|  |  |  |
| --- | --- | --- |
|  | swSSO v1.18  Guide d’administration |  |

**Contenu du document**

[1. Installation 4](#_Toc497412897)

[1.1. Principe général de fonctionnement 4](#_Toc497412898)

[1.2. Matrice de compatibilité client / serveur 4](#_Toc497412899)

[1.3. Installation du client swSSO 4](#_Toc497412900)

[1.4. Fichier de configuration swsso.ini – section [swSSO] 5](#_Toc497412901)

[1.5. Fichier d’aide en ligne 9](#_Toc497412902)

[1.6. Utilisation d'un logo personnalisé 9](#_Toc497412903)

[1.7. Installation du serveur de configuration 10](#_Toc497412904)

[1.8. Premier lancement du serveur d’administration 11](#_Toc497412905)

[2. Scénario faiblement ou fortement administré 14](#_Toc497412906)

[2.1. Introduction 14](#_Toc497412907)

[2.2. Scénario faiblement administré 14](#_Toc497412908)

[2.3. Scénario fortement administré 14](#_Toc497412909)

[2.4. Informations sur la gestion des configurations 15](#_Toc497412910)

[3. Configuration du client swSSO (base de registre) 17](#_Toc497412911)

[3.1. Clé EnterpriseOptions 17](#_Toc497412912)

[3.2. 23](#_Toc497412913)

[3.3. Clé ExcludedWindows 23](#_Toc497412914)

[3.4. Clé PasswordPolicy 23](#_Toc497412915)

[3.5. Clés GlobalPolicy et DomainPolicy 25](#_Toc497412916)

[3.6. Clé PwdGroupColors 29](#_Toc497412917)

[3.7. 30](#_Toc497412918)

[3.8. Logs 30](#_Toc497412919)

[3.9. Statistiques 32](#_Toc497412920)

[3.10. Configuration d'une boite mail pour demander l'ajout de configurations 32](#_Toc497412921)

[4. Client d'administration 34](#_Toc497412922)

[4.1. Principe 34](#_Toc497412923)

[4.2. Lancement du client d'administration 34](#_Toc497412924)

[4.3. Configuration du client d'administration 35](#_Toc497412925)

[5. Supervision et exploitation du serveur 36](#_Toc497412926)

[5.1. Supervision 36](#_Toc497412927)

[5.2. Exploitation 36](#_Toc497412928)

[5.3. Restrictions d’accès à l’IHM du serveur de configuration 38](#_Toc497412929)

[5.4. Logs 38](#_Toc497412930)

[5.5. Chiffrement des données sensibles en base 39](#_Toc497412931)

[6. Synchronisation avec le mot de passe Windows 40](#_Toc497412932)

[6.1. Principe 40](#_Toc497412933)

[6.2. Passage du mode mot de passe maître au mode synchronisé Windows 40](#_Toc497412934)

[6.3. Passage du mode synchronisé Windows au mode mot de passe maître 40](#_Toc497412935)

[6.4. Utilisation du mot de passe Windows comme mot de passe secondaire 40](#_Toc497412936)

[6.5. Synchronisation d'un groupe de mots de passe avec le mot de passe Windows 41](#_Toc497412937)

[7. Procédure de secours manuelle 42](#_Toc497412938)

[7.1. Principe général 42](#_Toc497412939)

[7.2. Configuration préalable 45](#_Toc497412940)

[7.3. Renouvellement du couple clé publique / clé privée 47](#_Toc497412941)

[7.4. Configuration d'une politique de mot de passe sur l'outil de swSSORecover 47](#_Toc497412942)

[7.5. Personnalisation du mail d'envoi de la response 47](#_Toc497412943)

[8. Procédure de secours automatique 49](#_Toc497412944)

[8.1. Avertissement 49](#_Toc497412945)

[8.2. Principe 49](#_Toc497412946)

[8.3. Installation du web service 49](#_Toc497412947)

[8.4. Configuration du client 51](#_Toc497412948)

[8.5. Test du web service 52](#_Toc497412949)

[8.6. Configuration des traces de swSSORecoverDll 52](#_Toc497412950)

[8.7. Gestion des erreurs en cours de transchiffrement 53](#_Toc497412951)

[9. Assistance au changement de mot de passe d'une application 54](#_Toc497412952)

[10. Traces 57](#_Toc497412953)

# Installation

## Principe général de fonctionnement

Le client swSSO installé sur les postes de travail s’appuie sur un serveur de configuration pour récupérer les configurations de SSO des applications préalablement publiées par un administrateur à l’aide du client d’admin (swSSO lancé avec le paramètre /admin, voir §4). Les configurations sont ensuite conservées localement dans un fichier .ini, afin que swSSO reste utilisable lorsque le serveur n’est pas joignable.

Les communications entre le client swSSO et le serveur de configuration se font par des requêtes HTTP(S).

## Matrice de compatibilité client / serveur

Le tableau ci-dessous indique la version serveur à utiliser en fonction de la version du client swSSO. 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 du client | Version du  serveur | Commentaire |
| 0.88 | webservice2 | Mode de fonctionnement nominal |
| 0.89 et 0.90 | webservice3 | Mode de fonctionnement nominal |
| webservice2 | 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 | Mode de fonctionnement nominal |
| 0.94 à 1.04 | webservice5 | Mode de fonctionnement nominal |
| 1.05+ | webservice5 | Fonctionnement en mode mono-domaine |
| webservice6 | Fonctionnement en mode multi-domaines |
| 1.14 | webservice5 | Fonctionnement en mode mono-domaine |
| webservice6 (6.5.2) | Fonctionnement en mode multi-domaines |
| **1.15+** | webservice5 | N’est plus supporté |
| webservice6 (6.5.2) | Fonctionne avec une restriction : l'information d'auto-publication ne remontera pas en base de données depuis le client d’admin et les informations d'auto-publication déjà présentes en base ne seront pas récupérées par les clients |
| **webservice6 (6.5.3)** | **Mode de fonctionnement nominal** |

## Installation du client swSSO

Si vous souhaitez utiliser la synchronisation de mot de passe Windows, vous devez utiliser l'installation 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 profil utilisateur ou encore sur un serveur de fichiers.

