GUIDE OPERATEUR

SECRETMANAGER V0.9-X

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

SAS ORASYS
Siège social : 2, route de la Noue – BP 76 – 91193 GIF SUR YVETTE
Tél. 01 64 86 58 21 - Fax 01 64 86 18 19 – **www.orasys.fr**
SAS au capital de 67 000 € - 484 508 528 R.C.S. EVRY - SIRET : 484 508 528 00045 - Code APE : 7022Z

HISTORIQUE DU DOCUMENT		
Version	**Date**	**Modifications**
1.0-0	02/07/2014	Création

DOCUMENTS DE REFERENCE		
Index	**Titre**	**Référence**
DR01	Guide d'Installation – SecretManager	Orasys - FR - Guide Installation - SecretManager v0.9-x – v1.0-0.pdf
DR02	Guide Utilisateur SecretManager	Orasys – FR – Guide Utilisateur – SecretManager v0.9-x – v1.0-0.pdf

TABLE DES MATIERES

1. MISE EN GARDE

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

Cette version passe désormais en « release candidate » (RC). Vous pouvez commencer à l'utiliser en Production.

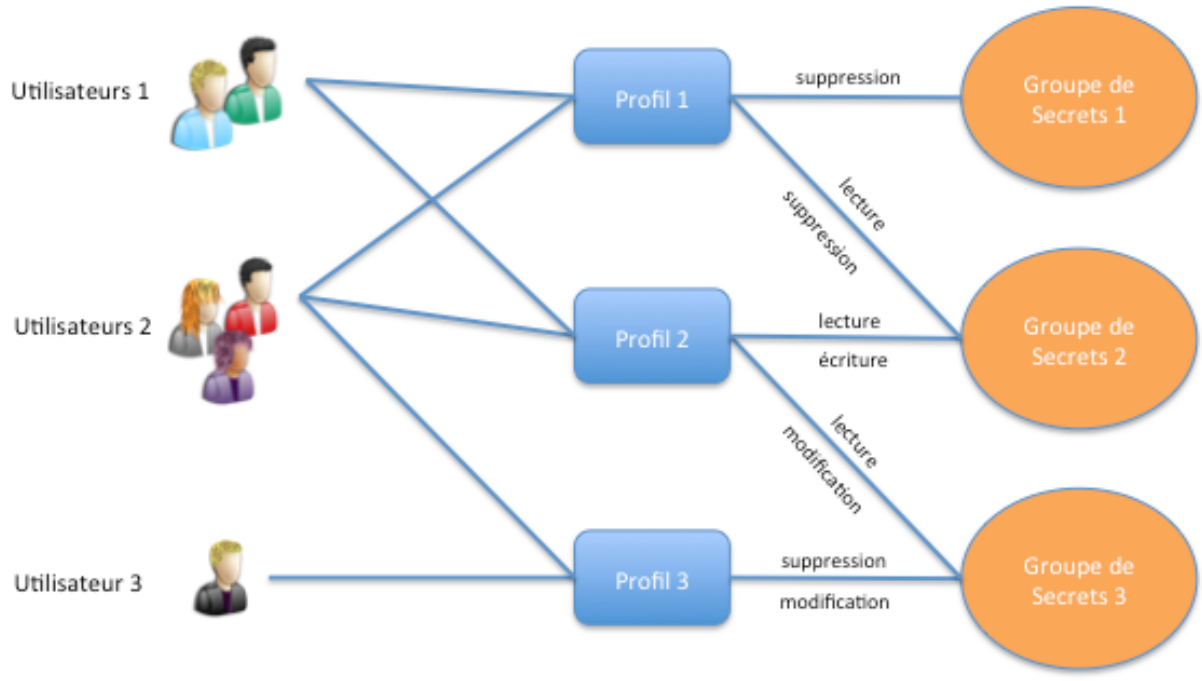
2. PRE-REQUIS

Le mode opératoire décrit ci-dessous ne vaut que si l'outil « **SecretManager** » a été installé conformément au « Guide d'Installation » (DR01) fournit dans le package d'installation.

