|  |
| --- |
| Guide d'Administration  SecretManager v0.8-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 | 02/07/2013 | Création |
| 1.1-0 | 09/05/2014 | Modifications :   * Nouvelle gestion des « Applications » associées aux « Secrets » ; * Mise en œuvre des restaurations ; * Redimensionnement du tableau d’affichage des « Secrets » en fonction de la taille de fenêtre.   Cette modification correspond à la version « 0.8-4 ». |

|  |  |  |
| --- | --- | --- |
| DOCUMENTS DE REFERENCE | | |
| Index | Titre | Référence |
| DR01 | Guide d’Installation – SecretManager | Orasys - FR - Guide Installation - SecretManager v0.4-x - v0.1-0.doc |

TABLE DES MATIERES

1. Mise en garde 10

2. Pré-requis 10

3. Fonctionnement global 10

4. Première connexion à l’outil « SecretManager » 10

5. Ergonomie des écrans 12

5.1. Entête des écrans 12

5.2. Zone titre 12

5.3. Zone corps 13

5.4. Zone pied de page 13

6. Fonctionnement global de l’outil « SecretManager » 13

7. Administration 14

7.1. Gestion des utilisateurs 14

7.1.1. Accéder à l’écran de gestion des utilisateurs 14

7.1.2. Ecran liste des utilisateurs 14

7.1.2.1. Colonne « Entité » 15

7.1.2.2. Colonne « Prénom » 15

7.1.2.3. Colonne « Nom » 15

7.1.2.4. Colonne « Nom de l’utilisateur » 15

7.1.2.5. Colonne « Dernière connexion » 15

7.1.2.6. Colonne « Administrateur » 15

7.1.2.7. Colonne « Statut » 15

7.1.2.8. Colonne « Actions » 16

7.1.3. Règles sur les données des « Utilisateurs » 16

7.1.4. Création d’un utilisateur 16

7.1.4.1. Liste déroulante « Entité » 16

7.1.4.2. Bouton « Gestion des entités » 16

7.1.4.3. Liste déroulante « Civilité » 16

7.1.4.4. Bouton « Gestion des civilités » 16

7.1.4.5. Champ « Nom d’utilisateur » 17

7.1.4.6. Boîte à cocher « Administrateur » 17

7.1.5. Modification d’un utilisateur 17

7.1.5.1. Liste déroulante « Entité » 17

7.1.5.2. Bouton « Gestion des entités » 17

7.1.5.3. Champ « Civilité » 17

7.1.5.4. Bouton « Gestion des civilités » 17

7.1.5.5. Champ « Nom d’utilisateur » 17

7.1.5.6. Boîte à cocher « Administrateur » 18

7.1.5.7. Bouton « Réinitialiser le mot de passe » 18

7.1.5.8. Bouton « Réinitialiser le nombre de tentative » 18

7.1.5.9. Bouton « Réinitialiser la date d’expiration » 18

7.1.5.10. Bouton « Désactiver l’utilisateur » « Activer l’utilisateur » 18

7.1.5.11. Bouton « Modifier » 18

7.1.5.12. Bouton « Annuler » 18

7.1.6. Suppression d’un utilisateur 18

7.1.6.1. Bouton « Supprimer » 18

7.1.6.2. Bouton « Annuler » 19

7.1.7. Visualisation d’un utilisateur 19

7.1.7.1. Bouton « Retour » 19

7.1.8. Association des Profils à une Identité 19

7.1.8.1. Boîtes à cocher 19

7.1.8.2. Bouton « Gestion des Profils » 19

7.1.8.3. Bouton « Associer des Groupes de Secrets » 19

7.2. Gestion des profils 20

7.2.1. Accéder à l’écran de gestion des profils 20

7.2.2. Ecran liste des « Profils » 21

7.2.2.1. Colonne « Libellé » 21

7.2.2.2. Colonne « Actions » 21

7.2.3. Règles sur un profil 21

7.2.4. Créer un nouveau profil 21

7.2.4.1. Champ « Libellé » 21

7.2.4.2. Bouton « Créer » 22

7.2.4.3. Bouton « Annuler » 22

7.2.5. Modifier un profil 22

7.2.5.1. Champ « Libellé » 22

7.2.5.2. Bouton « Modifier » 22

7.2.5.3. Bouton « Annuler » 22

7.2.5.4. Supprimer un profil 22

7.2.5.5. Bouton « Confirmer » 22

7.2.5.6. Bouton « Annuler » 22

7.2.6. Associer des « Groupes de Secrets » à un « Profil » 23

7.2.6.1. Champ « Droits » 23

7.2.6.2. Bouton « Gestion des Groupes de Secrets » 23

7.2.6.3. Bouton « Associer » 23

7.2.6.4. Bouton « Annuler » 23

7.3. Gestion des civilités 24

7.3.1. Accéder à l’écran de gestion des civilités 24

7.3.2. Ecran liste des civilités 24

7.3.2.1. Colonne « Prénom » 24

7.3.2.2. Colonne « Nom » 24

7.3.2.3. Colonne « Sexe » 24

7.3.2.4. Colonne « Actions » 24

7.3.2.5. Bouton « Retour » 25

7.3.2.6. Bouton « Créer » 25

7.3.3. Règles sur les civilités 25

7.3.4. Création 25

7.3.5. Modification d’une civilité 25

7.3.5.1. Champ « Prénom » 25

7.3.5.2. Champ « Nom » 25

7.3.5.3. Liste déroulante « Sexe » 26

7.3.5.4. Bouton « Créer » ou « Modifier » 26

7.3.5.5. Bouton « Annuler » 26

7.3.6. Suppression d’une civilité 26

7.3.6.1. Bouton « Confirmer » 26

7.3.6.2. Bouton « Annuler » 26

7.4. Gestion des Entités 26

7.4.1. Accéder à l’écran de gestion des entités 26

7.4.2. Ecran liste des entités 27

7.4.2.1. Colonne « Code » 27

7.4.2.2. Colonne « Libellé » 27

7.4.2.3. Colonne « Actions » 27

7.4.2.4. Bouton « Retour » 27

7.4.2.5. Bouton « Créer » 27

7.4.3. Règles sur les entités 27

7.4.4. Création ou Modification d’une entité 27

7.4.4.1. Champ « Code » 28

7.4.4.2. Champ « Libellé » 28

7.4.4.3. Bouton « Annuler » 28

7.4.4.4. Bouton « Créer » ou « Modifier » 28

7.4.5. Suppression d’une entité 28

7.4.5.1. Bouton « Annuler » 28

7.4.5.2. Bouton « Confirmer » 28

7.5. Gestion des Groupes de Secrets 29

7.5.1. Accéder à l’écran de gestion des groupes de secrets 29

7.5.2. Ecran liste des « Groupes de Secrets » 29

7.5.2.1. Colonne « Libellé » 29

7.5.2.2. Colonne « Alerte » 29

7.5.2.3. Colonne « Actions » 29

7.5.2.4. Bouton « Retour » 30

7.5.2.5. Bouton « Créer » 30

7.5.3. Règles sur les groupes de secrets 30

7.5.4. Création ou Modification d’un groupe de secrets 30

7.5.4.1. Champ « Libellé » 31

7.5.4.2. Boîte à cocher « Alerte » 31

7.5.4.3. Bouton « Annuler » 31

7.5.4.4. Bouton « Créer » ou « Modifier » 31

7.5.5. Suppression d’un groupe de secrets 31

7.5.5.1. Bouton « Annuler » 31

7.5.5.2. Bouton « Confirmer » 31

7.5.6. Associer des Profils à un Groupe de Secrets 31

7.5.6.1. L’influence des droits sur les associations 32

7.5.6.2. Associer des Droits 33

7.5.7. Gérer les Secrets dans un Groupe de Secrets 33

7.5.7.1. Colonne « Type » 34

7.5.7.2. Colonne « Environnement » 34

7.5.7.3. Colonne « Application » 34

7.5.7.4. Colonne « Hôte » 34

7.5.7.5. Colonne « Utilisateur » 34

7.5.7.6. Colonne « Alerte » 34

7.5.7.7. Colonne « Commentaire » 34

7.5.7.8. Colonne « Actions » 35

7.5.7.9. Bouton « Retour » 35

7.5.7.10. Bouton « Créer » 35

7.6. Gestion des Applications 35

7.6.1. Accéder à l’écran de gestion des Applications 35

7.6.2. Ecran liste des « Applications » 36

7.6.2.1. Colonne « Nom » 36

7.7. Gestion de l’historique 36

7.8. Gestion du SecretServer 37

7.8.1. Accéder à l’écran de gestion SecretServer 37

7.8.2. Ecran de gestion du SecretServer 38

7.8.2.1. Zone « Statut » 38

7.8.2.2. Zone « Charger la clé mère » 39

7.8.2.3. Champ « Insérer la valeur de la clé Opérateur » 39

7.8.3. Zone « Transchiffrer la Clé Mère » 39

7.8.4. Zone « Création d’une nouvelle clé Mère » 39

7.8.4.1. Bouton « Transchiffrer » 40

7.8.4.2. Bouton « Créer » 41

7.8.5. Zone « Eteindre le SecretServer » 41

7.9. Gestion des sauvegardes 42

7.9.1. Accéder à l’écran de « Gestion des sauvegardes » 42

7.9.2. Ecran de gestion des Sauvegardes 42

7.9.2.1. Zone « Gestion des sauvegardes » 42

7.9.2.2. Zone « Gestion des restaurations » 43

8. Tableau de bord standard 44

8.1. Bloc « Liste des Secrets » 45

8.1.1. Colonne « Groupe de Secrets » 46

8.1.2. Colonne « Type » 46

8.1.3. Colonne « Environnement » 46

8.1.4. Colonne « Application » 46

8.1.5. Colonne « Hôte » 46

8.1.6. Colonne « Utilisateur » 46

8.1.7. Colonne « Date d’expiration » 46

8.1.8. Colonne « Commentaire » 47

8.1.9. Colonne « Actions » 47

8.1.10. Bouton « Créer » 47

8.2. Recherche de Secrets 47

8.3. Créer ou modifier un Secret 48

8.3.1. Champ « Groupe de Secrets » 49

8.3.2. Champ « Type » 49

8.3.3. Champ « Environnement » 49

8.3.4. Champ « Application » 50

8.3.5. Champ « Hôte » 50

8.3.6. Champ « Utilisateur » 50

8.3.7. Champ « Mot de passe » 50

8.3.8. Champ « Commentaire » 50

8.3.9. Champ « Alerte » 50

8.3.10. Bouton « Modifier » 50

8.3.11. Bouton « Annuler » 50

8.4. Suppression d’un Secret 50

8.4.1. Bouton « Supprimer » 51

8.4.2. Bouton « Annuler » 51

8.5. Création d’un Secret 51

9. Gestion des préférences 51

9.1. Gestion des « Alertes » 51

9.1.1. Champ « Verbosité des alertes » 52

9.1.2. Champ « Alerte remontée via Syslog » 52

9.1.3. Champ « Alerte remontée via Courriel » 52

9.1.3.1. Le champ « De » 52

9.1.3.2. Le champ « A » 52

9.1.4. Bouton « Sauvegarder » 52

9.2. Gestion des « Connexions » 52

9.2.1. Temps avant expiration de la session 53

9.2.2. Authentification par mots de passe 53

9.2.2.1. Le champ « Taille minimum des mots de passe » 53

9.2.2.2. Le champ « Complexité des mots de passe » 54

9.2.2.3. Le champ « Durée de vie d’un utilisateur (en mois) » 54

9.2.2.4. Le champ « Nombre de tentative maximum » 54

9.2.2.5. Le champ « Mot de passe par défaut » 54

9.2.3. Authentification par Radius 54

9.2.3.1. Adresse IP du serveur Radius 54

9.2.3.2. Port d'authentification du serveur Radius 54

9.2.3.3. Port d'accounting du serveur Radius 54

9.2.3.4. Secret partagé de Radius 55

9.2.4. Authentification par LDAP 55

9.2.4.1. Adresse IP du serveur Radius 55

9.2.4.2. Port du serveur Radius 55

9.2.4.3. Version du protocole LDAP 55

9.2.4.4. Organisation du LDAP 55

9.2.4.5. Préfixe RDN LDAP 55

9.3. Gestion du « SecretServer » 55

9.3.1. Démarrer le « SecretServer » 56

9.3.2. Champ « Utiliser le SecretServer » 56

9.3.3. Zone Sécurisation des clés utilisées par le SecretServer 57

9.3.3.1. Clé Opérateur 57

9.3.3.2. Clé Mère 57

# 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.

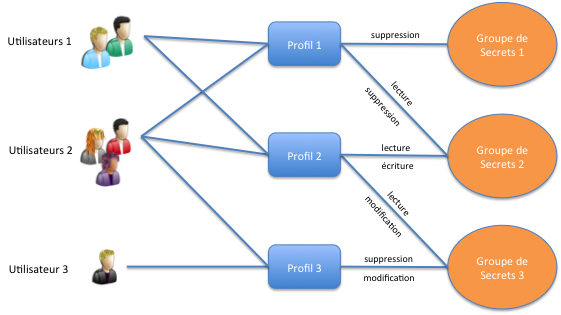
# Pré-requis

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).

# 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.

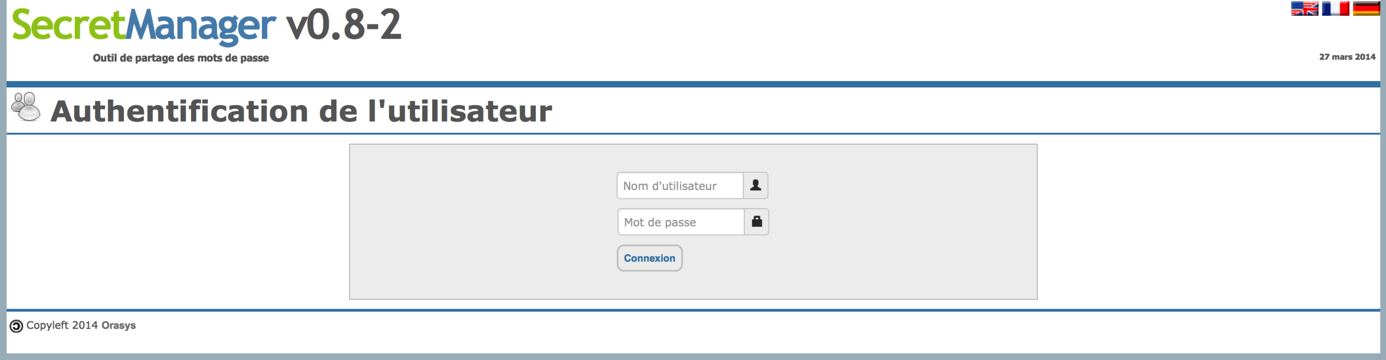


# Première connexion à l’outil « SecretManager »

Commencez par une connexion locale à votre serveur. Pour ce faire, utilisez votre navigateur et tapez :

https://10.192.120.1/

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.