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" "%appdata%\swsso\swsso.ini"

"c:\program files\swsso\swsso.exe" "\\serveur\partage\%USERNAME%.ini"

"c:\program files\swsso\swsso.exe" "\\serveur\partage\%USERNAME%\swsso.ini"

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

Les valeurs présentées dans le tableau ci-dessous peuvent être prédéfinies pour le déploiement, soit dans un fichier .ini créé pour chaque utilisateur, soit sous la clé de registre **DefaultIniValues** (à partir de la version 1.04). A partir de la version 1.14, ces mêmes valeurs peuvent être définies sous la clé **ChangeIniValues** pour forcer le changement dans les fichiers .ini existants. Pour définir ces valeurs en base de registre, vous devez utiliser le type DWORD pour toutes les valeurs numériques ou YES/NO (1=YES / 0=NO) et le type chaine pour les autres valeurs.

| 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. |
| 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.** |
| 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** |
| InternetExplorer | YES | Active (YES) / Désactive (NO) le SSO pour IE  **Disponible à partir de la version 1.03** |
| Firefox | YES | Active (YES) / Désactive (NO) le SSO pour Firefox  **Disponible à partir de la version 1.03** |
| Chrome | YES | Active (YES) / Désactive (NO) le SSO pour Chrome  **Disponible à partir de la version 1.03** |
| ShowLaunchAppWithoutCtrl | NO | NO : le double-clic sur l'icône swSSO ouvre la fenêtre de gestion des sites (pour ouvrir le lanceur d'applications il faut utiliser la combinaison CTRL+double-clic). Cette valeur correspond au fonctionnement des versions précédentes de swSSO  YES : le double-clic ouvre le lanceur d'applications (pour ouvrir la fenêtre de gestion des sites, il faut passer par le menu clic-droit)  **Disponible à partir de la version 1.08**  (remarque : ce paramètre de configuration sera disponible dans l'IHM dans une version ultérieure) |
| RecoveryKeyId | -1 | Définit une valeur qui, si elle est égale au préfixe de recoveryInfos de swSSO.ini, déclenche le recalcul des recoveryInfos à partir des informations RecoveryKeyId et RecoveryKeyValue stockées sous la clé EntrepriseOptions. Permet de débloquer des utilisateurs dont swSSO ne démarre plus suite à un décalage entre la clé de recouvrement présente en base de registre et les recoveryInfos enregistrés dans le .ini. Remarque : leurs configurations seront conservées, mais leurs identifiants et mot de passe seront perdus lors de cette opération. Les utilisateurs dont le recoveryInfos est correct ne seront bien sûr pas impactés, cette clé peut donc être définie pour l’ensemble du parc et pas seulement sur les utilisateurs à corriger.  **Disponible à partir de la version 1.14** |

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. |
| 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.** |
| 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. |
| 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** |
| lastADPwdChange | Date du dernier changement de mot de passe AD. Utilisé uniquement lorsque UseADPassword est défini dans GlobalPolicy.  **À partir de la version v1.03** |
| ADPwd | Mot de passe AD de l'utilisateur. Utilisé uniquement lorsque UseADPassword est défini dans GlobalPolicy.  **À partir de la version v1.03** |

## 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,

Le site [www.swsso.fr](http://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.

## Utilisation d'un logo personnalisé

A partir de la version 1.07, il est possible d'utiliser un logo personnalisé dans les IHM swSSO. Les logos doivent être fournis au format bitmap en deux tailles avec les noms suivants :

swssologo50.bmp (60x50 pixels) ;

swssologo90.bmp (60x90 pixels).

Les fichiers doivent être placés dans le même répertoire de l'exécutable swsso.exe.

## Installation du serveur de configuration

**Pré-requis :**

PHP5. Modifications à faire dans le fichier php.ini

1. Si non présente ou commentée, ajouter la ligne :

default\_charset = "UTF-8"

1. Configurer la valeur error\_reporting de manière à ne pas afficher les E\_DEPRECATED ni les E\_STRICT, par exemple :

error\_reporting=E\_ALL & ~E\_DEPRECATED & ~E\_STRICT

MySQL5. Modifications à faire dans le fichier my.ini : repérer la ligne sql-mode et la remplacer par sql-mode=""

**Installation du service Web :**

Décompresser swSSO v1.nn - Installation serveur.zip

A la racine de cette archive, vous trouverez l’ensemble des fichiers .php à déposer dans un même dossier sur votre serveur php

**Création de la base de données :**

Créer la base de données à l'aide du script creation\_database.sql fourni dans le sous-dossier database

**Création des tables :**

Créer les tables en exécutant chacun des fichiers .sql fournis dans le sous-dossier database.

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 variables.php (voir §5.4).

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 §5.5 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 §5.

**Vérification de l’installation :**

Saisir l’URL suivante depuis un navigateur :

http://<serveur>/webservice6.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.**

## Premier lancement du serveur d’administration

Saisir l’URL suivante depuis un navigateur :

**http://<serveur>/ws65/admin.php?action=menu**

Comme il s’agit de la première connexion, vous allez être redirigé vers la page ci-dessous pour créer le compte d’un superadministrateur. Le superadministrateur est un administrateur particulier qui a le droit de créer des administrateurs, de réinitialiser les mots de passe des administrateurs et de verrouiller / déverrouiller leurs comptes.



Saisissez les informations du compte, puis cliquez sur le bouton Créer. Vous êtes automatiquement redirigé vers la page ci-dessous :



Saisissez l’identifiant et le mot de passe défini précédemment, puis cliquez sur le bouton Connexion. La page suivante s’affiche :



Sur cette page, vous pouvez voir la liste de tous les administrateurs définis et leur rôle : admin ou superadmin. En cliquant sur le bouton Créer, vous pouvez créer un compte administrateur :



Saisissez les informations souhaitées et cliquer sur le bouton Créer. Vous revenez à la page de gestion des administrateurs :



Cliquez maintenant sur le bouton Déconnexion pour vous reconnecter avec le compte administrateur créé :



La page suivante s’affiche : il s’agit de l’interface permettant aux administrateurs de visualiser les configurations et de modifier certains éléments. Cette interface est décrite plus loin dans le document.