De plus, il est vivement recommandé d'utiliser le « **SecretManager** » avec le « **SecretServer** » afin de sécuriser au maximum votre clé de chiffrement en base de données (dite Clé Mère).

3. FONCTIONNEMENT GLOBAL

Le « **SecretManager** » permet de partager des « Groupes de Secrets » via des « Profils » qui sont rattachés à des « Utilisateurs ». Quand un « Utilisateur » dispose de plusieurs droits d'accès sur un même « Groupe de Secrets », seuls les droits d'accès les plus forts sont conservés.



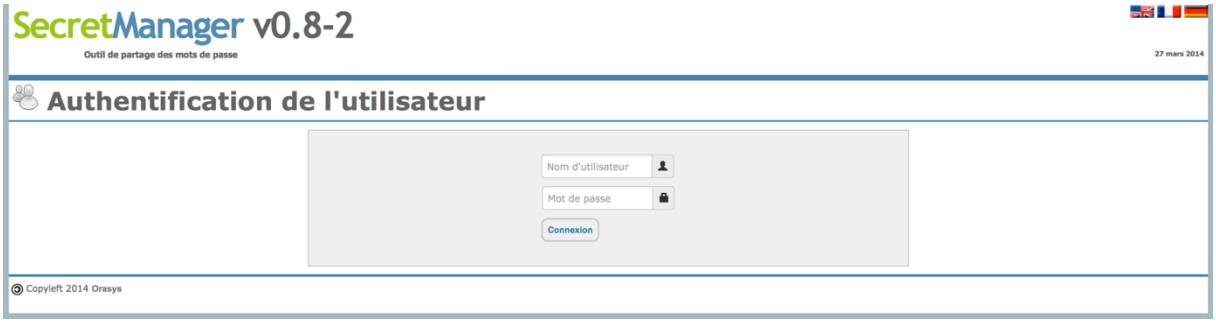
4. PREMIERE CONNEXION A L'OUTIL « SECRETMANAGER »

