5. Le champ « Mot de passe par défaut »

Quand l'administrateur créé un nouvel utilisateur, ce dernier se trouve créé avec ce mot de passe par défaut. Il sera obligé de le changer dès la première connexion.

7.2.5. Authentification par Radius

Attention : ces paramètres seront stockés dans le fichier :

`DIR_LIBRARIE/Config_Radius.inc.php` (`DIR_LIBRARIE` est une constante définie dans le fichier « `Constants.inc.php` »). Assurez-vous que le serveur « Apache » exécutant « **SecretManager** » est les droits d'écriture sur ce fichier.

Plutôt que d'utiliser un mot de passe statique, il est possible d'utiliser des authentifications Radius.

Pour ce faire, il faut renseigner les champs ci-dessous :

- Adresse IP du serveur Radius ;
- Port d'authentification du serveur Radius ;
- Port d'accounting du serveur Radius ;
- Secret partagé de Radius

Un serveur Radius est particulièrement intéressant pour gérer des mots de passe jetables.

7.2.5.1. Adresse IP du serveur Radius

Ce champ permet d'indiquer l'adresse IP du serveur Radius afin de pouvoir lui envoyer le « challenge » de l'utilisateur.

7.2.5.2. Port d'authentification du serveur Radius

Depuis quelques temps, la norme sur les ports Radius a changé. Mais au-delà de cette nouvelle norme, il est normal de pouvoir changer les ports afin de pouvoir s'intégrer dans des systèmes d'information complexes.

7.2.5.3. Port d'accounting du serveur Radius

Depuis quelques temps, la norme sur les ports Radius a changé. Mais au-delà de cette nouvelle norme, il est normal de pouvoir changer les ports afin de pouvoir s'intégrer dans des systèmes d'information complexes.

7.2.5.4. Secret partagé de Radius

Ce champ permet de définir le secret partagé entre « **SecretManager** » et le serveur Radius. Le secret est partagé est utilisé pour chiffrer et déchiffré les challenges envoyés au serveur Radius.

7.2.6. Authentification par LDAP

Attention : ces paramètres seront stockés dans le fichier :

`DIR_LIBRARIE/Config_LDAP.inc.php` (`DIR_LIBRARIE` est une constante définie dans le fichier « `Constants.inc.php` »). Assurez-vous que le serveur « Apache » exécutant « **SecretManager** » est les droits d'écriture sur ce fichier.

Plutôt que d'utiliser un mot de passe spécifique, il est possible d'utiliser son mot de passe d'Entreprise. Pour ce faire, « **SecretManager** » peut s'interface avec l'annuaire d'Entreprise.

Pour ce faire, il faut renseigner les champs ci-dessous :

- Adresse IP du serveur LDAP ;
- Port du serveur LDAP ;
- Version du protocole LDAP ;
- Organisation du LDAP ;
- Préfixe RDN LDAP.

En utilisant un annuaire d'Entreprise, vous pouvez mettre en place une authentification centralisée de toutes vos applications.

7.2.6.1. Adresse IP du serveur Radius

Ce champ permet d'indiquer l'adresse IP du serveur LDAP afin de pouvoir lui envoyer la « demande d'authentification » de l'utilisateur.

7.2.6.2. Port du serveur Radius

Ce champ permet de préciser le port d'écoute du serveur LDAP.

7.2.6.3. Version du protocole LDAP

Normalement, tous les derniers serveurs LDAP supportent la **version 3** du protocole LDAP. Toutefois, pour des raisons de compatibilité, il est possible de préciser une version inférieure.

7.2.6.4. Organisation du LDAP

Ce champ permet de définir l'organisation (au sens « ou ») retenu dans le LDAP. Cette information doit être récupérée auprès de l'Administrateur du LDAP.

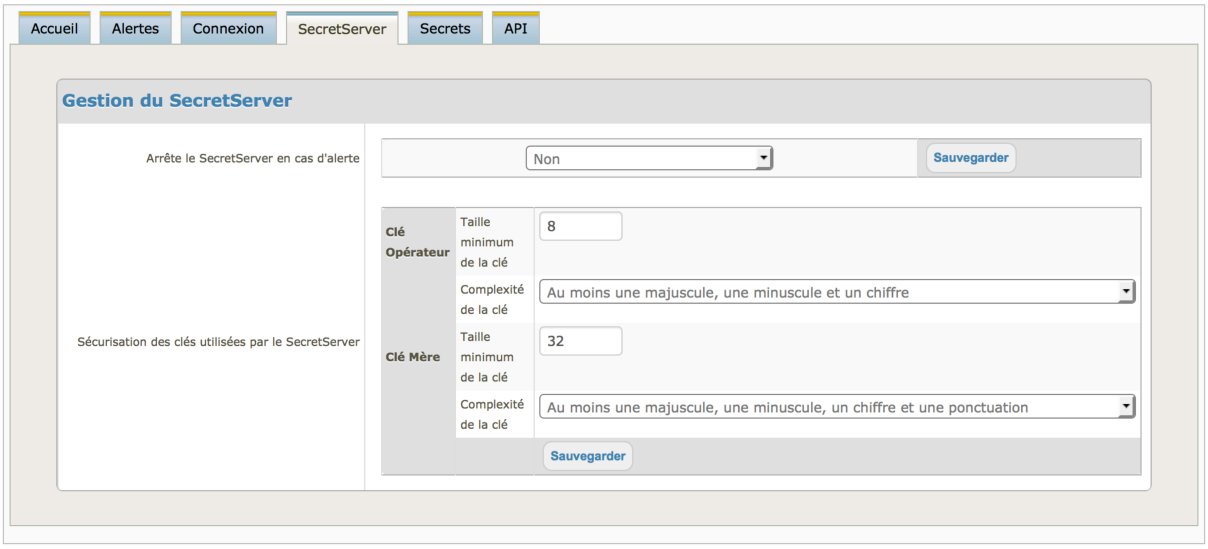
7.2.6.5. Préfixe RDN LDAP

Ce champ permet de définir le préfixe des « RDN » retenu dans le LDAP. Cette information doit également être récupérée auprès de l'Administrateur du LDAP.

7.3. Gestion du « SecretServer »

Le « **SecretServer** » est un service qui doit tourner en tâche de fond sur le serveur hébergeant le « **SecretManager** ». Ce service doit être démarré automatiquement lors des étapes de démarrage du serveur. L'initialisation du « **SecretServer** » doit faire l'objet d'une cérémonie d'initialisation. Effectivement, lors de la cérémonie d'initialisation, il faut utiliser la « clé Opérateur » utile au déchiffrement de la « clé Mère ». La clé Mère, quant à elle est utilisée pour chiffrer les Secrets à protéger dans la base de données du « **SecretManager** ».

Pour gérer le « **SecretServer** », l'Administrateur doit cliquer sur l'onglet « **SecretServer** ». Il arrivera dans l'écran ci-dessous :



Le « **SecretServer** » est un composant du « **SecretManager** ». Ce composant a pour rôle de protéger les clés et d'éviter qu'elles se retrouvent en clair dans un simple fichier.

Le « **SecretServer** » gère 3 clés :

1. La clé Mère : elle est utilisée pour chiffrer et déchiffrer les Secrets dans la base de données ;
2. La clé Opérateur : elle est utilisée pour chiffrer et déchiffrer la clé mère quand cette dernière est stockée dans son fichier ;
3. Les clés de transport : elles sont utilisées pour transporter les informations entre le « **SecretManager** » et le « **SecretServer** ». Ces dernières sont gérées automatiquement et ne nécessite aucune intervention particulière de la part de l'administrateur.

7.3.1. Démarrer le « SecretServer »

Le « **SecretServer** » ne peut pas être démarré par le « **SecretManager** ». Le « **SecretServer** » doit être démarré par l'Administrateur et sur le même serveur que le « **SecretManager** ». Pour plus d'information, il faut lire le document « » relatif à l'Installation de « **SecretManager** »

7.3.2. Champ « Arrête le SecretServer en cas d'alerte »

Le « **SecretServer** » participe aux contrôles d'intégrité des fichiers sensibles du « **SecretManager** ». Par conséquent, il peut générer des alertes quand il détecte que des fichiers sensibles ont été modifiés. Ce champ permet de pouvoir forcer l'arrêt du « **SecretServer** » afin de limiter le risque de perte de confidentialité.

7.3.3. Zone Sécurisation des clés utilisées par le SecretServer

7.3.3.1. Clé Opérateur

Le « **SecretManager** » peut proposer dans sa gestion la création de la clé « Opérateur », pour ce faire, il utilisera les valeurs précisées comme suit :

- Taille minimum de la clé ;
- Complexité de la clé.

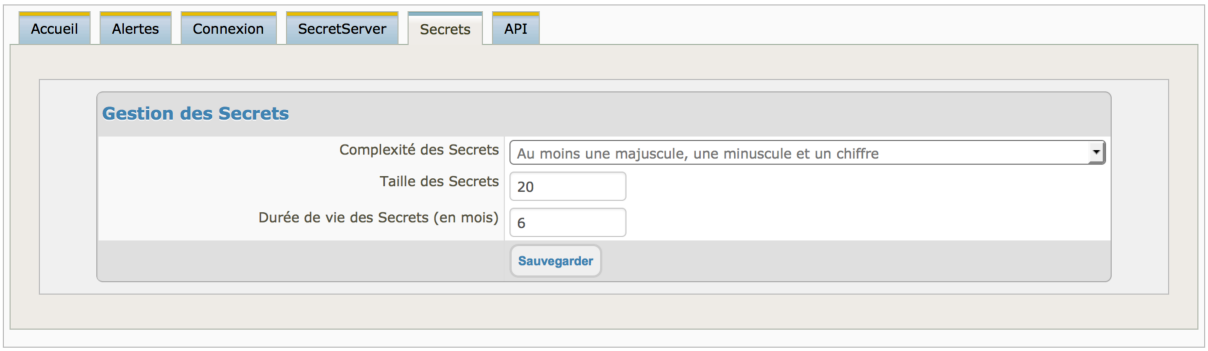
Une clé qui sera saisie manuellement recevra une notification lors de la saisie si la construction de la clé ne respecte pas ces deux valeurs. Pour autant, l'administrateur peut saisir une clé ne respectant pas les valeurs indiquées.

7.3.3.2. Clé Mère

La gestion de la clé Mère fonctionne sur le même principe que celle de la clé Opérateur.

7.4. Gestion des « Secrets »

Cet onglet permet de gérer la création automatique des Secrets quand ceux-ci sont créés par l'utilisation des boutons de « Création ».



7.4.1. Champ « Complexité des Secrets »

Il existe 4 niveaux de complexité :

1. Au moins une majuscule et une minuscule ;
2. Au moins une majuscule, une minuscule et un chiffre (choix par défaut) ;
3. Au moins une majuscule, une minuscule, un chiffre et une ponctuation ;
4. Au moins une majuscule, une minuscule, un chiffre, une ponctuation et un accentué ;

7.4.2. Champ « Taille des Secrets »

Taille minimum des Secrets quand ils seront créés.

7.4.3. Champ « Durée de vie des Secrets (en mois)

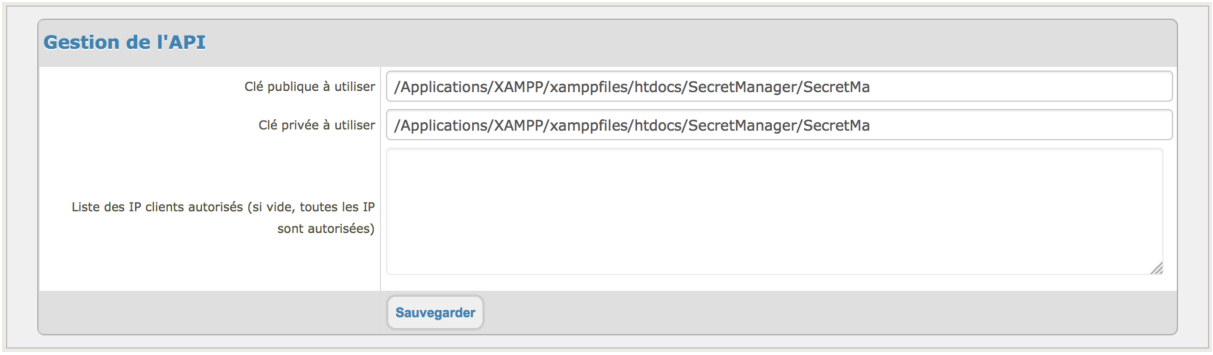
Nombre de mois à calculer à partir de la date de création.

7.4.4. Bouton « Sauvegarder »

Ce bouton permet de sauvegarder toutes les modifications qui ont été réalisées.

7.5. Gestion de l'API

Cet onglet permet de gérer le paramétrage de l'API.



7.5.1. Champ « Clé publique à utiliser »

Indique la localisation et le nom du fichier contenant certificat à utiliser par le Client utilisant l'API et pour chiffrer ses messages vers le Serveur.

7.5.2. Champ « Clé privée à utiliser »

Indique la localisation et le nom du fichier contenant la clé privé qui sera utilisé pour déchiffrer les requêtes envoyées par les Clients de l'API.

7.5.3. Champ « Liste des IP clients autorisés (si vide, toutes les IP sont autorisées) »

Indique toutes les adresses IP qui sont autorisées à utiliser l'API. Les adresses peuvent être séparées par des virgules ou des points virgules.