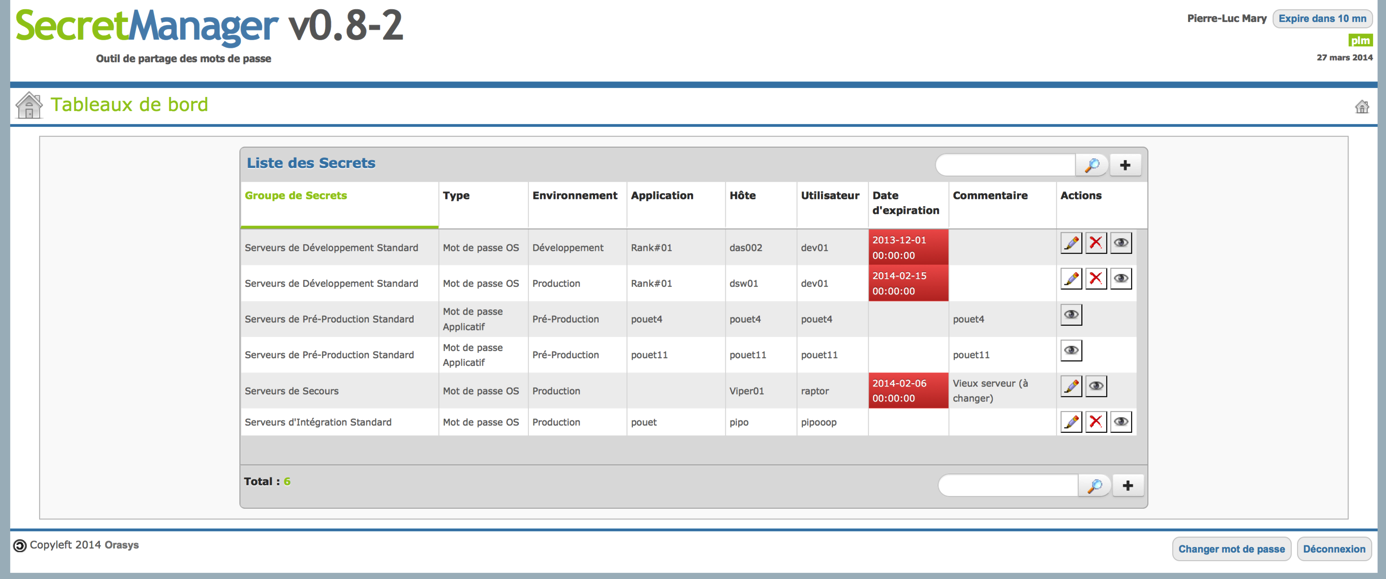
Après vous êtes identifié, vous devriez arriver sur l’écran ci-dessous :



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 :



# Ergonomie des écrans

## 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.

## 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 :

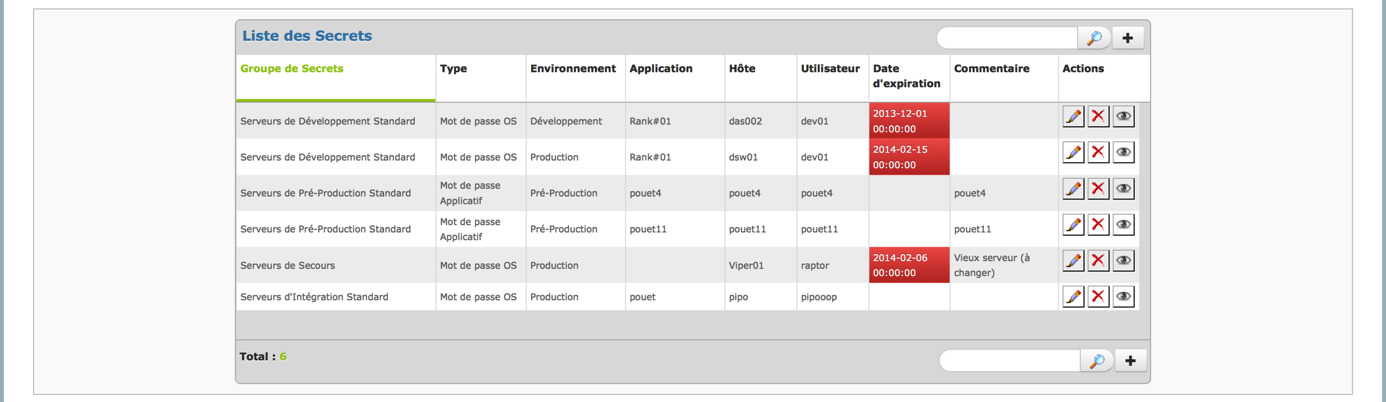


Le premier bouton permet d’avoir accès au « Tableau de bord », tous les utilisateurs y ont accès.

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 y ont accès).

## Zone corps



On trouve toutes les informations propres à chaque écran.

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

## 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.

# 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 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 » ;
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 ».

# Administration

## Gestion des utilisateurs

### Accéder à l’écran de gestion des utilisateurs

Pour accéder à l’écran de gestion des utilisateurs, l’administrateur doit utiliser le bouton ci-dessous :



Ensuite, 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.

### 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
* Statut
* Actions

#### Colonne « Entité »

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

#### Colonne « Prénom »

Cette information correspond au prénom usuel de l’utilisateur.

#### Colonne « Nom »

Cette information correspond au nom usuel de l’utilisateur.

#### Colonne « Nom de l’utilisateur »

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

#### Colonne « Dernière connexion »

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

#### 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.

#### 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 « 7.1.3 ».

#### 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 de l’utilisateur. |
|  | Ce bouton permet de supprimer de l’utilisateur. |
|  | Ce bouton permet de vérifier (visualiser en détail) de l’utilisateur. |
|  | Ce bouton permet d’associer des Profils à l’utilisateur. Les profils permettent de regrouper des accès à des Groupes de Secrets. |

### 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.

### Création d’un utilisateur

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



#### 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 ».

#### Bouton « Gestion des entités »

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

#### 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 ».

#### Bouton « Gestion des civilités »

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

#### 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.

#### Boîte à cocher « Administrateur »

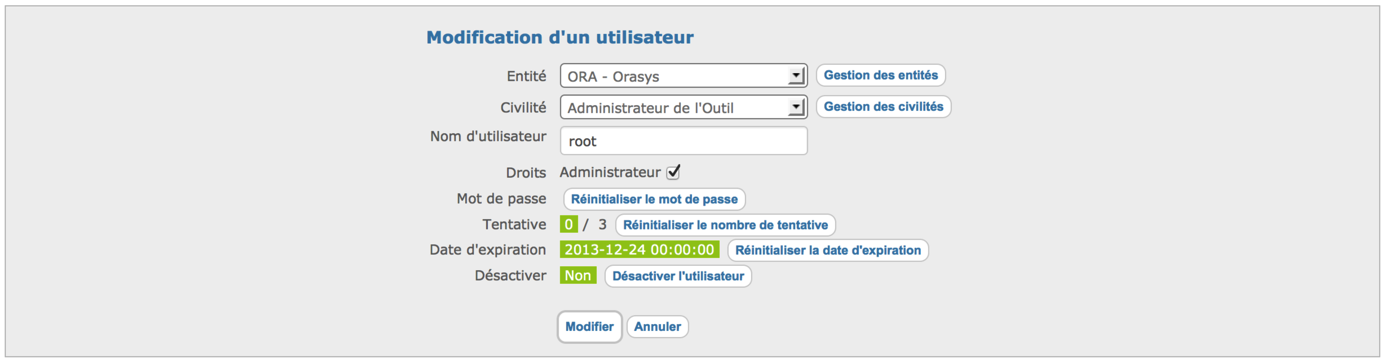
Cette boîte à cocher permet de donner ou pas le droit « Administrateur » à un utilisateur.

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.

**Remarque :** par défaut, le mot de passe d’Entreprise est affecté à la création de l’utilisateur. Voir le chapitre « 9.2.1 » pour plus d’information sur le mot de passe d’Entreprise.

### Modification d’un utilisateur

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



#### 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.

#### 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 ».

#### 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.

#### 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 ».

#### Champ « Nom d’utilisateur »

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

#### 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 ».

#### 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 « 9.2.2.5 » pour en savoir plus.

#### 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 « 9.2.2.4 » pour en savoir plus.

#### 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 « 9.2.2.3 » pour en savoir plus.

#### 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.

#### Bouton « Modifier »

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

#### Bouton « Annuler »

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

### Suppression d’un utilisateur

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



#### Bouton « Supprimer »

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

#### Bouton « Annuler »

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

### Visualisation d’un utilisateur

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

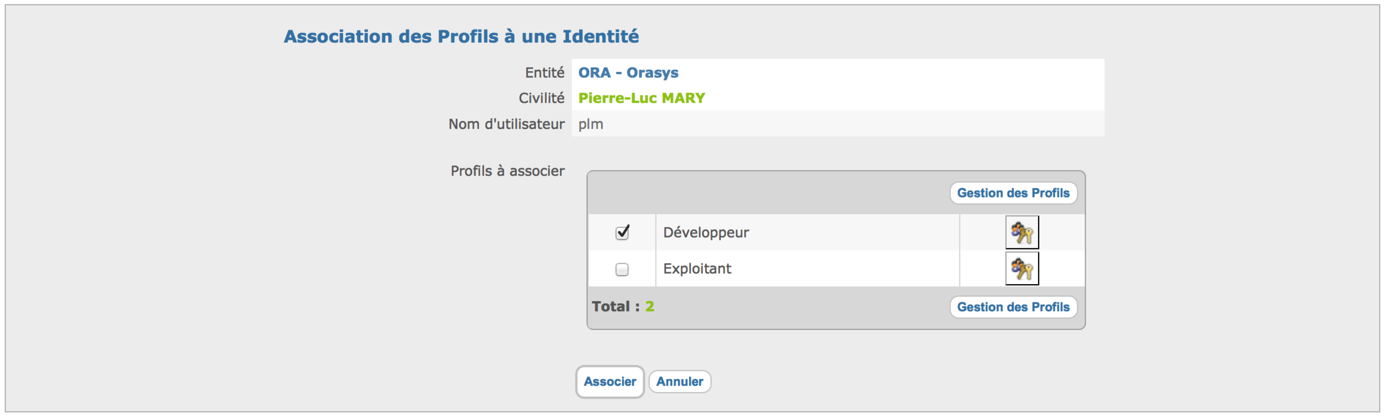


#### Bouton « Retour »

Ce bouton permet de retourner à la liste des utilisateurs.

### 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 ».

#### Boîtes à cocher

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

#### Bouton « Gestion des Profils »

Pour pouvoir ajouter ou supprimer des « Profils », l’administrateur peut utiliser ce bouton. Voir chapitre « Gestion des Profils » pour plus d’information.

#### Bouton « Associer des Groupes de Secrets »

En cliquant sur le bouton b_usrscr_2, vous arrivez sur l’écran ci-dessous :



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

## 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 « 7.1.8 » ;
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 :

### Accéder à l’écran de gestion des profils

Pour accéder à l’écran de gestion des profils, l’administrateur doit utiliser le bouton ci-dessous :

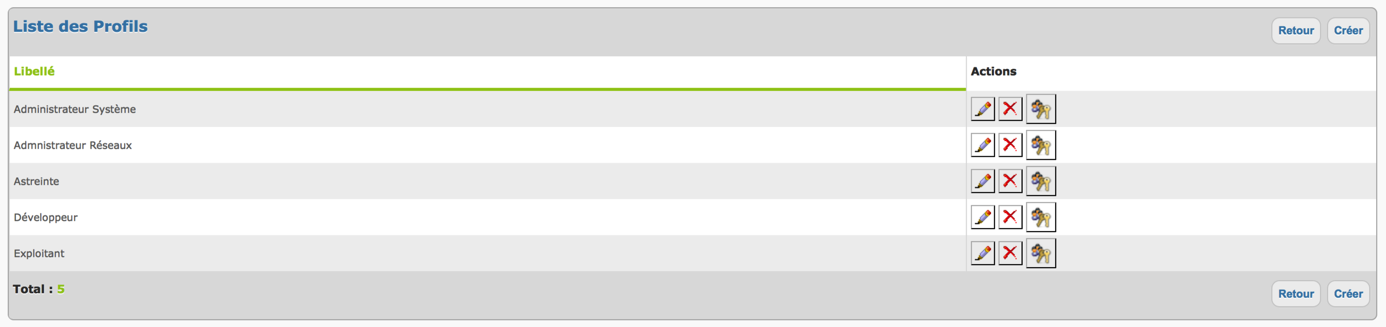


Ensuite, il faut utiliser la boite de synthèse dédiée aux Profils, comme dans l’exemple ci-dessous :



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

### Ecran liste des « Profils »



#### Colonne « Libellé »

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

#### 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 ». |

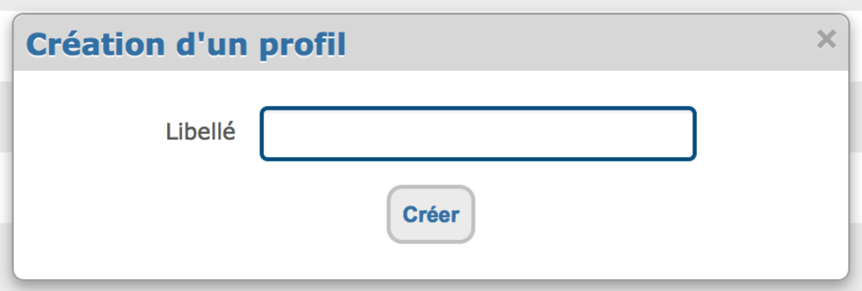
### Règles sur un profil

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

### 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 :



#### Champ « Libellé »

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

#### Bouton « Créer »

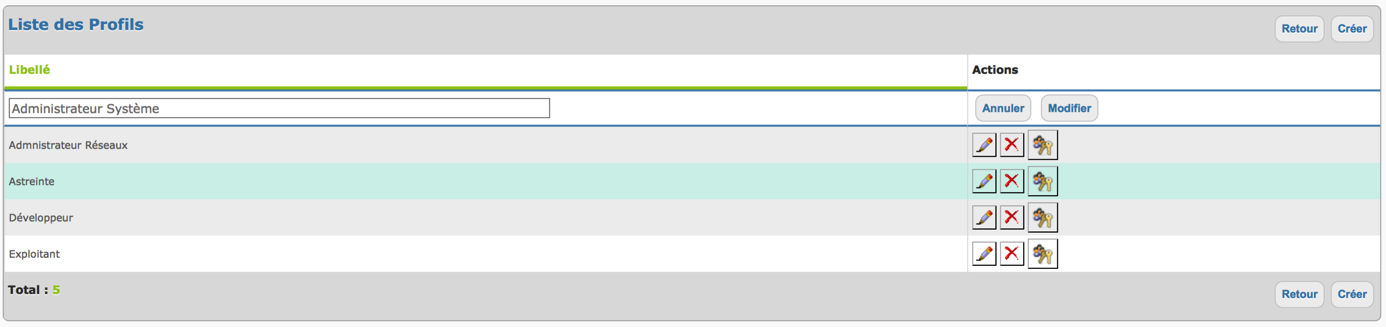
Ce bouton permet de valider la création d’un « Profil ».

