



## swSSO v1.18 – Release notes

### Evolutions :

- [ISSUE#363] : Il est désormais possible de masquer les onglets relatifs aux identifiants secondaires dans la fenêtre de gestion des sites et applications dans la clé :  
HKLM\SOFTWARE\{WOW6432Node}\swSSO\GlobalPolicy (ou DomainPolicy), valeur ShowAdditionalIds (type DWORD, valeur par défaut 1).
- [ISSUE#364] : Il est désormais possible de spécifier le chemin complet du fichier .ini dans la clé :  
HKLM\SOFTWARE\{WOW6432Node}\swSSO\EnterpriseOptions, valeur IniPathName (type chaîne). Cette configuration prévaut sur le chemin éventuellement passé en paramètre.
- [ISSUE#365] : Si vous souhaitez que swSSO s'arrête sans afficher de message d'erreur dans le cas où le fichier de configuration .ini est placé sur le réseau et que celui-ci n'est pas disponible, vous pouvez le spécifier dans la clé :  
HKLM\SOFTWARE\{WOW6432Node}\swSSO\EnterpriseOptions, valeur ExitIfNetworkUnavailable (type DWORD, valeur par défaut 0)
- [ISSUE#366] : Des statistiques non anonymisées (nom d'utilisateur en clair et nom du poste de travail non tronqué) peuvent désormais être produites, en ajoutant 0x10 à la valeur configurée dans la clé Stat. Concrètement :
  - Stat=0x01 : statistiques anonymisées dans un fichier
  - Stat=0x02 : statistiques anonymisées en base de données
  - Stat=0x03 : statistiques anonymisées dans un fichier et en base de données
  - Stat=0x11 : statistiques non anonymisées dans un fichier
  - Stat=0x12 : statistiques non anonymisées en base de données
  - Stat=0x13 : statistiques non anonymisées dans un fichier et en base de données
- [ISSUE#367] : Il est désormais possible d'automatiser le changement du mot de passe d'une application lorsque celui-ci est demandé. Pour commencer, vous devez définir la politique pour la génération de mot de passe en base de registre sous la clé :

HKLM\SOFTWARE\{WOW6432Node}\swSSO\NewPasswordPolicies\{nn} (nn peut prendre une valeur décimale à 2 chiffres entre 00 et 99 et constitue l'identifiant de la politique. Il sera référencé dans la configuration de la fenêtre de changement de mot de passe).

La politique est constituée de l'ensemble des valeurs décrites dans le tableau ci-dessous :

Nom de la valeur	Type	Défaut	Description
MinLength	DWORD	N/A	Longueur minimale du mot de passe généré. <b>Valeur obligatoire.</b>
MaxLength	DWORD	N/A	Longueur maximale du mot de passe généré. <b>Valeur obligatoire.</b>
MinUpperCase	DWORD	0	Nombre minimum de majuscules dans le mot de passe généré. <b>Valeur optionnelle</b> : si non définie ou à 0, le mot de passe généré ne contiendra aucune majuscule.

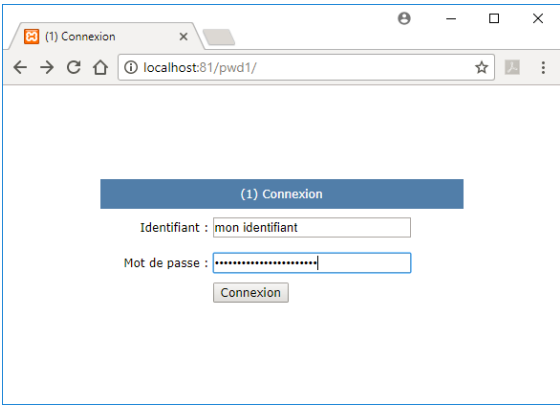
Nom de la valeur	Type	Défaut	Description
MinLowerCase	DWORD	0	Nombre minimum de minuscules dans le mot de passe généré. <b>Valeur optionnelle :</b> si non définie ou à 0, le mot de passe généré ne contiendra aucune minuscule.
MinNumbers	DWORD	0	Nombre minimum de chiffres dans le mot de passe généré. <b>Valeur optionnelle :</b> si non définie ou à 0, le mot de passe généré ne contiendra aucun chiffre.
