Sécurités Utilisateurs

Version 2.06.000

Le 11 mars 2019
Nos Réf. : iDApports_SécuritéUtilisateurs.docx

iD Systemes SAS au capital de 530 250 € - RCS Bordeaux - Siret 34328066500039 - N°TVA intracommunautaire : FR88343280665
Siège social : 18 av. de Chavailles, CS20227, 33525 Bruges Cedex, France - Tél. : +33 (0)5 56 11 28 28 - Fax :+33 (0)5 56 11 28 29
mail : contact@idsystemes.com - Web : www.idsystemes.com

Table des matières

1. OBJECTIF

Dans le cadre de la prise en compte de la RGPD dans nos applicatifs, la sécurité utilisateur a été améliorée. Actuellement :

- Les applications géraient :
  - L'accès au logiciel via un couple identifiant / mot de passe. Ce mot de passe est crypté.
  - La gestion des droits d'accès (par utilisateur et/ou par groupe d'utilisateurs)
- Les applications gèrent dorénavant :
  - La sécurité des mots de passe (complexité, longueur, période de validité, …)
  - Authentification avec SSO

2. SECURISATION DES MOTS DE PASSE

2.1. Complexité des mots de passe

Les logiciels iD n'imposent aucune politique de sécurité de mots de passe.
Le client détermine sa propre politique, et s'il le souhaite la renforcer dans le logiciel.

Des paramètres généraux ont été ajoutés précisant :

- La taille minimale du mot de passe
- La taille maximale du mot de passe
- Le nombre minimum de minuscule
- Le nombre minimum de majuscule
- Le nombre minimum de chiffres
- Le nombre minimum de caractères spéciaux
- La durée maximale (en jours) d'un mot de passe

2.2. SSO

Une autre possibilité de mettre en place des systèmes de SSO (Single Sign On) est disponible (depuis la version 2.06.000). Cela permet de déporter la sécurisation des comptes utilisateurs au système sous-jacent.

3. PARAMETRAGE

3.1. Fiche utilisateur

Dans le paramétrage général, les fiches "utilisateur" sont accessibles dans :

- Utilisateurs / droits d'accès > Utilisateurs

  - En création, le mot de passe doit obligatoirement être précisé.
  - Lors de la mise à jour, pour changer le mot de passe d'un utilisateur, il faut cocher la case « Changer le mot de passe » et indiquer le nouveau

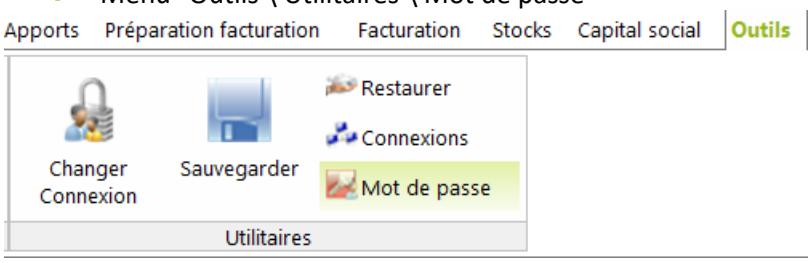
Le mot de passe est crypté en base de données (non réversible).

3.2. Changement de mot de passe

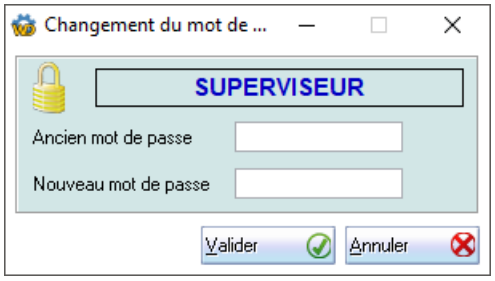
L'utilisateur peut changer son mot de passe, en allant dans :

- L'onglet "Général" du ruban, puis dans la partie "Informations". Il peut alors sélectionner l'option "Modifier mon mot de passe"

- Menu "Outils \ Utilitaires \ Mot de passe"



L'utilisateur doit alors renseigner son ancien mot de passe, puis le nouveau (2 fois pour confirmation)



3.3. Historisation des mots de passe

La table des utilisateurs contient le mot de passe courant, ainsi que la date de mise à jour. Une autre table permet de conserver l'historique des mots de passe des utilisateurs (toujours cryptés)