#### Bouton « Annuler »

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

### 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) :



#### Champ « Libellé »

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

#### Bouton « Modifier »

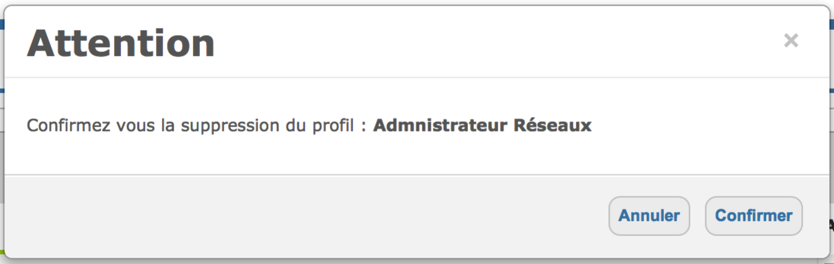
Ce bouton permet de sauvegarder la modification effectuée sur le « Profil ».

#### Bouton « Annuler »

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

#### 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 :



#### Bouton « Confirmer »

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

#### Bouton « Annuler »

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

### 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 :



#### 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 »

#### 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.

#### Bouton « Associer »

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

#### Bouton « Annuler »

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

## 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 « 7.1.3 » ;
2. En utilisant le bouton « Gérer les Civilités », à partir de l’écran « Tableaux de bord ».

### Accéder à l’écran de gestion des civilités

Pour accéder à l’écran de gestion des profils, l’administrateur doit utiliser le bouton ci-dessous :

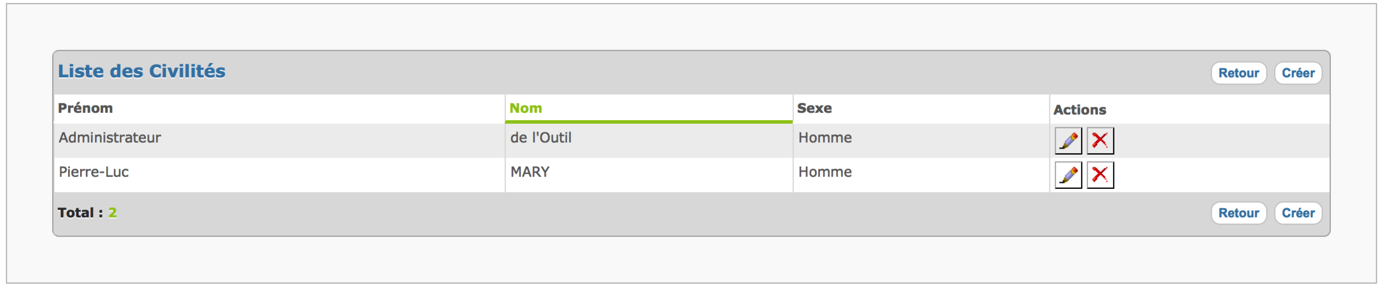


Ensuite, il faut utiliser la boite de synthèse dédiée aux Civilités, comme dans l’exemple ci-dessous :



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

### Ecran liste des civilités



#### Colonne « Prénom »

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

#### Colonne « Nom »

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

#### Colonne « Sexe »

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

#### 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 ». |

#### Bouton « Retour »

Ce bouton permet de revenir à l’écran précédent.

#### Bouton « Créer »

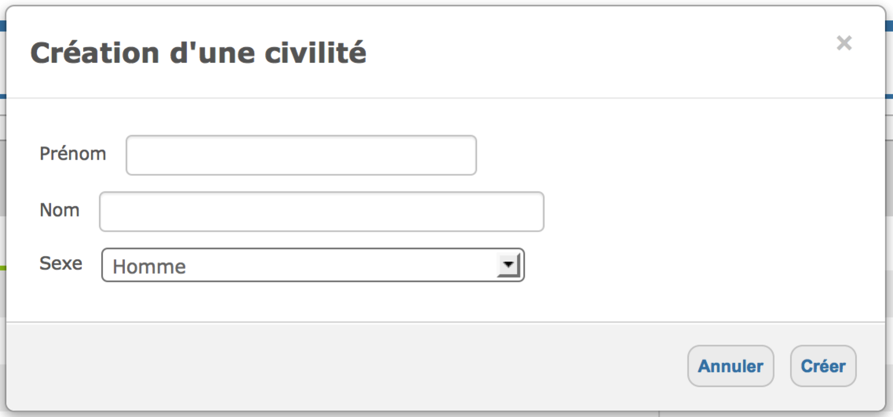
Ce bouton permet d’exécuter la création d’une nouvelle « Civilité ».

### Règles sur les civilités

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

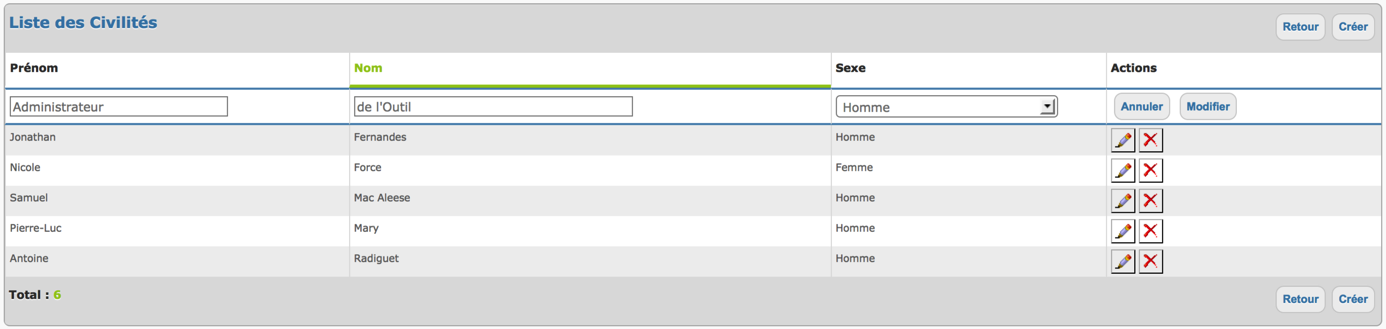
### Création

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



### 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 :



#### Champ « Prénom »

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

#### Champ « Nom »

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

#### Liste déroulante « Sexe »

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

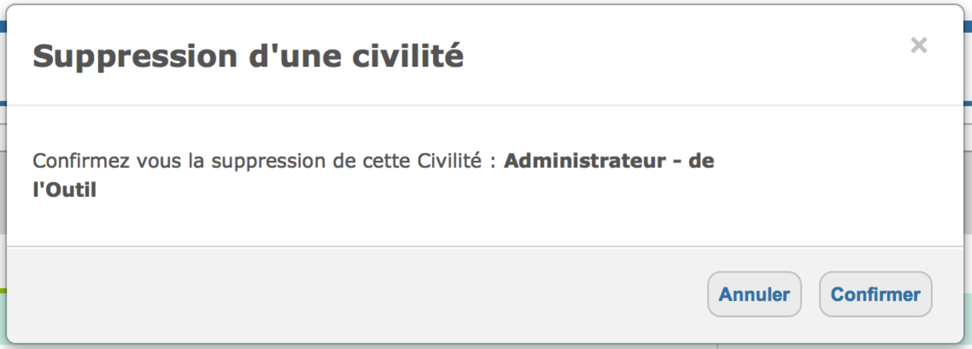
#### Bouton « Créer » ou « Modifier »

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

#### Bouton « Annuler »

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

### Suppression d’une civilité



#### Bouton « Confirmer »

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

#### Bouton « Annuler »

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

## 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 « 7.1.37.1.4.1 » ;
2. En utilisant le bouton « Gérer les Civilités », à partir de l’écran « Tableaux de bord ».

### Accéder à l’écran de gestion des entités

Pour accéder à l’écran de gestion des Entités, l’administrateur doit utiliser le bouton ci-dessous :



Ensuite, 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.

### Ecran liste des entités



#### Colonne « Code »

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

#### Colonne « Libellé »

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

#### 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 ». |

#### Bouton « Retour »

Ce bouton permet de revenir à l’écran précédent.

#### Bouton « Créer »

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

### Règles sur les entités

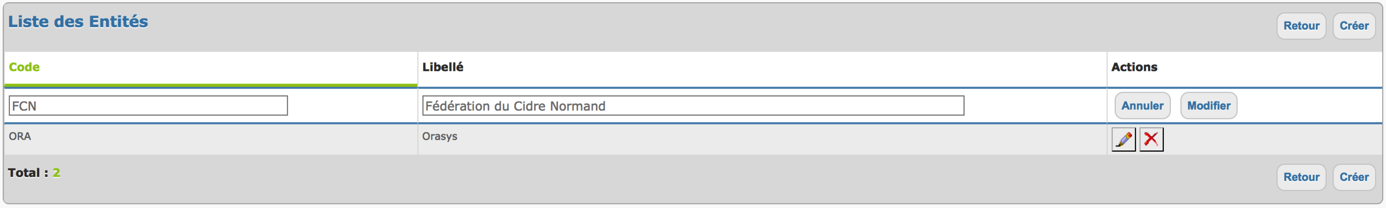
1. Il ne peut y avoir 2 « Entités » avec le même « Code » ou le même « Libellé ».

### 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 :



#### Champ « Code »

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

#### Champ « Libellé »

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

#### Bouton « Annuler »

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

#### Bouton « Créer » ou « Modifier »

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

### Suppression d’une entité

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



#### Bouton « Annuler »

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

#### Bouton « Confirmer »

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

## 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.

### 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 ci-dessous :

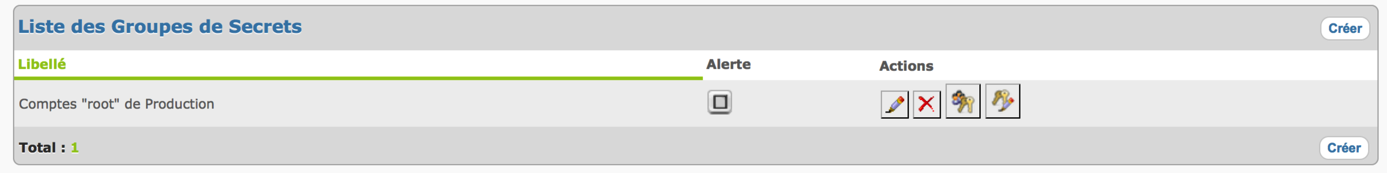


Ensuite, il faut utiliser la boite de synthèse dédiée aux Groupes de Secrets, comme dans l’exemple ci-dessous :



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

### Ecran liste des « Groupes de Secrets »



#### Colonne « Libellé »

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

#### 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 ».

#### 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 ». |

#### Bouton « Retour »

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

#### Bouton « Créer »

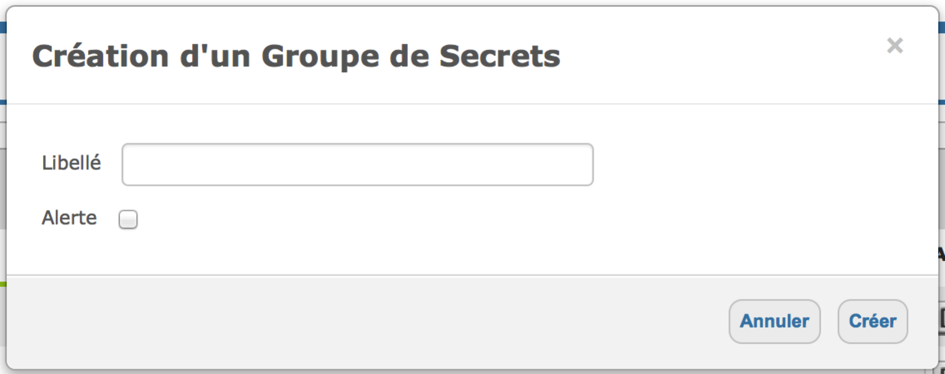
Ce bouton permet d’exécuter la création d’un nouveau « Groupe de Secrets ».

### Règles sur les groupes de secrets

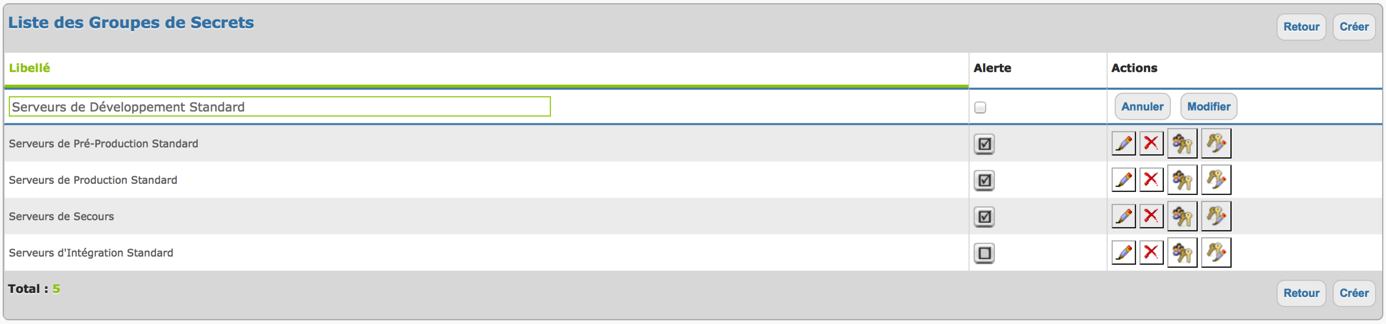
1. Il ne peut y avoir 2 « Groupes de Secrets » avec le même « Libellé ».