MinSpecialChars	DWORD	0	Nombre minimum de caractères spéciaux dans le mot de passe généré. Liste des caractères spéciaux utilisés par swSSO : &'(-_)=+}] {[,?;.:/*\$ <b>Valeur optionnelle :</b> si non définie ou à 0, le mot de passe généré ne contiendra aucun caractère spécial.
MaxCommonChars	DWORD	0	Nombre maximum d'occurrence d'un même caractère dans le mot de passe généré. <b>Valeur optionnelle :</b> si non définie ou à 0, le nombre d'occurrences n'est pas vérifié.
MaxConsecutiveCommonChars	DWORD	0	Nombre maximum d'occurrence consécutive d'un même caractère dans le mot de passe généré. <b>Valeur optionnelle :</b> si non définie ou à 0, le nombre d'occurrences n'est pas vérifié.
IdMaxCommonChars	DWORD	-1	Le mot de passe peut contenir au plus N caractères consécutifs de l'identifiant Windows (-1 = pas de restrictions, 0 = aucun caractère commun autorisé, 1 = le mot de passe peut contenir un caractère de l'identifiant, pas mais 2 consécutifs, 2 = le mot de passe peut contenir deux caractères consécutifs de l'identifiant, mais pas 3, etc.)

Le fichier NewPasswordPolicyExample.reg propose un exemple de configuration d'une politique permettant la génération d'un mot de passe entre 8 et 12 caractères, avec au moins 1 chiffre, 1 majuscule et 1 minuscule :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\swSSO\NewPasswordPolicies\01]
"MinLength"=dword:00000008
"MaxLength"=dword:0000000c
"MinUpperCase"=dword:00000001
"MinLowerCase"=dword:00000001
"MinNumbers"=dword:00000001
"MinSpecialChars"=dword:00000000
"MaxCommonChars"=dword:00000000
"MaxConsecutiveCommonChars"=dword:00000000
"IdMaxCommonChars"=dword:00000000
```

**Remarque :** il n'y a pas de contrôle de cohérence sur la politique, donc si vous exigez un mot de passe de 15 caractères numériques avec un maximum d'une occurrence pour chaque caractère, swSSO va tourner indéfiniment pour essayer de créer un mot de passe respectant la politique et devra être tué depuis le gestionnaire de tâches.

Ci-après un exemple de configuration de changement de mot de passe pour le site exemple disponible ici : [www.swsso.fr/pwd1](http://www.swsso.fr/pwd1).



### Configurer la **page de connexion** :

Configuration Champs complémentaires

Type Site Web (configuration simplifiée)

Titre de la fenêtre (1) Connexion\*

URL http://www.swsso.fr/pwd1/

Simulation de frappe clavier ?

Champ identifiant -1

Champ mot de passe 1

Validation [ENTER]

Puis définir un identifiant de groupe de mot de passe dans le champ « Groupe (mot de passe) » de l'onglet « Champs complémentaires », avec une valeur supérieure ou égale à 20 :

Configuration Champs complémentaires

Type 2ème identifiant

Nom 2ème identifiant

Type 3ème identifiant

Nom 3ème identifiant

Type 4ème identifiant

Nom 4ème identifiant

Groupe (mot de passe) 20

Configurer ensuite la **page de changement de mot de passe** en utilisant les identifiants complémentaires : le 2<sup>ème</sup> pour la 1<sup>ère</sup> saisie du nouveau mot de passe et le 3<sup>ème</sup> pour sa confirmation (ne rien renseigner dans les champs identifiant et mot de passe) :

Dans les champs 2<sup>ème</sup> et 3<sup>ème</sup> identifiants de l'onglet « Identifiants complémentaires », renseigner le mot clé %RANDOMnn% où nn correspond à l'identifiant de la politique définie précédemment.