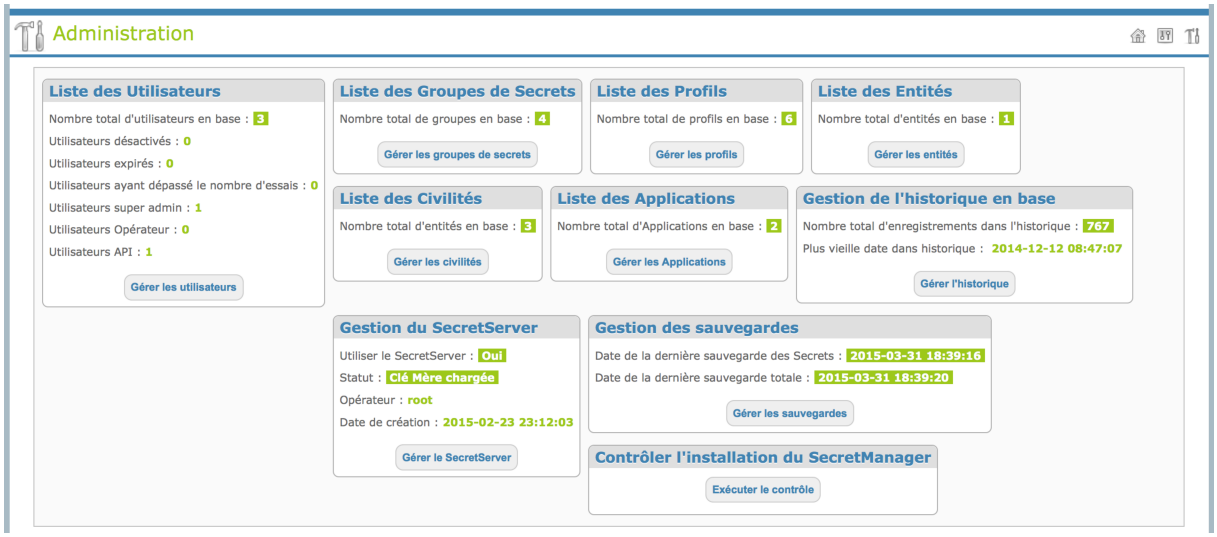
Si aucune adresse n'est précisée, alors toutes les adresses sont autorisées.

8. TABLEAU DE BORD DE L'ADMINISTRATION

8.1. Ecran central d'Administration

Pour accéder à l'écran central d'Administration, l'administrateur doit utiliser le bouton ci-dessous :

Il arrive dans l'écran ci-dessous :



Cet écran donne, en un coup d'œil, une vision globale des objets administrés par le « **SecretManager** ».

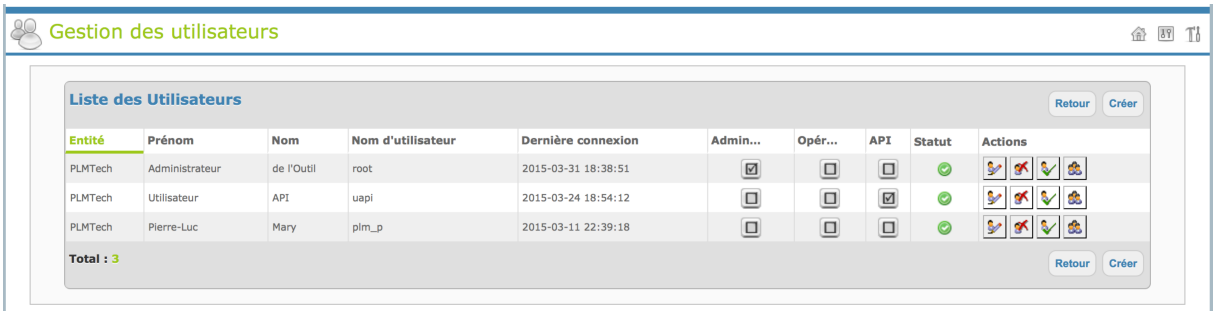
8.2. Gestion des utilisateurs

8.2.1. Accéder à l'écran de gestion des utilisateurs

Il faut utiliser la boite de synthèse dédiée aux Utilisateurs, comme dans l'exemple ci-dessous :

Le bouton « Gérer les utilisateurs » permet d'entrer dans l'écran de gestion des Utilisateurs.

8.2.2. Ecran liste des utilisateurs



Tous les utilisateurs créés doivent apparaître dans ce tableau.

Ce tableau est composé des colonnes suivantes :

- Entité
- Prénom
- Nom
- Nom d'utilisateur
- Dernière connexion
- Administrateur
- Opérateur
- API
- Statut
- Actions

8.2.2.1. Colonne « Entité »

Cette information correspond à l'entité (la société ou le service) de rattachement de l'utilisateur.

8.2.2.2. Colonne « Prénom »

Cette information correspond au prénom usuel de l'utilisateur.

8.2.2.3. Colonne « Nom »

Cette information correspond au nom usuel de l'utilisateur.

8.2.2.4. Colonne « Nom de l'utilisateur »

Cette information correspond au nom ou code de l'utilisateur (information utile à la connexion).

8.2.2.5. Colonne « Dernière connexion »

Cette information correspond à la date de dernière connexion réussie de l'utilisateur.

8.2.2.6. Colonne « Administrateur »

Cette information indique que l'utilisateur est un « administrateur ». Il peut donc accéder à tous les objets de l'outil et sans restriction d'accès aux secrets protégés par l'outil.

8.2.2.7. Colonne « Statut »

Cette information donne le statut de l'utilisateur. Ce statut peut avoir les valeurs suivantes :

Icône	Signification
	L'utilisateur ne rencontre aucun problème.
	L'utilisateur rencontre au moins un problème. Les problèmes possibles sont : Nombre de tentative de connexion excédé ; Utilisateur désactivé ; Date de dernière connexion trop ancienne ; Date d'expiration atteinte.

***Note** : la correction des problèmes sera vue dans le chapitre « **Erreur ! Source du renvoi introuvable.** ».*

8.2.2.8. Colonne « Actions »

Cette colonne contient tous les boutons permettant de gérer l'utilisateur courant (utilisateur situé sur la même ligne du tableau).

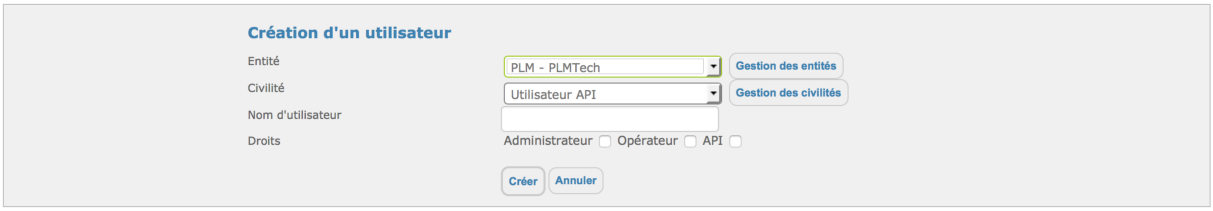
Bouton	Signification
	Ce bouton permet de modifier l'utilisateur de l'occurrence.
	Ce bouton permet de supprimer l'utilisateur de l'occurrence.
	Ce bouton permet de vérifier (visualiser en détail) l'utilisateur de l'occurrence.
	Ce bouton permet d'associer des Profils à l'utilisateur. Les profils permettent de regrouper des accès à des Groupes de Secrets.

8.2.3. Règles sur les données des « Utilisateurs »

1. Une Civilité peut être associée à plusieurs Utilisateurs ;
2. Un Utilisateur ne peut avoir qu'une seule Civilité ;
3. Le nom d'Utilisateur doit être unique.

8.2.4. Création d'un utilisateur

En cliquant sur le bouton « Créer », l'administrateur arrive dans l'écran ci-dessous :



8.2.4.1. Liste déroulante « Entité »

Cette liste présente les différentes « Entités » définies dans l'outil. Si cette liste n'était complète, l'Administrateur pourrait utiliser le bouton « Gestion des entités ».

8.2.4.2. Bouton « Gestion des entités »

Ce bouton permet de créer, modifier ou supprimer des « Entités ».

8.2.4.3. Liste déroulante « Civilité »

Cette liste présente les différentes « Civilités » définies dans l'outil. Si cette liste n'était complète, l'Administrateur pourrait utiliser le bouton « Gestion des civilités ».

8.2.4.4. Bouton « Gestion des civilités »

Ce bouton permet de créer, modifier ou supprimer des « Civilités ».

8.2.4.5. Champ « Nom d'utilisateur »

Ce champ permet à l'Administrateur de saisir le « Nom de l'utilisateur ». Cette information doit être unique dans l'outil. Le « Nom de l'utilisateur » représente le nom technique, le compte de l'usager. Ce champ doit être une chaine alphanumérique de maximum 20 caractères.

8.2.4.6. Boîte à cocher « Administrateur »

Cette boîte à cocher permet de donner ou pas le droit « Administrateur » à un utilisateur.

Attention : le droit « Administrateur » donne un accès TOTAL à TOUS les écrans de l'outil SecretManager. Cette boîte à cocher n'est donc pas à utiliser à la légère. Cette boîte à cocher stocke un booléen.

8.2.4.7. Boîte à cocher « Opérateur »

Cette boîte à cocher permet de donner ou pas le droit « Opérateur » à un utilisateur.

Ce droit permet d'accéder à certaines options de « l'Administrateur ». Comme pouvoir initialiser l'environnement de chiffrement (saisit de la clé opérateur qui protège la clé mère), d'arrêter le « SecretServer » et réaliser les sauvegardes et les restaurations de « SecretManager ».

8.2.4.8. Boîte à cocher « API »

Cette boîte à cocher permet de donner ou pas le droit « API » à un utilisateur. Ce droit interdit l'utilisateur de se connecter ultérieurement à l'IHM. Cet utilisateur sera limité à la création et à la modification de Secrets.

> ***Remarque :*** *par défaut, le mot de passe d'Entreprise est affecté à la création de l'utilisateur. Voir le chapitre « 7.2.4.5 » pour plus d'information sur le mot de passe d'Entreprise.*

8.2.5. Modification d'un utilisateur

En cliquant sur le bouton  , l'administrateur arrive sur l'écran ci-dessous :

8.2.5.1. Liste déroulante « Entité »

Permet de sélectionner l'entité de rattachement (la société) de l'Utilisateur. Cette information permet de pouvoir regrouper et classer les utilisateurs par la suite. Cela n'a pas d'incidence sur l'accès aux Secrets.

8.2.5.2. Bouton « Gestion des entités »

Ce bouton permet de pouvoir accéder directement à l'écran de gestion des « Entités ». Ainsi l'administrateur peut créer ou modifier une « Entité ».

8.2.5.3. Champ « Civilité »

Permet de sélectionner un prénom et nom à un Utilisateur. On note qu'une « Civilité » peut être rattaché à plusieurs « Utilisateurs », mais pas l'inverse. Effectivement, un « Utilisateur » ne peut avoir qu'une seule « Civilité ». Cette information permet également de pouvoir regrouper et classer les utilisateurs par la suite. Cela n'a pas d'incidence sur l'accès aux Secrets ultérieurement.

8.2.5.4. Bouton « Gestion des civilités »

Ce bouton permet de pouvoir accéder directement à l'écran de gestion des civilités. Ainsi l'administrateur peut créer ou modifier une « Civilité ».

8.2.5.5. Champ « Nom d'utilisateur »

Permet de spécifier le nom de l'utilisateur à la connexion (login). Ce nom doit être unique.

8.2.5.6. Boîte à cocher « Administrateur »

Cette boîte à cocher permet de préciser si l'utilisateur est un « administrateur » de l'outil « SecretManager ».

Important : on notera que n'importe quel utilisateur peut être « administrateur ». On comprend également que le compte « `root` » peut-être détruit. Il faut juste veiller à toujours avoir au moins un utilisateur « administrateur de l'outil.

A partir du moment où un Utilisateur est déclaré « administrateur », il accède à TOUS les secrets de l'outil et cela même s'il n'est pas rattaché à des « Profils ».

8.2.5.7. Boîte à cocher « Opérateur »

Cette boîte à cocher permet de donner ou pas le droit « Opérateur » à un utilisateur.

Ce droit permet d'accéder à certaines options de « l'Administrateur ». Comme pouvoir initialiser l'environnement de chiffrement (saisit de la clé opérateur qui protège la clé mère), d'arrêter le « SecretServer » et réaliser les sauvegardes et les restaurations de « SecretManager ».

8.2.5.8. Boîte à cocher « API »

Cette boîte à cocher permet de donner ou pas le droit « API » à un utilisateur. Ce droit interdit l'utilisateur de se connecter ultérieurement à l'IHM. Cet utilisateur sera limité à la création et à la modification de Secrets.

8.2.5.9. Bouton « Réinitialiser le mot de passe »

Ce bouton permet de redonner le mot de passe défini au niveau de l'Entreprise. Il oblige également l'utilisateur à changer de mot de passe à sa première connexion. Voir le chapitre « 7.2.4.5 » pour en savoir plus.

8.2.5.10. Bouton « Réinitialiser le nombre de tentative »

Chaque tentative de connexion est comptabilisée, au-delà du nombre déclaré au niveau de l'Entreprise l'utilisateur est bloqué. Toutefois, le bouton « Réinitialiser le nombre de tentative » permet de remettre à zéro ce compteur. Voir le chapitre « 7.2.4.4 » pour en savoir plus.

8.2.5.11. Bouton « Réinitialiser la date d'expiration »

A la création d'un utilisateur, une date d'expiration est automatiquement calculée à partir du nombre de mois définit au niveau de l'Entreprise. Le bouton « Réinitialiser la date d'expiration » permet de recalculer cette date. Voir le chapitre « 7.2.4.3 » pour en savoir plus.