# Scénario faiblement ou fortement administré

## Introduction

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

Un **scénario** **faiblement administré**: les configurations sont réalisées par un ou plusieurs administrateurs. 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. 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 §1.4.

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.

## 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

## 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

Activer les configurations récupérées sur le serveur :

HKLM\SOFTWARE\swSSO\EnterpriseOptions : ActivateNewConfigs=1

## 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’administrateur publie la configuration,

A tous les administrateurs ou 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 administrateur modifie la configuration et la remonte sur le serveur : le serveur peut ainsi « reconnaître » la configuration et la modifier côté serveur.

Lorsqu’un utilisateur récupère une configuration modifiée sur le serveur : le client swSSO peut ainsi « reconnaître » la configuration et la modifier côté client.

### Catégories

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

S’il s’agit d’un administrateur et qu’il publie 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 depuis le client d’administration, fenêtre Gestion des sites et Applications, onglet Domaines, clic-droit « Ajouter 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 ou en utilisant les clés de registre domainId et domainLabel sous la clé DefaultIniValues ;

Par configuration, en utilisant les clés de registre DomainRegKey et DomainRegValue sous la clé EnterpriseOptions ;

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 un ou plusieurs autre domaines dans la fenêtre suivante :



La colonne « Auto-publiée » permet d’indiquer si la configuration est auto-publiée pour les utilisateurs du domaine concerné. L’auto-publication s’active par la clé GetAutoPublishedConfigsAtStart (sous EnterpriseOptions) et n’intervient que si vous n’avez pas opté pour un mode de distribution automatique des configurations avec les clés GetAllConfigsAtFirstStart et/ou GetNewConfigsAtStart).

Par défaut, la valeur est toujours Non. Pour la modifier, il suffit de double-cliquer sur le « Non » pour le passer à « Oui » et inversement.

