swSSO v1.02

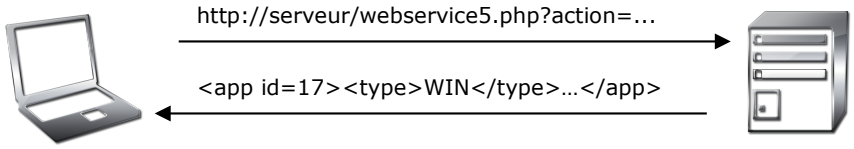
Guide d'administration

Contenu du document

1. Installation

1.1. Principe général de fonctionnement

Le client swsso.exe s'appuie sur un serveur de configuration pour récupérer les configurations de SSO des applications. Concrètement, à chaque fois que l'utilisateur sélectionne « Ajouter cette application » dans le menu clic-droit de l'icône swSSO ou à chaque lancement si la synchronisation des configurations est configurée, swsso.exe interroge le serveur de configuration (requête HTTP) qui lui retourne la ou les configurations sous forme d'un flux XML :



1.2. Stratégie de déploiement

Avant toute chose, vous devez choisir votre stratégie de déploiement. Pour le serveur de configuration, vous pouvez choisir d'utiliser :

- Un serveur de configuration privé sur internet (hébergement fourni par swSSO) ;
- Un serveur de configuration privé en interne ou sur internet (hébergement assuré par vos soins).

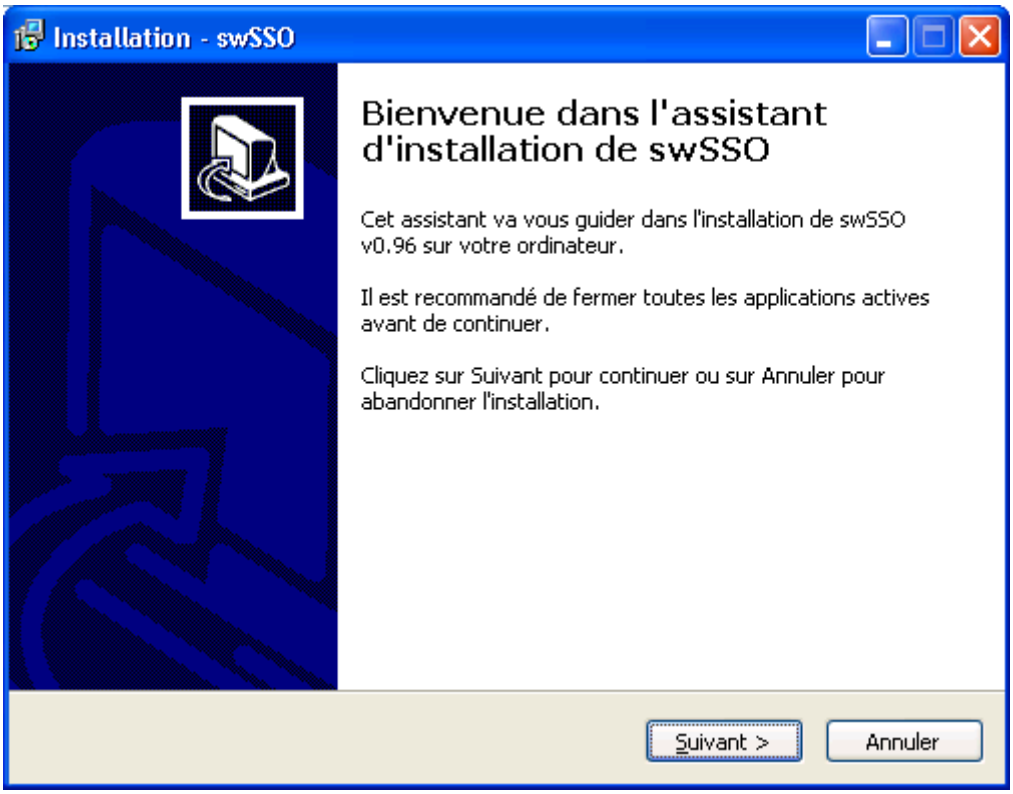
1.3. Matrice de compatibilité client / serveur

Le tableau ci-dessous indique la version serveur à utiliser en fonction de la version du client swsso.exe. Idéalement, vous devriez utiliser les versions marquées comme « mode de fonctionnement nominal ». D'autres combinaisons sont tolérées avec des restrictions qui sont précisées dans le tableau.

Version client (swsso.exe)	Version serveur	Commentaire
0.88	**webservice2.php**	Mode de fonctionnement nominal
0.89 et 0.90	**webservice3.php**	Mode de fonctionnement nominal
	webservice2.php	Dans ce cas les évolutions #77 (simulation de frappe clavier) et #96 (centralisation des noms des configurations) ne sont pas disponibles
0.91 à 0.93	**webservice4.php**	Mode de fonctionnement nominal
0.94+	**webservice5.php**	Mode de fonctionnement nominal

1.4. Installation du client swSSO

Si vous souhaitez utiliser la synchronisation de mot de passe Windows, vous devez utiliser l'installation swSSO-setup.exe, qui installe le client swSSO.exe et les modules annexes nécessaires (swSSOCM.dll et swSSOSVC.exe) :



Si vous souhaitez utiliser un mot de passe maître, vous pouvez déployer manuellement l'exécutable swsso.exe, soit seul, soit avec un fichier .ini préconfiguré :

- swsso.exe seul : dans ce cas, un fichier de configuration swsso.ini sera créé dans le répertoire de swsso.exe au premier lancement et vos utilisateurs auront la configuration par défaut pour l'ensemble des options.
- swsso.exe et un fichier .ini : dans ce cas, vous pouvez pré-remplir le fichier swsso.ini avec les options que vous souhaitez proposer à vos utilisateurs (si vous souhaitez qu'ils ne puissent pas modifier ces options, référez-vous au §3.4 pour connaître les possibilités de bridage de l'IHM). Vous pouvez aussi choisir de déposer le fichier swsso.ini dans un répertoire autre que celui de l'exécutable. Typiquement, vous choisirez de déployer swsso.exe dans le dossier « Program Files » et de déposer le fichier swsso.ini dans le dossier « Documents and Settings » lorsque les utilisateurs disposent d'un poste de travail dédié ou sur un serveur de fichiers lorsque les utilisateurs travaillent sur plusieurs postes de travail.

Voici quelques exemples de commandes de lancement que vous pouvez placer dans un raccourci, lui-même éventuellement placé dans le menu Démarrage de l'utilisateur pour lancer automatiquement swSSO à l'ouverture de session Windows :

```
"c:\program files\swsso\swsso.exe" "c:\Document and Settings\%USERNAME%\swsso.ini"
"c:\program files\swsso\swsso.exe" "\\serveur\partage\%USERNAME%.ini"
"c:\program files\swsso\swsso.exe" "\\serveur\partage\%USERNAME%\swsso.ini"
```

1.5. Fichier de configuration swsso.ini – section [swSSO]

Valeurs pouvant être prédéfinies pour le déploiement :

Nom de la valeur	Défaut	Description
sessionLock	NO	YES = verrouille swSSO lorsque la session Windows est verrouillée.
internetCheckVersion	YES/ NO	YES = vérifie au lancement si une nouvelle version est disponible. Valeur par défaut : - Toujours YES en version 1.00 et inférieures - A partir de la version 1.01 : YES sauf si ServerAddress configuré
internetCheckBeta	NO	YES = vérifie au lancement si une nouvelle version bêta est disponible.
internetGetConfig	NO	YES = autorise l'utilisateur à récupérer les configurations hébergées sur le serveur. NO = lorsque l'utilisateur sélectionne le menu « Ajouter cette application », swSSO ne se connecte pas au serveur mais construit localement une configuration pré-remplie, dont certains éléments doivent être vérifiés et/ou complétés par l'utilisateur.
internetManualPutConfig	NO	YES = autorise l'utilisateur à récupérer les configurations hébergées sur le serveur. Concrètement, affiche (YES) / masque (NO) le menu contextuel « Uploader sur le serveur » disponible sur les configurations dans la fenêtre de gestion des applications et sites.
Portal	-	Chemin complet du fichier portail.
x,y,cx,cy	-	Position (x,y) et dimension (cx,cy) de la fenêtre de gestion des applications et sites. Par défaut la fenêtre est affichée en base à droite de l'écran et mesure 667x480 pixels.
x2,y2,cx2,cy2	-	Position (x2,y2) et dimension (cx2,cy2) de la fenêtre de lancement d'application. Par défaut la fenêtre est affichée en base à droite de l'écran et mesure 384x549 pixels. **Disponible à partir de la version v0.91.**
LaunchTopMost	NO	YES = la fenêtre de lancement d'applications s'affiche au premier plan et ne peut pas être recouverte par une autre fenêtre. **Disponible à partir de la version v0.91.**
parseWindowsOnStart	YES	NO = les fenêtres déjà ouvertes au moment du lancement de swSSO ne seront jamais traitées **Disponible à partir de la version v0.93.**
domainId	1	Identifiant du domaine de rattachement de l'utilisateur **Disponible à partir de la version v0.94.**

Nom de la valeur	Défaut	Description
DomainLabel	Commun	Libellé du domaine de rattachement de l'utilisateur **Disponible à partir de la version v0.94.**
displayChangeAppPwdDialog	YES	YES = affiche la fenêtre indiquant à l'utilisateur que son mot de passe a été copié dans le presse papier lorsqu'il utilise la fonction d'assistance au changement de mot de passe d'une application **Disponible à partir de la version 0.99**

Par exemple, si vous déployez le fichier ci-dessous, swSSO ne vérifiera pas la disponibilité de nouvelles versions et se verrouillera à chaque fois que l'utilisateur verrouille sa session Windows.

```
[swSSO]
internetCheckVersion=NO
internetCheckBeta=NO
sessionLock=YES
```

Pour information uniquement, le tableau ci-dessous décrit la signification des valeurs figurant dans la section swSSO. Ces valeurs sont gérées dynamiquement par swSSO :

Nom de la valeur	Description
version	Version du fichier de configuration. Valeur inscrite automatiquement à la création du fichier. Ne pas modifier cette valeur.
pwdProtection	ENCRYPTED : les mots de passe sont chiffrés par une clé dérivant du mot de passe maître de l'utilisateur. ~~ENCODED : les mots de passe sont simplement brouillés : ils n'apparaissent pas en clair dans le fichier, mais ne sont pas protégés (tout utilisateur récupérant le fichier swsso.ini peut visualiser les mots de passe)~~ (**supprimé en version v0.98)** ~~NONE : les mots de passe sont en clairs dans le .ini.~~ (**supprimé en version v0.98)** WINDOWS : les mots de passe sont chiffrés avec une clé dérivant du mot de passe Windows de l'utilisateur (**disponible à partir de la version v0.96**)
pwdValue	Mot de passe maître.
LastPwdChange	Date du dernier changement de mot de passe chiffrée par le mot de passe de l'utilisateur. Si l'utilisateur modifie cette valeur ou la supprime, le changement de mot de passe lui sera imposé à la prochaine connexion.
pwdDAPIValue-<login windows>@<poste de travail>	Mot de passe maître mémorisé pour l'utilisateur « login windows » sur le poste de travail « poste de travail ». Une valeur est créée dans le fichier .ini pour chaque utilisation de swSSO sur un poste de travail et/ou avec un compte Windows différent. Cette valeur est créée à jour lorsque l'utilisateur demande à ne plus saisir son mot de passe principal swSSO.