8.2.5.12. Bouton « Désactiver l'utilisateur » « Activer l'utilisateur »

Permet de pouvoir désactiver un utilisateur. Le bouton « Désactiver l'utilisateur » permet de désactiver l'utilisateur. A l'issue de la désactivation, le bouton se transforme en « Activer l'utilisateur », afin de pouvoir réaliser l'action inverse.

8.2.5.13. Bouton « Modifier »

Ce bouton permet de pouvoir sauvegarder toutes les modifications qui ont été réalisées.

8.2.5.14. Bouton « Annuler »

Ce bouton permet de quitter l'écran sans sauvegarder les éventuelles modifications.

8.2.6. Suppression d'un utilisateur

En cliquant sur le bouton  , vous arrivez sur l'écran ci-dessous :

8.2.6.1. Bouton « Supprimer »

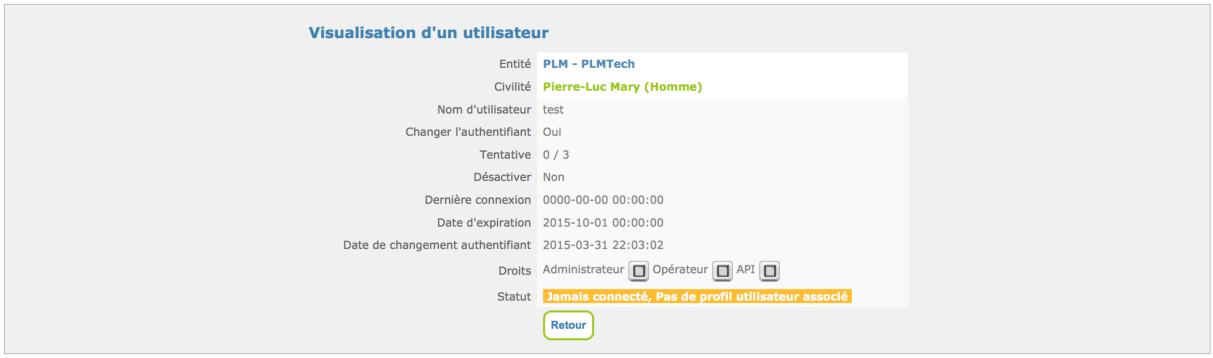
Ce bouton permet de valider la suppression de l'Utilisateur.

8.2.6.2. Bouton « Annuler »

Ce bouton permet de ne pas supprimer l'utilisateur et de revenir à la liste des utilisateurs.

8.2.7. Visualisation d'un utilisateur

En cliquant sur le bouton  , vous arrivez sur l'un des écrans ci-dessous :



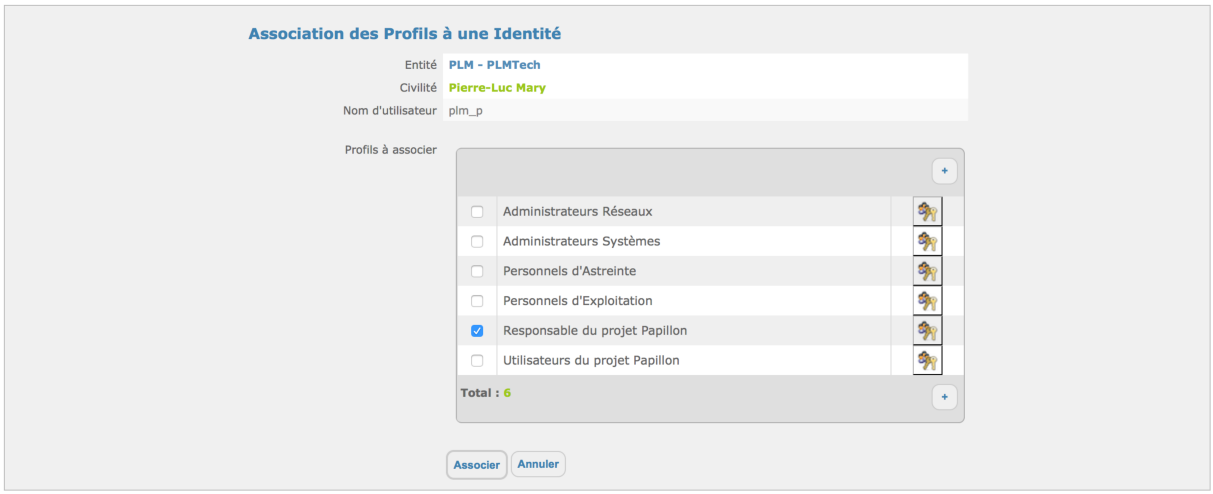
ou

8.2.7.1. Bouton « Retour »

Ce bouton permet de retourner à la liste des utilisateurs.

8.2.8. Association des Profils à une Identité

En cliquant sur le bouton  , vous arrivez sur l'écran ci-dessous :



Dans cet écran, il est possible de pouvoir associer ou pas des « Profils » à un « Utilisateur ». Ces profils permettent d'associer des accès à des « Groupes de Secrets ».

8.2.8.1. Bouton « + » (création d'un profil)

Ce bouton permet de créer à la volé un nouveau profil.

8.2.8.2. Boîtes à cocher

Ces boîtes à cocher permet d'associer ou non des « Profils » à un « Utilisateur ».

8.2.8.3. Bouton « Associer des Groupes de Secrets »

En cliquant sur le bouton  , vous arrivez sur l'écran ci-dessous :

Cet écran permet d'associer des droits entre le Profil sélectionné et les Groupes de Secrets existants.

8.3. Gestion des profils

Les profils ont 2 usages :

1. Ils permettent de regrouper l'accès à un ou plusieurs « Groupes de Secrets », tout en précisant un droit sur ces « Groupes de Secrets ».
2. Ils permettent de simplifier les associations entre les « Utilisateurs » et les « Groupes de Secrets ». Car, il n'est plus nécessaire de définir pour chaque « Utilisateur » les « Groupes de Secrets » auquel il a accès.

Il existe 2 façons d'accéder à l'écran de « Gestion des Profils » :

1. En passant par les écrans de Gestions des Utilisateurs, voir chapitre « 8.2.8 » ;
2. En utilisant le bouton « Gérer les Profils », à partir de l'écran « Tableaux de bord ».

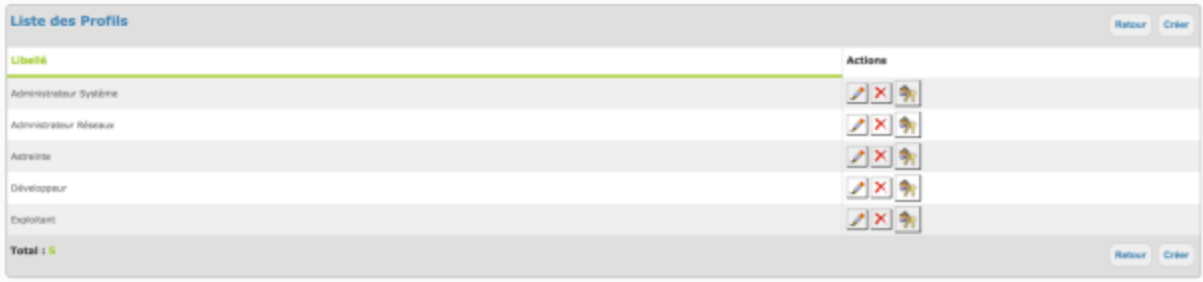
Dans les 2 cas, l'administrateur arrive dans l'écran ci-dessous :

8.3.1. Accéder à l'écran de gestion des profils

A partir de l'écran « Administration », il faut utiliser la boite de synthèse dédiée aux Profils, comme dans l'exemple ci-dessous :

Le bouton « Gérer les profils » permet d'entrer dans l'écran de gestion des Profils.

8.3.2. Ecran liste des « Profils »



8.3.3. Colonne « Libellé »

Le libellé est l'information textuelle d'un « Profil ».

8.3.4. Colonne « Actions »

Cette colonne contient tous les boutons permettant de gérer l'utilisateur courant (utilisateur situé sur la même ligne du tableau).

Bouton	Signification
	Ce bouton permet de modifier le « Profil ».
	Ce bouton permet de supprimer le « Profil ».
	Ce bouton permet d'associer des « Groupes de Secrets » au « Profil ».

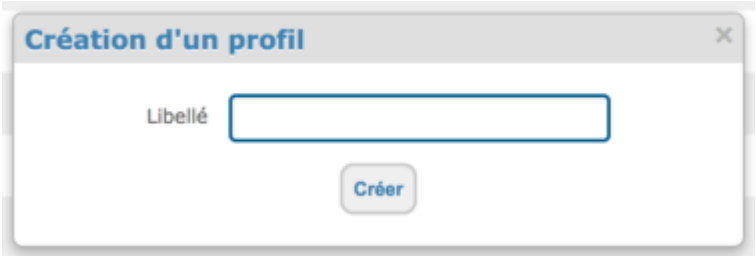
8.3.5. Règles sur un profil

1. Le libellé d'un profil doit être unique.

8.3.6. Créer un nouveau profil

Pour créer un nouveau profil, l'administrateur doit utiliser le bouton suivant : 

Ce bouton permet d'arriver dans l'écran ci-dessous :



8.3.6.1. Champ « Libellé »

Le libellé est le nom intelligible attribué à un « Profil ». C'est une chaîne alphanumérique de maximum 60 caractères.

8.3.6.2. Bouton « Créer »

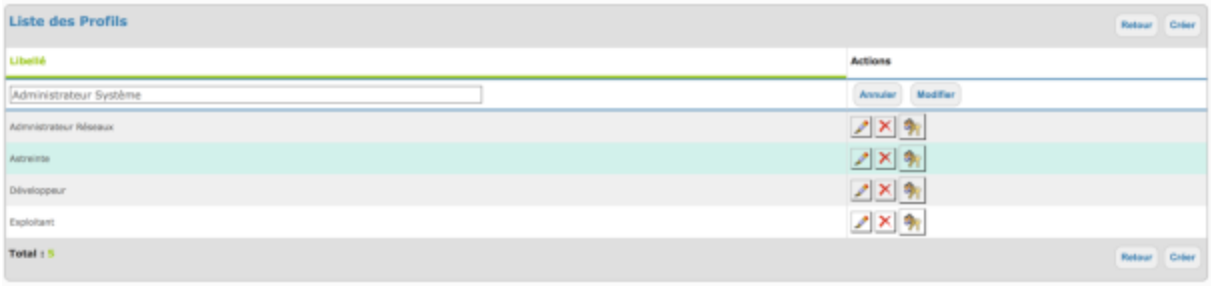
Ce bouton permet de valider la création d'un « Profil ».

8.3.6.3. Bouton « Annuler »

Ce bouton permet de quitter sans créer le profil et de revenir à la liste des « Profils ».

8.3.7. Modifier un profil

Pour modifier un « Profil », l'administrateur doit se positionner sur le bouton  de l'occurrence du « Profil » à modifier. L'administrateur verra l'occurrence devenir modifiable comme dans l'exemple ci-dessous (on parle de modification directement en ligne) :



8.3.7.1. Champ « Libellé »

L'administrateur peut changer le libellé du « Profil ».

8.3.7.2. Bouton « Modifier »

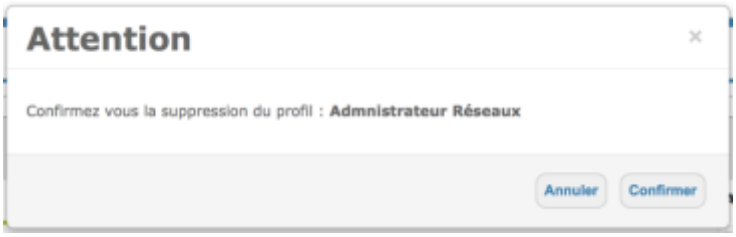
Ce bouton permet de sauvegarder la modification effectuée sur le « Profil ».

8.3.7.3. Bouton « Annuler »

Ce bouton permet de quitter l'écran sans sauvegarder la modification du « Profil ».

8.3.7.4. Supprimer un profil

Pour supprimer un « Profil », l'administrateur doit se positionner sur le bouton  de l'occurrence du « Profil » à supprimer. L'administrateur arrivera sur l'écran ci-dessous :



8.3.7.5. Bouton « Confirmer »

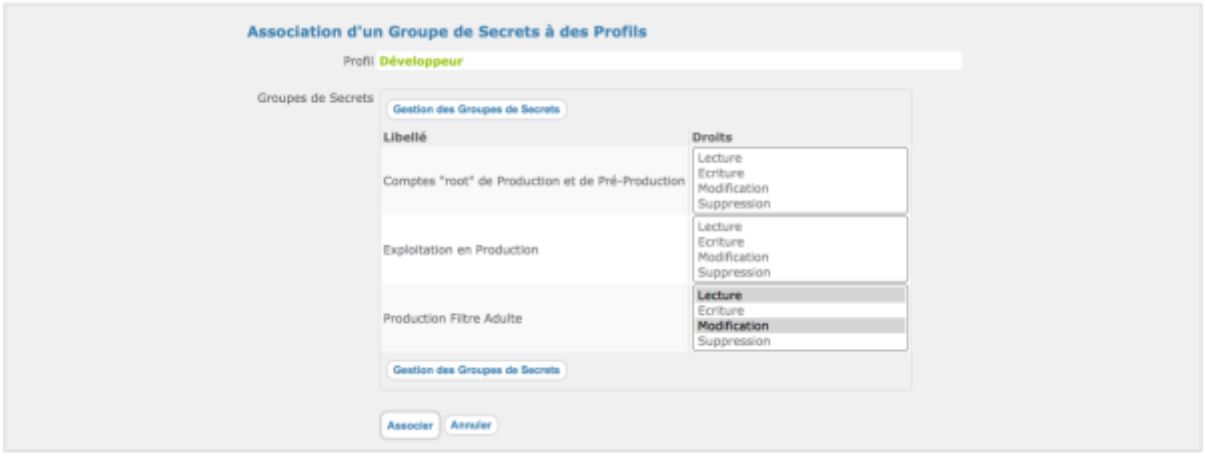
Ce bouton permet de confirmer la suppression du « Profil ».