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://10.192.120.1/
```

Attention : il s'agit d'une adresse d'exemple

Vous devriez obtenir l'écran ci-dessous :



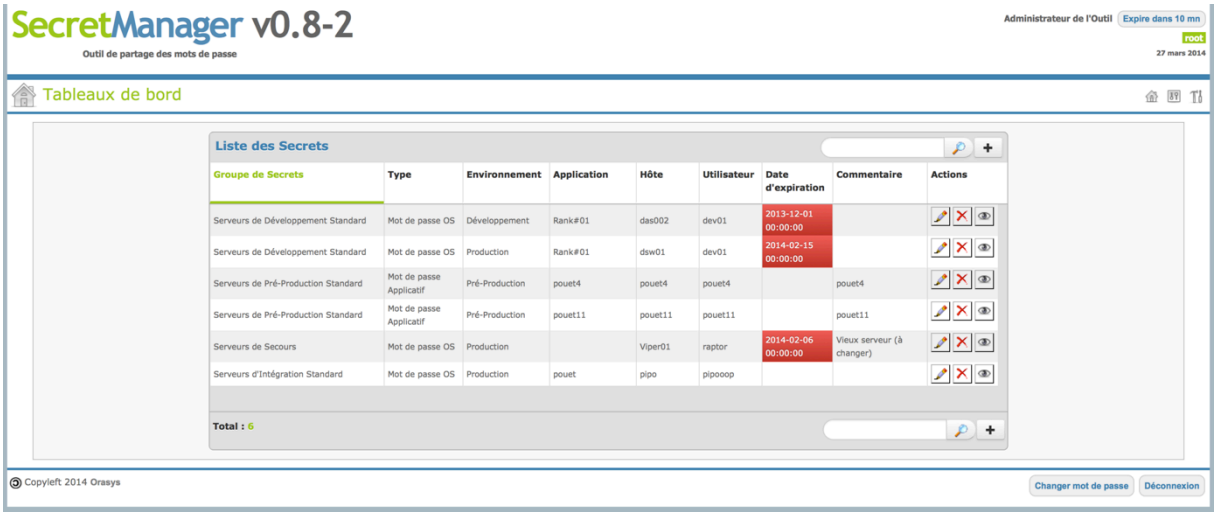
Si vous venez d'installer l'outil, il n'existe qu'un seul utilisateur par défaut.

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 : *« 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.*

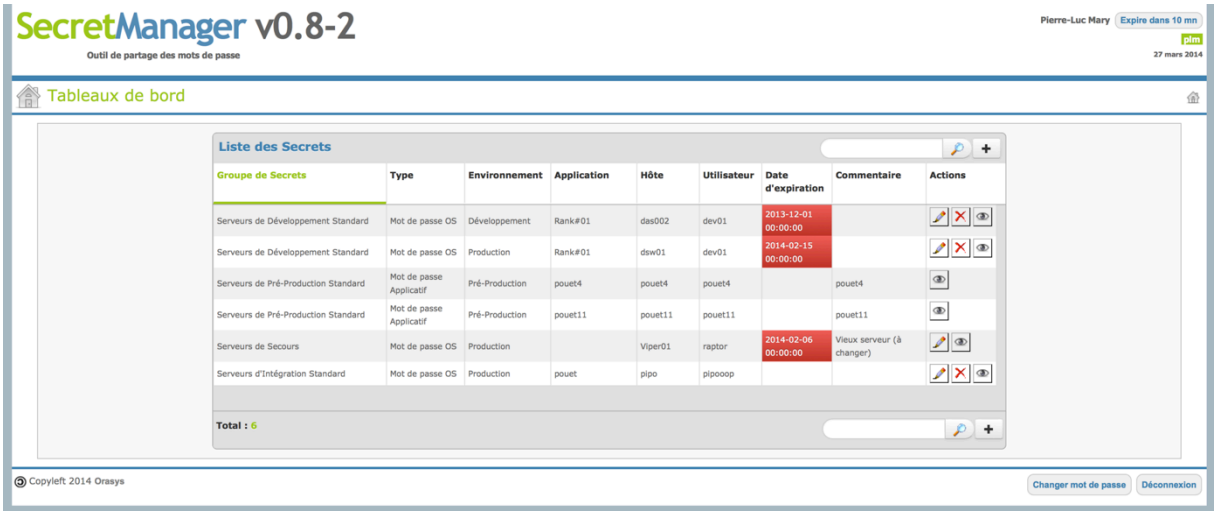
Après vous êtes identifié, vous devriez arriver sur l'écran ci-dessous :



Cet écran est votre tableau de bord, il vous donne accès à tout ce dont 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 :



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.

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.

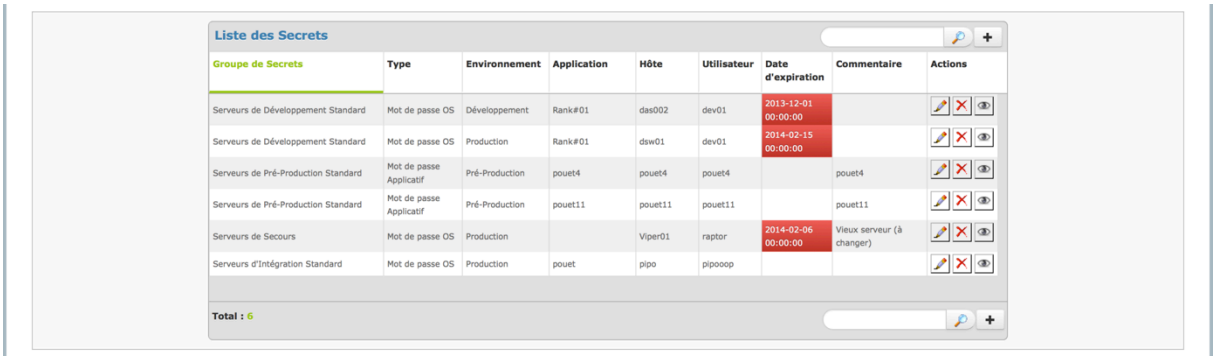
Un administrateur dispose de tous les boutons :

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 » (les Administrateurs et les Opérateurs y ont accès).

5.3. Zone corps



On trouve toutes les informations propres à chaque écran.

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 la société Orasys (http://www.orasys.fr) 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 des « Utilisateurs ».

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