Nom de la valeur	Description
Computers	Liste des noms de postes de travail sur lequels une configuration proxy est définie. Les noms sont séparés par le signe « : », qui doit également terminer la ligne. Exemple : Computers=STATION01:STATION02:STATION03: Pour chaque poste de travail référencé dans cette liste doivent exister les 4 valeurs ci-dessous.
CollapsedCategs	Liste les identifiants des catégories « repliées » dans la fenêtre de gestion des applications et sites. **À partir de la version v0.92**
internetUseProxy-<poste de travail>	YES = utiliser un proxy sur ce poste de travail pour accéder au serveur de configuration.
ProxyURL-<poste de travail>	URL et port du proxy (exemple : http://monproxy:8080)
ProxyUser-<poste de travail>	Si le proxy demande une authentification, renseigner ici le login.
ProxyPwd-<poste de travail>	Si le proxy demande une authentification, renseigner ici le mot de pase.
lastConfigUpdate	Date de dernière vérification des configurations sur le serveur (format : AAAAMMJJHHMMSS)
recoveryInfos	Informations techniques nécessaires à la procédure de secours. Ces informations sont créées à la première connexion, modifiées à chaque changement de mot de passe et ne doivent pas être effacées. **À partir de la version v0.96**
recoveryRunning	Informations techniques générées lors du déclenchement de la procédure de secours. Ces informations sont effacées une fois la procédure terminée. **À partir de la version v0.96**

1.6. Fichier d'aide en ligne

La version actuelle de swSSO ne fournit pas d'aide en ligne. Si vous le souhaitez, vous pouvez construire un fichier d'aide nommé swSSO.chm et le placer dans le même dossier que swSSO.exe : il sera alors ouvert dès lors que l'utilisateur fera appel à l'aide en ligne sur l'une des fenêtres de swSSO (touche F1). Vous pouvez également télécharger le manuel utilisateur au format pdf et le placer dans le dossier de swSSO.exe.

Dans l'ordre, lorsque l'utilisateur appuie sur F1, swSSO essaie d'ouvrir :

- swSSO.chm,
- swSSO vM.mm - Manuel utilisateur.pdf,
- swSSO.pdf,
- La page « manuel utilisateur » du site www.swsso.fr.

Remarque : ci-dessus, vM.mm désigne la version où M=Majeur et m=mineur, par exemple v0.96 pour la version 0.96.

1.7. Mise en place d'un serveur de configuration en interne

Pré-requis :

- PHP5
- MySQL5

Installation du service Web :

- Déposer les fichiers admin.php, functions.php, util.php, variables.php et webservice5.php sur votre serveur php

Création de la base de données :

```
CREATE DATABASE `swsso` DEFAULT CHARACTER SET utf8 COLLATE utf8_unicode_ci;
```

Création des tables :

- Créer les tables à l'aide des scripts : creation_table_categ.sql, creation_table_config.sql, creation_table_domains.sql, creation_table_logs.sql et creation_table_stats.sql.
  Remarque : la création des tables de logs et de statistiques est optionnelle. Si vous ne souhaitez pas les créer, vous devez cependant modifier la configuration dans le fichier variable.php (voir §4.4).
  Attention, si vous souhaitez chiffrer les valeurs sensibles en base de données, vous devez utiliser le script creation_table_config_chiffrement.sql au lieu de creation_table_config.sql. Référez-vous au §4.5 pour plus d'informations.
- Modifier le fichier variables.php pour spécifier les éléments suivants :

```
define("_HOST_", "dbserver");     <- nom du serveur hébergeant la base
define("_DB_",   "dbname");       <- nom de la base de données
define("_USER_", "dbuser");       <- utilisateur MySQL
define("_PWD_",  "dbpassword");   <- mot de passe utilisateur MySQL
```

  Remarque : les autres paramètres disponibles dans le fichier variable.php sont décrits dans le §4.

Vérification de l'installation :

- Lancer la requête suivante depuis un navigateur :

```
http://<serveur>/webservice5.php?action=isalive
```

  L'affichage doit être le suivant :

```
ALIVE
```

  Cette étape valide la bonne installation du serveur php et de la base de données.

2. Scénario collaboratif, faiblement ou fortement administré

2.1. Introduction

Trois scénarios de déploiement peuvent être envisagés en fonction de votre contexte :

- Un **scénario collaboratif**, dans lequel tous les utilisateurs peuvent réaliser et partager des configurations de SSO. Ce scénario est à réserver à des déploiements sur un petit nombre d'utilisateurs dotés de compétences informatiques suffisantes pour réaliser les configurations.
- Un **scénario faiblement administré** : les configurations sont réalisées par un ou plusieurs administrateurs clairement identifiés. Les utilisateurs récupèrent les configurations à la demande (menu clic-droit sur l'icône swSSO, item « Ajouter cette application »), peuvent éventuellement créer leurs propres configurations ou modifier les configurations existantes, mais n'ont pas le droit de les remonter sur le serveur. Les utilisateurs ne peuvent pas modifier les options de configuration.
- Un **scénario fortement administré** : les configurations sont réalisées par un ou plusieurs administrateurs clairement identifiés. Les utilisateurs récupèrent l'ensemble des configurations disponibles au premier lancement. Ensuite, à chaque lancement, ils récupèrent les modifications apportées par le ou les administrateurs : ajouts, modifications et suppressions. Ils ne peuvent pas créer leurs propres configurations ni modifier ou supprimer les configurations récupérées sur le serveur. Ils ne sont pas non plus libres de gérer les catégories. Ils ne peuvent pas modifier les options de configuration.

Les paragraphes suivants spécifient le paramétrage à utiliser pour implémenter ces différents scénarios. Ce ne sont bien évidemment que des exemples : vous pouvez affiner les paramètres en fonction de vos besoins.

Selon leur nature, les paramètres doivent être définis :

- Dans un fichier **swsso.ini** que vous devrez déployer pour tous vos utilisateurs. Ce fichier contient les valeurs par défaut pour les options de configuration modifiables depuis le menu « Options ». Si vous ne souhaitez pas pré-configurer des options pour vos utilisateurs, vous n'avez pas besoin de déployer de fichier swsso.ini. Les valeurs personnalisables du fichier swsso.ini sont décrites au §1.5.
- En base de registre sous la clé **HKLM\SOFTWARE\swSSO**. Ces paramètres définissent les autorisations de vos utilisateurs : en fonction des paramètres, les interfaces de configuration sont bridées ou masquées. Les paramètres de base de registre sont décrits au §3.

2.2. Scénario collaboratif

C'est le mode de fonctionnement par défaut de swSSO. C'est ainsi que fonctionne la version personnelle de swSSO : tout internaute utilisant swSSO peut réaliser des configurations et les remonter sur le serveur Internet pour les partager avec les autres internautes.

Pour implémenter ce scénario, vous devez :

- Activer l'option de remontée des configurations :
  Fichier swsso.ini, section [swSSO], internetManualPutConfig=YES

2.3. Scénario faiblement administré

Pour implémenter ce scénario, vous devez :

- Interdire à vos utilisateurs de voir ou modifier les options de configuration : **HKLM\SOFTWARE\swSSO\GlobalPolicy : ShowOptions = 0**

2.4. Scénario fortement administré

Pour implémenter ce scénario, vous devez :

- Interdire à vos utilisateurs de voir ou modifier les options de configuration : **HKLM\SOFTWARE\swSSO\GlobalPolicy : ShowOptions = 0**
- Interdire à vos utilisateurs de créer ou modifier les configurations : **HKML\SOFTWARE\swSSO\GlobalPolicy : ModifiyApplicationConfig = 0**
- Proposer la récupération des configurations au premier lancement de swSSO : **HKLM\SOFTWARE\swSSO\EnterpriseOptions** : **GetAllConfigsAtFirstStart =1**
- Récupérer les nouvelles configurations disponibles sur le serveur à chaque lancement : **HKLM\SOFTWARE\swSSO\EnterpriseOptions** : **GetNewConfigsAtStart =1**
- Récupérer les configurations modifiées sur le serveur à chaque lancement : **HKLM\SOFTWARE\swSSO\EnterpriseOptions** : **GetModifiedConfigsAtStart =1**
- Désactiver les configurations archivées à chaque lancement : **HKLM\SOFTWARE\swSSO\EnterpriseOptions** : **DisableArchivedConfigsAtStart=1**
- Interdire la suppression des configurations récupérées sur le serveur : **HKLM\SOFTWARE\swSSO\EnterpriseOptions** : **AllowManagedConfigsDeletion=0**
- Forcer le classement des applications dans les catégories définies en central : **HKLM\SOFTWARE\swSSO\EnterpriseOptions : CategoryManagement=1**
- Activer les configurations récupérées sur le serveur : **HKLM\SOFTWARE\swSSO\EnterpriseOptions : ActivateNewConfigs=1**

2.5. Informations sur la gestion des configurations

Applications

Dans la base de données sur le serveur, chaque configuration d'application a un identifiant unique alloué par le serveur lorsqu'elle est remontée pour la première fois. Cet identifiant est communiqué :

- A l'utilisateur qui vient de remonter la configuration,
- A tous les utilisateurs qui vont la récupérer ultérieurement.

Ainsi, tous les utilisateurs ont dans leur fichier swSSO.ini des configurations clairement identifiées. Ceci est utile :

- Lorsqu'un utilisateur modifie la configuration et la remonte sur le serveur : le serveur peut ainsi « reconnaître » la configuration et la modifier.
- Lorsqu'un utilisateur récupère une configuration modifiée sur le serveur : le client swSSO peut ainsi « reconnaître » la configuration et la modifier.

Remarque : si deux utilisateurs réalisent une même configuration et demandent tous les deux à la remonter, celle-ci sera présente en double dans la base. En effet, la « clé » est bien l'identifiant de la configuration et non ses caractéristiques. C'est pourquoi il est important que les utilisateurs « contributeurs » aient le réflexe de toujours récupérer les configurations depuis le serveur avant de chercher à les créer ! Cela dit, une configuration présente en double dans la base ne pose pas de problème de fonctionnement :

- Le serveur retourne toujours la configuration la plus récente : pour cela, il se base sur la date de dernière mise à jour ou à défaut sur l'ordre de création ;
- Dans le cas d'un scénario fortement administré, ce mode de fonctionnement peut même être souhaitable dans certains cas : par exemple, si vos utilisateurs ont plusieurs comptes pour se connecter à une même application, cela vous permet de préparer les configurations de manière à ce qu'ils les récupèrent au premier lancement.

Catégories

Lorsqu'un utilisateur crée une catégorie dans swSSO, un identifiant local (valeur <10000) est attribué à la configuration.

Si l'utilisateur remonte la configuration d'une application appartenant à cette catégorie, la catégorie est également remontée sur le serveur :

- Si la catégorie existe déjà (vérification par rapport à son identifiant), rien n'est fait, sauf si le libellé a changé, auquel cas le nouveau libellé fourni par le client remplace le libellé connu en base de données ;
- Sinon, la catégorie est créée en base : un identifiant unique (valeur >=10000) est alors alloué à cette catégorie et redescendu sur le client. L'identifiant local de la catégorie est alors modifié, cette modification étant répercutée sur toutes les applications de la catégorie.

Domaines

Par défaut, toutes les configurations sont rattachées à un domaine unique, dénommé domaine « Commun ». Il est possible de définir d'autres domaines, afin de distribuer des configurations différentes à des populations d'utilisateurs différentes :

- Les configurations rattachées au domaine « Commun » sont distribuées à tous les utilisateurs, quel que soit leur domaine de rattachement ;
- Les configurations rattachées à un autre domaine ne sont distribuées qu'aux utilisateurs rattachés à ce domaine.