### 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 :



#### Champ « Libellé »

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

#### 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 ».

#### Bouton « Annuler »

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

#### Bouton « Créer » ou « Modifier »

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

### Suppression d’un groupe de secrets

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



#### Bouton « Annuler »

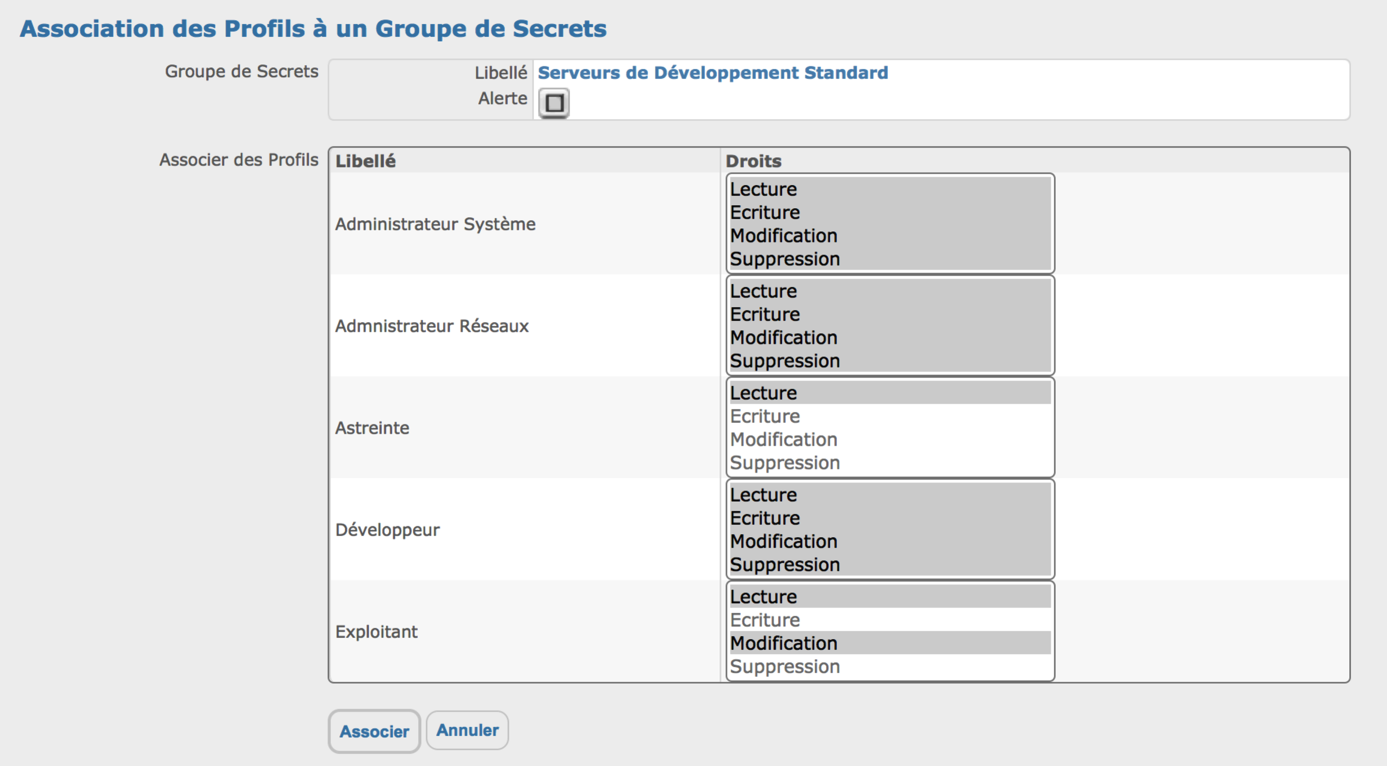
Ce bouton permet de revenir à l’écran précédent, sans supprimer le « Groupe de Secrets ».

#### Bouton « Confirmer »

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

### 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 ».

#### L’influence des droits sur les associations

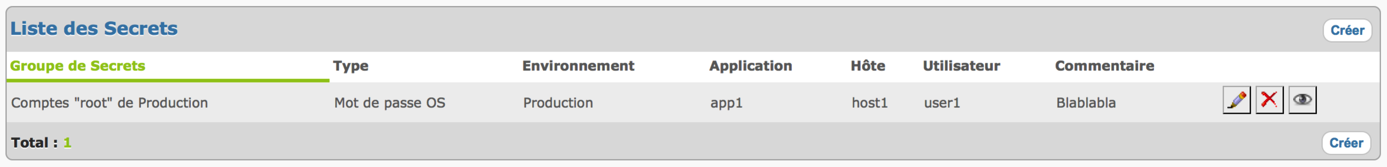
Si aucun « Droit » n’est sélectionné, le « Groupe de Secrets » n’apparaitra jamais auprès des utilisateurs (à l’exception de ceux qui ont le privilège « Administrateur »).

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 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 au moins un droit d’écriture sur un des Groupes de Secrets auxquels il a accès.  Toutefois, il ne pourra créer un Secret que dans les listes qui seront disponibles dans 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. |

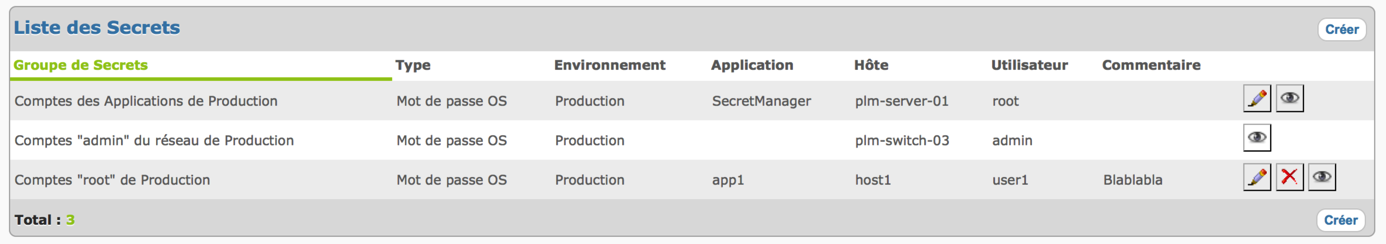
#### Associer des Droits

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 :

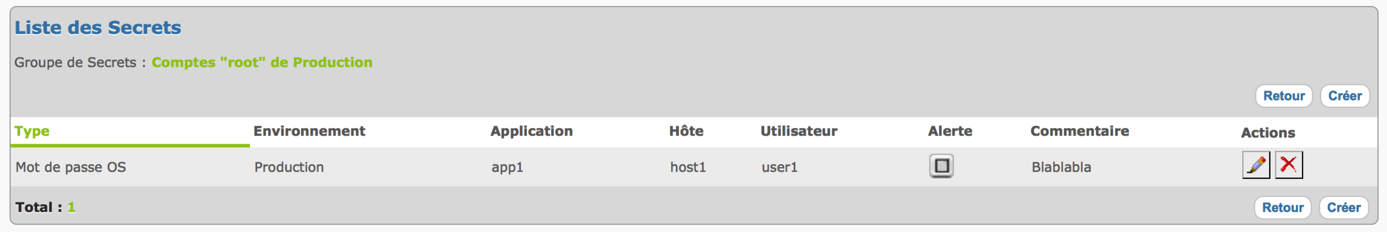


Dans cet exemple, on comprend que l’utilisateur connecté à les droits suivants :

* 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 ».

### 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 :



#### Colonne « Type »

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

**SecretManager** gère 2 types :

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

#### 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. Test.

**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.

#### Colonne « Application »

Ce champ est libre en saisie pour l’Administrateur et il n’est pas obligatoire. Il permet de pouvoir rattacher le « Secret » à une « Application ».

#### 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 « Equipement ».

#### Colonne « Utilisateur »

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

#### 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 ».

#### 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 ».

#### Colonne « Actions »

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

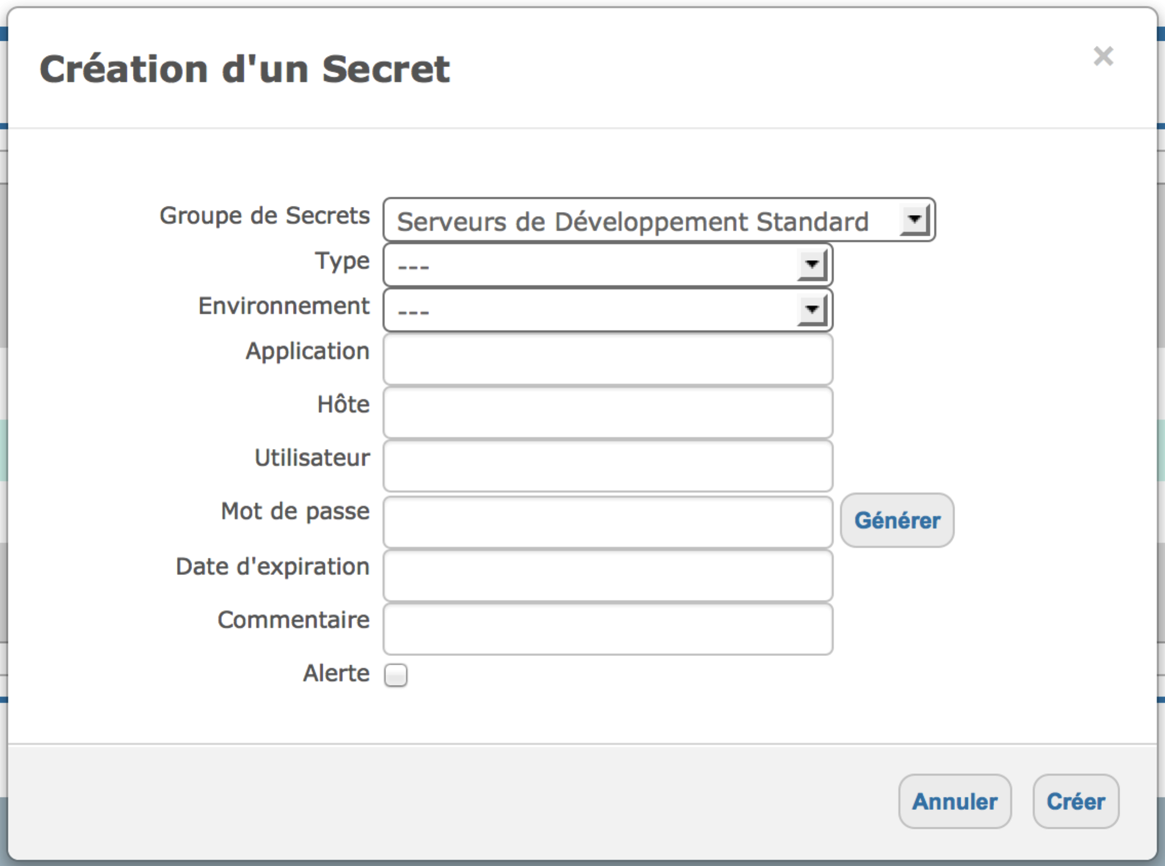
| Bouton | Signification |
| --- | --- |
|  | Ce bouton permet de modifier le « Secret ». |
|  | Ce bouton permet de supprimer le « Secret ». |

#### Bouton « Retour »

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

#### 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 :



## Gestion des Applications

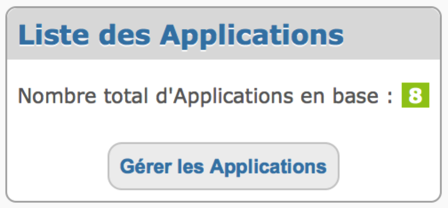
Les « Applications » sont particulièrement importantes quand on crée des « Secrets » de type « mots de passe applicatif ».

### Accéder à l’écran de gestion des Applications

Pour accéder à l’écran de gestion des Applications, l’administrateur doit utiliser le bouton ci-dessous :

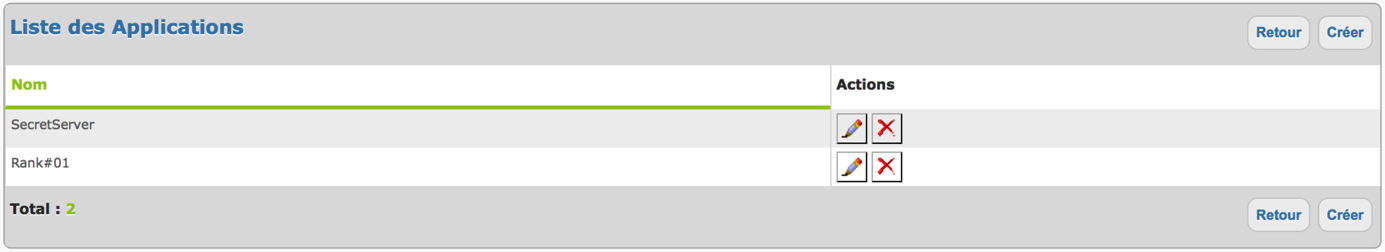


Ensuite, il faut utiliser la boite de synthèse dédiée aux Applications, comme dans l’exemple ci-dessous :



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

### Ecran liste des « Applications »



#### Colonne « Nom »

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

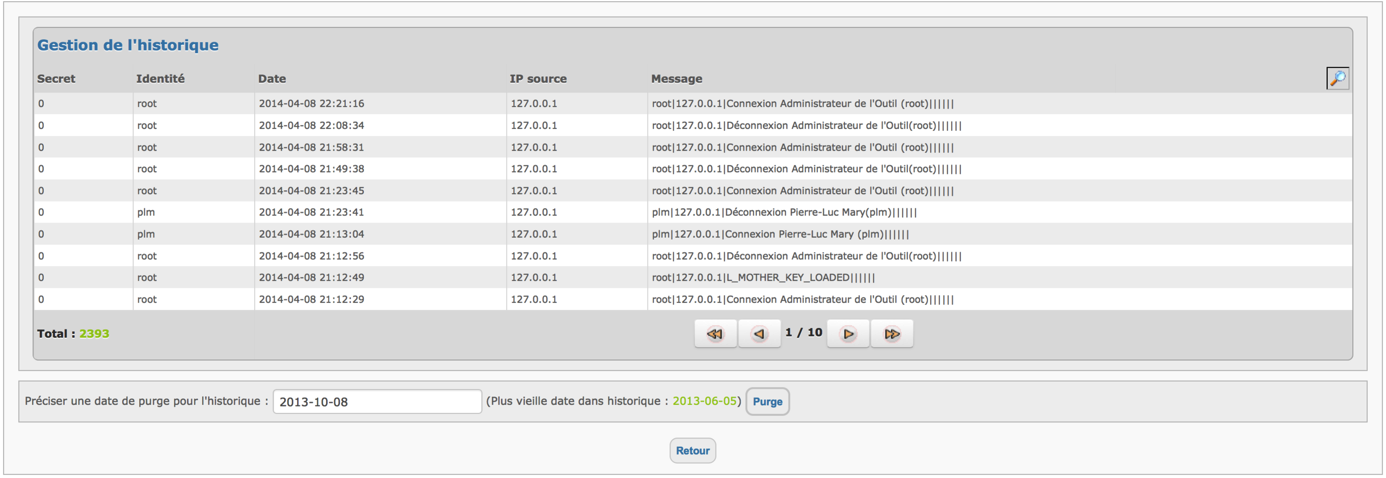
Ci-dessous le tableau de correspondance des droits et des incidences sur l’IHM

|  |  |
| --- | --- |
| Bouton | Fonction |
|  | Ce bouton permet de modifier le nom d’une Application. |
|  | Ce bouton permet de supprimer le nom d’une Application. |

## Gestion de l’historique

Toutes les actions réalisées dans l’outil « **SecretManager** » sont tracées dans l’historique. Une partie de ces actions peut être envoyée en plus sur d’autres canaux. Il s’agit des Secrets qui sont sous contrôle (voir les chapitres 7.5.4.2, 7.5.7.6 et 9.1).