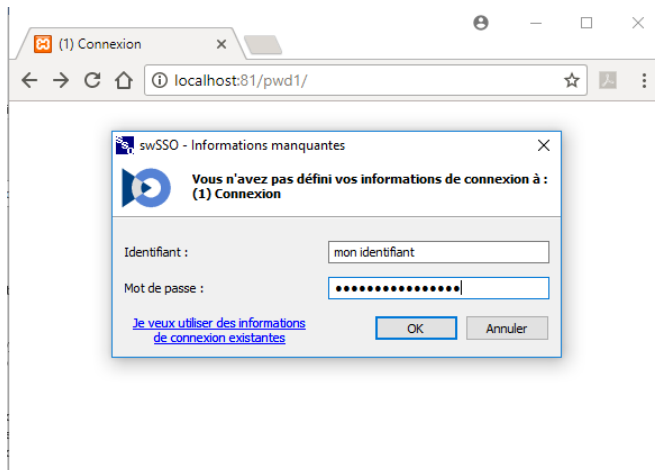
Dans les champs type et nom des deux identifiants complémentaires, saisir la position absolue des champs mot de passe.

Enfin, dans le champ « Groupe (mot de passe) » de l'onglet « Champs complémentaires », saisir le même identifiant que dans la configuration de la page de connexion.

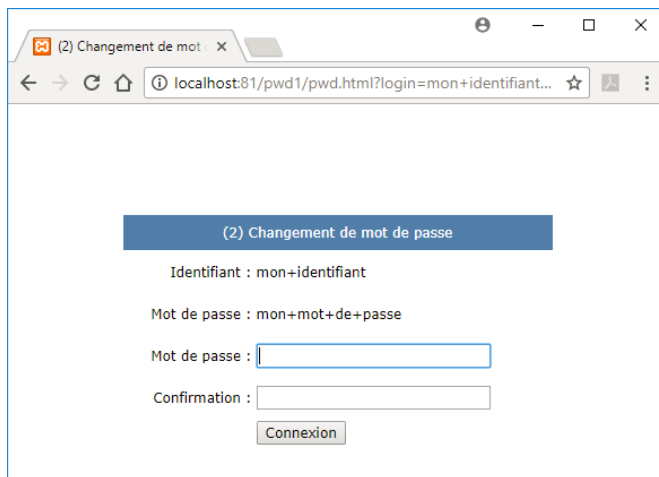
Identifiant et mot de passe		Identifiants complémentaires
2 <sup>ème</sup> identifiant	%RANDOM01%	
3 <sup>ème</sup> identifiant	%RANDOM01%	
4 <sup>ème</sup> identifiant		
Configuration		Champs complémentaires
Type 2 <sup>ème</sup> identifiant	Champ de saisie (html : input)	
Nom 2 <sup>ème</sup> identifiant	1	
Type 3 <sup>ème</sup> identifiant	Champ de saisie (html : input)	
Nom 3 <sup>ème</sup> identifiant	2	
Type 4 <sup>ème</sup> identifiant		
Nom 4 <sup>ème</sup> identifiant		
Groupe (mot de passe)	20	

Publier ensuite les deux configurations. Voici la cinématique de changement du mot passe sur le client swSSO :

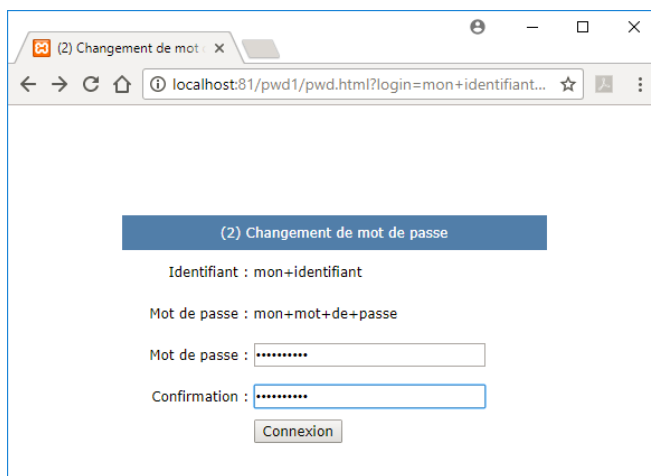
- 1) Au premier accès à l'application, l'utilisateur est invité à saisir son identifiant et son mot de passe dans swSSO. Le remplissage du formulaire de connexion se fait automatiquement.