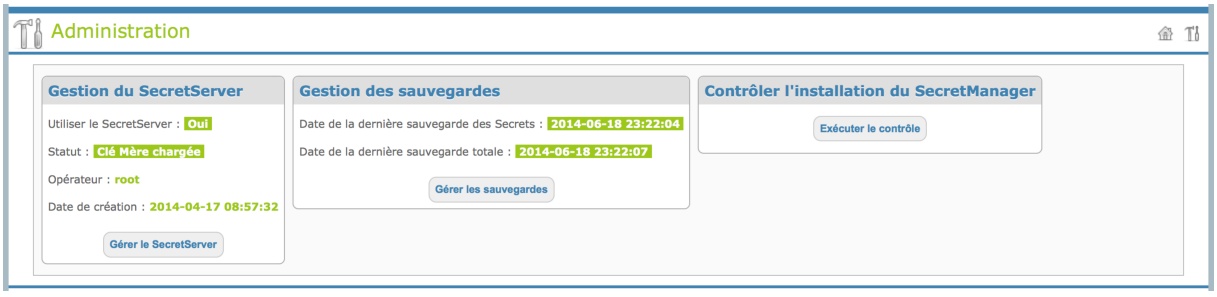
Les « Profils » donnent des accès à des « Groupes de Secrets ». La notion d'accès est importante. Effectivement, on définit un « droit d'accès » entre un « Profil » et un « Groupe de Secrets ». Il existe 4 droits dans l'outil :

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 » ;
3. Modification : l'utilisateur peut modifier les « Secrets » dans le « Groupe de Secrets » ;
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 ».

7. ACTIONS DE L'OPERATEUR

7.1. Ecran central d'Administration de l'Opérateur



Cet écran donne, en un coup d'œil, une vision globale des objets que peut administrer l'Opérateur dans « SecretManager ».

7.2. Gestion du SecretServer

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

7.2.1. Accéder à l'écran de gestion SecretServer

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

Ensuite, 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.

7.2.2. Ecran de gestion du SecretServer

7.2.2.1. 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 :

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

7.2.2.2. 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 pourraint 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.