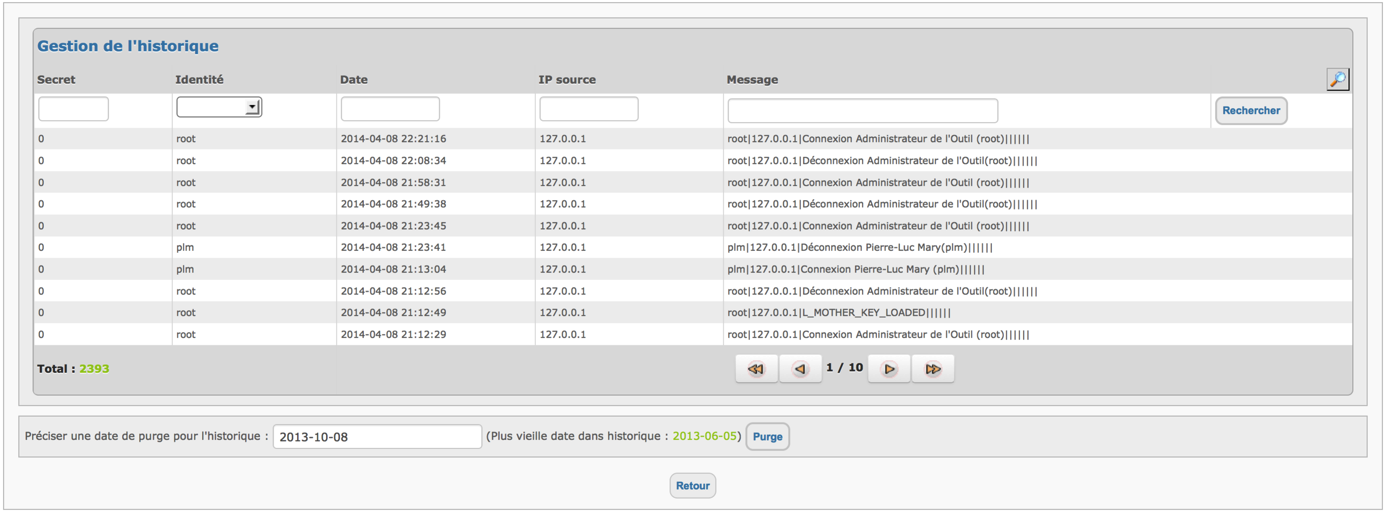
Les actions sont classées par date décroissante et elles sont regroupées par groupe de 10 occurrences. Comme dans l’exemple ci-dessous :



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) |
|  | 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) |

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.

## Gestion du SecretServer

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

### 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 :

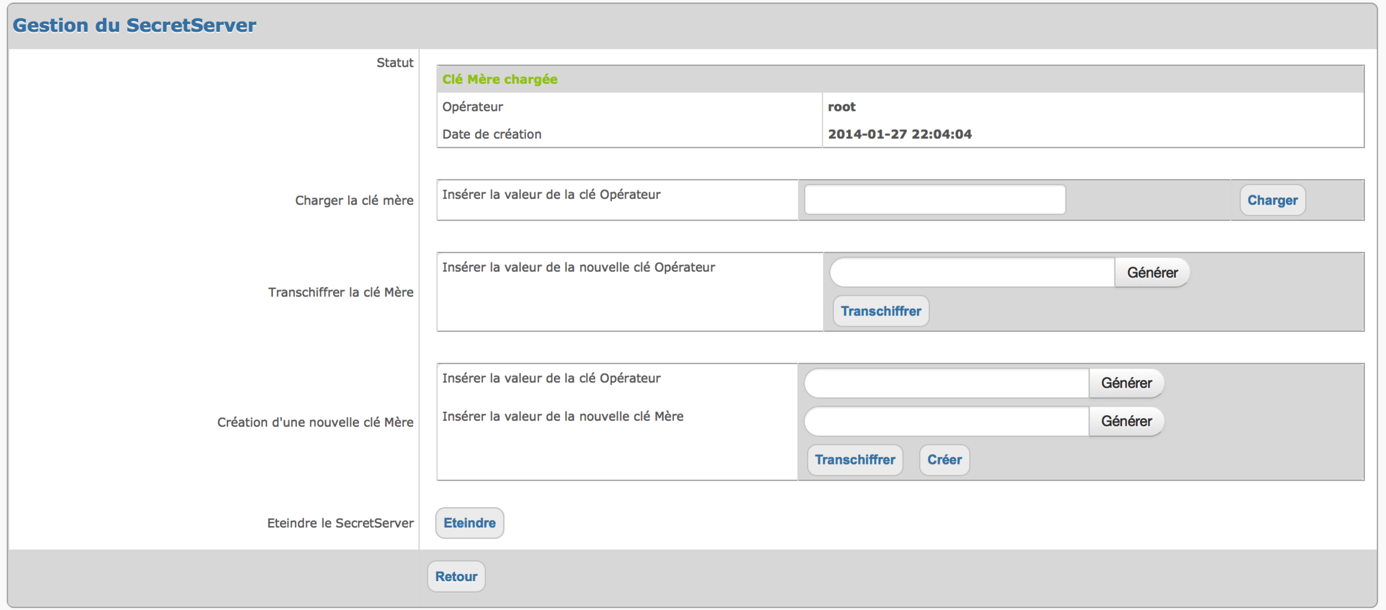


Ensuite, il faut utiliser la boite de synthèse dédiée aux SecretServer, comme dans l’exemple ci-dessous :



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

### Ecran de gestion du SecretServer

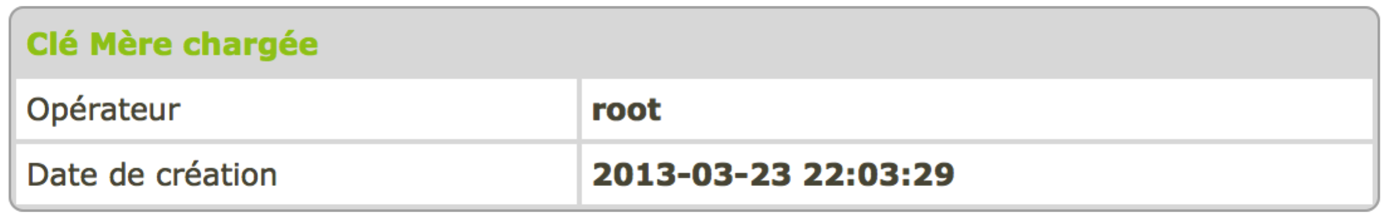


#### Zone « Statut »

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 :



#### Zone « Charger la clé mère »

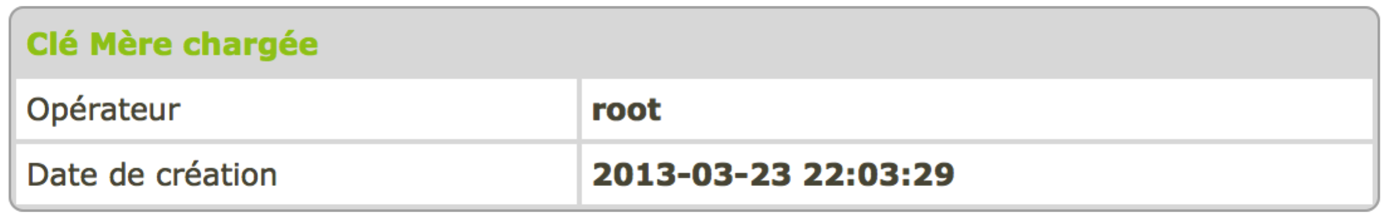
Pour charger une clé « Mère », il faut être en mesure de la déchiffrer. Pour cela, l’Administrateur doit disposer de la clé « Opérateur ». Seule cette clé permet de déchiffrer la clé « Mère » et ainsi la charger dans la mémoire du « **SecretServer** ».

**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 :



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.

#### 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.

### 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 9.3.3). 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.

### 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 ».

#### Bouton « Transchiffrer »

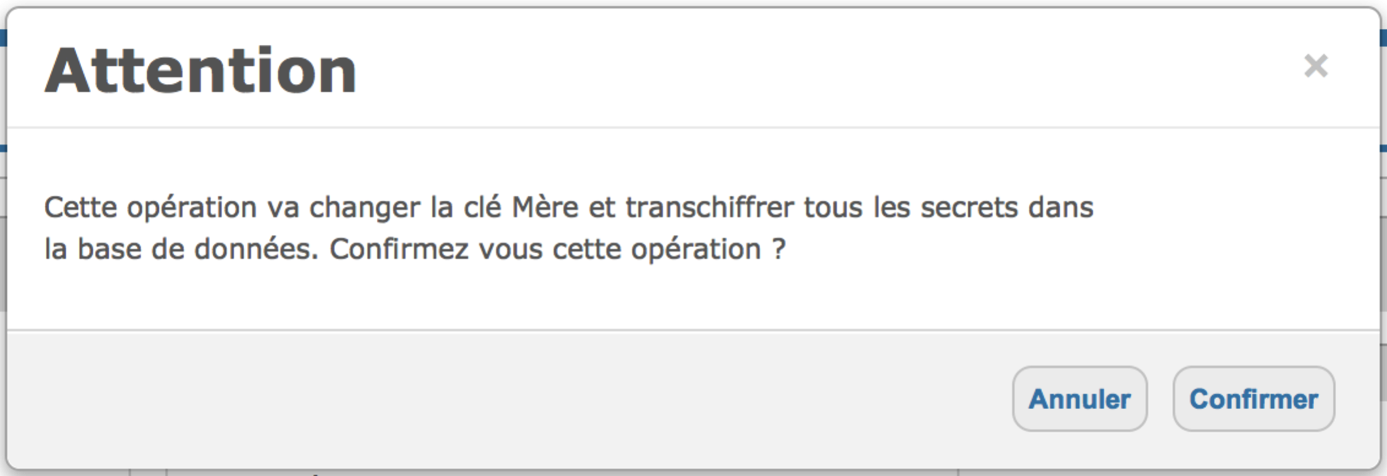
Ce bouton est à utiliser, si une clé Mère existe déjà et que l’on souhaite transchiffrer les « Secrets » qui ont déjà été insérés dans la base de données de « **SecretManager** ». Effectivement, avec ce bouton chaque Secret est déchiffré avec l’ancienne clé Mère et chiffré avec la nouvelle clé Mère.

Prenons l’exemple ci-dessous :



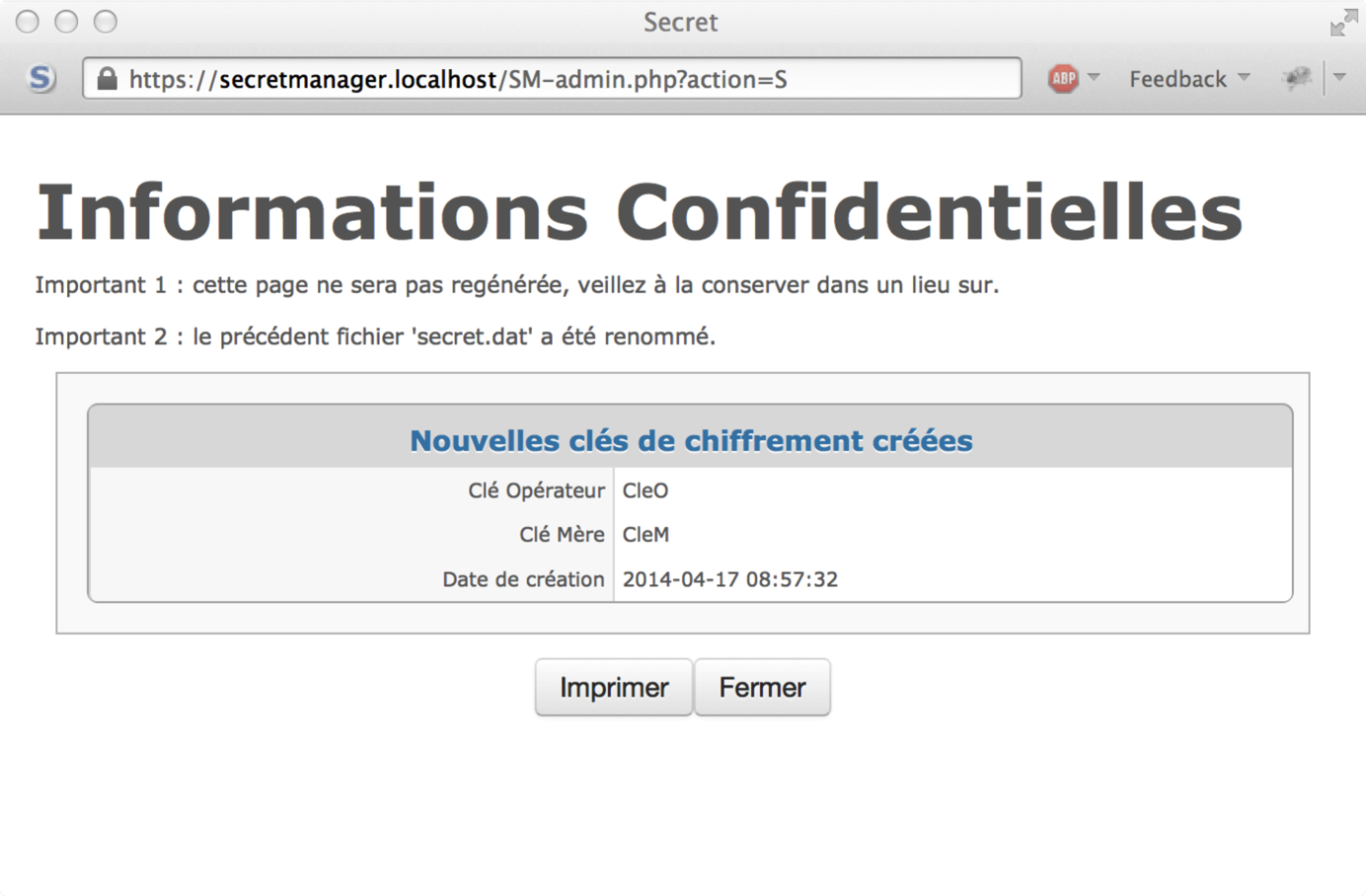
On voit que l’on va créer la clé Mère ayant une valeur « CleM » et chiffrée par la clé Opérateur ayant la valeur « CleO ». On notera que des avertissements sont levés par la présence du drapeau . Effectivement, les valeurs des clés sont largement inférieures à ce qui pratique habituellement.

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.