La création des domaines se fait au niveau de l'interface d'administration du serveur de configuration (menu « Ajouter ou supprimer un domaine »).

Le rattachement d'un utilisateur à un domaine peut être réalisé :

- Par configuration, en déployant un fichier swsso.ini dans lequel les informations domainId et domainLabel de la section [swSSO] sont renseignées ;
- Par l'utilisateur lui-même : au premier lancement de swSSO, une liste des domaines disponibles lui est présentée.

L'administrateur de chaque domaine décide, lorsqu'il souhaite remonter une configuration sur le serveur, si elle doit être placée dans le domaine « Commun » ou dans le domaine qu'il administre (menu « Uploader (domaine commun) » ou « Uploader (domaine x) ».

3. Configuration du client swSSO (base de registre)

3.1. Clé EnterpriseOptions

HKEY_LOCAL_MACHINE\SOFTWARE\(Wow6432Node\)swSSO\EnterpriseOptions

Nom de la valeur	Type	Défaut	Description
ActivateNewConfigs	DWORD	0	Active (1) / désactive (0) les configurations récupérées au démarrage depuis le serveur. Par défaut les configurations sont désactivées pour permettre à l'utilisateur de renseigner son login/mdp dans la fenêtre de gestion des sites et applications. Si, au moment où l'utilisateur accès à l'application, une configuration est activée et que le login/mdp n'est pas connu pour cette application, une fenêtre de saisie demande les informations manquantes à l'utilisateur, puis le SSO est réalisé. **Disponible à partir de la version v0.91.**
AllowManagedConfigsDeletion	DWORD	1	Autorise (1) / interdit (0) la suppression des configurations récupérées depuis le serveur ou uploadées vers le serveur. **Disponible à partir de la version v0.91.**
CategoryManagement	DWORD	0	Active (1) / Désactive (0) la gestion des catégories sur le serveur. Si activé, les identifiants et libellés des catégories sont stockés sur le serveur : ainsi, les configurations récupérées par les utilisateurs sont stockées dans la catégorie définie lors de la création de la configuration. **Disponible à partir de la version v0.91.**
DisableArchivedConfigsAtStart	DWORD	0	A chaque lancement de swSSO, désactive (1) / ne désactive pas (0) les configurations archivées sur le serveur depuis le dernier lancement de swSSO. **Disponible à partir de la version v0.91.**

Nom de la valeur	Type	Défaut	Description
DisplayConfigsNotifications	DWORD	1	Affiche (1) / n'affiche pas (0) les messages de notification d'ajout / modification / suppression des configurations au démarrage. **Disponible à partir de la version v0.92.**
ErrorMessageConfigNotFound	Chaîne	->	Message affiché lorsque la configuration demandée par l'utilisateur (menu « Ajouter cette application ») n'existe pas sur le serveur. Si vous ne définissez pas cette valeur, c'est le message suivant qui est affiché avec 2 boutons (oui / non) : « La configuration pour ce site n'a pas été trouvée. Voulez-vous la faire manuellement ? » Si vous définissez cette valeur, les boutons oui / non sont remplacés par un unique bouton OK. L'utilisateur ne pourra alors pas faire la configuration manuellement.
ErrorMessageIniFile	Chaîne	->	Message affiché lorsque la lecture du fichier swsso.ini échoue au démarrage de swSSO. Si vous ne définissez pas cette valeur, c'est le message suivant qui est affiché : « Une erreur est survenue lors de la lecture du fichier de configuration. Merci de contacter le support. »
ErrorMessageServerNotAvailable	Chaîne	->	Message affiché lorsque le serveur de configuration n'est pas joignable. Si vous ne définissez pas cette valeur, c'est le message suivant qui est affiché : « Impossible de joindre le serveur swSSO. Veuillez vérifier votre configuration proxy (menu Propriétés, onglet Options). »

Nom de la valeur	Type	Défaut	Description
GetAllConfigsAtFirstStart	DWORD	0	Propose (1) / ne propose pas (0) à l'utilisateur de récupérer toutes les configurations disponibles sur le serveur au premier lancement de swSSO. Remarque : si DisplayConfigsNotifications=1, GetAllConfigsAtFirstStart=1 ne propose pas mais impose silencieusement la récupération des configurations. Attention, cette valeur doit être placée à 1 si vous souhaitez que le choix du domaine soit proposé à l'utilisateur au 1er lancement. **Disponible à partir de la version v0.91.**
GetModifiedConfigsAtStart	DWORD	0	A chaque lancement de swSSO, récupère (1) / ne récupère pas (0) les configurations modifiées sur le serveur depuis le dernier lancement de swSSO. **Disponible à partir de la version v0.91.**
GetNewConfigsAtStart	DWORD	0	A chaque lancement de swSSO, récupère (1) / ne récupère pas (0) les nouvelles configurations ajoutées sur le serveur depuis le dernier lancement de swSSO. **Disponible à partir de la version v0.91.**
MaxConfigs	DWORD	500	Nombre maximum de configurations stockées par le client.
ServerAddress	Chaîne	ws.swsso.fr	Adresse du serveur de configuration.
WebServiceAddress	Chaîne	/webservice5.php	Chemin relatif du webservice de configuration
WelcomeMessage	Chaîne	->	Personnalisation du message inscrit dans la fenêtre de bienvenue de swSSO (les 3 lignes commençant par « Vous devez définir un mot de passe... » **Disponible à partir de la version v1.01.**

3.2. Clé ExcludedWindows

HKEY_LOCAL_MACHINE\SOFTWARE\(Wow6432Node\)swSSO\ExcludedWindows

Les menus « Ajouter cette application » ou « Se connecter à cette application » fonctionnent en récupérant le titre de la fenêtre en avant-plan. Dans le cas où des fenêtres toujours visibles (gestionnaire de tâches si configuré « toujours visible » par exemple) ou des barres d'outils (la barre « Quick Launch » de Windows) sont présentes à l'écran, les actions liées à ces menus ne fonctionnent pas toujours. Il est possible de spécifier une liste de titres (25 maximum, numérotés de 0 à 24) à exclure :

Nom de la valeur	Type	Description
0	Chaîne	Titre de la 1ère fenêtre à exclure
…	…	…
24	Chaîne	Titre de la 25ème fenêtre à exclure

3.3. Clé PasswordPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\(Wow6432Node\)swSSO\PasswordPolicy :

Nom de la valeur	Type	Défaut	Description
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.)
MaxAge	DWORD	0	Durée maximale de validité du mot de passe. Le changement du mot de passe est imposé à l'utilisateur au-delà de cette période. Remarque : la date du dernier changement de mot de passe est sauvegardée chiffrée par le mot de passe de l'utilisateur dans le fichier swsso.ini dans la section [swSSO], clé LastPwdChange. Si l'utilisateur modifie cette valeur ou la supprime, le changement de mot de passe lui sera imposé à la prochaine connexion.
Message	Chaîne	->	Si vous souhaitez afficher un message personnalisé à vos utilisateurs lorsque leur mot de passe ne satisfait pas aux exigences de votre politique, saisissez-le ici. A défaut, swSSO affichera ce message : Votre nouveau mot de passe n'est pas conforme aux règles de composition imposées par votre entreprise. Veuillez en choisir un autre.

Nom de la valeur	Type	Défaut	Description
MinAge	DWORD	0	Durée minimale de validité du mot de passe. Le changement du mot de passe est interdit à l'utilisateur pendant cette période (exemple : mettre la valeur à 1 pour interdire à l'utilisateur de changer deux fois son mot de passe dans la même journée).
MinLength	DWORD	0	Nombre minimum de caractères
MinLetters	DWORD	0	Nombre minimum de lettres (a-z / A-Z)
MinLowerCase	DWORD	0	Nombre minimum de majuscules (A-Z)
MinNumbers	DWORD	0	Nombre minimum de chiffres (0-9)
MinRules	DWORD	0	Définit le nombre de règles qui doivent être respectées parmi ces 4 : MinUpperCase, MinLowerCase, MinNumbers et MinSpecialChars. La valeur 0 (par défaut) assure la compatibilité avec les versions précédentes et signifie que toutes les règles définies doivent être respectées. Les autres valeurs permettent de demander aux utilisateurs de constituer leur mot de passe avec des caractères issus de n jeux de caractères parmi les m définis. **Disponible à partir de la version v0.86.**
MinSpecialChars	DWORD	0	Nombre minimum de caractères spéciaux (tous caractères autres que lettres et chiffres)
MinUpperCase	DWORD	0	Nombre minimum de minuscules (a-z)

3.4. Clé GlobalPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\(Wow6432Node\)swSSO\GlobalPolicy :

Nom de la valeur	Type	Défaut	Description
CheckVersionOption	DWORD	1	Autorise (1) / interdit (0) la modification de l'option "Vérifier les mises à jour au démarrage"
GetConfigOption	DWORD	1	Autorise (1) / interdit (0) la modification de l'option "Récupérer les informations de configuration..."
ManualPutConfigOption	DWORD	1	Autorise (1) / interdit (0) la modification de l'option "Sur demande, mettre à disposition mes informations de configuration..." **Disponible à partir de la version v0.89.**
ModifyApplicationConfig	DWORD	1	Autorise (1) / interdit (0) la modification des paramètres affichés dans les onglets "Configuration" et "Champs complémentaires" de la fenêtre "Gestion des sites et applications". **Disponible à partir de la version v0.86**.

Nom de la valeur	Type	Défaut	Description
OldPwdAutoFill	DWORD	0	Essaie (1) / n'essaie pas (0) de remplir à l'aveugle le champ ancien mot de passe dans la procédure d'assistance au changement de mot de passe **Disponible à partir de la version v0.99.**
OpenConfigFile	DWORD	1	Affiche (1) / masque (0) le bouton Ouvrir dans l'onglet "A propos"
PasswordChoiceLevel	DWORD	1	Définit les options autorisées dans la fenêtre de bienvenue swSSO (celle qui est affichée au premier lancement) : 1 : tout est autorisé 2 : le choix "mots de passe non chiffrés" est interdit 3 : seul le choix "définir un mot de passe maître" est autorisé (dans ce cas, une fenêtre simplifiée est affichée) 4 : la fenêtre de bienvenue n'est pas affichée et swSSO utilise le mot de passe Windows de l'utilisateur pour dériver la clé de chiffrement des mots de passe secondaires. Remarque : positionner cette valeur à 4 sur une installation existante permet de forcer la migration du mode « mot de passe maître » au mode « mot de passe Windows ». (**valeur disponible à partir de la version v0.96**)
ProxyOption	DWORD	1	Autorise (1) / interdit (0) la modification des paramètres proxy
ReactivateWithoutPwd	DWORD	0	1 : Réactive swSSO sans saisie du mot de passe maître. **Disponible à partir de la version v1.01.**
SavePasswordOption	DWORD	1	Affiche (1) / masque (0) la case à cocher permettant à l'utilisateur de demander à ne plus saisir son mot de passe swSSO sur son poste de travail.
SavePortal	DWORD	1	Affiche (1) / masque (0) le bouton "Parcourir" dans l'onglet "A propos"
SessionLockOption	DWORD	1	Autorise (1) / interdit (0) la modification de l'option "Désactiver swSSO lorsque je verrouille ma session Windows"
ShowAddAccountMenu	DWORD	1	Montre (1) / cache (0) l'item « Ajouter un compte » dans le menu clic-droit de la fenêtre de gestion des sites et applications. **Disponible à partir de la version v0.97.**
ShowAddAppMenu	DWORD	1	Montre (1) / cache (0) l'item « Ajouter une application » dans le menu clic-droit de la fenêtre de gestion des sites et applications. **Disponible à partir de la version v0.92, modifiée en v0.99** (cf. ShowAddThisApp)