8.3.7.6. Bouton « Annuler »

Ce bouton permet de quitter l'écran sans supprimer le « Profil ».

8.3.8. Associer des « Groupes de Secrets » à un « Profil »

Pour associer des « Groupes de Secrets » à un « Profil », l'administrateur doit se positionner sur le bouton  de l'occurrence du « Profil » à associer. L'administrateur arrivera sur l'écran ci-dessous :



8.3.8.1. Champ « Droits »

Il existe 4 niveaux de Droits :

1. Lecture : permet de pouvoir lire les « Secrets » contenus dans le « Groupe de Secrets » ;

2. Ecriture : permet de créer de nouveaux « Secrets » dans le « Groupe de Secrets » (dans l'écran « Tableaux de bord », le bouton « Créer » est disponible à l'utilisateur) ;
3. Modification : permet de modifier des « Secrets » contenus dans le « Groupe de Secrets » (dans l'écran « Tableaux de bord », le bouton « Modifier » est disponible sur l'occurrence pour lequel l'utilisateur à ce droit) ;
4. Suppression : permet de supprimer des « Secrets » contenus dans le « Groupe de Secrets » (dans l'écran « Tableaux de bord », le bouton « Supprimer » est disponible sur l'occurrence pour lequel l'utilisateur à ce droit).

Pour les sélectionner, l'Administrateur doit cliquer sur le ou les droits à sélectionner. Un droit, quand il est sélectionné, est en surbrillance.

Les droits s'attribuent sur chaque « Groupe de Secrets »

8.3.8.2. Bouton « Gestion des Groupes de Secrets »

Ce bouton permet d'accéder à l'écran de gestion des « Groupes de Secrets », se reporter au chapitre idoine pour plus d'information sur cette gestion.

8.3.8.3. Bouton « Associer »

Ce bouton sauvegarde tous les « Droits » que vous avez attribués entre ce « Profil » et ces « Groupes de Secrets ».

8.3.8.4. Bouton « Annuler »

Ce bouton quitte l'écran sans sauvegarder les modifications qui ont été effectuées.

8.4. Gestion des civilités

Les civilités permettent d'associer un prénom et un nom usuel à la notion d'utilisateur dans l'outil.

Il existe 2 façons d'arriver sur l'écran de « Gestion des civilités » :

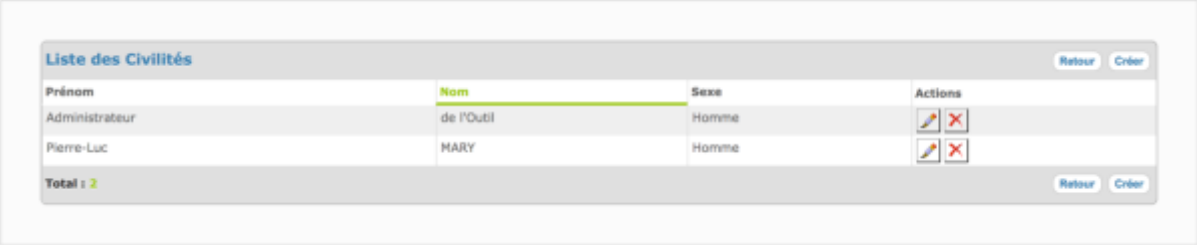
1. En passant par les écrans de Gestions des Utilisateurs, voir chapitre « **Erreur ! Source du renvoi introuvable.** » ;
2. En utilisant le bouton « Gérer les Civilités », à partir de l'écran « Tableaux de bord ».

8.4.1. Accéder à l'écran de gestion des civilités

A partir de l'écran « Administration », il faut utiliser la boite de synthèse dédiée aux Civilités, comme dans l'exemple ci-dessous :

Le bouton « Gérer les civilités » permet d'entrer dans l'écran de gestion des Civilités.

8.4.2. Ecran liste des civilités



8.4.2.1. Colonne « Prénom »

Le « Prénom » est une des informations usuelles de la « Civilité ».

8.4.2.2. Colonne « Nom »

Le « Nom » est une des informations usuelles de la « Civilité ».

8.4.2.3. Colonne « Sexe »

Le « Sexe » est une information complémentaire permettant de limiter les homonymes.

8.4.2.4. Colonne « Actions »

Cette colonne contient tous les boutons permettant de gérer l'utilisateur courant (utilisateur situé sur la même ligne du tableau).

Bouton	Signification
	Ce bouton permet de modifier la « Civilité ».
	Ce bouton permet de supprimer la « Civilité ».

8.4.2.5. Bouton « Retour »

Ce bouton permet de revenir à l'écran précédent.

8.4.2.6. Bouton « Créer »

Ce bouton permet d'exécuter la création d'une nouvelle « Civilité ».

8.4.3. Règles sur les civilités

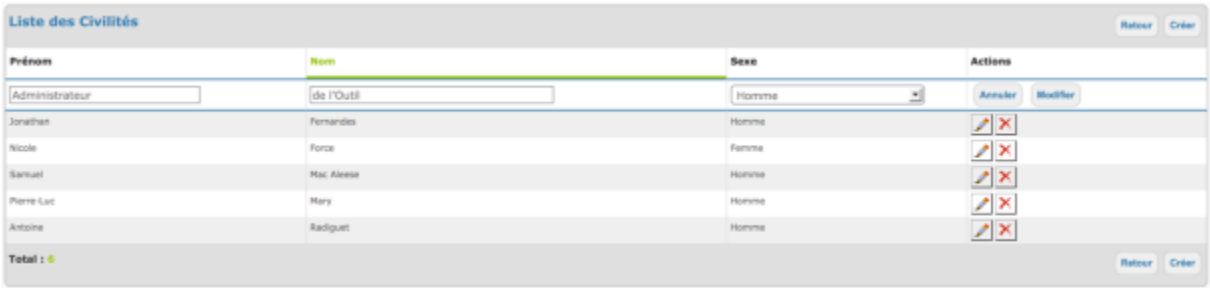
1. Il ne peut y avoir 2 civilités ayant un même prénom, nom et sexe.

8.4.4. Création

Pour créer une civilité, l'administrateur doit cliquer sur le bouton « Créer ». Il arrivera sur l'écran ci-dessous :

8.4.5. Modification d'une civilité

Pour modifier une civilité, l'administrateur doit cliquer sur le bouton «  » de l'occurrence à modifier.
Alors l'occurrence se modifiera (en ligne) comme ci-dessous :



8.4.5.1. Champ « Prénom »

Le « Prénom » est une chaîne alphanumérique de maximum 25 caractères.

8.4.5.2. Champ « Nom »

Le « Nom » est une chaîne alphanumérique de maximum 35 caractères.

8.4.5.3. Liste déroulante « Sexe »

Cette liste permet de sélectionner le sexe à attribuer à la « Civilité ».

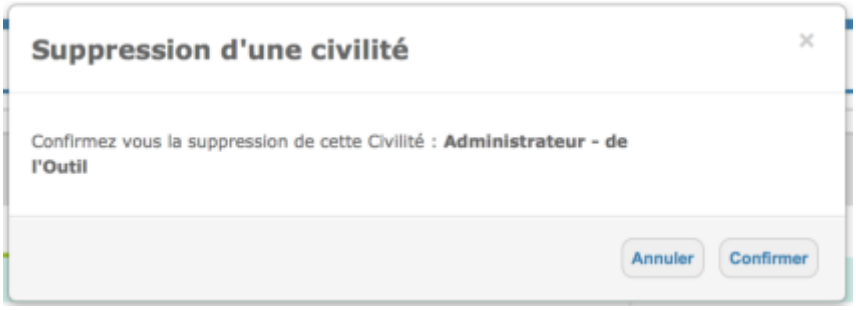
8.4.5.4. Bouton « Créer » ou « Modifier »

Ce bouton permet de valider la création ou la modification de la « Civilité ».

8.4.5.5. Bouton « Annuler »

Ce bouton permet de quitter l'écran sans avoir créer ou modifier la « Civilité ».

8.4.6. Suppression d'une civilité



8.4.6.1. Bouton « Confirmer »

Ce bouton permet de valider la suppression de la « Civilité » sélectionnée.

8.4.6.2. Bouton « Annuler »

Ce bouton permet d'abandonner la suppression de la « Civilité » sélectionnée.

8.5. Gestion des Entités

Les « Entités » permettent de pouvoir regrouper les utilisateurs. Ce regroupement ne permet pas d'avoir accès à des « Secrets », il permet véritablement les utilisateurs entre eux.

Il existe 2 façons d'arriver sur l'écran de « Gestion des entités » :

1. En passant par les écrans de Gestions des Utilisateurs, voir chapitre « **Erreur ! Source du renvoi introuvable.**8.2.4.1 » ;
2. En utilisant le bouton « Gérer les Civilités », à partir de l'écran « Tableaux de bord ».

8.5.1. Accéder à l'écran de gestion des entités

A partie de l'écran « Administration », il faut utiliser la boite de synthèse dédiée aux Entités, comme dans l'exemple ci-dessous :

Le bouton « Gérer les entités » permet d'entrer dans l'écran de gestion des Entités.

8.5.2. Ecran liste des entités

8.5.2.1. Colonne « Code »

Le « Code » est le nom court d'une « Entité ».

8.5.2.2. Colonne « Libellé »

Le « Libellé » est le nom long d'une « Entité ».

8.5.2.3. Colonne « Actions »

Cette colonne contient tous les boutons permettant de gérer l'utilisateur courant (utilisateur situé sur la même ligne du tableau).

Bouton	Signification
	Ce bouton permet de modifier le « Entité ».
	Ce bouton permet de supprimer le « Entité ».

8.5.2.4. Bouton « Retour »

Ce bouton permet de revenir à l'écran précédent.

8.5.2.5. Bouton « Créer »

Ce bouton permet d'exécuter la création d'une nouvelle « Entité ».

8.5.3. Règles sur les entités

1. Il ne peut y avoir 2 « Entités » avec le même « Code » ou le même « Libellé ».

8.5.4. Création ou Modification d'une entité

Pour créer une « Entité », l'administrateur doit cliquer sur le bouton « Créer ». Il arrivera sur l'écran ci-dessous :

En revanche, si l'administrateur utilise le bouton «  », l'occurrence deviendra modifiable, comme dans l'exemple ci-dessous :

8.5.4.1. Champ « Code »

Le « Code » est une chaîne alphanumérique de maximum 10 caractères.

8.5.4.2. Champ « Libellé »

Le « Libellé » est une chaîne alphanumérique de maximum 60 caractères.

8.5.4.3. Bouton « Annuler »

Ce bouton permet de revenir à l'écran précédent, sans créer ou modifier une « Entité ».

8.5.4.4. Bouton « Créer » ou « Modifier »

Ces boutons, en fonction des cas, permettent de valider la création ou la modification de « l'Entité ».

8.5.5. Suppression d'une entité

Pour supprimer une « Entité », l'administrateur doit cliquer sur le bouton «  ». Il arrivera sur l'écran ci-dessous :

8.5.5.1. Bouton « Annuler »

Ce bouton permet de revenir à l'écran précédent, sans supprimer une « Entité ».

8.5.5.2. Bouton « Confirmer »

Ce bouton permet de valider la suppression de « l'Entité ».

8.6. Gestion des Groupes de Secrets

Les « Groupes de Secrets » permettent de pouvoir regrouper les « Secrets » de même sensibilité. C'est avec les « Groupes de Sécurité » que l'on gère les droits accès aux « Secrets ». Les droits d'accès se définissent au moment de l'association d'un « Groupe de Secrets » et d'un « Profil Utilisateur ». Effectivement, d'un « Profil Utilisateur » à un autre, il peut être utile de pouvoir attribuer des droits d'accès en fonction du rôle des Utilisateurs.

Les « Droits d'accès » possibles sur un « Groupe de Secrets » sont :

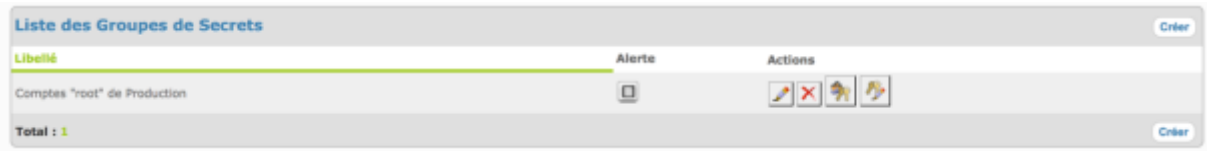
1. Lecture ;
2. Ecriture ;
3. Modification ;
4. Suppression.

8.6.1. Accéder à l'écran de gestion des groupes de secrets

Pour accéder à l'écran de gestion des Groupes de Secrets, l'administrateur doit utiliser le bouton comme dans l'exemple ci-dessous :

Le bouton « Gérer les groupes de secrets » permet d'entrer dans l'écran de gestion des Groupes de Secrets.