#### 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** ».

### 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.

## Gestion des sauvegardes

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

### 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 :

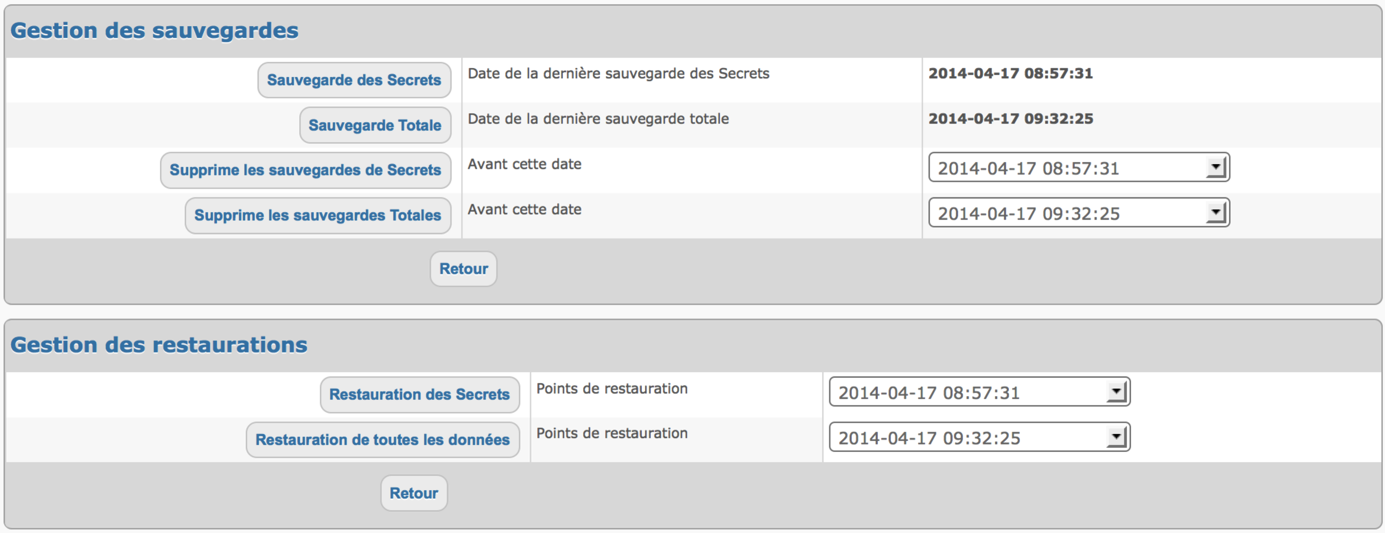


Ensuite, il faut utiliser la boite de synthèse dédiée à la Sauvegarde, comme dans l’exemple ci-dessous :



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

### Ecran de gestion des Sauvegardes



#### 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. |

#### Zone « Gestion des restaurations »

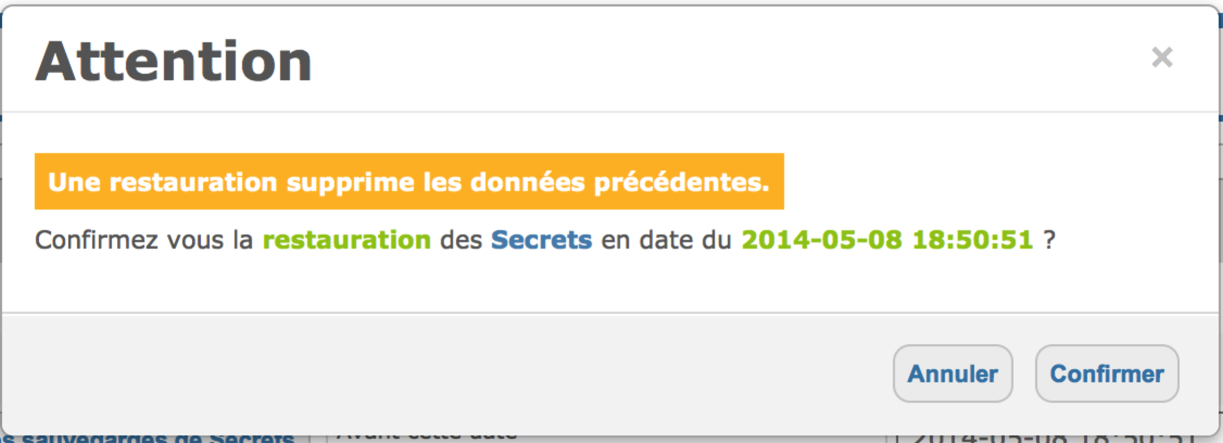
Cette zone abrite plusieurs boutons qui réalisent les actions ci-dessous :

|  |  |
| --- | --- |
| 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** ». |

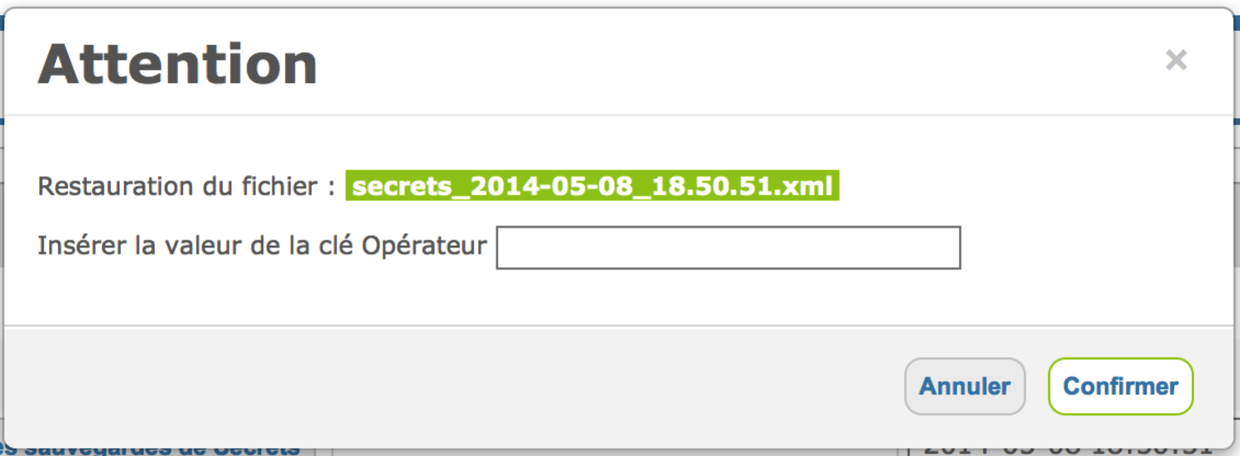
**Attention**: Quelle que soit la restauration, les tables impactées (par rapport au type de restauration) sont systématiquement vidées avant la restauration.

**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.

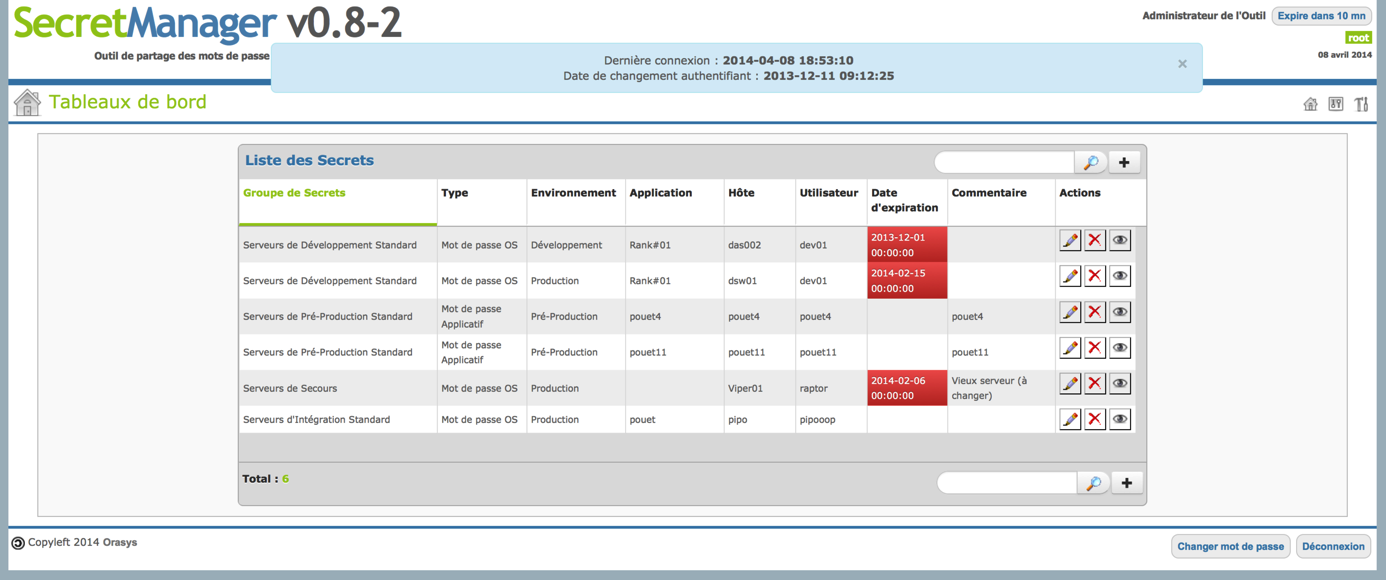
Cette mesure permet de s’assurer que l’administrateur restaure un fichier qu’il maitrise.

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.

# Tableau de bord standard

Un utilisateur n’étant pas « Administrateur » aura plutôt un tableau de bord qui ressemble à l’écran ci-dessous :



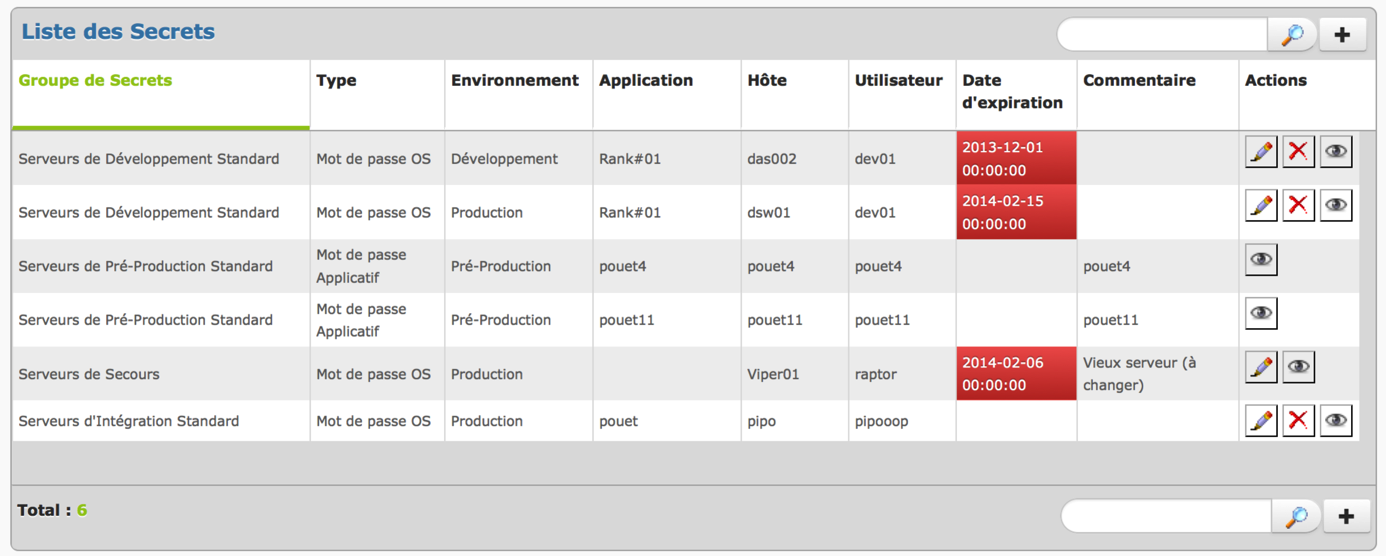
Quand un utilisateur vient de se connecter, il est informé :

* De la date de sa dernière connexion ;
* De la date de son dernier changement d’authentifiant (mot de passe).

Ensuite, l’utilisateur distingue tous les Secrets auxquels il a accès.

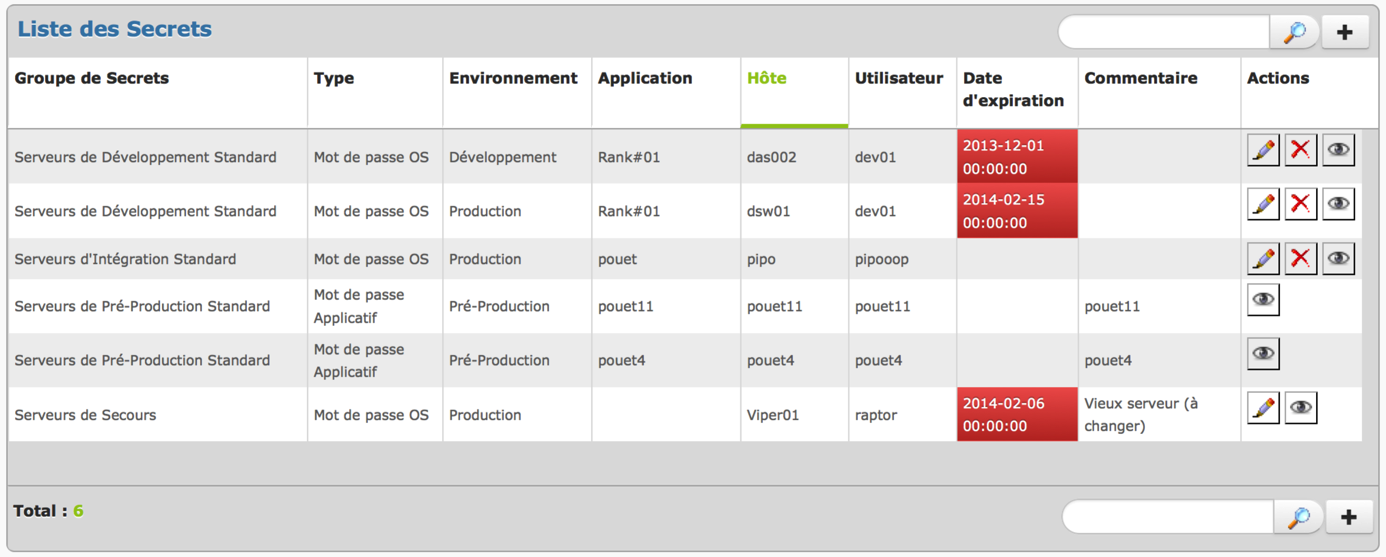
## Bloc « Liste des Secrets »

Ce bloc affiche tous les Secrets auxquels à accès l’utilisateur.

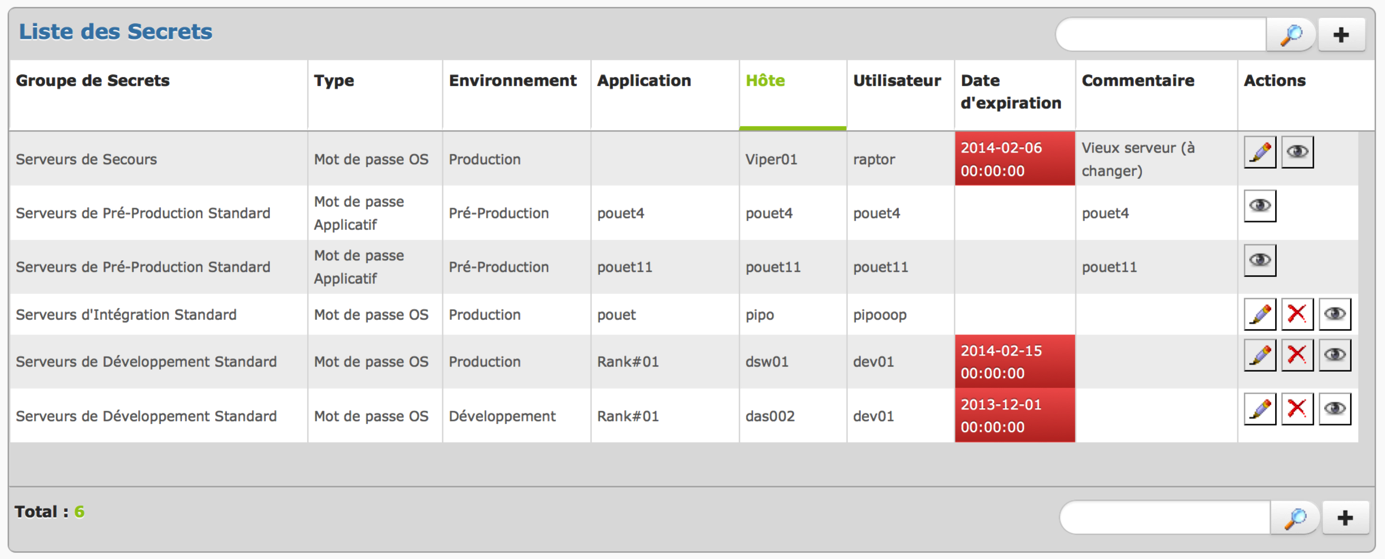


Il est possible de classer les informations en cliquant sur les titres de colonne. Ainsi l’information est triée de façon lexicographique croissante. Cependant, si on clique de nouveau sur le titre de la colonne, l’information est cette fois-ci triée de façon lexicographique décroissante.