# Configuration du client swSSO (base de registre)

## 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 v0.91.** |
| AdminDeleteConfigsOnServer | DWORD | 0 | Active (1) / désactive (0) la suppression sur le serveur des configurations et catégories supprimées sur le client d'administration  **Disponible à partir de la v1.07.** |
| AllowManagedConfigsDeletion | DWORD | 1 | Autorise (1) / interdit (0) la suppression des configurations récupérées depuis le serveur.  **Disponible à partir de la v0.91.** |
| AllowManagedConfigsModification | DWORD | 1 | Autorise (1) / interdit (0) la modification des configurations récupérées depuis le serveur.  **Disponible à partir de la v1.07.** |
| AskThisAppMessage | Chaîne | Aucune | Message affiché dans la boite de dialogue qui s’affiche lorsque l’utilisateur sélectionne le menu « Demander l’ajout de cette application ».  La boite de message affiche un lien vers l’adresse mail configurée dans la clé ConfigNotFoundMailTo (voir §3.8) et présente un unique bouton Fermer.  **Disponible à partir de la v1.14.** |
| CategoryAutoUpdate | DWORD | 0 | Active (1) / Désactive (0) la mise à jour automatique sur le serveur de la catégorie d'une application lorsqu'elle et déplacée d'une catégorie à une autre dans l'IHM client.  Ne fonctionne que si CategoryManagement=1  **Disponible à partir de la v1.06.** |
| 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 v0.91.** |
| CheckCertificates | DWORD | 1 | Vérifie (1) / ne vérifie pas (0) la validité des certificats serveurs.  **Disponible à partir de la v1.08.** |
| ConfigNotFoundMailTo | Chaine | [swSSO] | Adresse mail de la BAL  **Disponible à partir de la v1.08**. |
| ConfigNotFoundMailSubject | Chaine | Vide | Objet du mail  **Disponible à partir de la v1.08**. |
| ConfigNotFoundMailBody | Chaine | Vide | Contenu du mail  **Disponible à partir de la v1.08**. |
| 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 v0.91.** |
| 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 v0.92.** |
| DisplayWindowsPasswordChange | DWORD | 1 | Affiche (1) / n’affiche pas (0) le message de notification de changement du mot de passe Windows (concerne le mode avec synchronisation du mot de passe uniquement)  **Disponible à partir de la v1.05.** |
| DomainRegKey | Chaîne | Aucune | Définit le nom complet de la clé dans laquelle se trouve la valeur qui contient le libellé du domaine de rattachement de l’utilisateur. Exemple : HKLM\SOFTWARE\MonApplication. HKLM et HKCU sont utilisables.  **Disponible à partir de la v1.14.** |
| DomainRegValue | Chaîne | Aucune | Définit le nom de la valeur qui contient le libellé du domaine de rattachement de l’utilisateur. Permet de rattacher l’utilisateur automatiquement à un domaine de configuration en fonction d’un élément de configuration extérieur à swSSO. Cette valeur est vérifiée à chaque lancement et à chaque rafraichissement des droits, ce qui permet de prendre en compte de manière transparente les changements d’appartenance un domaine. Exemple : SecteurMetier.  **Disponible à partir de la v1.14.** |
| 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 bouton Ajouter et un bouton Fermer, avec optionnellement un lien vers une boite mail à contacter pour demander l'ajout de configuration (voir §3.8). |
| 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). » |
| ErrorTitleConfigNotFound | Chaîne | -> | Titre de la boite de message affichée lorsque la configuration demandée par l’utilisateur (menu « Ajouter cette application ») n’existe pas sur le serveur. Valeur par défaut : « Configuration non trouvée ».  **Disponible à partir de la v1.14.** |
| 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 v0.91.** |
| GetAutoPublishedConfigsAtStart | DWORD | 0 | Active (1) / désactive (0) la récupération automatique des configurations marquées comme « à ublier automatiquement ».  **Disponible à partir de la v1.14.** |
| 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 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 v0.91.** |
| MaxConfigs | DWORD | 500 | Nombre maximum de configurations stockées par le client.  **Disponible à partir de la v1.01.** |
| RecoveryWebserviceActive | DWORD | 0 | Active (1) / désactive (0) l'appel au web service.  **Disponible à partir de la v1.08**. |
| RecoveryWebserviceHTTPS | DWORD | 0 | 0=HTTP / 1=HTTPS  **Disponible à partir de la v1.08**. |
| RecoveryWebserviceManual Backup | DWORD | 1 | Bascule (1) / ne bascule pas (0) vers la procédure manuelle de recouvrement en cas d'échec d'appel du web service  **Disponible à partir de la v1.08**. |
| RecoveryWebserviceNbTry | DWORD | 1 | Nombre de tentatives d'appel au web service  **Disponible à partir de la v1.10**. |
| RecoveryWebservicePort | DWORD | 80 | Port pour l'accès au web service  **Disponible à partir de la v1.08**. |
| RecoveryWebserviceServer | Chaîne | - | FQDN du serveur  (ex : monserveur.mondomaine)  **Disponible à partir de la v1.08**. |
| RecoveryWebserviceTimeout | DWORD | 10 | Temps d'attente de la réponse du web service. Si temps dépassé, bascule vers la procédure manuelle de challenge/response.  **Disponible à partir de la v1.08**. |
| RecoveryWebserviceURL | Chaîne | - | URL d'appel du service  (ex : /swsso/resync.ea)  **Disponible à partir de la v1.08**. |
| RecoveryWebserviceWaitBeforeRetry | DWORD | 1000 | Temps d'attente entre deux tentatives d'appel du web service (en millisecondes)  **Disponible à partir de la v1.10.** |
| RefreshRightsFrequency | DWORD | 0 | Définit la fréquence de rafraîchissement automatique des droits (en minutes). Si 0, pas de rafraîchissement automatique.  **Disponible à partir de la v1.07** |
| RemoveDeletedConfigsAtStart | DWORD | 0 | Supprime les configurations qui n'existent plus côté serveur (soit parce qu'elles sont été supprimées, soit parce que l'utilisateur a changé de domaine par exemple).  **Disponible à partir de la v1.07** |
| ServerAddress | Chaîne | ws.swsso.fr | Adresse du serveur de configuration. |
| ServerAddress2 | Chaîne | Aucun | Adresse du serveur de configuration de secours  **Disponible à partir de la v1.14** |
| ServerPort | DWORD | 80 | Port pour l'accès au serveur de configuration.  **Disponible à partir de la v1.03** |
| ServerPort2 | DWORD | 80 | Port pour l'accès au serveur de configuration de secours  **Disponible à partir de la v1.14** |
| ServerHTTPS | DWORD | 0 | 0=HTTP 1=HTTPS  **Disponible à partir de la v1.03.** |
| ServerHTTPS2 | DWORD | 0 | 0=HTTP 1=HTTPS (serveur de secours)  **Disponible à partir de la v1.14** |
| SyncSecondaryPasswordActive | DWORD | 0 | Active (1) / désactive (0) la mise à jour des mots de passe secondaires  **Disponible à partir de la v1.08**. |
| SyncSecondaryPasswordGroup | DWORD | -1 | Groupe d'applications sur lequel la modification s'applique  **Disponible à partir de la v1.08**. |
| SyncSecondaryPasswordOU | Chaîne | Vide | OU dans laquelle doit se trouver l'utilisateur pour que la modification de mot de passe s'applique. Si la clé est vide ou non définie, la modification de mot de passe s'applique quelle que soit l'OU dans laquelle se trouve l'utilisateur  **Disponible à partir de la v1.08**. |
| UseADPassword | DWORD | 0 | Si 1, la variable%ADPASSWORD% permet d'utiliser le mot de passe AD comme mot de passe secondaire. Si ce paramètre est utilisé en mode mot de passe maître, l'utilisateur devra saisir son mot de passe AD au lancement de swSSO à chaque fois que son mot de passe aura été modifié dans l'AD.  **Disponible à partir de la v1.03.** |
| UseSquareForManagedConfigs | DWORD | 1 | Si 1 (valeur par défaut), les configurations définies par l’administrateur apparaissent avec une forme carrée dans la fenêtre de gestion des sites et applications.  **Disponible à partir de la v1.16.** |
| WaitBeforeNewSSO | DWORD | 120 | Temps d'attente (en secondes) avant nouvelle tentative de SSO sur un site web  **Disponible à partir de la v1.08** |
| WebServiceAddress | Chaîne | /webservice5 .php | Chemin relatif du webservice de configuration |
| WebServiceAddress2 | Chaîne | Aucun | Chemin relatif du webservice de configuration de secours  **Disponible à partir de la v1.14** |
| WebServiceTimeout | DWORD | 8 | Timeout d’appel du serveur de configuration, avant abandon ou bascule vers le serveur de secours si configuré  **Disponible à partir de la v1.14** |
| WebServiceTimeout2 | DWORD | 8 | Timeout d’appel du serveur de configuration de secours  **Disponible à partir de la v1.14** |
| 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 v1.01.** |

## 

## 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 |

Comme dans le paramétrage des configurations de SSO :

Le caractère joker \* est accepté en début et/ou milieu et/ou fin, uniquement dans les cas suivants : \*titre, titre\*,\*titre\*,ti\*tre,\*ti\*tre,ti\*tre\*,\*ti\*tre\*.

Les syntaxes avec plusieurs jokers en milieu de chaîne ne sont pas acceptés, comme par exemple : ti\*t\*re

La comparaison ne tient pas compte de la casse.

## 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. |
| 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 | 8 | Nombre minimum de caractères |
| MinLetters | DWORD | 1 | Nombre minimum de lettres (a-z / A-Z) |
| MinLowerCase | DWORD | 1 | Nombre minimum de minuscules (a-z) |
| MinNumbers | DWORD | 1 | 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 v0.86. |
| MinSpecialChars | DWORD | 0 | Nombre minimum de caractères spéciaux (tous caractères autres que lettres et chiffres) |
| MinUpperCase | DWORD | 1 | Nombre minimum de majuscules (A-Z) |

## Clés GlobalPolicy et DomainPolicy

HKEY\_LOCAL\_MACHINE\SOFTWARE\(Wow6432Node\)swSSO\GlobalPolicy

HKEY\_LOCAL\_MACHINE\SOFTWARE\(Wow6432Node\)swSSO\DomainPolicy (disponible à partir de la v1.14)