7.2.2.3. 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.

7.2.3. 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.

7.3. Gestion des sauvegardes

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

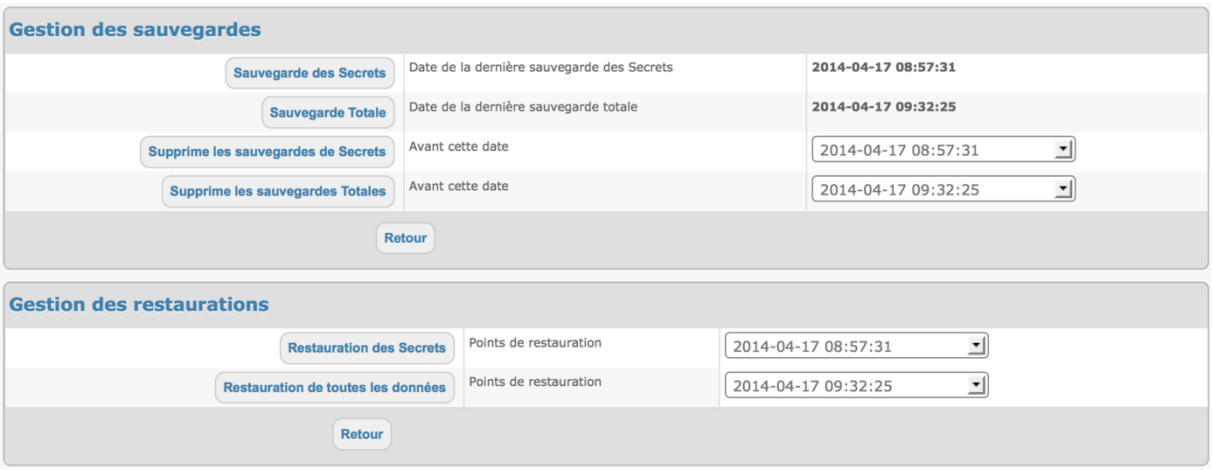
7.3.1. Accéder à l'écran de « Gestion des sauvegardes »

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

Ensuite, 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.

7.3.2. Ecran de gestion des Sauvegardes



7.3.2.1. 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.

7.3.2.2. Zone « Gestion des restaurations »

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

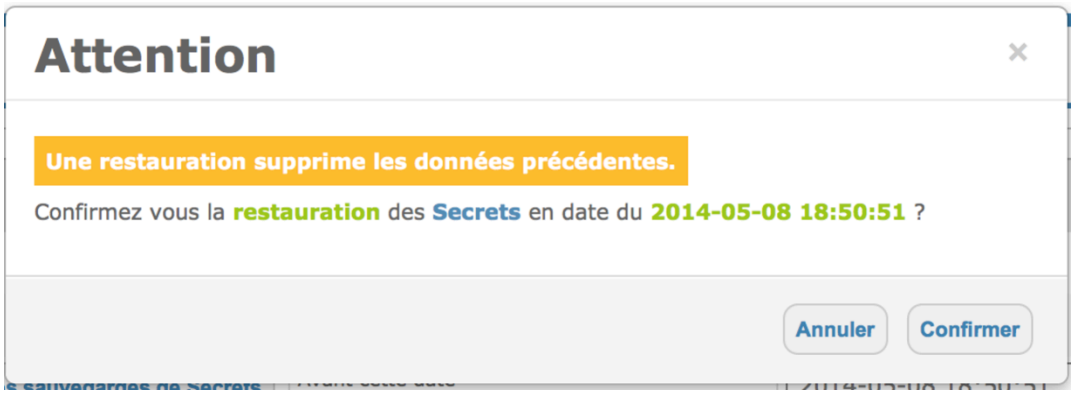
Bouton	Action
`Restauration des Secrets`	L'Administrateur doit choisir une date parmi celles proposées dans la liste déroulantes (ce sont en fait les dates correspondantes aux dernières sauvegardes). Après avoir sélectionné la date, l'Administrateur clique sur le bouton « `Restauration des Secrets` ». 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** ».

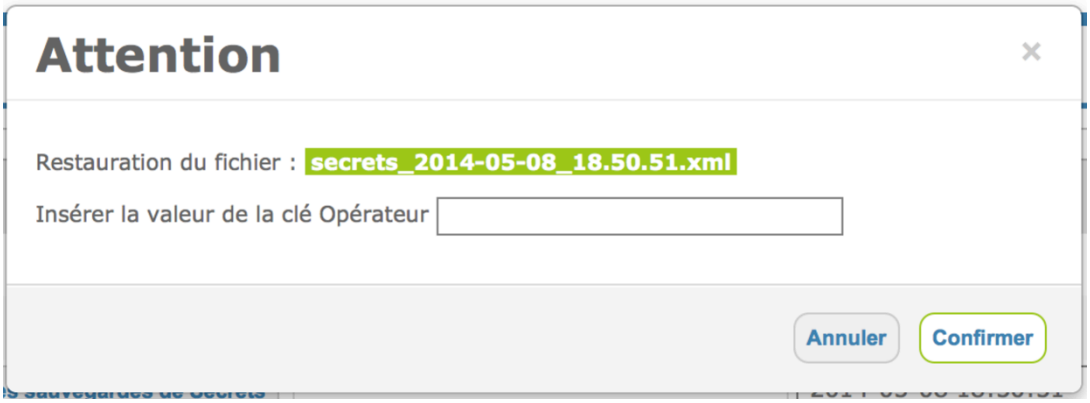
Attention : Quelle que soit la restauration, les tables impactées (par rapport au type de restauration) sont systématiquement vidées avant la restauration.

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.