Par exemple, si on clique sur le titre de la colonne « Hôte », on pourrait obtenir le résultat ci-dessous :



En recliquant, sur le titre de la colonne « Hôte », on obtiendrait le résultat ci-dessous :



La présence des boutons dans la colonne « Actions » dépend des droits que l’utilisateur a sur le « Groupe de Secrets ».

### Colonne « Groupe de Secrets »

Cette colonne rappelle à quel « Groupe de Secrets » le Secret est rattaché.

**Rappel :** c’est par les Groupes de Secrets que l’on partage les Secrets, soit en les associant à des Profils.

### Colonne « Type »

Cette colonne rappelle le « Type » du Secret.

**Remarque :** il est possible de changer le libellé des types (voir chapitre sur la gestion Multilingue de l’outil). Retenez que l’outil ne gère que l’outil ne gère que **3** types pour le moment.

### Colonne « Environnement »

Cette colonne rappelle à quel « Environnement » le Secret est rattaché.

**Remarque :** il est possible de changer le libellé des environnements (voir chapitre sur la gestion Multilingue de l’outil). Retenez que l’outil ne gère que l’outil ne gère que **4** environnements pour le moment.

### Colonne « Application »

Cette colonne rappelle à quelle « Application » le Secret est rattaché.

**Remarque**: il s’agit désormais d’une liste déroulante. Pour ajouter ou supprimer une application dans cette liste, il faut désormais utiliser l’écran spécifique de gestion des Applications.

### Colonne « Hôte »

Cette colonne rappelle à quel « Hôte » (équipement) le Secret est rattaché.

### Colonne « Utilisateur »

Cette colonne rappelle quel est le nom de « l’Utilisateur » constituant le Secret.

### Colonne « Date d’expiration »

Cette colonne rappelle à « l’Utilisateur » que le « Secret » a expiré.

On notera que la colonne peut avoir différentes couleurs qui fonctionnent sur le principe suivant :

* Rouge : quand la date d’expiration est inférieure à 2 jours ou que la date est dépassée (par rapport à la date courante).
* Orange : quand la date d’expiration est inférieure à 7 jours ou que la date est dépassée (par rapport à la date courante).

**Note**: cette information est déclarative. Un « Secret » peut avoir une date d’expiration sans avoir réellement expiré. Cette information peut être utilisée pour rappeler aux « Utilisateurs » qu’il est temps de renouveler un « Secret ».

### Colonne « Commentaire »

Cette colonne rappelle le « Commentaire » qui est associé au Secret.

### 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 ». |
|  | Ce bouton permet d’afficher le « Secret » (Notez qu’un clique sur l’occurrence produit le même récultat). |

### Bouton « Créer »

Ce bouton permet d’exécuter la création d’un nouveau « Secret » dans le « Groupe de Secret » sélectionné.

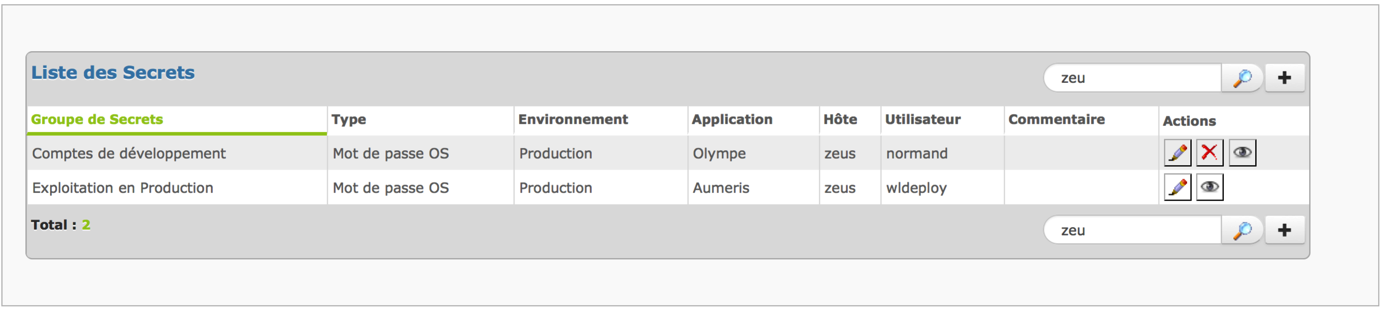
## Recherche de Secrets

Par défaut, tous les Secrets auxquels l’utilisateur a accès s’affichent. Toutefois, l’utilisateur peut décider de restreindre cet affichage, ou ne rechercher qu’un Secret particulier. Pour ce faire, il utilisera le champ ci-dessous :

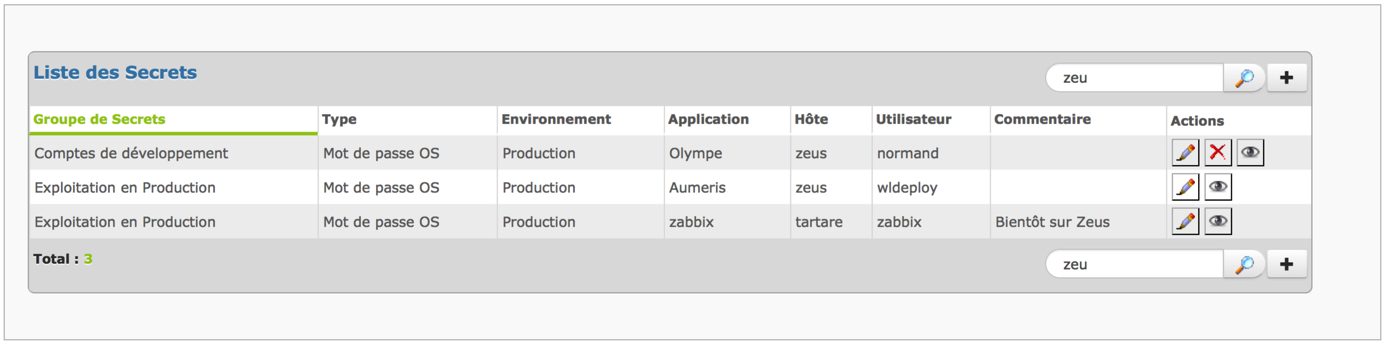


Ce champ réalise une recherche sur toutes les colonnes constituant un Secret.

Par exemple, en tapant « zeu », l’outil recherchera tous les secrets contenant « zeu » dans ses colonnes. Toujours dans le cadre de notre exemple voici ce qui apparaitrait :



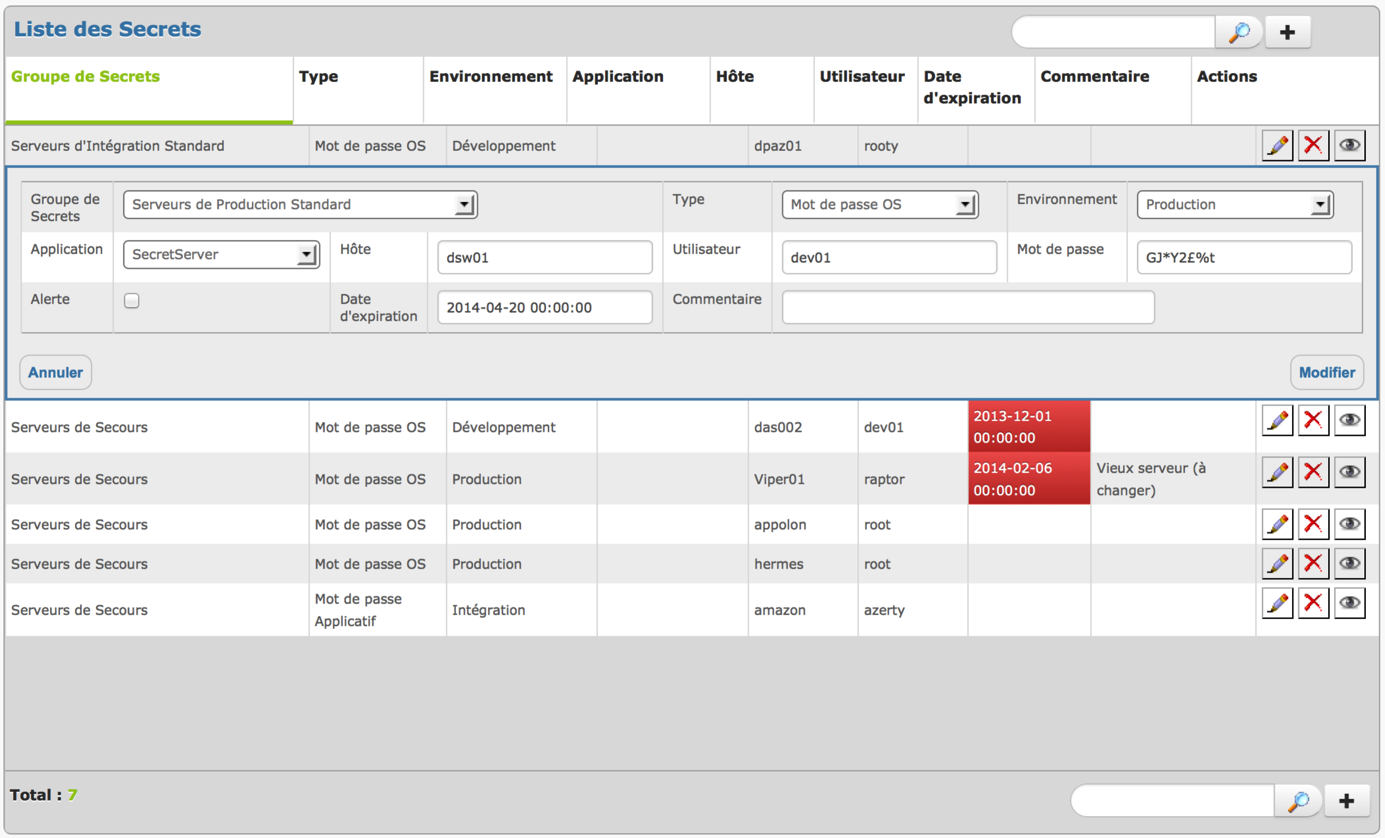
Si, par exemple, un secret avait eu un commentaire contenant « zeus » ce dernier serait apparu également. Par exemple :



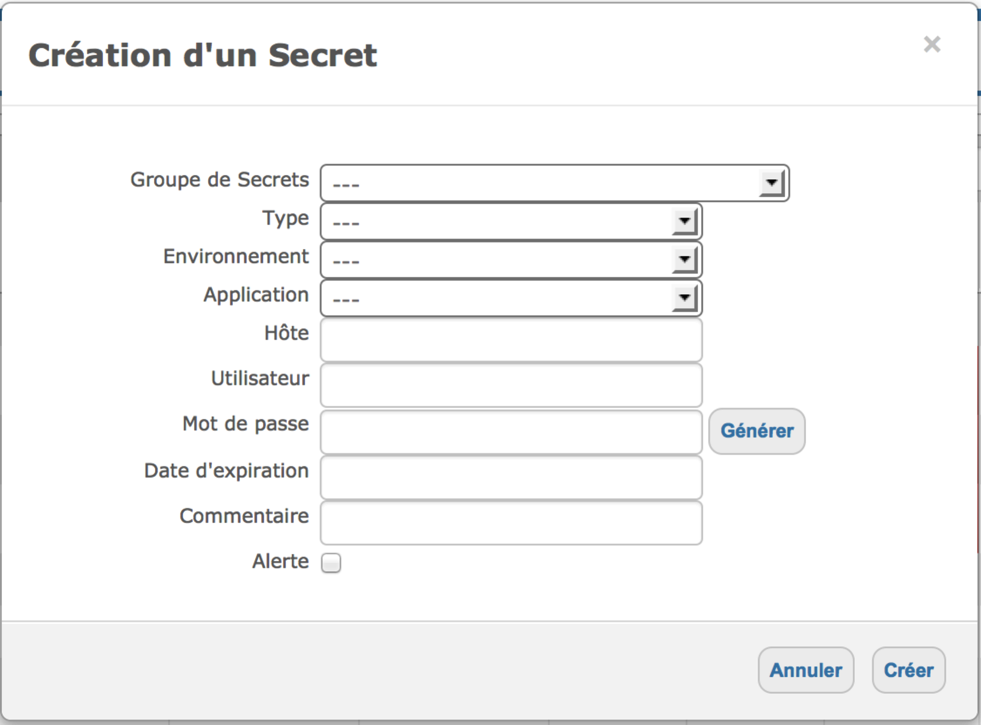
**Astuce :** Pour réafficher tous les Secrets auxquels un utilisateur a accès, il faut supprimer les caractères de recherche.

## Créer ou modifier un Secret

Après avoir cliqué sur le bouton «  », l’Utilisateur arrivera dans l’écran ci-dessous :



En revanche, si l’utilisateur utilise le bouton, la fenêtre ci-dessous apparaitra :



### Champ « Groupe de Secrets »

Cette liste déroulante contient tous les « Groupes de Secrets » auxquels à droit l’utilisateur en écriture. Les « Groupes de Secrets » sont le résultat des créations précédentes.

### Champ « Type »

Cette liste déroulante contient tous les « Types » gérés par l’outil **SecretManager**. Pour le moment les « Types » gérés par l’outil sont :

* Mot de passe OS ;
* Mot de passe Applicatif ;
* Mot de passe de test.

**Remarque :** il est possible de changer le libellé des types (voir chapitre sur la gestion Multilingue de l’outil). Retenez que l’outil ne gère que **3** types pour le moment.

### Champ « Environnement »

Cette liste déroulante contient tous les « Environnements » gérés par l’outil **SecretManager**. Pour le moment les « Environnements » gérés par l’outil sont :

* Production ;
* Pré-Production ;
* Intégration ;
* Test.