Par défaut, ce sont les GlobalPolicy qui s'appliquent ; si des valeurs sont définies pour le domaine, elles prennent le dessus. Pour cela, il suffit de créer une clé DomainPolicy (au même niveau que la clé GlobalPolicy), puis de créer une sous-clé pour chaque domaine portant comme nom le libellé du domaine et de stocker les paramètres de configuration dans cette sous-clé.

| Nom de la valeur | Type | Défaut | Description |
| --- | --- | --- | --- |
| CheckIniIntegrity | DWORD | 0 | Vérifie (1) / Ne vérifie pas (0) si le fichier .ini a été modifié par l'utilisateur directement sans passer par l'IHM de swSSO.  **Disponible à partir de la v1.03.** |
| 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…"  Remarque : si cette valeur est positionnée à 0 (interdit), l’utilisateur ne pourra pas publier de configuration même s’il a internetManualPutConfig=YES dans son fichier .ini.  **Disponible à partir de la v0.89.** |
| MasterPwdExpiration | DWORD | -1 | Avec la valeur -1, le mot de passe maître n'est plus redemandé pendant 5 minutes après sa saisie. Cette valeur est configurable par l'utilisateur dans la fenêtre Options : il peut choisir une valeur entre 0 (le mot de passe est demandé systématiquement) et 60 (le mot de passe n'est pas redemandé pendant 60 minutes).  L'administrateur peut définir une valeur par défaut en base de registre grâce à cette clé. L'utilisateur garde malgré tout la possibilité de modifier la valeur dans les options, mais uniquement avec une valeur inférieure.  **Disponible à partir de la v1.14.** |
| 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 v0.86**. |
| 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 v0.99.** |
| OpenConfigFile | DWORD | 1 | Affiche (1) / masque (0) le bouton Ouvrir dans l'onglet "A propos" |
| PasswordChoiceLevel | DWORD | 3 | Définit le mode d’authentification :  3 : mot de passe maître. Au lancement, une fenêtre de bienvenue est affichée, invitant l’utilisateur à définir un mot de passe maître.  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 : il est possible à tout moment de passer de l’un à l’autre des modes en modifiant cette valeur. (**valeur disponible à partir de la 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 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 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 v0.92, modifiée en v0.99** (cf. ShowAddThisApp) |
| 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 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 v0.99.** |
| ShowAskThisAppMenu | DWORD | 0 | Montre (1) / cache (0) l'item « Demander l’ajout de cette application » dans le menu clic-droit de l'icône swSSO.  **Disponible à partir de la v1.14.** |
| ShowAutoLockOption | DWORD | 1 | Montre (1) / cache (0) l'item « Détecter les erreurs de connexion à cette application » dans la fenêtre de gestion des sites et applications.  **Disponible à partir de la v1.04.** |
| ShowBrowsers | DWORD | 1 | Affiche (1) / masque (0) l'onglet Options dans la fenêtre de propriétés.  **Disponible à partir de la v1.04.** |
| 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 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 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 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 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 v0.97.** |
| ShowHelpMenu | DWORD | 0 | Affiche (1) / masque (0) le menu Aide.  **Disponible à partir de la v1.13.** |
| 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 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 v0.97.** |
| ShowOptions | DWORD | 1 | Affiche (1) / masque (0) l'onglet Options dans la fenêtre de propriétés. |
| ShowPasswordGroup | DWORD | 2 | Affiche / masque le champ groupe de mot de passe dans l'onglet "Champs complémentaires" de la fenêtre de gestion des site:  0 = champ masqué  1 = champ affiché  2 = champ affiché ou masqué en fonction de la case à cocher "Sur demande, mettre mes informations de configuration à disposition des autres utilisateurs" dans la fenêtre Options  **Disponible à partir de la v1.08.** |
| 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. |
| ShowPutInSafeBoxMenu | DWORD | 1 | Affiche (1) / masque (0) le menu « Mettre un compte au coffre » dans la fenêtre de gestion des sites et applications.  **Disponible à partir de la v1.14.** |
| ShowQuitMenu | DWORD | 1 | Affiche (1) / masque (0) le menu Quitter.  **Disponible à partir de la v1.08.** |
| ShowRefreshRightsMenu | DWORD | 0 | Montre (1) / cache (0) l'item « Rafaîchir mes droits » dans le menu clic-droit de l'icône swSSO.  **Disponible à partir de la v1.06.** |
| 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 v0.97.** |
| ShowSystrayIcon | DWORD | 1 | Montre (1) / cache (0) l’icône swSSO dans le systray.  **Disponible à partir de la v1.15.** |
| ShowUploadWithIdPwdMenu | DWORD | 0 | Montre (1) / cache (0) l'item « Publier avec identifiant et mot de passe » dans le menu clic-droit de la fenêtre de gestion des sites et applications.  **Disponible à partir de la v1.03.**  **Modifié en v1.06 :**  ce paramètre n'affiche plus le menu « Publier avec identifiant et mot de passe », mais à partir du moment où sa valeur est à 1, le ou les identifiants et/ou mot de passe sont automatiquement publiés dès lors qu'ils sont renseignés dans l'IHM. |
| 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 v0.86.** |
| ViewConfigFilePath | DWORD | 1 | Affiche (1) / masque (0) le chemin complet du fichier swsso.ini dans l'onglet "A propos" |
| ViewServerInfos | DWORD | 1 | Affiche (1) / masque (0) l’URL du serveur de configuration swSSO dans l'onglet "A propos"  **Disponible à partir de la v1.14.** |

## Clé PwdGroupColors

HKEY\_LOCAL\_MACHINE\SOFTWARE\(Wow6432Node\)swSSO\PwdGroupColors

Pour permettre de les identifier facilement, les applications appartenant au même groupe de mot de passe sont désormais colorées dans la fenêtre de gestion des sites et applications. Des couleurs par défaut sont définies pour les groupes 0 à 4 :



Ces couleurs peuvent être modifiées et complétées pour des groupes supplémentaires par configuration en base de registre sous la clé PwdGroupColors (même principe que pour les fenêtres exclues, la numérotation commence forcément à 0 et l'énumération des valeurs s'arrête au premier trou dans la liste) :

|  |  |  |
| --- | --- | --- |
| Nom de la valeur | Type | Description |
| 0 | Chaîne | Couleur du 1er groupe de mot de passe (format : R,G,B) |
| … | … | … |
| 24 | Chaîne | Couleur du 25ème groupe de mot de passe (format : R,G,B) |