8.6.2. Ecran liste des « Groupes de Secrets »



8.6.2.1. Colonne « Libellé »

Le « Libellé » est le nom d'un « Groupe de Secrets ».

8.6.2.2. Colonne « Alerte »

La boîte à cocher permet de remonter une alerte pour tous les « Secrets » qui seront accédés par la suite. Les moyens de remonter des alertes sont paramétrables. Il faut se reporter au chapitre 9 « Gestion des préférences ».

8.6.2.3. Colonne « Actions »

Cette colonne contient tous les boutons permettant de gérer l'utilisateur courant (utilisateur situé sur la même ligne du tableau).

Bouton	Signification
	Ce bouton permet de modifier le « Groupe de Secrets ».
	Ce bouton permet de supprimer le « Groupe de Secrets ».
	Ce bouton permet d'associer un « Groupe de Secrets » avec un « Profil Utilisateur ».
	Ce bouton permet de gérer les « Secrets » dans le « Groupe de Secrets ».

8.6.2.4. Bouton « Retour »

Ce bouton permet de revenir à l'écran précédent (écran tableau de bord).

8.6.2.5. Bouton « Créer »

Ce bouton permet d'exécuter la création d'un nouveau « Groupe de Secrets ».

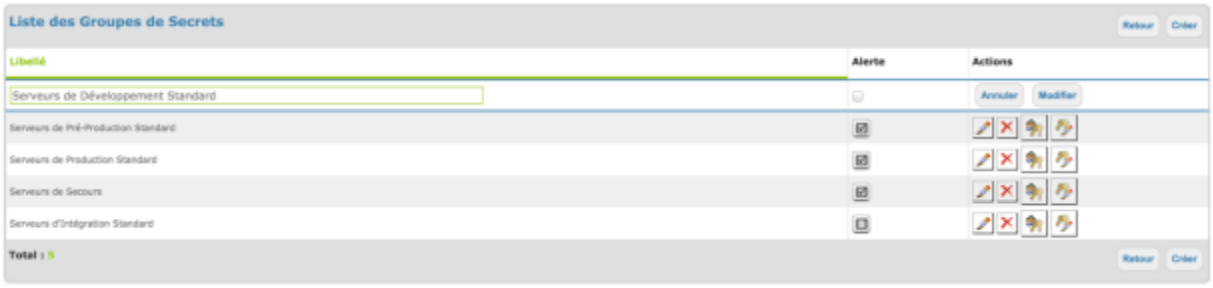
8.6.3. Règles sur les groupes de secrets

1. Il ne peut y avoir 2 « Groupes de Secrets » avec le même « Libellé ».

8.6.4. Création ou Modification d'un groupe de secrets

Pour créer un « Groupe de Secrets », l'administrateur doit cliquer sur le bouton « Créer ». Il arrivera sur l'écran ci-dessous :

Pour modifier un Groupe de Secrets, il faut utiliser le bouton «  » sur l'occurrence désirée. La modification s'effectuera en ligne et les informations deviendront modifiables, comme dans l'exemple ci-dessous :



8.6.4.1. Champ « Libellé »

Le « Libellé » est une chaîne alphanumérique de maximum 60 caractères.

8.6.4.2. Boîte à cocher « Alerte »

Cette boîte à cocher permet de notifier, sous forme d'alerte (pour plus d'information se reporter au chapitre « Gestion des préférences », onglet « Alertes »), les accès qui seront fait sur tous les « Secrets » contenus dans ce « Groupe de Secrets ».

8.6.4.3. Bouton « Annuler »

Ce bouton permet de revenir à l'écran précédent, sans créer une « Entité ».

8.6.4.4. Bouton « Créer » ou « Modifier »

Ces boutons, en fonction des cas, permettent de valider la création ou la modification du « Groupe de Secrets ».

8.6.5. Suppression d'un groupe de secrets

Pour supprimer une « Entité », l'administrateur doit cliquer sur le bouton «  ». Il arrivera sur l'écran ci-dessous :

8.6.5.1. Bouton « Annuler »

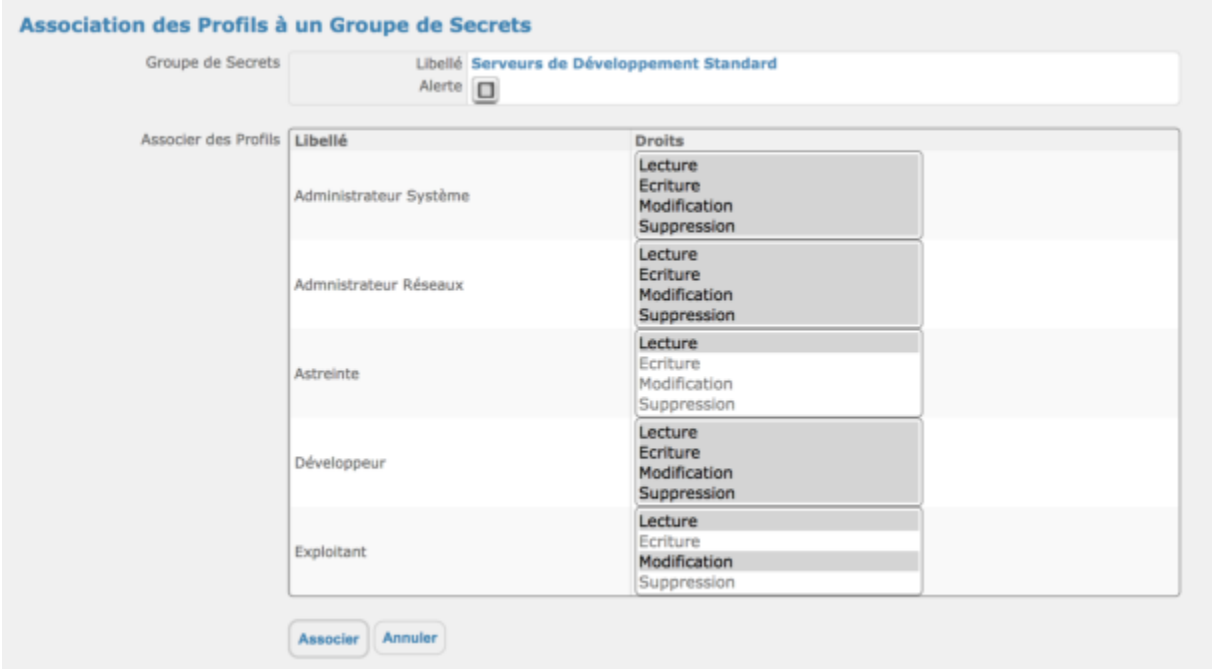
Ce bouton permet de revenir à l'écran précédent, sans supprimer le « Groupe de Secrets ».

8.6.5.2. Bouton « Confirmer »

Ce bouton permet de valider la suppression du « Groupe de Secrets ».

8.6.6. Associer des Profils à un Groupe de Secrets

Pour associer des « Profils » à un « Groupe de Secrets », il faut utiliser le bouton «  ». En utilisant ce bouton, l'administrateur arrive sur l'écran ci-dessous :



Dans cet écran, l'administrateur peut associer des « Profils » au « Groupe de Secrets » sélectionné. En créant cette association, il est possible de préciser les « droits d'accès ».

8.6.6.1. L'influence des droits sur les associations

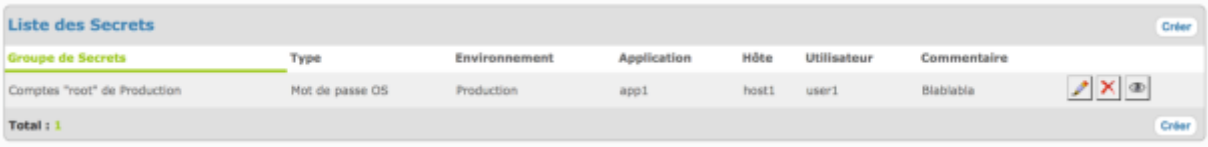
Si aucun « Droit » n'est sélectionné, le « Groupe de Secrets » n'apparaitra jamais auprès des utilisateurs (à l'exception de ceux qui ont le privilège « Administrateur »).

En revanche, le « Groupe de Secrets » apparaîtra pour les utilisateurs qui sont rattachés à un « Profil » pour lequel il y a au moins un « Droit ».

Dans la mesure où l'utilisateur est rattaché à plusieurs « Profils » et que ces profils accèdent à un même « Secret », l'utilisateur récupérera touts les « Droits » fournis par ces « Profils ».

Par la suite, chaque « Droit » restreindra l'accès aux données (restriction au niveau de l'API) mais aura également une influence sur l'IHM de l'outil.

Ci-dessous, un exemple de liste de secrets pour lequel à tous les droits sur le Groupe de Secrets :



Ci-dessous le tableau de correspondance des droits et des incidences sur l'IHM

Droit	**Impact sur l'IHM**
Lecture	L'occurrence peut apparaître dans les listes de Secrets. Le bouton «  » est également disponible pour voir le détail du Secret.
Ecriture	Le bouton « Créer » est disponible si l'utilisateur a

Droit	Impact sur l'IHM
	au moins un droit d'écriture sur un des Groupes de Secrets auxquels il a accès. Toutefois, il ne pourra créer un Secret qu'avec les Groupes qui lui seront proposés dans la liste de l'écran de création.
Modification	Le bouton «  » est disponible sur les Secrets que l'utilisateur peut modifier et uniquement sur les Secrets pour lesquels il a ce droit. Ce droit est différent de celui d'une création. Effectivement, un utilisateur pourrait n'avoir qu'à maintenir des Secrets existants sans pour autant avoir le droit d'en créer de nouveau.
Suppression	Le bouton «  » est disponible sur les Secrets que l'utilisateur peut supprimer et uniquement sur les Secrets pour lesquels il a ce droit.

8.6.6.2. Associer des Droits

Pour associer un « Droit » à un profil, il faut se placer sur l'occurrence du « Profil » à gérer et à cliquer sur le ou les « Droits » souhaités.

Dans l'exemple ci-dessus, les « Droits » suivants ont été donnés :

- Le profil « Administrateur Réseaux » peut **lire** et **modifier** les secrets contenus dans le groupe de secrets « Comptes « root » de Production ».
- Le profil « Administrateur Systèmes » à tous les « droits » sur les secrets contenus dans le groupe de secrets « Comptes « root » de Production ».
- Le profil « Personnel Astreinte » peut **seulement lire** les secrets contenus dans le groupe de secrets « Comptes « root » de Production ».

Pour mieux illustrer le concept, on pourrait très bien imaginer le cas ci-dessous :

Dans cet exemple, on comprend que l'utilisateur connecté à les droits suivants :

- Il a au moins le droit de créer un secret dans un groupe : présence du bouton « Créer » ;
- Il peut lire et modifier les secrets contenus dans le groupe de secret « Comptes des applications de Production » ;

- Il peut uniquement lire les secrets du groupe de secrets « Comptes « admin » du réseau de Production ;
- Il peut tout (à priori) tout faire sur le groupe de secrets « Compte « root » de Production ».

8.6.7. Gérer les Secrets dans un Groupe de Secrets

Pour gérer des « Secrets » dans un « Groupe de Secrets », il faut utiliser le bouton «  ». En utilisant ce bouton, l'administrateur arrive sur l'écran ci-dessous :

8.6.7.1. Colonne « Type »

Le « Type » est une information pour préciser la nature et aider au classement des secrets.

SecretManager gère 3 types :

1. Mot de passe OS ;
2. Mot de passe applicatif ;
3. Mot de passe document.

8.6.7.2. Colonne « Environnement »

L'environnement tout comme le « Type » permet de classer les secrets.

SecretManager gère 4 environnements :

1. Production ;
2. Pré-production ;
3. Intégration ;
4. Développement.

> ***Remarque :*** *il est possible de modifier ces libellés (voir le chapitre sur la gestion Multilingue de l'outil). Toutefois, **SecretManager** ne gère que 4 niveaux pour le moment.*

8.6.7.3. Colonne « Application »

Ce champ est une liste des Applications qui ont été créées précédemment par l'Administrateur. Il n'est pas obligatoire. Il permet de pouvoir rattacher le « Secret » à une « Application ».

8.6.7.4. Colonne « Hôte »

Ce champ est libre en saisie pour l'Administrateur et il est obligatoire. Il permet de pouvoir rattacher le « Secret » à un « Serveur » ou à un « Lien ». Dans le cadre d'un lien, l'information commencera par la chaîne « http » ou « www » et dans ces cas, l'Hôte sera directement cliquable.

8.6.7.5. Colonne « Utilisateur »

Ce champ est libre en saisie pour l'Administrateur et il est obligatoire. Il constitue le « Secret ».

8.6.7.6. Colonne « Alerte »

La boîte à cocher permet de remonter une alerte pour ce « Secret » quand il sera accédé par la suite. Les moyens de remonter des alertes sont paramétrables. Il faut se reporter au chapitre « Gestion des préférences ».

8.6.7.7. Colonne « Commentaire »

Ce champ est libre en saisie pour l'Administrateur et il n'est pas obligatoire. Il permet de pouvoir donner des informations complémentaires sur le « Secret ».

8.6.7.8. Colonne « Actions »

Cette colonne contient tous les boutons permettant de gérer le Secret courant (Secret en surbrillance dans le tableau).