Nom de la valeur	Type	Défaut	Description
ShowAddCategMenu	DWORD	1	Montre (1) / cache (0) l'item « Ajouter une catégorie » dans le menu clic-droit de la fenêtre de gestion des sites et applications. **Disponible à partir de la version v0.97.**
ShowAddThisAppMenu	DWORD	1	Montre (1) / cache (0) l'item « Ajouter cette application » dans le menu clic-droit de l'icône swSSO. **Disponible à partir de la version v0.99.**
ShowChangeAppPwdMenu	DWORD	0	Montre (1) / cache (0) l'item « Changer le mot de passe de cette application » dans le menu clic-droit de l'icône swSSO. **Disponible à partir de la version v0.99.**
ShowChangeCategIdsMenu	DWORD	1	Montre (1) / cache (0) le menu contextuel « Identifiants et mot de passe » sur les catégories. Ce menu permet de modifier d'un coup un ou plusieurs identifiants et/ou le mot de passe de toutes les applications d'une catégorie. **Disponible à partir de la version 0.91**.
ShowDeleteMenu	DWORD	1	Montre (1) / cache (0) l'item « Supprimer » dans le menu clic-droit de la fenêtre de gestion des sites et applications. **Disponible à partir de la version v0.97.**
ShowDuplicateMenu	DWORD	1	Montre (1) / cache (0) l'item « Dupliquer » dans le menu clic-droit de la fenêtre de gestion des sites et applications. **Disponible à partir de la version v0.97.**
ShowEnableDisableMenu	DWORD	1	Montre (1) / cache (0) les items « Activer » et « Désactiver » dans le menu clic-droit de la fenêtre de gestion des sites et applications. **Disponible à partir de la version v0.97.**
ShowLaunchAppMenu	DWORD	1	Montre (1) / cache (0) les menus et les champs liés au lancement d'applications depuis swSSO. Cela concerne le menu clic-droit sur l'icône swSSO, le menu contextuel des applications dans la fenêtre « Gestion des sites et applications » ainsi que le champ « Lancement » et le bouton « Parcourir » de cette même fenêtre. **Disponible à partir de la version v0.91.**
ShowMoveMenu	DWORD	1	Montre (1) / cache (0) l'item « Déplacer vers » dans le menu clic-droit de la fenêtre de gestion des sites et applications. **Disponible à partir de la version v0.97.**
ShowOptions	DWORD	1	Affiche (1) / masque (0) l'onglet Options dans la fenêtre de propriétés.

Nom de la valeur	Type	Défaut	Description
ShowPasswordOption	DWORD	1	Affiche (1) / masque (0) la loupe qui permet à l'utilisateur de visualiser le mot de passe d'une application ou d'un site.
ShowRenameMenu	DWORD	1	Montre (1) / cache (0) l'item « Renommer » dans le menu clic-droit de la fenêtre de gestion des sites et applications. **Disponible à partir de la version v0.97.**
ViewApplicationConfig	DWORD	1	Affiche (1) / masque (0) les onglets "Configuration" et "Champs complémentaires" de la fenêtre "Gestion des sites et applications". **Disponible à partir de la version v0.86.**
ViewConfigFilePath	DWORD	1	Affiche (1) / masque (0) le chemin complet du fichier swsso.ini dans l'onglet "A propos"

3.5. Logs

Les événements tracés par **swSSO.exe** sont les suivants :

Identifiant	Type	Message
1	Information	Authentification primaire réussie
2	Information	Arrêt de swSSO
3	Avertissement	Echec d'authentification primaire : mot de passe incorrect
4	Information	Authentification sur l'application <NOM APPLICATION> avec l'identifiant <IDENTIFIANT>
5	Avertissement	Échec d'authentification sur l'application <NOM APPLICATION> avec l'identifiant <IDENTIFIANT>
6	Erreur	Fichier <chemin complet du fichier .ini> corrompu
7	Erreur	Erreur technique - Impossible de démarrer swSSO
8	Information	Verrouillage de swSSO
9	Information	Déverrouillage réussi
10	Avertissement	Échec de déverrouillage : mot de passe incorrect
11	Information	Changement du mot de passe primaire réussi
12	Avertissement	Échec de changement de mot de passe primaire : ancien mot de passe incorrect
13	Erreur	Échec de changement de mot de passe primaire : erreur technique
14	Erreur	Le serveur de configuration ne répond pas (<URL du serveur>)
15	Information	Mise a jour des configurations : <X> ajouts, <Y> modifications, <Z> désactivations
16	Information	Une procédure de secours a été demandée par l'utilisateur
17	Information	La procédure de secours a réussi
18	Erreur	La procédure de secours a échoué
19	Information	Changement du mot de passe de l'application <X> pour le compte <Y>

Les événements tracés par l'outil de réinitialisation **swSSORecover.exe** sont les suivants :

Identifiant	Type	Message
1	Information	Démarrage de l'outil swSSORecover.exe
2	Information	Arrêt de l'outil swSSORecover.exe
3	Information	Nouvelle clé importée : <IDENTIFIANT DE LA CLE>
4	Avertissement	Échec d'ouverture du keystore : mot de passe incorrect
5	Avertissement	Échec d'import de la clé <IDENTIFIANT DE LA CLE> : mot de passe incorrect
6	Information	Demande de recouvrement traitée pour l'utilisateur <IDENTIFIANT UTILISATEUR>
7	Information	Changement de mot de passe du keystore

La configuration se fait sous la clé ci-dessous, pour l'ensemble des modules swSSO qui produisent des logs :

HKEY_LOCAL_MACHINE\SOFTWARE\swSSO\EnterpriseOptions

Nom de la valeur	Type	Défaut	Description
LogLevel	DWORD	0	0 : pas de log 1 : erreurs seulement 2 : 1 + avertissements 3 : 2 + log des authentifications secondaires sur les configurations managées uniquement (celles récupérées depuis le serveur) 4 : 3 + log des authentifications secondaires sur les configurations créées par l'utilisateur
LogFileName	Chaîne	-	Chemin complet du fichier de log. Si non renseigné, pas de log fichier.
WindowsEventLog	DWORD	0	Génération des logs dans le journal d'événements Windows.

Afin que les messages soient correctement affichés dans le journal d'événements de Windows, vous devez également créer la clé swSSO avec les valeurs suivantes :

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\swSSO]

"EventMessageFile"="c:\\swsso\\swsso.exe" (remplacer par le chemin complet d'installation de swsso.exe)

"TypesSupported"=dword:00000007

3.6. Traces

Les traces peuvent être utiles pour investiguer les problèmes que vous rencontreriez avec swSSO. La première chose à faire est d'utiliser la "version trace", la version de base ne générant aucune trace quelle que soit la configuration en base de registre.

HKEY_LOCAL_MACHINE\SOFTWARE\swSSO\Trace

Nom de la valeur	Type	Défaut	Description
FileName	Chaîne	c:\swssotrace.txt	Chemin complet du fichier trace
FileSize	DWORD	20 Mo	Taille max. (fichier tournant)
Level	DWORD	3	0 : pas de traces 1 : erreurs seulement 3 : 1 + entrée/sorties de fonctions 4 : 3 + informations 5 : 4 + informations + debug 6 : 5 + mots de passe

Attention : au niveau 6, les mots de passe sont inscrits en clair dans le fichier traces ! Utilisez toujours le niveau 5 pour les traces à envoyer au support.

3.7. Statistiques

swSSO peut générer un fichier de statistique local nommé swsso.stat, reprenant le nom du fichier swsso.ini de l'utilisateur avec l'extension .stat en remplacement de l'extension .ini. Le fichier généré est un fichier CSV au format suivant :

```
USERNAME;COMPUTERNAME;date dernière connexion réussie AAAAMMJJ;nb d'applications actives;nbsssoréalisés
```

La configuration se fait sous la clé ci-dessous :

HKEY_LOCAL_MACHINE\SOFTWARE\swSSO\EnterpriseOptions

Nom de la valeur	Type	Défaut	Description
Stat	DWORD	0	Génère (1) / ne génère pas (0) de fichier de statistiques **Disponible à partir de la version v0.99.**

4. Supervision et exploitation du serveur

4.1. Supervision

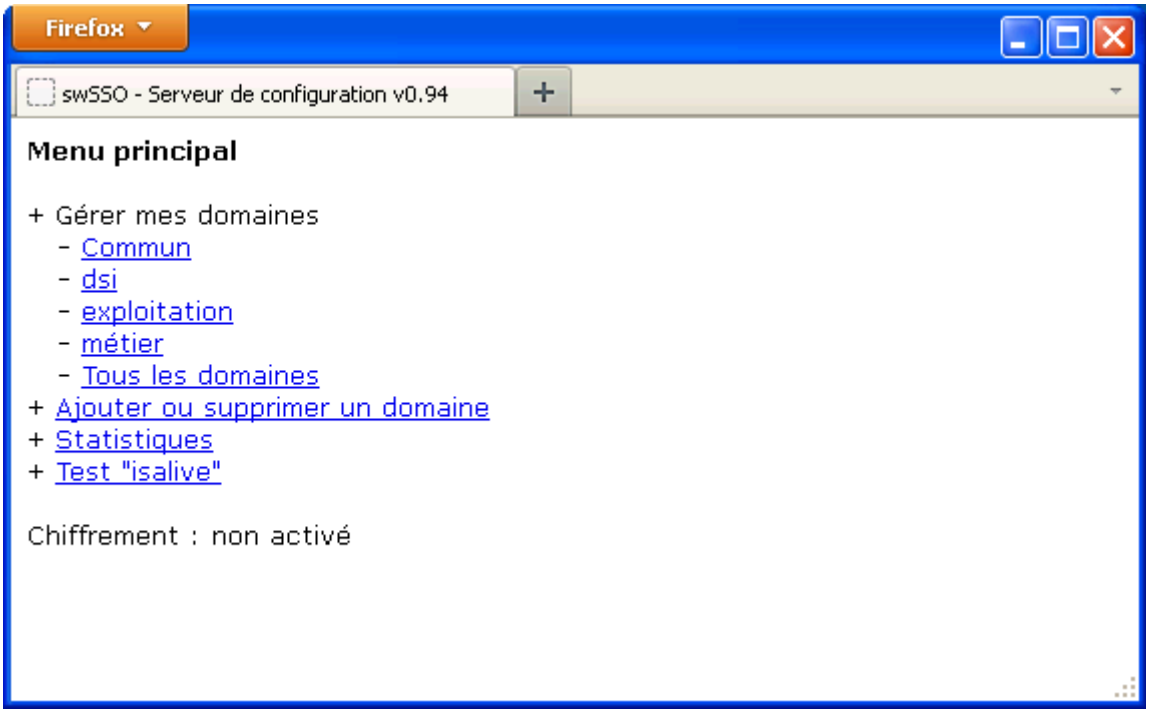
Pour vérifier que le serveur de configuration est opérationnel, il suffit de solliciter le test de vie du serveur avec l'URL suivante :

```
http://<adresse sur serveur/webservice5.php?action=isalive
```

Cette URL sollicite le serveur PHP et réalise une connexion à la base de données. Si le fonctionnement est correct, le serveur retourne simplement une trame HTTP contenant le mot ALIVE (sans aucune balise HTML).