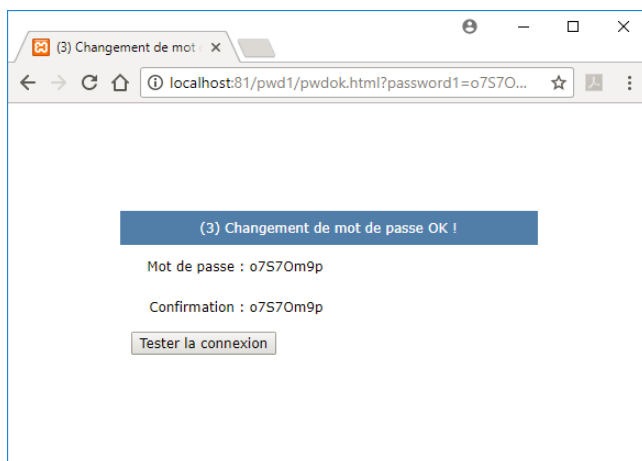
- 2) Dans la démonstration, l'application impose le changement de mot de passe en affichant une page demandant à l'utilisateur de définir un nouveau mot de passe à saisir en double (cas courants : première connexion à l'application ou expiration du mot de passe) :



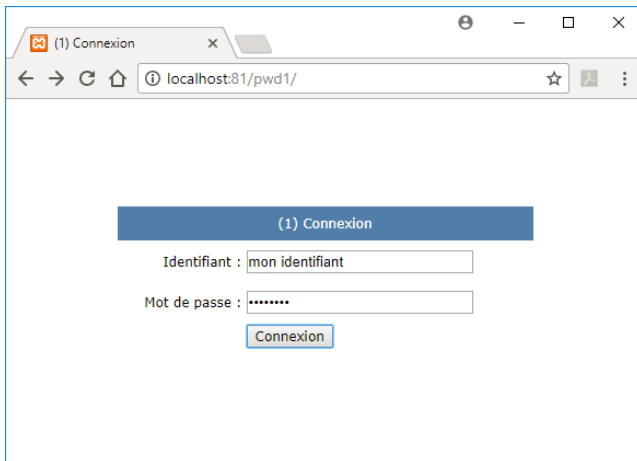
- 3) swSSO génère un mot de passe respectant la politique définie et le saisit dans les deux champs, puis valide le formulaire :



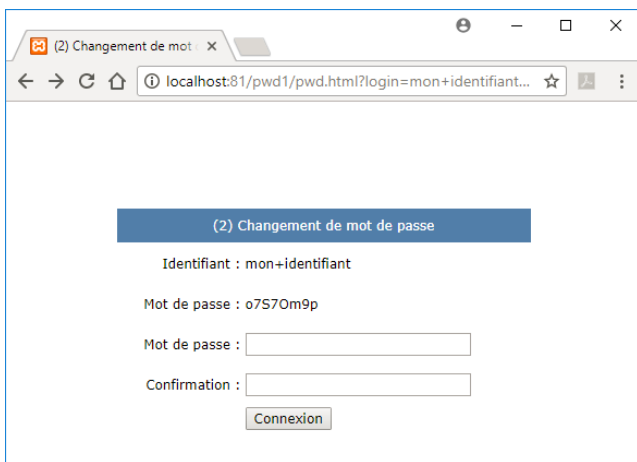
- 4) La page de confirmation de changement de mot de passe de l'application s'affiche (et pour le test uniquement, présente les deux mots de passe qui ont été saisis) :



- 5) Pour vérifier que le nouveau mot de passe défini a bien été enregistré par swSSO, fermer le navigateur et ouvrir à nouveau la page [www.swsso.fr/pwd1](http://www.swsso.fr/pwd1) (ou cliquer sur le bouton « Tester la connexion ». Dans ce cas, si le SSO ne déclenche pas sur la page de connexion, sélectionner le menu clic-droit / Se connecter à l'application). Le formulaire se remplit automatiquement :



La page suivante permet de vérifier que le mot de passe saisi dans la page de connexion est bien celui qui a été généré précédemment :



**Remarque :** le changement de mot de passe automatique fonctionne également si la page de changement de mot de passe demande également de saisir l'ancien mot de passe. Il suffit d'adapter la configuration de la page de changement de mot de passe comme indiqué ci-dessous :

	<p>Configurer la <b>page de changement de mot de passe</b> comme précédemment, mais en renseignant la position du champ mot de passe qui sera utilisée pour saisir l'ancien mot de passe (ici 1 puisqu'il s'agit du 1<sup>er</sup> champ mot de passe dans la fenêtre) :</p>
--	--

	Identifiant et mot de passe <span style="float: right;">Identifiants complémentaires</span> Identifiant <input type="text"/> Mot de passe <input type="password"/>
	Configuration <span style="float: right;">Champs complémentaires</span> Type <span style="float: right;">Site Web (configuration simplifiée)</span> Titre de la fenêtre <span style="float: right;">(2) Changement de mot de passe*</span> URL <span style="float: right;">http://localhost:81/pwd2/pwd.html*</span> <input type="checkbox"/> Simulation de frappe clavier  Champ identifiant <input type="text"/> Champ mot de passe <span style="float: right;">1</span> Validation <span style="float: right;">[ENTER]</span>

Le reste de la configuration ne change pas.