**Remarque :** il est possible de changer le libellé des environnements (voir chapitre sur la gestion Multilingue de l’outil). Retenez que l’outil ne gère que l’outil ne gère que **4** environnements pour le moment.

### Champ « Application »

Cette liste déroulante contient toutes les « Applications » disponibles. Les « Applications » sont le résultat des créations précédentes. Ce champ n’est pas obligatoire.

### Champ « Hôte »

Ce champ libre de saisie de 255 caractères permet de rattacher un Secret à un Hôte (équipement). Cette information permet de retrouver plus vite un Secret parmi d’autres Secrets. Ce champ est obligatoire, car il s’associe avec le champ « Utilisateur ». Il y a effectivement une contrainte qui interdit d’avoir plusieurs utilisateurs identiques sur un même Hôte.

### Champ « Utilisateur »

Ce champ libre de saisie de 100 caractères permet de définir un Secret. Ce champ est obligatoire, car il s’associe avec le champ « Hôte » afin d’éviter d’avoir des doublons d’Utilisateur sur un même Hôte.

### Champ « Mot de passe »

Ce champ libre de saisie de 100 caractères permet de définir un Secret. Ce champ est obligatoire et il est stocké chiffré dans la Base de Données car il est confidentiel.

### Champ « Commentaire »

Ce champ libre de saisie de 100 caractères permet d’apporter des informations complémentaires sur un Secret. Ce champ n’est pas obligatoire.

### Champ « 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 ».

### Bouton « Modifier »

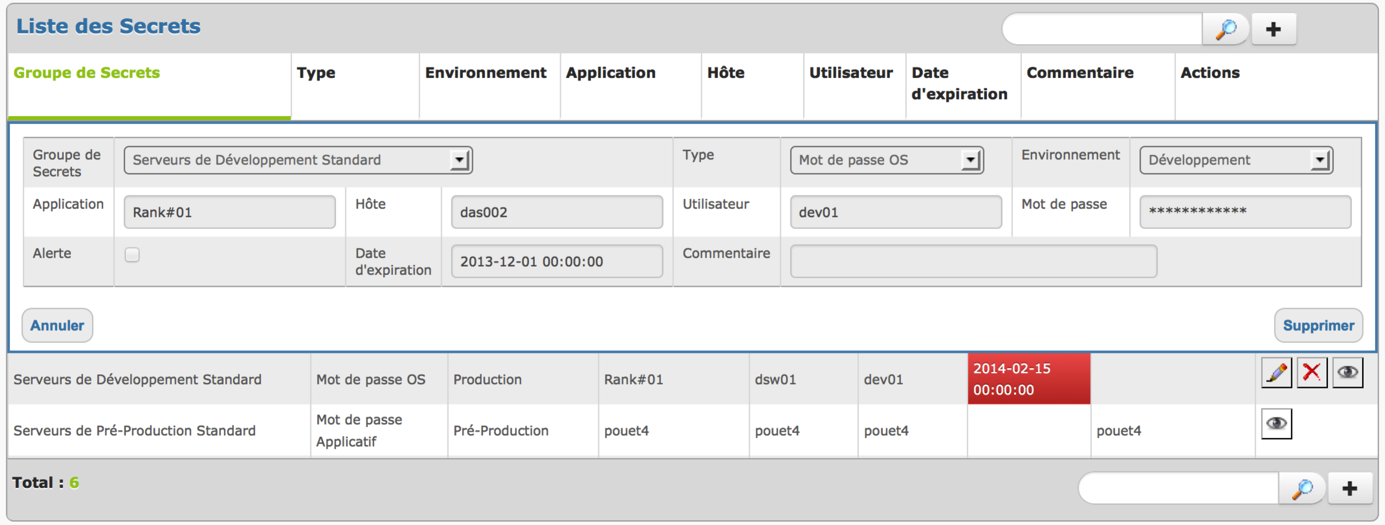
Ce bouton sauvegarde les modifications qui ont été effectuées dans les champs ci-dessus.

### Bouton « Annuler »

Ce bouton abandonne toutes les modifications qui auraient pu être faites dans les champs ci-dessus et permet à l’utilisateur de revenir sur la liste des Secrets auxquels il a accès.

## Suppression d’un Secret

Après avoir cliqué sur le bouton «  », l’Utilisateur arrivera dans l’écran ci-dessous :



On notera que le mot de passe est masqué dans ce cas.

### Bouton « Supprimer »

Ce bouton valide la suppression du Secret affiché.

### Bouton « Annuler »

Ce bouton abandonne la suppression en cours et permet à l’utilisateur de revenir sur la liste des Secrets auxquels il a accès.

## Création d’un Secret

La création d’un Secret s’appuie sur le même fonctionnement qu’une modification au détail près que l’écran est vide au lieu de contenir de précédentes saisies.

Voir chapitre « 8.3 ».

# Gestion des préférences

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 «  ».

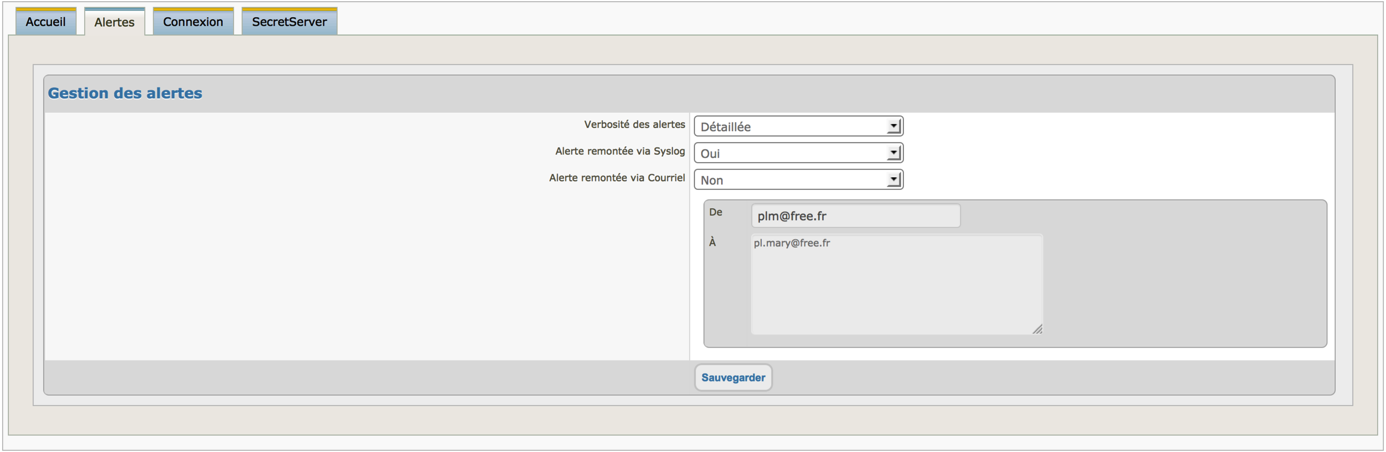
Il arrive ensuite sur l’écran ci-dessous :



## Gestion des « Alertes »

Pour tracer l’accès aux Secrets, il a été mis à la disposition de l’Administrateur une gestion des alertes. Les alertes peuvent être mises au niveau des « Groupes de Secrets », par conséquent tous les accès aux « Secrets » seront notifiés sous forme d’alerte, ou les alertes peuvent être gérées au niveau du « Secret », par conséquent, seul ce secret remontera une alerte.

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 :



Remarque : toutes les actions majeures de l’outil sont notifiées dans le journal interne de **SecretManager**. Cet onglet permet de notifier des alertes en plus du journal interne.

### Champ « Verbosité des alertes »

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

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

La verbosité « normale » remonte seulement l’information pertinente, alors que la verbosité « détaillée » donne des détails sur les fonctions internes utilisées.

### Champ « Alerte remontée via Syslog »

Si cette option est activée, les alertes émises seront remontées via le flux « Syslog » du serveur hébergeant **SecretManager**.

### 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 de **SecretManager**.

#### Le champ « De »

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

#### Le champ « A »

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

### Bouton « Sauvegarder »

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

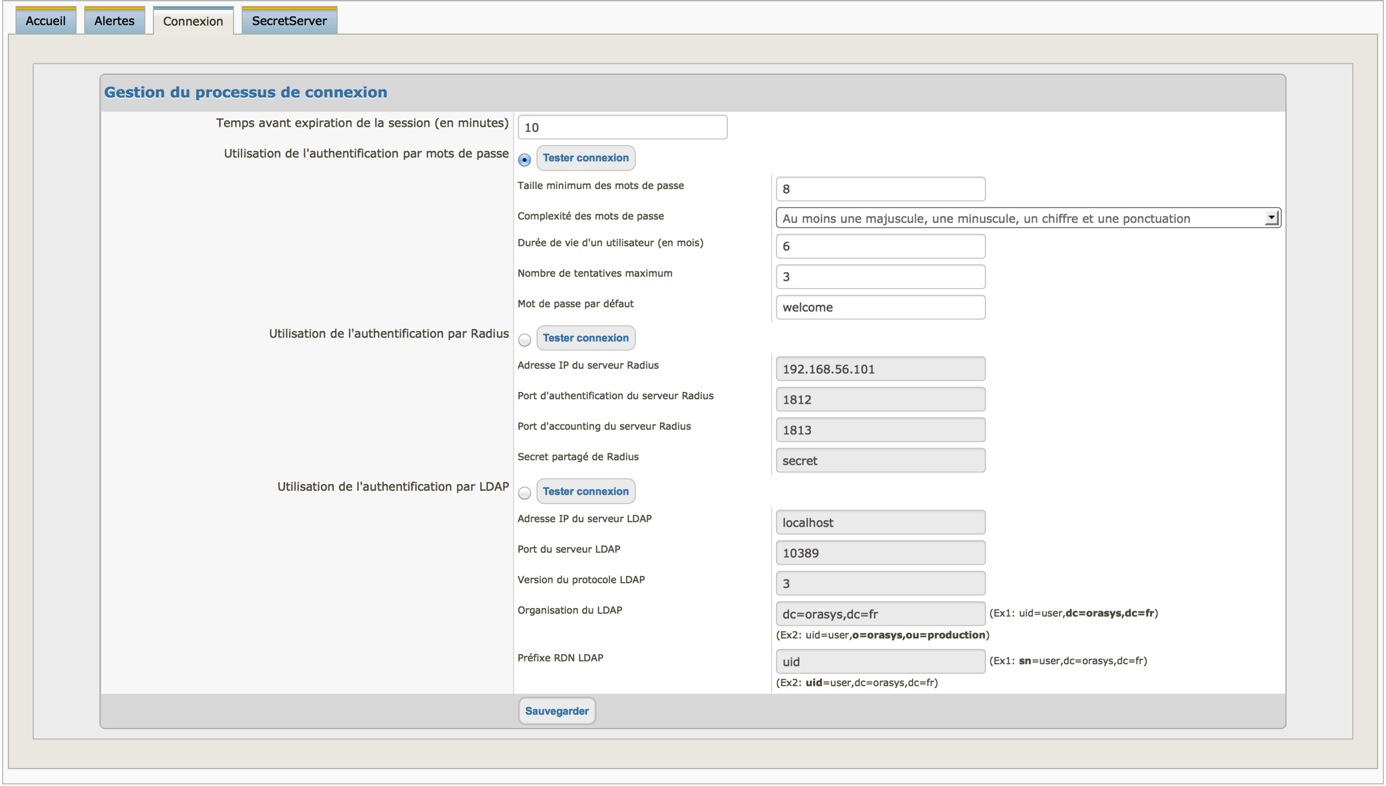
**Important**: si l’Administrateur change d’onglet sans avoir sauvegardé, il perd ses modifications.

## 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 **SecretManager**. Toutefois, afin de faciliter l’intégration de **SecretManager**, il est possible de décentraliser l’authentification :

* Sur un serveur Radius ;
* Sur un serveur LDAP.

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 ;
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.

### 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.

### 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** ».

#### 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.

#### 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.

#### 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.

#### 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.

#### 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.

### 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.

#### 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.

#### 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.

#### 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.

#### 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.

### 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.

#### 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.

#### Port du serveur Radius

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

#### 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.

#### 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.

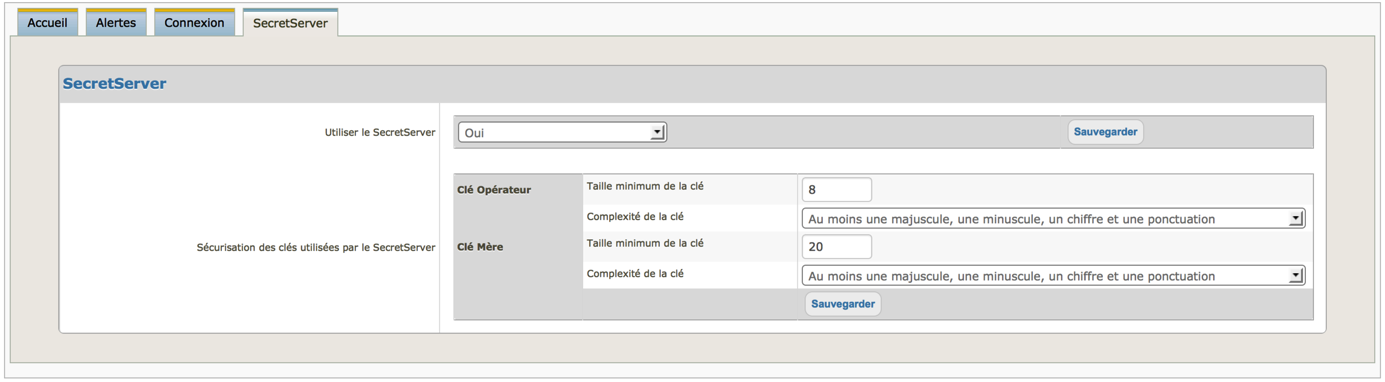
#### Préfixe RDN LDAP

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.

## 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.

L’utilisation du « **SecretServer** » n’est pas obligatoire, mais est fortement conseillée.

### 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 « DR01 » relatif à l’Installation de « **SecretManager** »

### Champ « Utiliser le SecretServer »

Ce champ permet à l’Administrateur de choisir s’il utilisera ou pas le « **SecretServer** » (la valeur par défaut sera à « Oui »).

Quand la valeur est à « Non », la clé « Mère » est stockée en clair dans le fichier « Libraries/Config\_Hash.inc.php ».

**Attention**: comme la clé Mère est en clair dans son fichier, toute personne ayant accès à ce fichier pourra déchiffrer tous les Secrets protégés par le « **SecretManager** ». Ce mode est déconseillé.

En revanche, si la valeur est à « Oui », la clé « Mère » est stockée chiffrée par la clé « Opérateur » dans le fichier « Libraries/secret.dat ». La clé « Opérateur » est la clé conservée par les Exploitants par ailleurs (indépendamment du « **SecretManager** »). La clé « Opérateur » est à fournir après chaque démarrage du « **SecretServer** ».

### Zone Sécurisation des clés utilisées par le SecretServer

#### 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 ?

#### Clé Mère

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