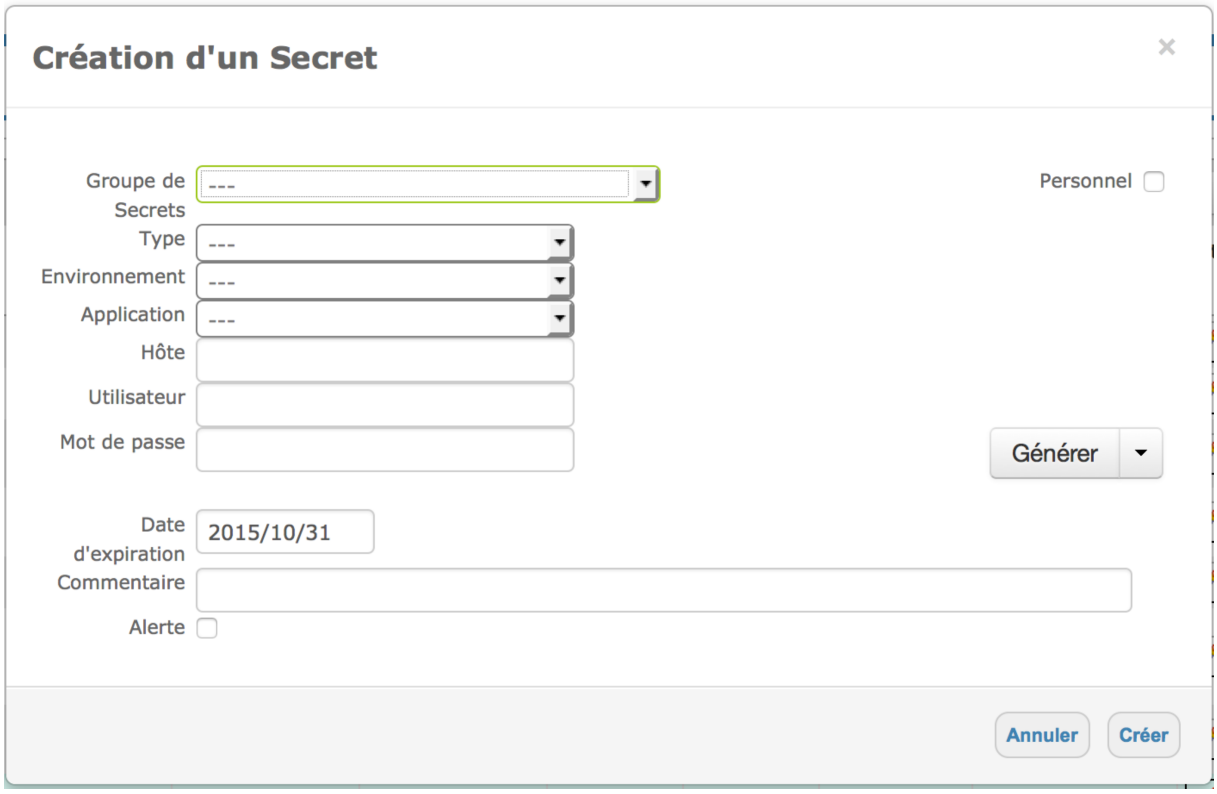
Bouton	Signification
	Ce bouton permet de modifier le « Secret ».
	Ce bouton permet de supprimer le « Secret ».

8.6.7.9. Bouton « Retour »

Ce bouton permet de revenir à l'écran précédent (écran Liste des Groupes de Secrets).

8.6.7.10. Bouton « Créer »

Ce bouton permet d'exécuter la création d'un nouveau « Secret » dans le « Groupe de Secret » sélectionné. Cela affiche l'écran de création ci-dessous :

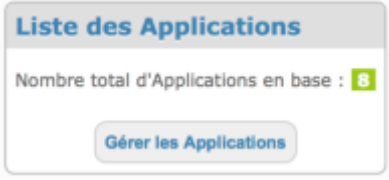


8.7. Gestion des Applications

Les « Applications » sont particulièrement importantes quand on crée des « Secrets » de type « mots de passe applicatif ».

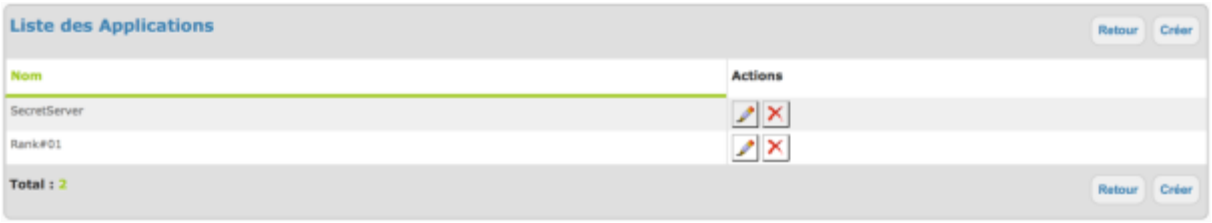
8.7.1. Accéder à l'écran de gestion des Applications

A partir de l'écran « Administration », il faut utiliser la boite de synthèse dédiée aux Applications, comme dans l'exemple ci-dessous :



Le bouton « Gérer les groupes de secrets » permet d'entrer dans l'écran de gestion des Groupes de Secrets.

8.7.2. Ecran liste des « Applications »



8.7.2.1. Colonne « Nom »

Le « Nom » est le nom d'une « Application ».

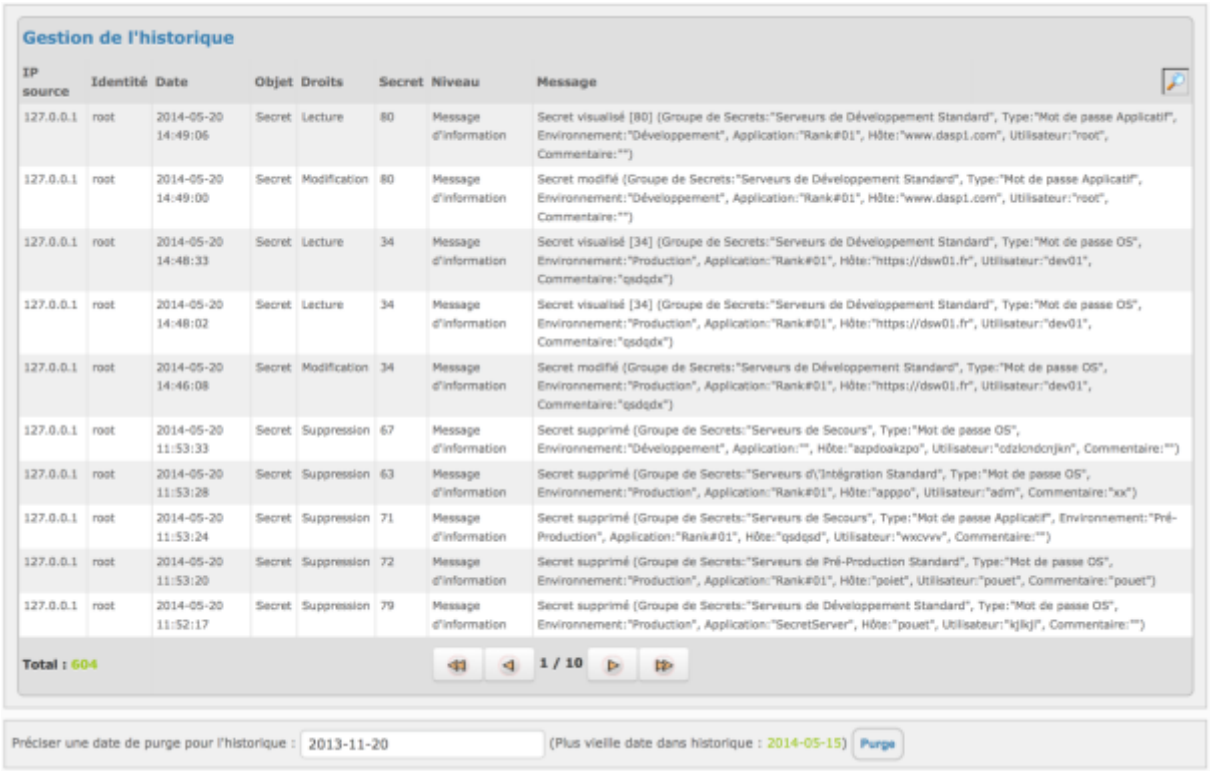
Ci-dessous le tableau de correspondance des droits et des incidences sur l'IHM

Bouton	Fonction
	Ce bouton permet de modifier le nom d'une Application.
	Ce bouton permet de supprimer le nom d'une Application.

8.8. Gestion de l'historique

Toutes les actions réalisées dans l'outil « SecretManager » sont tracées dans l'historique. Les opérations sur les Secrets (quand ces derniers sont mis sous surveillance) peuvent être envoyée en plus sur d'autres canaux. Il s'agit des Secrets qui sont sous contrôle (voir les chapitres 8.6.4.2, 8.6.7.6 et 7.1).

Les actions sont classées par date décroissante et elles sont regroupées par groupe de 10 occurrences. Comme dans l'exemple ci-dessous :



Cet exemple est de niveau détaillé.

8.8.1. Colonne « IP Source »

Donne l'adresse IP de l'utilisateur qui a réalisé cette action.

8.8.2. Colonne « Identité »

Donne le nom de l'utilisateur qui a réalisé cette action.

8.8.3. Colonne « Objet »

Donne le type d'objet sur lequel l'action c'est réalisée.

8.8.4. Colonne « Droits »

L'outil utilise 4 droits :

1. Lecture ;
2. Création ;
3. Modification ;
4. Suppression.

Cette colonne informe du Droit qui a été utilisé par l'utilisateur sur l'Objet.

8.8.5. Colonne « Secret »

Donne le numéro du Secret qui a été la cible de l'action. Cette colonne n'est renseigné que quand l'Objet est de type « Secret ».

8.8.6. Colonne « Niveau »

Donne le niveau d'alerte dans l'historique. Pour le moment seul 2 niveaux sont gérés :

1. Message d'information (LOG_INFO) ;
2. Condition d'erreur (LOG_ERR).

8.8.7. Colonne « Message »

Donne le détail de l'action.

Ces messages sont donc de la forme :

- Le libellé de l'action
- Parfois suivi de l'identifiant de l'objet qui a été accédé. Ce dernier sera entre crochet droit « [» ;
- Le détail de l'objet entre parenthèse « (» (si l'option « Verbosité des Alertes » est à « détaillée ».

Ci-dessous l'exemple d'un Secret qui a été visualisé (avec une verbosité à détaillée) :

```
Secret visualisé [80] (Groupe de Secrets:"Serveurs de Développement Standard",
Type:"Mot de passe Applicatif", Environnement:"Développement",
Application:"Rank#01", Hôte:"www.dasp1.com", Utilisateur:"root", Commentaire:"")
```

Le libellé de l'action est « Secret visualisé », l'identifiant du secret est « [80] » et le détaille de l'action est « (Groupe de Secrets:"Serveurs de Développement Standard", Type:"Mot de passe Applicatif", Environnement:"Développement", Application:"Rank#01", Hôte:"www.dasp1.com", Utilisateur:"root", Commentaire:"") ».

Si la verbosité était à normal, le même message aurait été :

```
Secret visualisé [80]
```

8.8.8. Boutons de navigation

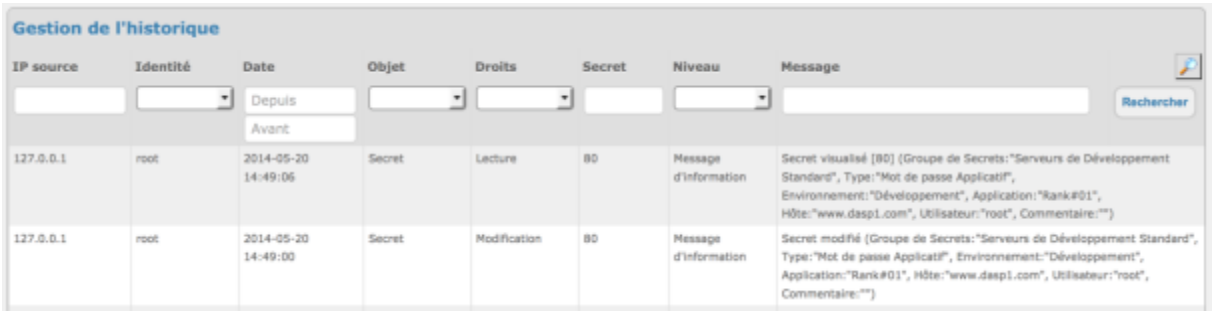
Pour naviguer d'un groupe de 10 à un autre, il faut utiliser les boutons ci-dessous :

Bouton	Action
	Se positionne sur les 10 premières occurrences de l'historique (soit les dernières actions recueillies)

Bouton	Action
	Se positionne sur les 10 occurrences précédentes
	Se positionne sur les 10 occurrences suivantes
	Se positionne sur les 10 dernières occurrences de l'historique (soit les premières actions recueillies)

8.8.9. Critères de recherche

Il est possible de lancer des recherches dans cet historique. Pour cela, l'Administrateur clique sur le bouton «  ». Après ce clique, l'écran se transforme comme ci-dessous :



L'Administrateur peut renseigner tout ou partie des champs mis à sa disposition. Pour lancer la recherche, il faut cliquer sur le bouton « Rechercher ».

Au-delà d'un certain temps, il peut être nécessaire de purger l'historique. Pour cela, il faut utiliser le bloc en fin de la page d'historique.

Par défaut, il est proposé de conserver 6 mois d'historique en ligne (mais il ne s'agit que d'une proposition). Après avoir défini une date et après avoir cliqué sur le bouton « Purge », toutes les actions antérieures à cette date seront supprimées de la base de données.