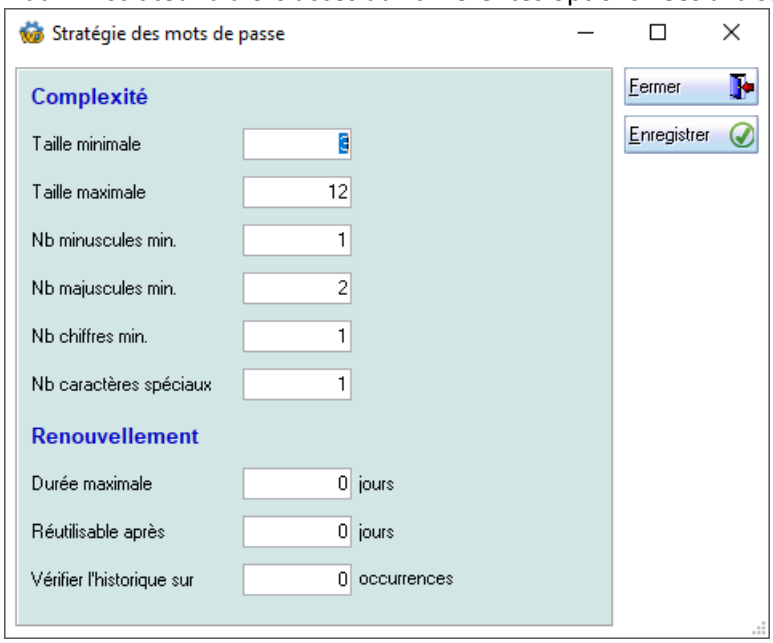
3.4. Renforcement des mots de passe

Par défaut, il n'existe aucune règle sur la constitution des mots de passe.
Vous pouvez définir votre politique de gestion des mots de passe.

Dans le "paramétrage général", la stratégie de mot de passe se trouve dans

- "Utilisateurs \ droits d'accès > Options et droits d'accès", puis dans la partie "Gestion des connexions" option "Stratégie des mots de passe".

L'administrateur a alors accès aux différentes options liées à la stratégie des mots de passe :



Préciser les stratégies suivantes (combinables) :

- La taille minimale du mot de passe

- La taille maximale du mot de passe
- Le nombre minimum de minuscule
- Le nombre minimum de majuscule
- Le nombre minimum de chiffres
- Le nombre minimum de caractères spéciaux
- La durée maximale (en jours) d'un mot de passe
- Le nombre de jours minimum entre 2 utilisations d'un même mot de passe
- Le nombre de changements minimums entre 2 utilisations d'un même mot de passe

Pour toutes ces options, « 0 » permet de ne pas prendre en compte le critère.

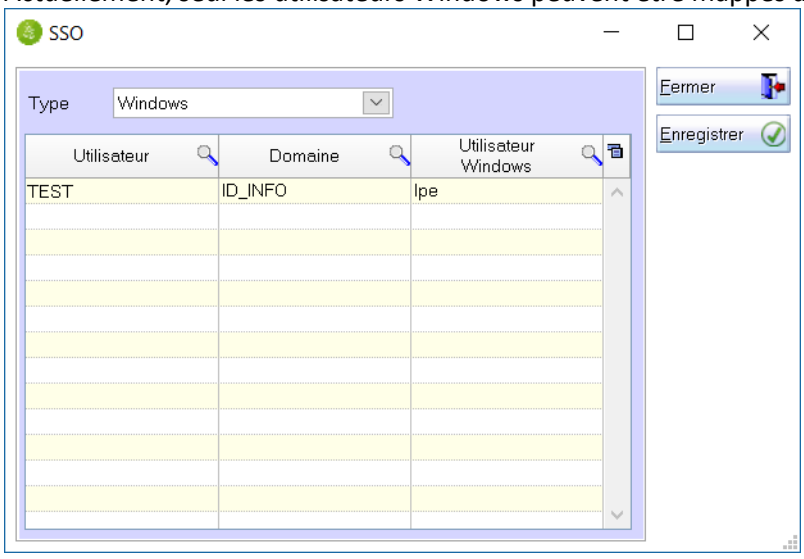
3.5. Authentification avec SSO

La partie authentification peut être déléguée à un système tiers. Pour cela, on associe un utilisateur du système d'authentification à un utilisateur logiciel. Ainsi, tout le reste du logiciel fonctionne de manière similaire ; seul l'authentification est déléguée.

Cela se configure via :

- "Utilisateurs \ droits d'accès > Options et droits d'accès", puis dans la partie "Gestion des connexions" option "Gestion du SSO".

Actuellement, seul les utilisateurs Windows peuvent être mappés aux utilisateurs logiciel.



Au lancement du logiciel, avec le SSO activé, la connexion se passe ainsi :

- L'utilisateur Windows courant n'est pas associé à un utilisateur logiciel : il doit alors se connecter explicitement avec un utilisateur / mot de passe logiciel
- L'utilisateur Windows courant est associé à un utilisateur logiciel inactif : la connexion est refusée
- L'utilisateur Windows courant est associé à un utilisateur « superviseur » : la connexion est refusée
- L'utilisateur Windows courant est associé à un utilisateur et a accès à une seule base applicative : la connexion est validée directement sans action de l'utilisateur

› L'utilisateur Windows courant est associé à un utilisateur et a accès à plusieurs bases applicatives : l'utilisateur doit choisir sa base et valider (sans possibilité de changer l'utilisateur logiciel)

La connexion est automatique et passe donc la fenêtre de connexion.
En cas de dépannage, il peut être nécessaire de se connecter avec un utilisateur logiciel ayant plus de droits (un administrateur, superviseur, …).

3.6. Note

Toutes les informations liées aux utilisateurs (utilisateurs, groupes, droits d'accès, stratégie de mot de passe, historique) sont conservées dans la base "vitpar". Ces informations ne sont donc pas liées à la base applicative, mais à la base d'utilisateurs.