Exemple :



## 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 |

Les événements tracés par le module de chaînage de mot de passe **swSSOCM.dll** sont les suivants :

| Identifiant | Type | Message |
| --- | --- | --- |
| 1 | Erreur | Service swSSOSVC not started |

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](file:///\\\\swsso\\swsso.exe)" (remplacer par le chemin complet d'installation de swsso.exe)

"TypesSupported"=dword:00000007

## Statistiques

swSSO peut générer des statistiques :

Soit dans un fichier de statistiques 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

Soit en les remontant en base de données, dans la table stats. Pour bénéficier de cette nouvelle fonctionnalité, il faut installer la version 5.6 (pour les utilisateurs en webservice5.php) ou la version 6.4 (pour les utilisateurs en webservice6.php), créer la nouvelle table de statistiques (avec le script creation\_table\_stats.sql) et configurer les deux variables suivantes dans le fichier variables.php :   
\_SEPARATOR\_ : séparateur pour les exports CSV   
\_STATOVERWRITE\_ : TRUE (chaque remontée de stat écrase la ligne précédemment remontée pour cet utilisateur) ou FALSE (les lignes sont ajoutées sans gestion d'unicité – la table grossit indéfiniment)   
Les statistiques sont ensuite exportables au format CSV :   
- Soit en cliquant sur le lien « Télécharger les statistiques » dans l'IHM d'admin   
- Soit en appelant l'URL http://<serveur>/export.php?data=stats

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 | 0 : pas de statistiques générées  1 : statistiques générées dans un fichier **(disponible à partir de la v0.99)**  2 : statistiques remontées en base de données (disponible à partir de la v1.07)  3 : les deux ! |

## Configuration d'une boite mail pour demander l'ajout de configurations

Lorsque l'utilisateur demande à ajouter une configuration et que celle-ci n'est pas présente en base de données, un message configurable en base de registre s'affiche (clé EnterpriseOptions\ErrorMessageConfigNotFound). Ce message peut maintenant être enrichi d'un nom de BAL à contacter pour demander l'ajout de la configuration.



Ce nom ainsi que des éléments de formatage du mail sont paramétrables en base de registre sous la clé : **HKEY\_LOCAL\_MACHINE\SOFTWARE\(Wow6432Node\)swSSO\EnterpriseOptions**

| Nom de la valeur | Type | Défaut | Description |
| --- | --- | --- | --- |
| ConfigNotFoundMailTo | Chaine | [swSSO] | Adresse mail de la BAL |
| ConfigNotFoundMailSubject | Chaine | Vide | Objet du mail |
| ConfigNotFoundMailBody | Chaine | Vide | Contenu du mail |

Pour insérer des sauts de ligne dans le contenu du mail, utiliser %0D. Les éléments techniques (titre et URL) permettant d'identifier la configuration demandée par l'utilisateur sont automatiquement ajoutés en fin de mail.

Exemple :

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\swSSO\EnterpriseOptions]

"ConfigNotFoundMailTo"="destinataire@mail.com"

"ConfigNotFoundMailSubject"="[swSSO] Ajout d'une nouvelle configuration"

"ConfigNotFoundMailBody"="Bonjour,%0D%0DMerci de bien vouloir ajouter la configuration pour l'application suivante :%0D"



# Client d'administration

## Principe

Depuis la version 1.07, il est possible de réaliser l'ensemble des opérations d'administration depuis le client swSSO lancé en mode « administrateur » :

|  |  |  |
| --- | --- | --- |
| Opération | Version 1.06- | Version 1.07+ |
| Ajout d'une configuration | Client | Client |
| Modification d'une configuration | Client | Client |
| Suppression d'une configuration | Serveur | Client ou serveur |
| Ajout d'un domaine | Serveur | Client ou serveur |
| Renommage d'un domaine | Non disponible | Client |
| Suppression d'un domaine | Serveur | Client ou serveur |
| Ajout d'une catégorie | Client | Client |
| Renommage d'une catégorie | Client | Client |
| Suppression d'une catégorie | Serveur | Client ou serveur |

## Lancement du client d'administration

Le client d'administration peut être lancé en parallèle du client de SSO standard avec la ligne de commande suivante :

swsso /admin

Le lancement diffère en fonction de la configuration swSSO :

En mode mot de passe maître, le mot de passe maître doit être saisi (comme pour le lancement du client classique) : ce mot de passe est vérifié auprès du serveur de configuration. Si le mot de passe est incorrect ou si le compte de l’administrateur est verrouillé sur le serveur, un message d’erreur s’affiche : l’administrateur peut malgré tout travailler en local, mais ne pourra pas publier de configurations sur le serveur. Lorsque l’administrateur change son mot de passe maître, le changement de mot de passe est propagé sur le serveur.

En mode mot de passe synchronisé Windows, aucune saisie de mot de passe n'est nécessaire : c’est le mot de passe Windows qui est utilisé pour ouvrir une session sur le serveur de configuration. Si le mot de passe Windows est désynchronisé avec le serveur ou si le compte de l’administrateur est verrouillé sur le serveur, un message d’erreur s’affiche : l’administrateur peut malgré tout travailler en local, mais ne pourra pas publier de configurations sur le serveur. Lorsque l’administrateur change son mot de passe Windows, le changement de mot de passe est propagé sur le serveur.

En mode sans mot de passe, un mot de passe administrateur doit être défini au 1er lancement :



Il sera demandé à chaque lancement ultérieur :



Ce mot de passe peut être réinitialisé via l'IHM serveur :



Lorsqu'il est lancé avec le paramètre /admin, le client swSSO :

N’énumère pas les fenêtres, ne réalise pas de SSO ;

Affiche un bandeau rouge en haut de la fenêtre de gestion des sites et applications pour le distinguer du client standard. Ce bandeau présente des informations non directement visibles par les utilisateurs, notamment les identifiants des configurations, catégories et domaines :

L’icône swSSO dans la zone de notification est sur fond rouge au lieu de bleu.