8.9. Gestion du référentiel interne de l'outil

Certains Administrateurs m'ont fait remarquer que l'outil « **SecretManager** » pouvait être limité en terme :

- D'environnement ;
- De type de Secrets.

Dans l'absolue, c'est vrai. Pour autant, on peut facilement personnaliser le référentiel interne de l'outil.

Il y a 2 étapes à respecter :

1. Mise à jour de la table dans la base de données ;
2. Mise à jour des libellés associés.

8.9.1. Ajout ou modification d'un « Environnement »

Les environnements sont stockés dans la table « `env_environments` ». Par défaut, il y a 4 environnements :

1. L_Environment_1
2. L_Environment_2
3. L_Environment_3
4. L_Environment_4

La logique voudrait que l'on incrémente ce numéro pour créer de nouveaux événements. Toutefois, l'Administrateur peut créer le libellé de son choix.

Pour notre exemple, nous suivrons la logique.

Voici la requête à exécuter et à conserver dans un fichier spécifique pour créer un nouvel événement :

```
INSERT INTO `env_environments` (`env_id`, `env_name`) VALUES
(5, 'L_Environment_5') ;
```

Ensuite, il faut maintenir l'équilibre entre le nom d'environnement nouvellement créé et les fichiers des libellés.

Les fichiers à maintenir sont « `*_labels_referentials.php` ». L'étoile est à remplacer par le code langue que vous souhaitez maintenir.

Prenons l'exemple du fichier des libellés Français : « `fr_labels_referentials.php` ». Dans ce fichier, il faudra créer une nouvelle variable portant le même nom que celui que vous avez inséré dans la base. Si on continue sur l'exemple précédent, il faudra créer la variable « `$L_Environment_5` » et lui donner le libellé adapté. Par exemple :

```
$L_Environment_5 = 'Secours';
```

Dans cet exemple, nous venons d'ajouter l'environnement de « `Secours` ». Notez que vous pouvez, dans ce même fichier, modifier les environnements précédemment créés.

8.9.2. Ajout ou modification d'un « Type de Secret »

Les environnements sont stockés dans la table « `stp_secret_types` ». Par défaut, il y a 3 types :

1. L_Secret_Type_1
2. L_Secret_Type_2
3. L_Secret_Type_3

La logique voudrait que l'on incrémente ce numéro pour créer de nouveaux types. Toutefois, l'Administrateur peut créer le libellé de son choix.

Pour notre exemple, nous suivrons la logique.

Voici la requête à exécuter et à conserver dans un fichier spécifique pour créer un nouvel événement :

```
INSERT INTO `stp_secret_types` (`stp_id`, `stp_name`) VALUES
(3, 'L_Secret_Type_3') ;
```

Ensuite, il faut maintenir l'équilibre entre le nom d'environnement nouvellement créé et les fichiers des libellés.

Les fichiers à maintenir sont « `*_labels_referentials.php` ». L'étoile est à remplacer par le code langue que vous souhaitez maintenir.

Prenons l'exemple du fichier des libellés Français : « `fr_labels_referentials.php` ». Dans ce fichier, il faudra créer une nouvelle variable portant le même nom que celui que vous avez inséré dans la base. Si on continue sur l'exemple précédent, il faudra créer la variable « `$L_Secret_Type_3` » et lui donner le libellé adapté. Par exemple :

```
$L_Secret_Type_3 = 'Mot de passe temporaire';
```

Dans cet exemple, nous venons d'ajouter le Type de Secret de « `Mot de passe temporaire` ». Notez que vous pouvez, dans ce même fichier, modifier les types de secret précédemment créés.

8.10. Gestion du SecretServer

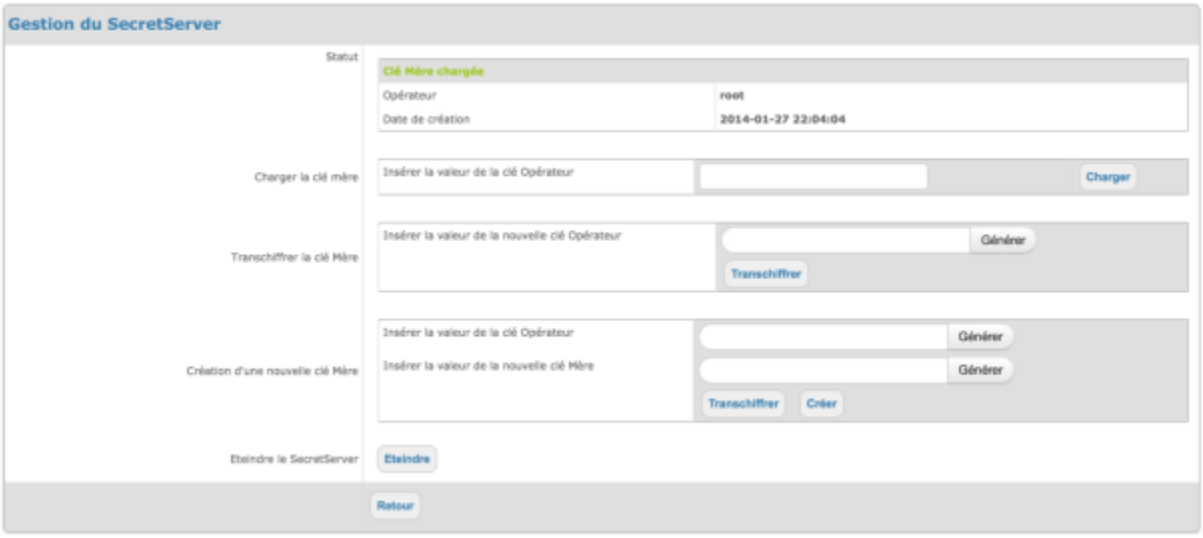
A partir du tableau de bord d'Administration, il est possible d'accéder aux fonctions du SecretServer.

8.10.1. Accéder à l'écran de gestion SecretServer

Dans l'écran « Administration », il faut utiliser la boite de synthèse dédiée aux « SecretServer », comme dans l'exemple ci-dessous :

Le bouton « Gérer le SecretServer » permet d'entrer dans l'écran de gestion du SecretServer.

8.10.2. Ecran de gestion du SecretServer

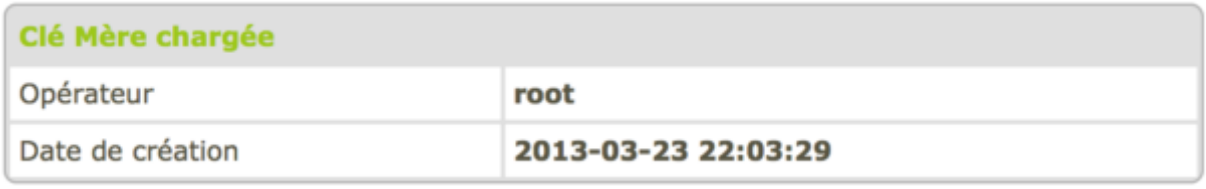


8.10.2.1. Zone « Statut »

Ce champ informe l'Administrateur sur l'état du « SecretServer ».

Par exemple, si le « SecretServer » n'est pas encore démarré par l'Administrateur, le statut doit être à : SecretServer non démarré

Cependant, si une clé Mère est chargé dans le « SecretServer », cette zone contiendra un écran ressemblant à l'image ci-dessous :



8.10.2.2. Zone « Charger la clé mère »

Pour charger une clé « Mère », il faut être en mesure de la déchiffrer. Pour cela, l'Administrateur doit disposer de la clé « Opérateur ». Seule cette clé permet de déchiffrer la clé « Mère » et ainsi la charger dans la mémoire du « SecretServer ».

Remarque : *il est préférable de définir un rôle de porteur pour la clé opérateur afin d'éviter qu'un Administrateur ait tous les pouvoirs.*

Si le « SecretServer » est démarré et que la clé mère n'a pas été déchiffrée, le statut du « SecretServer » doit indiquer : Clé mère non chargée

Pour charger la clé « Mère », l'Administrateur doit insérer dans le champ « Insérer la clé opérateur » la valeur de la clé « Opérateur » et cliquer sur le bouton « Charger ». Dans certaine Entreprise, la notion « d'Opérateur de Sécurité » ou « Porteur de Secret » existe, dès lors ces personnes pourraient être sollicitées lors des démarrages du « SecretServer ».

Après avoir été chargée, le statut du « SecretServer » doit passer à un écran ressemblant à l'image ci-dessous :

Clé Mère chargée	
Opérateur	**root**
Date de création	**2013-03-23 22:03:29**

La notion « d'Opérateur » est le nom de connexion de l'Administrateur qui a créé la clé mère.

La date de « Date de création » est la date à laquelle la clé mère a été créée. Cela peut, par exemple, aider à gérer la crypto-période de la clé mère.

8.10.2.3. Champ « Insérer la valeur de la clé Opérateur »

Dans ce champ, l'Administrateur entre la valeur de la clé « Opérateur » afin de permettre au « SecretServer » de pouvoir déchiffrer la clé Mère qui est stockée dans son fichier et de la charger dans sa mémoire.

8.10.3. Zone « Transchiffrer la Clé Mère »

Cette zone permet à l'Administrateur de chiffrer la clé Mère résidente en mémoire du « SecretServer » dans son fichier d'origine avec la clé qu'il aura précisé dans le champ « Insérer la valeur de la nouvelle clé Opérateur ». Cela revient à transchiffrer la clé Mère soit de la rechiffrer avec une nouvelle clé, sans pour autant changer la valeur de la clé Mère.

Le bouton « Générer » permet de créer une nouvelle clé conformément à ce qui aura été défini dans l'écran de « Gestion des Préférences » (voir chapitre 7.3.3). Toutefois, l'Administrateur peut également saisir la valeur de son choix. Il aura juste un avertissement (non bloquant) s'il ne respecte les règles de construction définies dans les « Préférences ».

Important : par la suite, c'est bien avec la nouvelle clé Opérateur qu'il faudra charger la clé Mère.

8.10.4. Zone « Création d'une nouvelle clé Mère »

Cette zone permet à l'Administrateur d'insérer une clé Opérateur (clé qui va chiffrer la clé Mère) à l'aide du champ « Insérer la valeur de la clé Opérateur » et une clé Mère à l'aide du champ « Insérer la valeur de la nouvelle clé Mère ».

8.10.4.1. Bouton « Transchiffrer »

Ce bouton est à utiliser, si une clé Mère existe déjà et que l'on souhaite transchiffrer les « Secrets » qui ont déjà été insérés dans la base de données de « SecretManager ». Effectivement, avec ce bouton chaque Secret est déchiffré avec l'ancienne clé Mère et chiffré avec la nouvelle clé Mère.

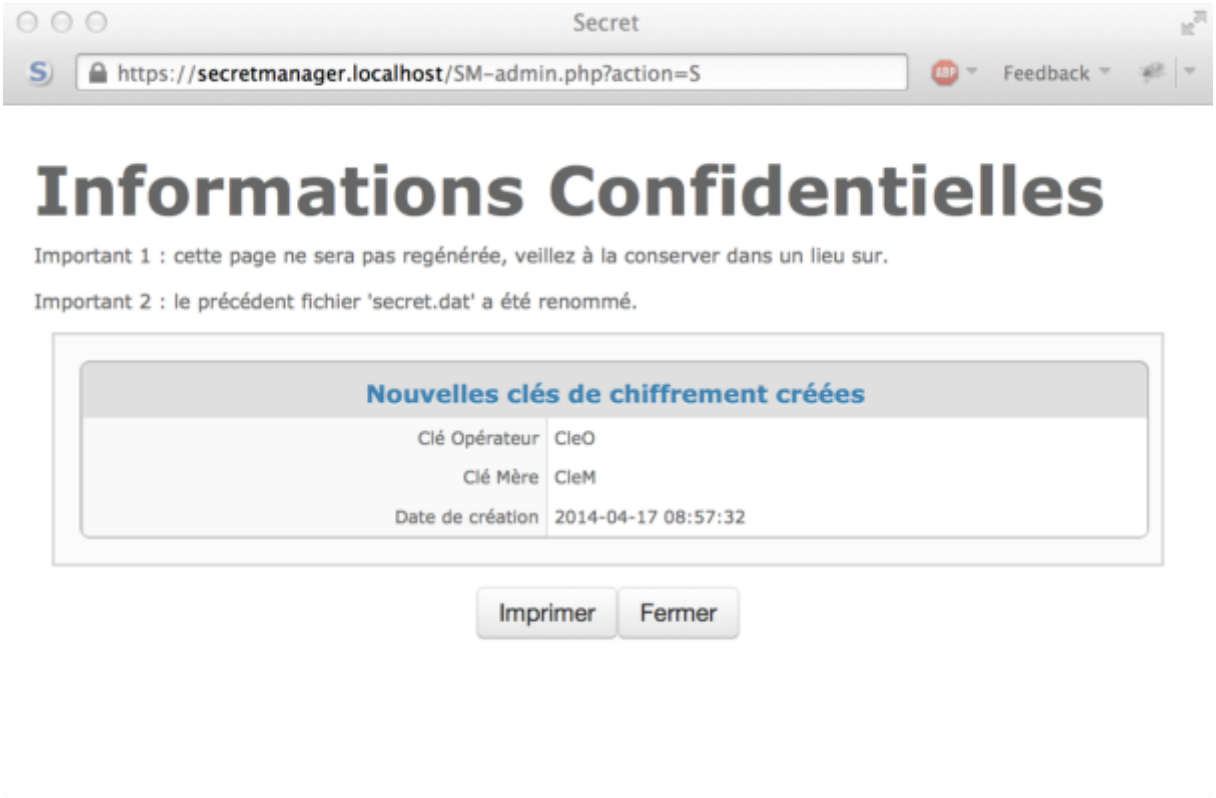
Prenons l'exemple ci-dessous :

On voit que l'on va créer la clé Mère ayant une valeur « CleM » et chiffrée par la clé Opérateur ayant la valeur « CleO ». On notera que des avertissements sont levés par la présence du drapeau . Effectivement, les valeurs des clés sont largement inférieures à ce qui pratique habituellement.