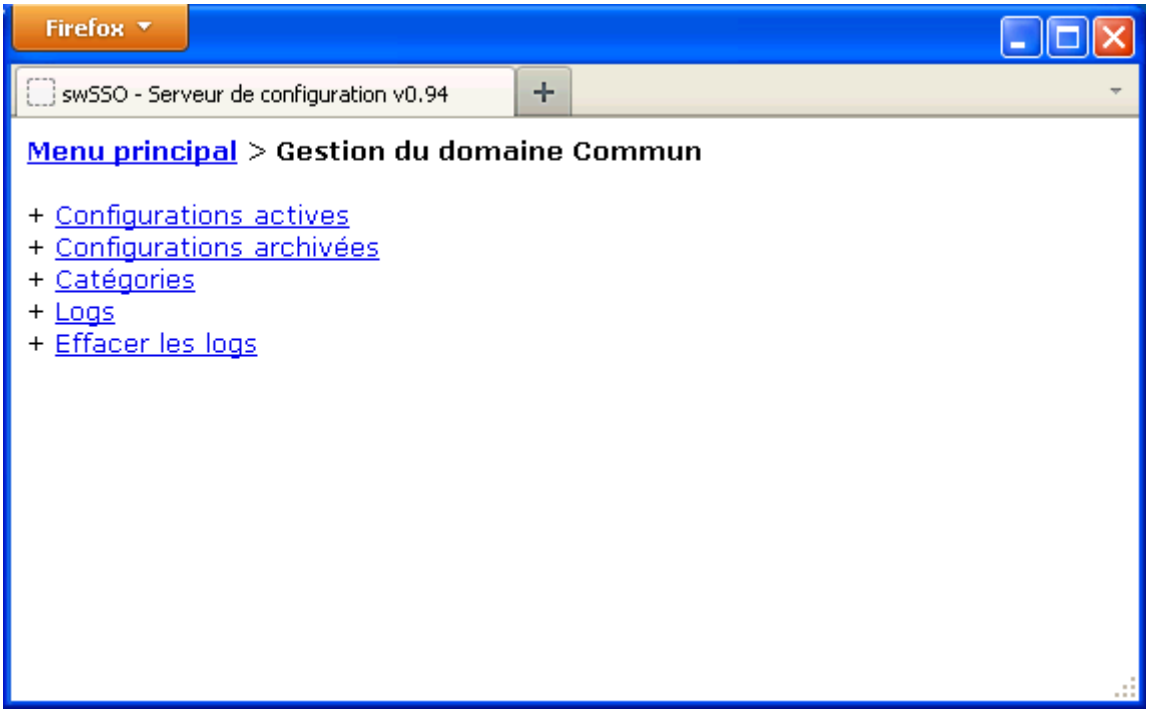
4.2. Exploitation

L'URL http://serveur/admin.php?action=menu vous donne accès au menu suivant :



- **Gérer mes domaines :** permet de gérer les configurations, les catégories et les logs de chacun des domaines (voir ci-dessous).
- **Ajouter ou supprimer un domaine :** permet de consulter la liste des domaines et d'en ajouter/supprimer. Par défaut, un domaine unique existe (dénommé « Commun »).
- **Statistiques :** affiche le nombre d'appels à la commande getversion qui permet de connaître la version en cours. Comme cette commande est appelée à chaque lancement de swSSO (si vous avez conservé cette option), ces statistiques vous permettent de visualiser le nombre de lancements de swSSO. Remarque : cette option n'est disponible que si vous avez activé les statistiques dans le fichier variables.php (_STATS_). Dans le cas contraire les logs ne sont pas produits.
- **Test isalive** : test de vie du serveur de configuration (voir §4.1).

La sélection d'un domaine dans le menu « Gérer mes domaines » donne accès aux fonctionnalités suivantes :



- **Configurations actives** : présentation de la liste des configurations actives du domaine, avec l'ensemble de leurs caractéristiques. Vous pourrez, à partir de la liste présentée, archiver des configurations. Si vous avez choisi l'option *DisableArchivedConfigsAtStart*, les configurations archivées seront automatiquement désactivées côté client au prochain lancement de swSSO.
- **Configurations archivées** : présentation de la liste des configurations archivées du domaine. Vous pourrez, à partir de la liste présentée, supprimer définitivement des configurations précédemment archivées. Cette opération n'est pas répercutée côté client, elle vous permet simplement de faire du « ménage » dans votre base de données.
- **Catégories** : présentation de la liste des catégories du domaine. Vous pourrez, à partir de la liste présentée, supprimer définitivement des catégories. Attention à bien vérifier que plus aucune configuration n'est rattachée à une catégorie avant de la supprimer.
- **Logs** : permet de visualiser toutes les demandes de configuration effectuées par les utilisateurs du domaine. Le champ résultat affiche le nombre de configurations retournées. Vous pouvez utiliser ces logs pour identifier les configurations manquantes. Remarque : cette option n'est disponible que si vous avez activé les logs dans le fichier variables.php (_LOGS_). Dans le cas contraire les logs ne sont pas produits.
- **Effacer les logs** : permet d'effacer les logs produits à chaque demande de configuration effectuée par les utilisateurs. Vous devriez prévoir d'effacer régulièrement les logs : la fréquence dépend du nombre d'utilisateurs. Un nettoyage mensuel est préconisé pour ne pas alourdir inutilement la base de configuration swSSO. Remarque : cette option n'est disponible que si vous avez activé les logs dans le fichier variables.php (_LOGS_).

4.3. Restriction d'accès à l'IHM du serveur de configuration

Vous pouvez, à l'aide des paramètres du fichier variables.php, restreindre l'accès aux différents écrans du serveur de configuration :

```
/*-------------------------------------------------------------------------
OPTIONS
-------------------------------------------------------------------------*/

define("_SHOWMENU_","TRUE"); // TRUE|FALSE (affichage menu autorise / interdit)

define("_MENUSUFFIX_","xxx"); // "protection" de l'URL presentant le menu

define("_READSUFFIX_","yyy"); // "protection" des URLs permettant la lecture
                                 de la base

define("_WRITESUFFIX_","zzz"); // "protection" des URLs permettant la
                                  modification de la base
```

Explication :

- _SHOWMENU_ : en attribuant la valeur FALSE, vous désactivez l'affichage du menu. Un utilisateur appelant l'URL http://<adresse sur serveur/webservice5.php?action=menu ne verra plus le menu, mais un message indiquant que le menu n'est pas activé.
- _MENUSUFFIX_ : protège l'URL menu (voir ci-dessous).
- _READSUFFIX_ : protège les URLs showall, showold, showlogs et showcategories (voir ci-dessous).
- _WRITESUFFIX_ : protège les URLS deletelogs, archiveconfig, deleteconfig et deletecateg (voir ci-dessous).

L'idée de la protection est relativement simple : elle consiste simplement à concaténer la clé que vous aurez définie à chacune des URLs. Cela permet d'éviter qu'un utilisateur ayant connaissance des URL génériques de swSSO puisse accéder aux fonctions disponibles sur votre serveur de configuration.

Par exemple, si vous définissez _MENUSUFFIX_ à "abc123", vous devrez saisir l'URL :

http://<adresse sur serveur/admin.php?action=menuabc123

au lieu de :

http://<adresse sur serveur/admin.php?action=menu

4.4. Logs et statistiques

Vous pouvez, à l'aide des paramètres du fichier variables.php, définir si vous souhaitez produire des logs et des statistiques d'utilisation de swSSO :

```
/*-------------------------------------------------------------------------
OPTIONS
-------------------------------------------------------------------------*/

define("_LOGS_","TRUE");  // TRUE | FALSE (génère des logs a chaque getconfig)

define("_STATS_","TRUE"); // TRUE | FALSE (incrémente un compteur a chaque
getversion)
```

4.5. Chiffrement des données sensibles en base

ATTENTION : le choix de chiffrer ou non les données doit être fait une fois pour toutes et ne peut pas être modifié une fois la base de données créée.

Les paramètres du fichier variables.php permettent d'activer le chiffrement en base de données des colonnes titre, url, szName et szFullPathName qui contiennent potentiellement des informations sensibles (urls, adresses IP, …) :

```
/*-------------------------------------------------------------------------
CHIFFREMENT DES COLONNES titre, url, szName et szFullPathName
-------------------------------------------------------------------------*/

define("_ENCRYPT_","FALSE");      // TRUE | FALSE (chiffre / ne chiffre pas)

define("_AESPWD_","my password"); // Mot de passe pour chiffrement
```

Si vous souhaitez activer le chiffrement, vous devez :

- Remplacer la valeur FALSE par TRUE dans la définition de la constante _ENCRYPT_ ;
- Renseigner le mot de passe à utiliser pour le chiffrement dans la définition de la constante _AESPWD_.

Pensez à protéger le fichier variables.php avec des ACL adaptées pour empêcher une personne malveillante d'avoir accès en lecture au mot de passe de chiffrement.

Pensez également à créer la table « config » avec le script ad hoc :

- creation_table_config.sql si vous gardez la valeur par défaut _ENCRYPT_=FALSE ;
- creation_table_config_chiffrement.sql si vous optez pour _ENCRYPT_=TRUE;

5. Synchronisation avec le mot de passe Windows

5.1. Principe

La version v0.96 apporte un nouveau mode de fonctionnement, évitant à l'utilisateur d'avoir un mot de passe maître à définir et à saisir au lancement de swSSO : la synchronisation avec le mot de passe Windows.

Pour activer ce mode, il faut positionner la clé de registre :

HKEY_LOCAL_MACHINE\SOFTWARE\swSSO\GlobalPolicy :

Nom de la valeur	Type	Valeur
PasswordChoiceLevel	DWORD	4

Ainsi, au 1er lancement de swSSO, la fenêtre de bienvenue n'est pas affichée et swSSO utilise le mot de passe Windows de l'utilisateur pour calculer la clé de chiffrement des mots de passe secondaires.

Ensuite, à chaque fois que l'utilisateur modifie son mot de passe Windows, le changement est détecté par swSSO et une nouvelle clé de chiffrement est calculée : les mots de passe secondaires sont déchiffrés avec l'ancienne clé et rechiffrés avec la nouvelle.

Cas particuliers :

- Si swSSO n'est pas lancé au moment où l'utilisateur change son mot de passe Windows, mais que le service swSSOSVC.exe est bien démarré (il s'agit d'un service en mode démarrage automatique qui ne doit pas être arrêté), le nouveau mot de passe est conservé par swSSOSVC.exe jusqu'au prochain lancement de swSSO.
- En revanche, si le service swSSOSVC.exe n'est pas démarré ou si par exemple le mot de passe de l'utilisateur est réinitialisé dans l'AD, swSSO ne pourra pas être informé du changement de mot de passe et l'utilisateur devra démarrer une procédure de secours.

5.2. Migration du mode mot de passe maître au mode synchronisé Windows

Sur une installation existante, il suffit de configurer la clé de registre présentée au paragraphe précédent à la valeur 4 : au prochain lancement de swSSO, le mot de passe Windows sera utilisé pour générer une nouvelle clé de chiffrement des mots de passe secondaires, qui seront alors déchiffrés avec l'ancienne clé (celle dérivée du mot de passe maître) et rechiffrés avec la nouvelle (celle dérivée du mot de passe Windows). Toutes les informations relatives au mot de passe maître précédemment utilisé sont supprimées du fichier swsso.ini.