- [ISSUE#370] : Le temps d'attente du démarrage du service swSSOSVC est désormais configurable dans la clé HKLM\SOFTWARE\swSSO\CM, valeur ServiceTimeout (type DWORD, valeur par défaut 60 secondes). Ce paramètre ne doit être positionné que sur des machines lentes sur lesquelles le service swSSOSVC démarre trop tard, générant une erreur au démarrage de swSSO avec le message « swSSO ne peut pas utiliser votre compte Windows ».

### **Bugs corrigés :**

- [ISSUE#360] : Le compte Windows ne pouvait pas être utilisé si l'identifiant de l'utilisateur était différent dans le SamAccountName (ex : domaine\userid1) et l'UPN ([userid2@domaine.fr](mailto:userid2@domaine.fr))
- [ISSUE#361] : En mode « mot de passe Windows », les configurations utilisant %ADPASSWORD% ne fonctionnaient plus, sauf si UseADPassword était positionné à 1 (ce qu'il ne faut faire qu'en mode mot de passe maître, sinon le mot de passe Windows est demandé à l'utilisateur à chaque fois qu'il est changé).
- [ISSUE#362] : swSSO ne démarrait pas s'il était lancé par un utilisateur avec un profil Citrix de type « mandatory profile ».
- [ISSUE#368] : Le nombre maximum de sessions utilisateurs simultanées sur une même machine a été porté de 100 à 200.
- [ISSUE#369] : Le service swSSOSVC.exe ne s'installait plus sur les OS XP et 2003.

### **Problèmes connus :**

- [ISSUE#345] : L'installation de Skype 2016 Entreprise bloque le fonctionnement de swSSO. Les versions 16.0.4266.1001 et 16.0.4534.1000 posent problème, en revanche la version 16.0.7329.1054 ne pose pas de problème. Les versions antérieures à 2016 ne posent pas non plus de problème.
- [ISSUE#347] : Le SSO avec Edge ne fonctionne plus depuis la version 40.15063.0.0 apportée par la mise à jour Windows 10 / Creators update 1703



- [ISSUE#354] : Les mises à jour majeures de Windows 10 suppriment une clé de registre qui bloque le fonctionnement de swSSO. Il faut soit repositionner la clé à la main, soit réinstaller swSSO (voir ici : <https://www.swsso.fr/?p=32882&lang=fr>)
- [ISSUE#371] : Incompatibilité partielle avec Firefox Quantum (version 57). Il y a 2 problèmes :
  1. Le mode multi-processeur n'est pas compatible avec swSSO. Cela s'explique par le fait que Mozilla n'a pas implémenté les API d'accessibilité dans ce mode. Néanmoins, comme indiqué ici (<https://support.mozilla.org/fr/kb/accessibilite-pas-disponible-multi-processus>), Firefox détecte que swSSO utilise les API d'accessibilité et bascule automatiquement en mode mono-processeur (arrêt/relance nécessaire). Il est également possible de forcer l'activation de l'accessibilité avec le paramètre indiqué dans ce même article (`browser.tabs.remote.force-enable=true`).
  2. Dès que plusieurs onglets sont ouverts, le fonctionnement du SSO est aléatoire. En conservant uniquement un onglet ouvert, le fonctionnement est toujours OK.