## Configuration du client d'administration

Les clés de registre permettant de configurer le client d'administration sont les mêmes que celles permettant de configurer le client standard, mais sont placées dans une clé différente :

HKLM\SOFTWARE\swSSOAdmin

# Supervision et exploitation du serveur

## 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).

## 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).
* **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.
* **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 »).
* **Télécharger les statistiques :** téléchargement au format CSV du fichier de statistiques (voir §3.7).
* **Test isalive** : test de vie du serveur de configuration (voir §5.1).
* **Déconnexion :** fermeture de la session administrateur sur le serveur.

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.
* **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\_).

## Restrictions 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/admin.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

## Logs

Vous pouvez, à l’aide des paramètres du fichier variables.php, définir si vous souhaitez produire des logs d’appels du serveur de configuration :

/\*--------------------------------------------------------------------------

OPTIONS

---------------------------------------------------------------------------\*/

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

## 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;

# Synchronisation avec le mot de passe Windows

## 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.

## Passage 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.

## Passage du mode synchronisé Windows au mode mot de passe maître

Sur une installation existante, il suffit de configurer la clé de registre présentée au paragraphe précédent à la valeur 3 : au prochain lancement de swSSO, l'utilisateur devra saisir son mot de passe Windows qui deviendra son mot de passe maître. Il pourra bien sûr le modifier s'il souhaite utiliser un autre mot de passe. Toutes les informations relatives au mot de passe Windows sont supprimées du fichier swsso.ini.

## Utilisation du mot de passe Windows comme mot de passe secondaire

Pour utiliser le mot de passe Windows comme mot de passe secondaire, il suffit de renseigner %ADPASSWORD% dans le champ mot de passe de la configuration de l'application. Au moment de renseigner le formulaire d'authentification de l'application, swSSO utilisera le mot de passe Windows pour remplir le champ mot de passe :



Si vous souhaitez distribuer automatiquement des configurations contenant ce champ mot de passe pré-renseigné avec cette valeur, vous devez impérativement utiliser le serveur avec les tables chiffrées et avoir configuré la valeur GlobalPolicy\ShowUploadWithIdPwdMenu à 1.

## Synchronisation d'un groupe de mots de passe avec le mot de passe Windows

swSSO peut être configuré pour appliquer le mot de passe Windows sur un ensemble d'applications. Pour cela, swSSO vérifie la présence de l'utilisateur dans une OU définie en base de registre (optionnel), puis applique le mot de passe d'ouverture de session Windows dans toutes les entrées du groupe mot de passe défini en base de registre, en excluant les applications dont l'identifiant ne correspond pas à l'identifiant Windows. Cette opération est faite à chaque lancement de swSSO et à chaque fois que swSSO est notifié d'un changement de mot de passe Windows.   
Ce comportement ce configure dans la clé :   
**HKEY\_LOCAL\_MACHINE\SOFTWARE\(Wow6432Node\)swSSO\EnterpriseOptions**

| Nom de la valeur | Type | Défaut | Description |
| --- | --- | --- | --- |
| SyncSecondaryPasswordActive | DWORD | 0 | Active (1) / désactive (0) la mise à jour des mots de passe secondaires |
| SyncSecondaryPasswordGroup | DWORD | -1 | Groupe d'applications sur lequel la modification s'applique |
| SyncSecondaryPasswordOU | Chaîne | Vide | OU dans laquelle doit se trouver l'utilisateur pour que la modification de mot de passe s'applique. Si la clé est vide ou non définie, la modification de mot de passe s'applique quelle que soit l'OU dans laquelle se trouve l'utilisateur |

# Procédure de secours manuelle

## 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.



## 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.



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

## 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.

## 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.

## 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"



# Procédure de secours automatique

## Avertissement

Ce chapitre concerne uniquement l'utilisation de swSSO en mode mot de passe synchronisé (PasswordChoiceLevel=4). En mode mot de passe maître, seule la procédure de secours manuelle est disponible.

## Principe

Une désynchronisation de mot de passe peut se produire lorsque le mot de passe Windows de l'utilisateur est changé ailleurs que sur son poste de travail, par exemple :

Par l'utilisateur lui-même sur un autre poste de travail (sauf swSSO est installé sur cet autre poste de travail et partage le même fichier swsso.ini) ;

Par un opérateur du support qui réinitialise le mot de passe de l'utilisateur sur la console Active Directory ;

Par une synchronisation de mot de passe provenant d'un autre annuaire.

Lorsque le client swSSO détecte une désynchronisation de mot de passe, il invoque le web service de resynchronisation en lui fournissant un challenge. En retour, il reçoit une réponse qui lui permet de réinitialiser le mot de passe maître swSSO avec le mot de passe Windows de l’utilisateur et de transchiffrer les mots de passe secondaires (déchiffrement avec la clé correspondant à l’ancien mot de passe Windows et rechiffrement avec la clé correspondant au nouveau mot de passe Windows). Techniquement, c'est simplement une automatisation de la procédure de secours, dans laquelle un web service remplace l'opérateur du support et l'application swSSORecover.exe.

Si le web service ne répond pas (serveur indisponible, timeout) ou retourne une erreur, le client swSSO bascule sur la procédure de secours manuelle et affiche le challenge à l’utilisateur, sauf si vous avez configuré la clé RecoveryWebserviceManualBackup à 0.

## Installation du web service

**1) Installation du service swSSORecoverSvc.exe**

Créer un compte utilisateur local qui servira à faire tourner le service système swSSORecoverSvc. Dans la suite de la procédure, les balisent suivantes doivent être remplacées par les informations concernant le compte de service :

{IMPERSONNATION\_DOMAINE} : domaine ou nom du serveur si compte local ;

{IMPERSONNATION\_UTILISATEUR} : identifiant du compte ;

{IMPERSONNATION\_MDP} : mot de passe du compte.