Attention : si la version installée est une version 0.92 ou antérieure, il faut impérativement suivre la procédure suivante (nécessaire car la version 0.93 a apporté une modification du chiffrement du mot de passe maître et des mots de passe secondaires) :

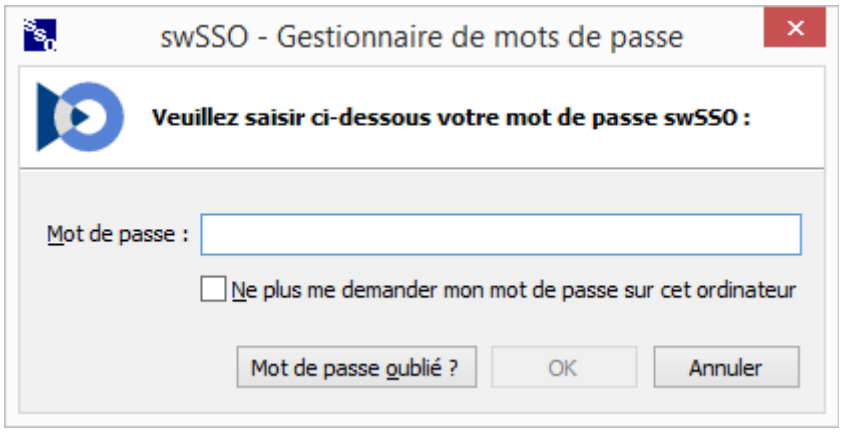
- Positionner la clé de registre PasswordChoiceLevel=3 ;
- Installer la version 0.96 ;
- Lancer swSSO.exe et se connecter au moins une fois avec le mot de passe maître, de manière à faire la migration de sécurisation du mot de passe maître et des mots de passe secondaires ;
- Rebooter (si pas fait à la fin de l'installation de la version 0.96) ;
- Positionner la clé de registre PasswordChoiceLevel=4 ;
- Lancer swSSO et saisir une dernière fois le mot de passe maître swSSO.

6. Procédure de secours

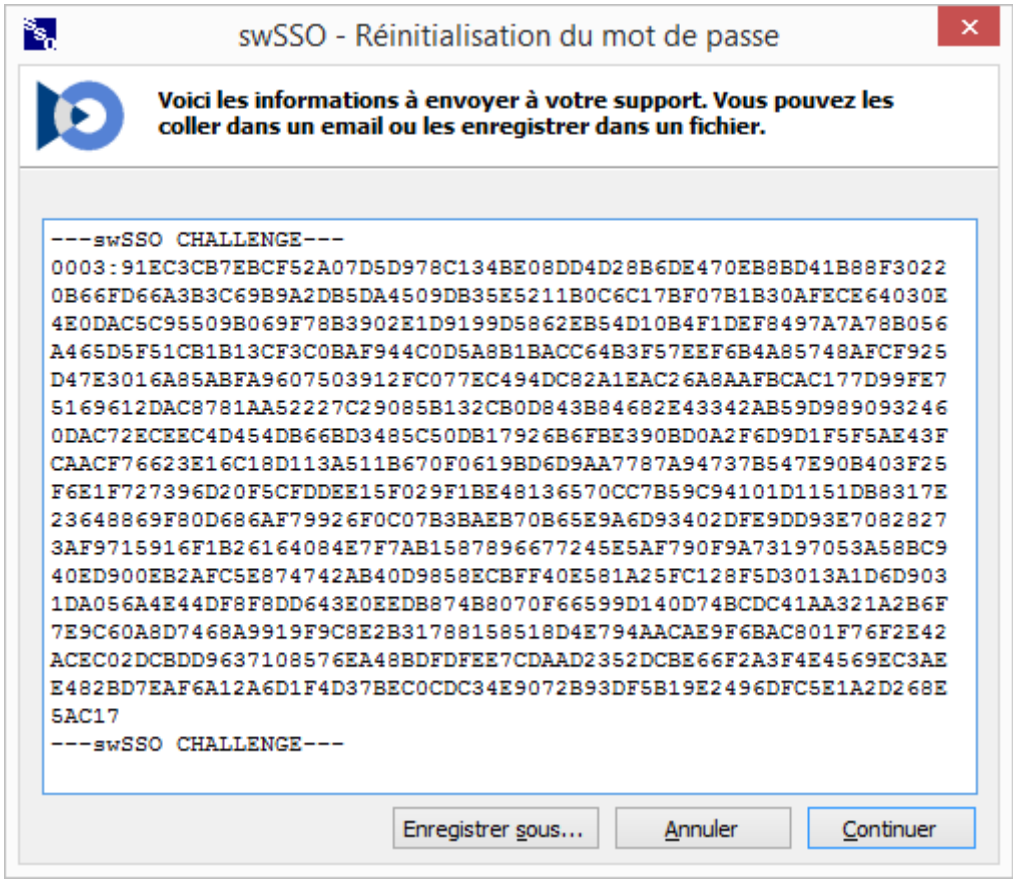
6.1. Principe général

La cinématique de la procédure de secours est la suivante :

- L'utilisateur clique sur le bouton « Mot de passe oublié » (cas de l'utilisation d'un mot de passe maître) ou swSSO détecte une désynchronisation du mot de passe Windows.

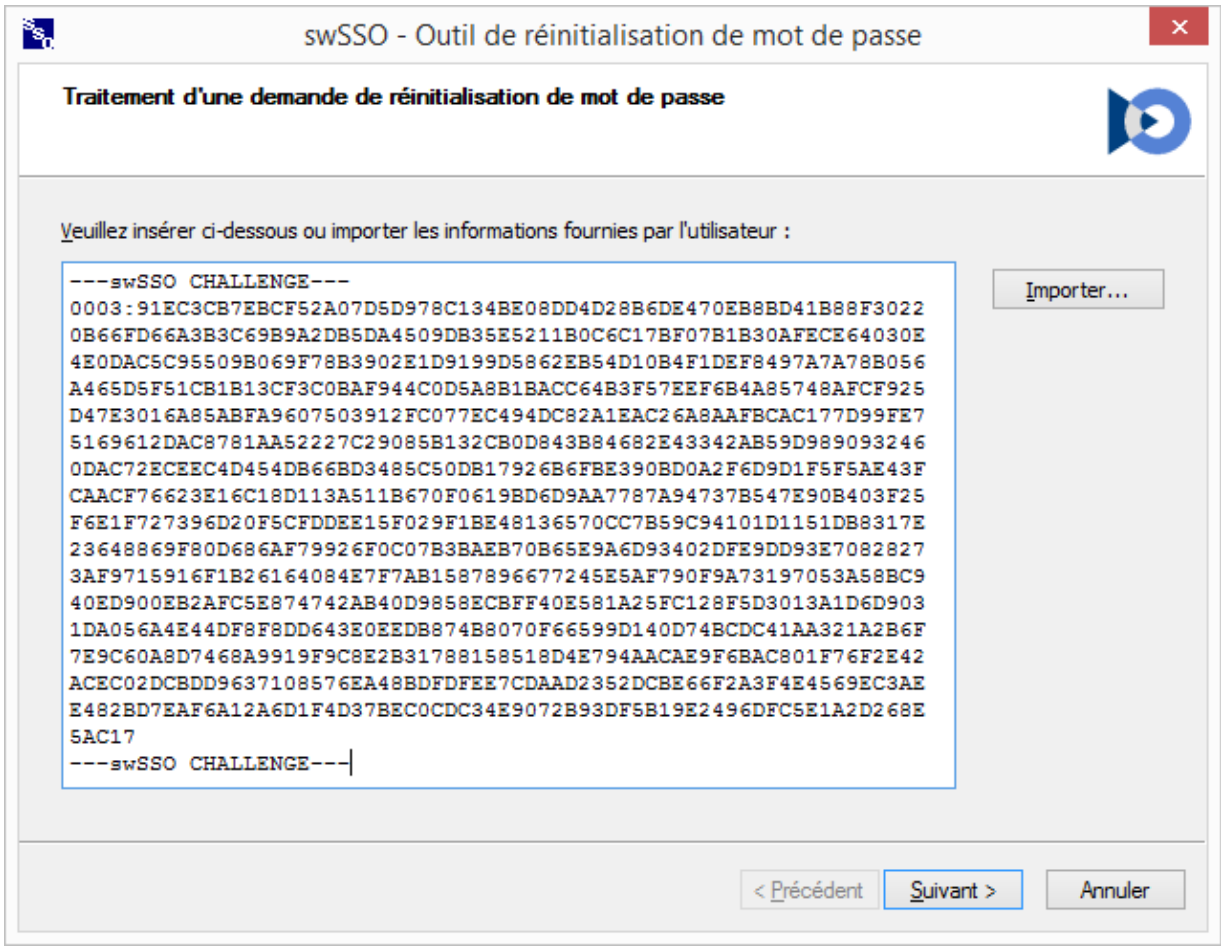


- swSSO génère une séquence de caractères, dénommée challenge par la suite, et l'affiche à l'utilisateur. L'utilisateur copie le challenge dans le presse-papier ou l'enregistre dans un fichier texte. Il clique ensuite sur le bouton « Continuer ».

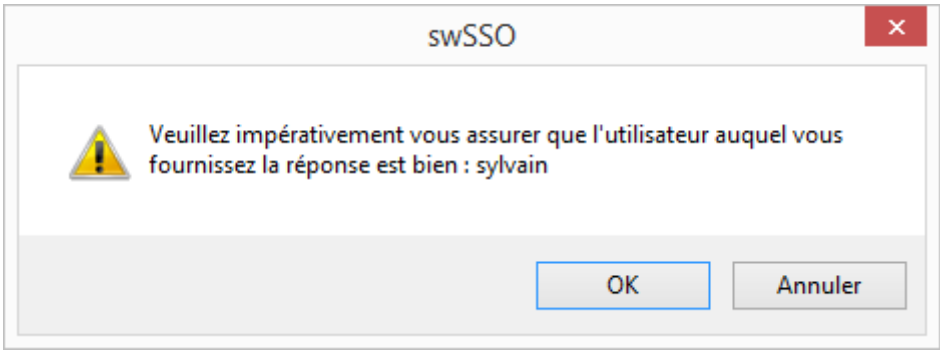


- L'utilisateur envoie ce challenge par ses propres moyens au support (par mail s'il a encore accès à sa messagerie ou en utilisant la messagerie d'un collègue par exemple).