Afin d'attirer l'attention de l'Administrateur, le panneau ci-dessous apparaît après que l'Administrateur ait appuyé sur le bouton « Transchiffrer » :

Si l'utilisateur clique sur le bouton « Confirmer » alors le transchiffrement de la base est lancé.

A l'issue du transchiffrement, l'écran ci-dessous apparaitra :



Cet écran rappelle la clé « Opérateur » qui a été utilisée ainsi que la clé « Mère » qui sera utilisée pour chiffrer les « Secrets ».

Important : Il vous appartient de sauvegarder ces informations, sachant qu'elles sont confidentielles et qu'elles ne seront jamais refournies par la suite.

8.10.4.2. Bouton « Créer »

Le déroulement est similaire à un transchiffrement. On renseigne les clés et on lance l'opération par le bouton « Créer ».

Cependant, il n'y aura pas le transchiffrement des clés préexistantes dans la base de données du « SecretManager ». Seul un nouveau fichier contenant la clé Mère, elle-même, chiffrée par la clé Opérateur sera créé. Le « SecretServer » disposera dans sa mémoire de la nouvelle clé Mère.

Important 1 : si le « SecretManager » contenait déjà des Secrets, ces derniers ne sont pas perdus. Toutefois, les mots de passe associés sont devenus illisibles et sont considérés comme perdus. Il faut donc en saisir de nouveau.

***Rappel** : La clé opérateur est la seule clé qui doit être rappelée à chaque démarrage du « SecretServer ».*

Important 2 : la clé Opérateur doit être confiée à une personne de confiance.

D'un point de vue sécuritaire, le Porteur de la « clé Opérateur » ne devrait pas être un administrateur système ou réseau impacté par la gestion des secrets dans le « SecretManager ».

8.10.5. Zone « Eteindre le SecretServer »

Autant, il n'est pas possible de démarrer le « SecretServer » à partir de l'interface du « SecretManager », car il faut être Administrateur du serveur hébergeant le « SecretManager »,

autant il est possible d'envoyer une information d'arrêt au « SecretManager ». Il est également possible d'arrêter le « SecretServer » par des instructions systèmes, mais ce n'est pas la bonne façon car potentiellement, vous pourriez arrêter une opération de mise à jour, et donc de faire perdre des modifications à des utilisateurs.

8.11. Gestion des sauvegardes

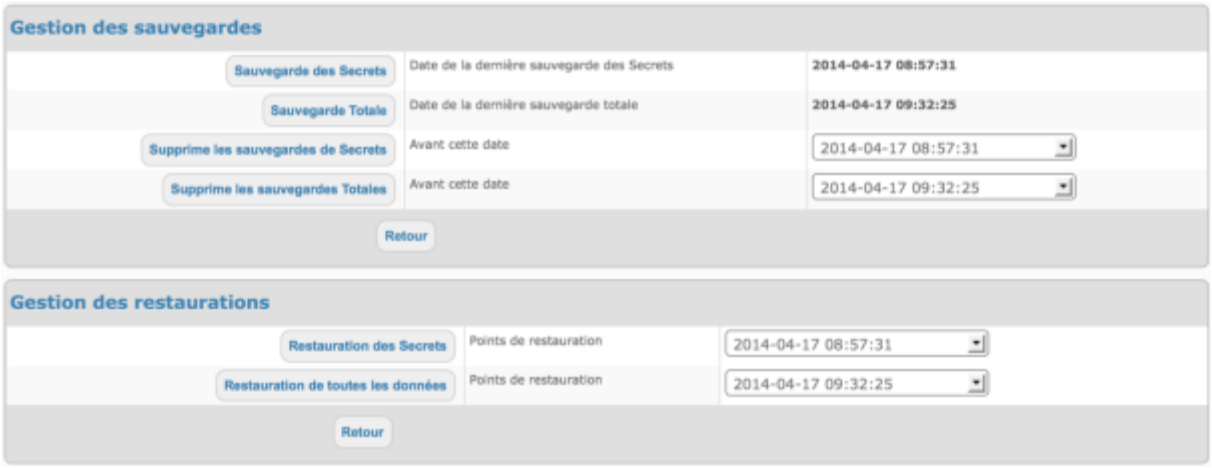
A partir du tableau de bord d'Administration, il est possible d'accéder aux fonctions de Sauvegarde et de Restauration.

8.11.1. Accéder à l'écran de « Gestion des sauvegardes »

Dans l'écran « Administration », il faut utiliser la boite de synthèse dédiée à la Sauvegarde, comme dans l'exemple ci-dessous :

Le bouton « Gérer les sauvegardes » permet d'entrer dans l'écran de gestion des Sauvegardes.

8.11.2. Ecran de gestion des Sauvegardes



8.11.2.1. Zone « Gestion des sauvegardes »

Cette zone abrite plusieurs boutons qui réalisent les actions ci-dessous :

Bouton	Action
`Sauvegarde des Secrets`	Sauvegarde tous les Secrets de la base dans un fichier XML. Les Secrets restent chiffrés par leur clé Mère. Cette dernière est également sauvegardée, mais elle reste chiffrée par sa clé Opérateur.
`Sauvegarde totale`	Réalise la sauvegarde des Secrets (comme vu ci-dessus), plus toutes les autres tables de « SecretManager ».
`Supprime les sauvegardes de Secrets`	L'Administrateur doit choisir une date parmi celles proposées dans la liste déroulantes (ce sont en fait les dates correspondantes aux dernières sauvegardes). Après avoir sélectionné la date, l'Administrateur clique sur le bouton « `Supprime les sauvegardes de Secrets` ». Toutes les sauvegardes de Secrets antérieures à la date sélectionnées sont détruites.
`Supprime les sauvegardes Totales`	L'Administrateur doit choisir une date parmi celles proposées dans la liste déroulantes (ce sont en fait les dates correspondantes aux dernières sauvegardes). Après avoir sélectionné la date, l'Administrateur clique sur le bouton « `Supprime les sauvegardes Totales` ». Toutes les sauvegardes Totales antérieures à la date sélectionnées sont détruites.

8.11.2.2. Zone « Gestion des restaurations »

Cette zone abrite plusieurs boutons qui réalisent les actions ci-dessous :

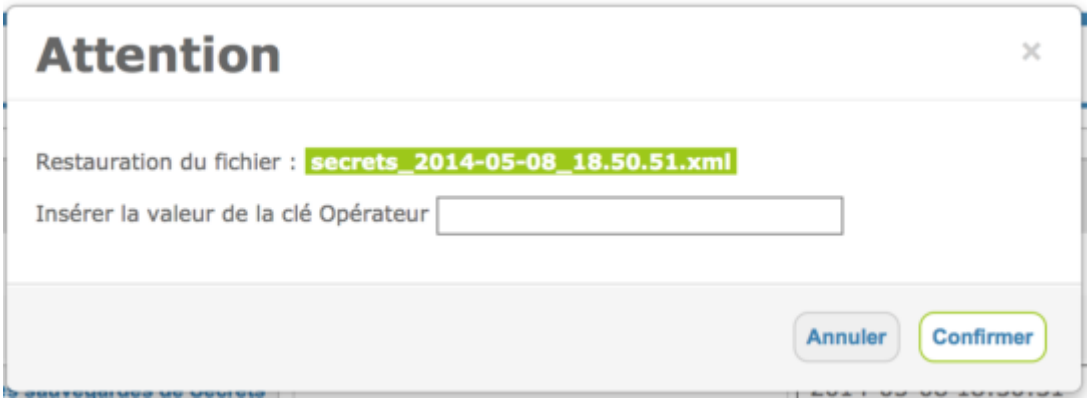
Bouton	Action
`Restauration des Secrets`	L'Administrateur doit choisir une date parmi celles proposées dans la liste déroulantes (ce sont en fait les dates correspondantes aux dernières sauvegardes). Après avoir sélectionné la date, l'Administrateur clique sur le bouton « `Restauration des Secrets` ». Tous les Secrets contenus dans le fichier de sauvegarde sélectionné seront insérés dans la base de données de « SecretManager ».
`Restauration de toutes les données`	L'Administrateur doit choisir une date parmi celles proposées dans la liste déroulantes (ce sont en fait les dates correspondantes aux dernières sauvegardes). Après avoir sélectionné la date, l'Administrateur clique sur le bouton « `Restauration de toutes les données` ». Toutes les Données contenus dans le fichier de sauvegarde sélectionné seront insérées dans la base de données de « SecretManager ».

Attention : Quelle que soit la restauration, les tables impactées (par rapport au type de restauration) sont systématiquement vidées avant la restauration.

Première étape d'une restauration :

On valide le type de restauration ainsi que la date sélectionnée, comme dans l'exemple ci-dessous :

Après avoir confirmé, on bascule dans la fenêtre ci-dessous :



L'Administrateur doit fournir la clé Opérateur associé au fichier à restaurer.

Cette mesure permet de s'assurer que l'administrateur restaure un fichier qu'il maitrise.

C'est en confirmant cette dernière fenêtre que les étapes suivantes seront respectivement réalisées :

1. Ouverture du fichier à restaurer et vérification du déchiffrement de la clé Mère ;
2. Sauvegarde de la clé Mère du fichier de restauration dans le fichier du SecretServer ;
3. Chargement de la clé Mère précédemment stockée dans la mémoire du SecretServer ;
4. Vidage des tables et insertions des données dans les tables.

9. GESTION DE L'INTEGRITE DU SECRETMANAGER ET DU SECRETSERVER

Le contrôle d'intégrité est une nouveauté depuis la version 0.9-0 de « SecretManager ».

Désormais, le « SecretManager » supervise l'intégrité du « SecretServer » et inversement. Pour ce faire, « SecretManager » et « SecretServer » dispose de deux fichiers pour gérer cette intégrité :

1. files_integrity.dat : contient l'empreinte de tous les fichiers sensibles de SecretManager (fichier utilisé par le « SecretManager ») ;
2. file_integrity.dat : contient l'empreinte du fichier précédent (fichier utilisé par le « SecretServer »).

Ces deux fichiers sont fournis dans le « package d'installation », ils garantissent que les fichiers sont intègres à leur livraison.

9.1. Contrôle par le SecretManager

A chaque fois qu'un utilisateur souhaite accéder à un Secret, le « SecretManager » vérifie que ces fichiers sensibles n'ont pas été altérés. Pour ce faire, il utilise le fichier « `files_integrity.dat` » et compare que les « hashs » contenus dans ce fichier sont identiques à ceux qui viennent d'être recalculés. Dans le cas, contraire, le « SecretManager » affiche un message sous la forme suivante :

Ce panneau affiche le ou les fichiers sensibles qui ont été modifiés.

Dans l'historique du « SecretManager », on trouvera une occurrence ressemblant à celle ci-dessous :

Objet	Droits	Niveau	Message
Clé Mère	Lecture	Condition d'erreur	Alerte sur l'intégrité des fichiers sensibles de SecretManager (/Applications/XAMPP/xamppfiles/htdocs/SecretManager/SM-preferences.php /Applications/XAMPP/xamppfiles/htdocs/SecretManager/Libraries/Ajax_preferences.js /Applications/XAMPP/xamppfiles/htdocs/SecretManager/Libraries/Class_I

9.1.1. Pour revenir à un état normal

Pour revenir à un état normal, il faut récupérer les fichiers d'origines à partir du « package d'installation » (archive d'installation récupérée sur le site de « SecretManager »).

Si on reprend l'exemple ci-dessus, il convient de restaurer les fichiers :

```
- SM-preferences.php
- Ajax_preferences.js
- Class_IICA_Authentications_PDO.inc.php
```

9.2. Contrôle par le SecretServer

Le « SecretServer » vérifie à chaque accès à un « Secret » que les fichiers de contrôle du « SecretManager » n'ont pas été modifiés. Les fichiers de contrôle du « SecretServer » sont chargés dans sa mémoire à son démarrage. Ainsi, si une personne arrive à modifier un fichier de contrôle durant l'exécution du « SecretServer », ce dernier sans rendra compte.

Voici les messages d'erreur qui peuvent apparaître dans les traces du « SecretServer » quand ce dernier découvre une modification d'un fichier de contrôle d'intégrité :

```
%E *** Alerte d'intégrité sur le fichier : MASTER_INTEGRITY_FILE ***
```

Le « SecretServer » vient de remarquer que le fichier « `files_integrity.dat` » a été modifié.

```
%E *** Alerte d'intégrité sur le fichier : SECRETSERVER_INTEGRITY_FILE ***
```

Le « SecretServer » vient de remarquer que le fichier « `file_integrity.dat` » a été modifié.

9.2.1. Pour revenir à un état normal

Pour revenir à un état normal, il faut récupérer les fichiers d'origines à partir du « package d'installation » (archive d'installation récupérée sur le site de « SecretManager »).

En fonction du message d'erreur reçu, il faudra restaurer :

```
files_integrity.dat
```

ou

```
file_integrity.dat
```