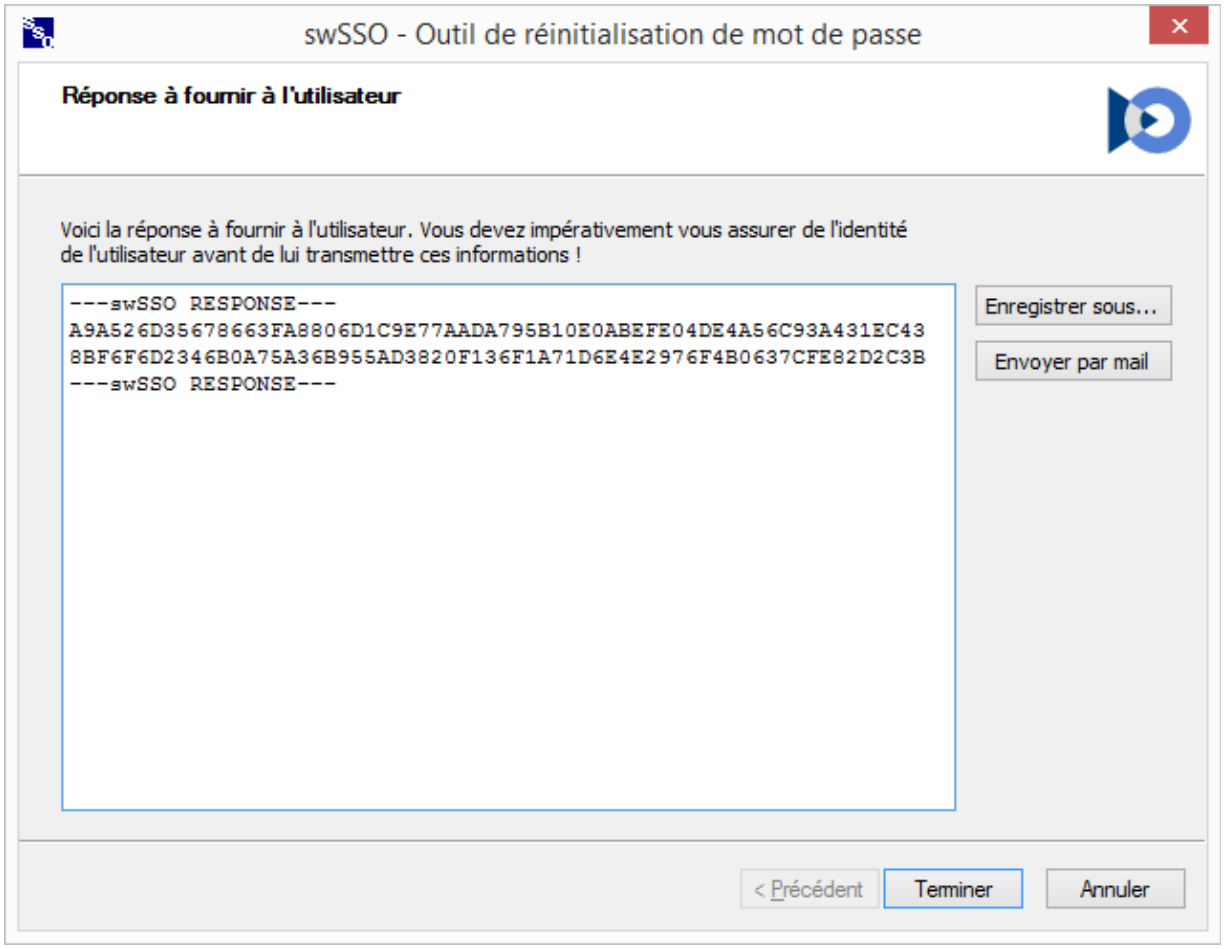
- L'opérateur du support colle le challenge (ou importe le fichier texte) reçu par mail dans l'outil de réinitialisation de mot de passe.



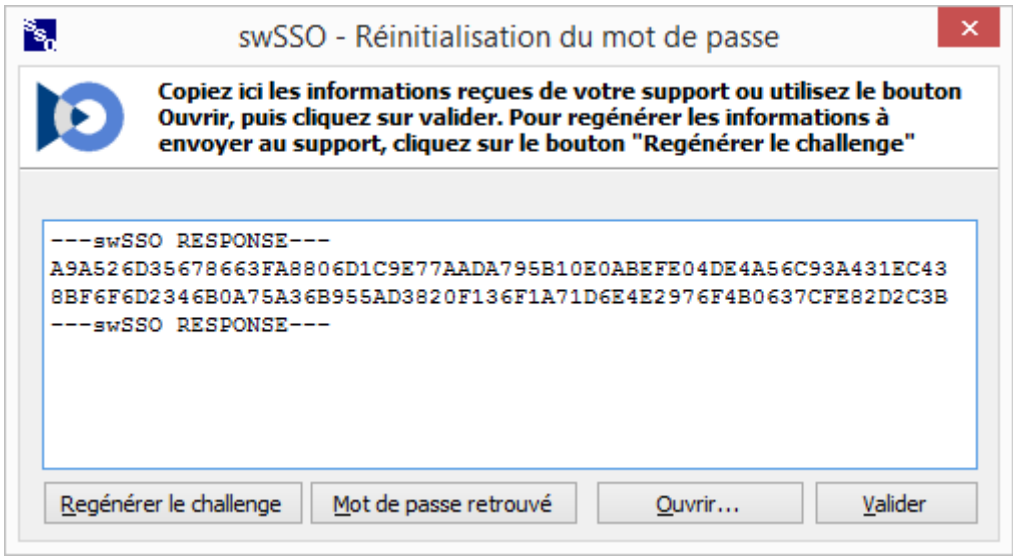
- Le nom du compte Windows de l'utilisateur ayant émis le challenge est affiché à l'écran. L'opérateur du support doit impérativement s'assurer que nom de compte Windows affiché correspond bien à l'utilisateur qui a fait la demande de secours.



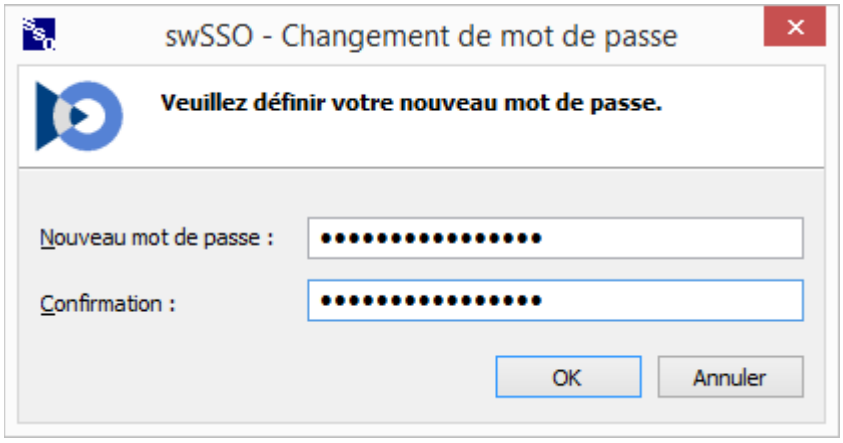
- Une réponse est générée : l'opérateur du support copie la réponse dans le presse-papier, l'enregistre dans un fichier texte ou clique sur le bouton « Envoyer par mail » (dans ce cas, un mail est automatiquement généré avec la réponse, l'opérateur du support n'a qu'à renseigner une adresse mail consultable par l'utilisateur et à envoyer le mail).



- L'utilisateur copie la réponse (ou importe le fichier texte) reçu par mail dans la fenêtre qui lui est présentée.



- Dans le cas où un mot de passe maître est utilisé, l'utilisateur doit alors en définir un nouveau. Sinon, le mot de passe Windows est automatiquement resynchronisé et l'utilisateur peut continuer à utiliser swSSO.



6.2. Configuration préalable

Pour activer la procédure de secours, il faut :

- Générer un couple clé publique / clé privée ;
- Importer la clé privée dans l'outil de réinitialisation de mot de passe ;
- Déployer la clé publique sur les postes de travail.

1) Génération d'un couple clé publique / clé privée avec l'outil swSSOGenKey.exe

Lancer l'outil swSSOGenKey.exe avec en paramètre l'identifiant de la clé à créer, par exemple 1 pour la première clé. L'identifiant permet à swSSO de reconnaître la clé utilisée lors d'une demande de secours. Il est ainsi possible de renouveler régulièrement la clé comme décrit plus loin dans ce document.

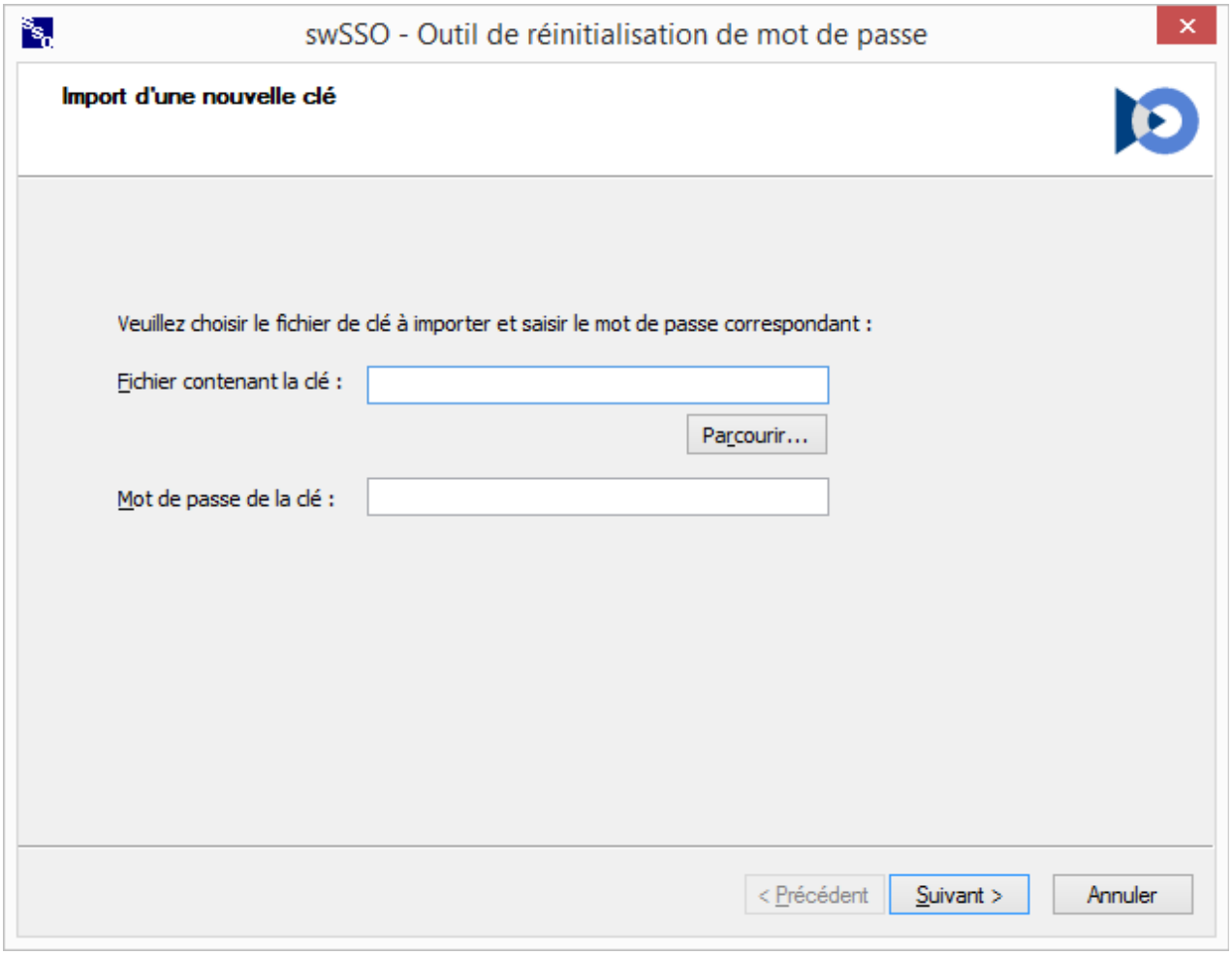
```
C:\swsso>swSSOGenKey.exe 1

swSSOGenKey (C) 2013 Sylvain Werdefroy
Generation de cle RSA pour l'outil de reinitialisation de mot de passe

Veuillez patienter pendant la generation de la cle RSA 2048 (id:0001)
Generation de la cle terminee.
Veuillez saisir le mot de passe qui protegera la cle (10 caractes min.) :
**********
Export de la cle termine.
-> Fichier cle publique x86 : swSSO-PublicKey-x86-0001.reg
-> Fichier cle publique x64 : swSSO-PublicKey-x64-0001.reg
-> Fichier cle privee       : swSSO-PrivateKey-0001.txt
```

Un mot de passe est demandé pour protéger la clé privée. Ce mot de passe devra être saisi pour importer la clé dans le keystore de l'outil de réinitialisation de mot de passe. Ensuite, il n'est plus utile et doit être conservé dans un endroit sécurisé si jamais la clé devait à nouveau être importée (réinstallation du poste de travail d'un opérateur ou arrivée d'un nouvel opérateur au support par exemple).

2) Import de la clé privée dans l'outil de réinitialisation de mot de passe (swSSORecover.exe)

Au premier lancement de swSSORecover.exe, l'opérateur du support doit :

- Définir un mot de passe qui protège le keystore ;
- Importer la ou les clés privées dans le keystore.



Une fois cette étape réalisée, l'opérateur du support peut commencer à dépanner les utilisateurs.

3) Déploiement de la clé publique sur les postes de travail

La clé privée est packagée dans un fichier .reg par l'outil swSSOGenKey.exe, permettant sa diffusion sur les postes de travail. Le format du fichier est le suivant :

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\swSSO\EnterpriseOptions]
"RecoveryKeyId"=dword:00000001
"RecoveryKeyValue"=hex:06,02,00,00,00,A4,00,00,52,53,41,31,00,08,00,00,01,00,01,00,45,66,50,88,2B,
1C,EB,5B,53,68,2C,37,CD,66,93,7B,D5,7A,37,F9,62,97,B5,20,D9,77,06,11,62,5B,21,4C,02,C8,7E,E9,B3,66
,A3,FE,C9,C3,6B,56,E3,55,1A,B3,64,87,6F,A2,52,C0,4F,98,CD,D8,4D,37,B8,91,62,D8,DA,6C,E1,08,22,99,2
3,17,79,18,C0,55,DE,9A,FF,D3,4F,78,6B,31,D0,81,90,5D,46,1A,28,57,A0,93,2D,8E,6D,89,BF,FD,56,C4,EC,
60,DD,BF,00,A3,FF,F6,70,BA,5C,41,2D,69,97,FF,31,3E,D9,1E,43,87,A1,3D,7F,5F,8F,79,6A,22,90,51,72,FF
,BB,DF,FA,45,CF,07,A6,EB,95,FE,87,11,23,41,37,49,C1,05,BE,D9,6C,DC,45,A2,A7,FE,F1,9F,01,0D,78,94,0
E,C0,EA,D0,FF,B6,FC,EB,82,08,2F,D1,C0,94,5C,F2,D8,8C,E0,E0,09,80,C0,71,1A,EC,E0,8A,3E,1F,49,38,D0,
E0,57,93,4C,AC,02,C7,14,56,AB,05,BB,44,20,BE,73,A6,44,30,8A,7A,0D,88,1D,E5,C4,3B,03,6A,D6,E1,12,35
,26,46,53,70,96,37,91,9C,E8,C8,66,A5,15,A3,10,5B,EE,9F,5E,33,D6,B6
```

6.3. Renouvellement du couple clé publique / clé privée

Il est possible de renouveler le couple clé publique / clé privée. Pour cela, il faut :

- Générer un nouveau couple clé publique / clé privée avec swSSOGenKey.exe, en choisissant un identifiant différent de ceux déjà existants ;
- Importer la nouvelle clé privée dans l'outil swSSORecover.exe, et ceci sur tous les postes des opérateurs du support ;
- Déployer la nouvelle clé publique sur les postes de travail.

L'identifiant du couple de clé étant fourni dans le challenge, l'outil de réinitialisation de mot de passe détermine automatiquement quelle clé utiliser pour réaliser la procédure de secours.

6.4. Configuration d'une politique de mot de passe sur l'outil de swSSORecover

La configuration se fait sous la clé suivante :

HKEY_LOCAL_MACHINE\SOFTWARE\swSSO\RecoverPolicy

Les valeurs à configurer sont les mêmes que pour swSSO, voir §3.3, à l'exception des valeurs MinAge et MaxAge qui ne sont pas implémentées.

6.5. Personnalisation du mail d'envoi de la response

La configuration se fait sous la clé suivante :

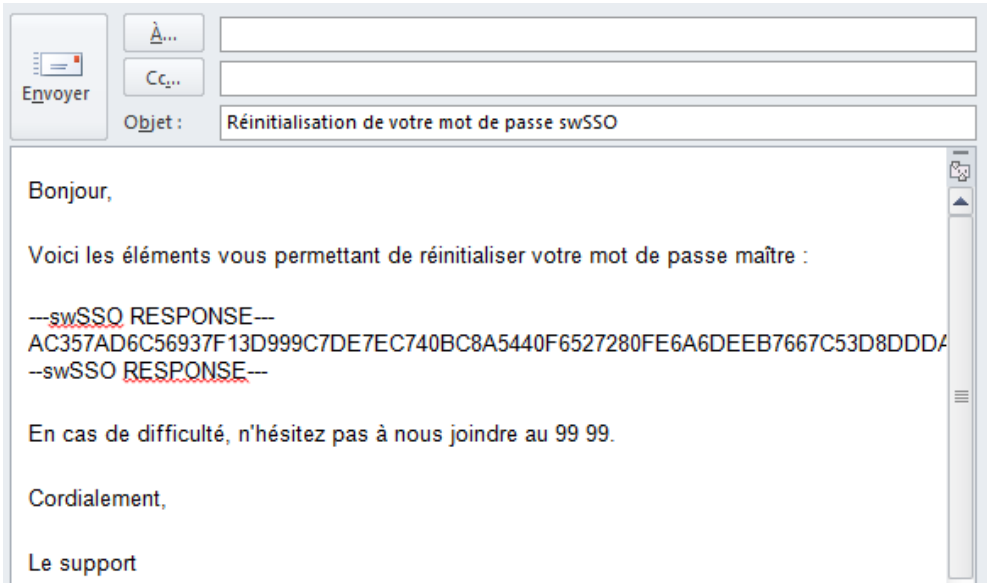
HKEY_LOCAL_MACHINE\SOFTWARE\swSSO\RecoverOptions

Nom de la valeur	Type	Défaut	Description
MailSubject	Chaîne	-	Objet du mail. Si non renseigné, l'objet par défaut est [swSSO]
MailBodyBefore	Chaîne	-	Message à placer en début de mail, avant la response
MailBodyAfter	Chaîne	-	Message à placer en fin de mail, après la response

Remarque : pour insérer des sauts de ligne dans le mail, utiliser %0D.

Exemple :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\swSSO\RecoverOptions]

"MailSubject"="Réinitialisation de votre mot de passe swSSO"

"MailBodyBefore"="Bonjour,%0D%0DVoici les éléments vous permettant de réinitialiser votre mot de passe maître :"

"MailBodyAfter"="En cas de difficulté, n'hésitez pas à nous joindre au 99 99.%0D%0DCordialement, %0D%0DLe support"
```


Envoyer
À...
Cc...
Objet :
Réinitialisation de votre mot de passe swSSO
Bonjour,
Voici les éléments vous permettant de réinitialiser votre mot de passe maître :
---swSSO RESPONSE---
AC357AD6C56937F13D999C7DE7EC740BC8A5440F6527280FE6A6DEEB7667C53D8DDD
--swSSO RESPONSE---
En cas de difficulté, n'hésitez pas à nous joindre au 99 99.
Cordialement,
Le support

7. Assistance au changement de mot de passe d'une application

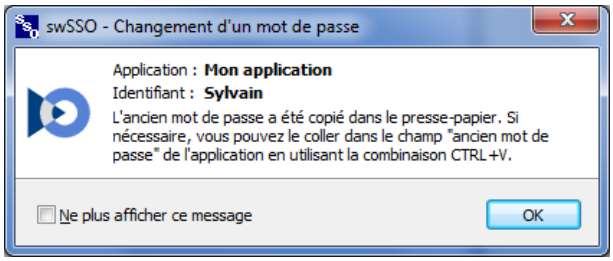
Avertissement : cette fonctionnalité expérimentale consiste uniquement en une assistance et ne se substitue pas à l'utilisateur pour la réalisation du changement du mot de passe d'une application. Par ailleurs elle se base sur l'hypothèse qu'elle est déclenchée suite à une authentification réalisée par swSSO : typiquement lorsque, à la suite d'une authentification, une application impose un changement de mot de passe à l'utilisateur (mot de passe expiré).

Pour activer le menu permettant à l'utilisateur d'accéder à l'assistance au changement de mot de passe d'une application, positionner la clé suivante :

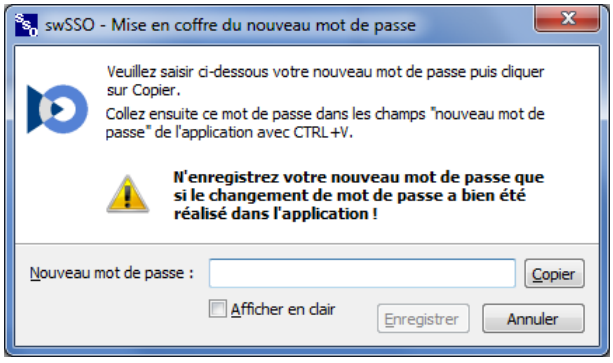
HKLM\SOFTWARE\swSSO\GlobalPolicy : ShowChangeAppPwdMenu = 1

Le fonctionnement est le suivant :

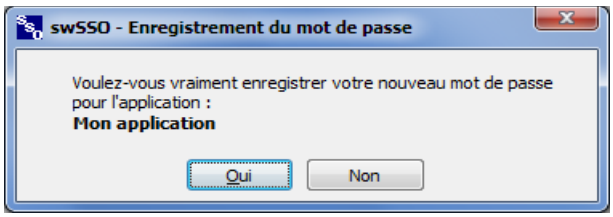
1. swSSO réalise l'authentification sur une application : celle-ci demande à l'utilisateur de changer son mot de passe qui a expiré.
2. L'utilisateur fait clic-droit sur l'icône swSSO et choisit le nouveau menu « Changer le mot de passe de cette application »
3. S'il retrouve la fenêtre de l'application et si la saisie automatique est configurée (voir ci-dessous), swSSO remet la fenêtre au premier plan et saisit l'ancien mot de passe de l'utilisateur à l'aveugle, en supposant a) que l'application demande de saisir l'ancien mot de passe et b) que le champ « ancien mot de passe » a le focus.
4. swSSO stocke l'ancien mot de passe dans le presse papier et affiche un message à l'utilisateur lui expliquant qu'il peut coller son ancien mot de passe dans l'application si celle-ci lui demande et que la saisie n'a pas été faite par swSSO :



5. Lorsque l'utilisateur clique sur OK, une nouvelle fenêtre s'affiche. Il est invité à définir son nouveau mot de passe pour l'application, puis peut ensuite cliquer sur le bouton copier pour mettre ce nouveau mot de passe dans le presse-papier et ainsi le coller facilement dans les champs de saisie de nouveau mot de passe de l'application. Une fois que l'application a accepté le changement de mot de passe, l'utilisateur clique sur Enregistrer pour mettre en coffre son nouveau mot de passe dans swSSO :



6. Un message de confirmation s'affiche alors, afin d'obtenir la confirmation de l'utilisateur avant de remplacer son ancien mot de passe par le nouveau dans le coffre :



Pour activer ou désactiver la saisie à l'aveugle de l'ancien mot de passe, positionner la clé suivante :

HKLM\SOFTWARE\swSSO\GlobalPolicy : OldPwdAutoFill = 0 (désactivé) ou 1 (activé)