Ouvrir une invite de commande en tant qu'administrateur

Lancer la commande swSSORecoverSvc.exe install



Ouvrir services.msc et sélectionner le service nommé « swSSORecover service »



Clic-droit propriétés, onglet Connexion :



Cocher « Ce compte » et saisir :

Dans ce compte{IMPERSONNATION\_DOMAINE}\{IMPERSONNATION\_UTILISATEUR}

Dans mot de passe et confirmer le mot de passe : {IMPERSONNATION\_MDP}

Cliquer sur OK pour fermer les propriétés du service

Démarrer le service

**2) Installation et configuration de la DLL swSSORecoverDll.dll**

Copier le fichier swSSORecoverDll.dll dans le dossier de votre choix (attention à choisir la bonne version de la DLL – 32 ou 64 bits – en fonction du système d'exploitation du serveur sur lequel elle est installée) ;

Ajouter ce dossier à la variable d'environnement PATH ;

Copier le keystore préalablement créé comme indiqué dans le chapitre consacré à la procédure de secours manuelle dans le dossier de votre choix. Remarque : en cas de renouvellement de clé, ne pas oublier de copier le nouveau keystore.

Copier le fichier de configuration swSSORecoverDll.ini dans le même dossier que la DLL.

Son contenu est le suivant :

[Keystore]

Filename=

Password=

| Paramètre | Description |
| --- | --- |
| Filename | Chemin complet d’accès au fichier keystore |
| Password | Mot de passe du keystore. Le mot de passe est chiffré, voir procédure ci-dessous. |

Copier les fichiers swSSOPwdProtect.dll et EncryptPassword.ps1 dans un même dossier sur le serveur.

Exécuter les lignes de commandes suivantes depuis une invite de commande :

powershell –executionpolicy unrestricted

.\EncryptPassword.ps1 <mot de passe du keystore>

En sortie, un fichier password.txt contenant le mot de passe chiffré est généré. Si le fichier password.txt existe déjà, il est écrasé.

Copier le contenu du fichier password.txt dans la valeur Password du fichier swSSORecoverDll.ini. Conserver le fichier password.txt pour l'étape suivante.

**3) Installation et configuration du web service**

Le web service est fourni à titre d'exemple d'utilisation de la dll swSSORecoverDll.dll.

Pour l'utiliser, il faut déposer le dossier complet swSSORecoverWS sur un serveur IIS avec le framework .NET 4.5. Le site web doit être impérativement configuré en authentification intégrée Windows, afin de garantir l'identité de l'utilisateur appelant.

La configuration du web service se fait au travers du fichier web.config :

<appSettings>

<add key="domain" value="{IMPERSONNATION\_DOMAINE}"/>

<add key="user" value="{IMPERSONNATION\_UTILISATEUR}"/>

<add key="password" value="{IMPERSONNATION\_MDP}"/>

<add key="debug" value="0"/>

<add key="dllpath" value="{Dossier contenant swSSORecoverDll.dll}"/>

</appSettings>

| Nom de la clé | Description |
| --- | --- |
| domain | Voir description de {IMPERSONNATION\_DOMAINE} plus haut |
| user | Voir description de {IMPERSONNATION\_UTILISATEUR} plus haut |
| password | Voir description de {IMPERSONNATION\_MDP} plus haut.  Valeur à reprendre dans le fichier password.txt généré précédemment |
| debug | 0 (mode sans traces) ou 1 (mode avec traces). Les traces sont envoyées dans le flux de la réponse. |
| dllpath | Dossier contenant la dll swSSORecoverDll.dll  Exemple : d:\swsso\bin |

A ce stade, vous pouvez supprimer le fichier password.txt.

## Configuration du client

L'appel au web service de resynchronisation se configure sur le client dans la clé :   
**HKEY\_LOCAL\_MACHINE\SOFTWARE\(Wow6432Node\)swSSO\EnterpriseOptions**

| Nom de la valeur | Type | Défaut | Description |
| --- | --- | --- | --- |
| RecoveryWebserviceActive | DWORD | 0 | Active (1) / désactive (0) l'appel au web service.  **Disponible à partir de la v1.08**. |
| RecoveryWebserviceHTTPS | DWORD | 0 | 0=HTTP / 1=HTTPS  **Disponible à partir de la v1.08**. |
| RecoveryWebserviceManual Backup | DWORD | 1 | Bascule (1) / ne bascule pas (0) vers la procédure manuelle de recouvrement en cas d'échec d'appel du web service  **Disponible à partir de la v1.08**. |
| RecoveryWebserviceNbTry | DWORD | 1 | Nombre de tentatives d'appel au web service  **Disponible à partir de la v1.10**. |
| RecoveryWebservicePort | DWORD | 80 | Port pour l'accès au web service  **Disponible à partir de la v1.08**. |
| RecoveryWebserviceServer | Chaîne | - | FQDN du serveur  (ex : monserveur.mondomaine)  **Disponible à partir de la v1.08**. |
| RecoveryWebserviceTimeout | DWORD | 10 | Temps d'attente de la réponse du web service. Si temps dépassé, bascule vers la procédure manuelle de challenge/response.  **Disponible à partir de la v1.08**. |
| RecoveryWebserviceURL | Chaîne | - | URL d'appel du service  (ex : /swsso/resync.ea)  **Disponible à partir de la v1.08**. |
| RecoveryWebserviceWaitBeforeRetry | DWORD | 1000 | Temps d'attente entre deux tentatives d'appel du web service (en millisecondes)  **Disponible à partir de la v1.10.** |

## Test du web service

Faire une copie de sauvegarde de votre fichier swsso.ini ou utiliser un fichier de test ;

Ouvrir le fichier swsso.ini et repérer la clé CheckSynchro dans la section swSSO ;

Modifier la valeur de la clé CheckSynchro, par exemple en remplaçant les 4 derniers caractères par 0000 ;

Lancer swSSO : si la fenêtre de challenge apparaît au bout de quelques secondes, c'est que l'appel au web service de resynchronisation a échoué. Dans le cas contraire, la resynchronisation a fonctionné.

## Configuration des traces de swSSORecoverDll

Depuis la version 1.10, la version release et la version debug de swSSORecoverDll produisent des traces, dont la configuration se fait désormais dans le fichier swSSORecoverDll.ini (et non plus en base de registre), à placer dans le même dossier que la dll.

Exemple de configuration dans le fichier swSSORecoverDll.ini :

[Logs]   
Filename=c:\temp\swssotracerecoverdll.txt   
Filesize=100   
Level=5

|  |  |  |  |
| --- | --- | --- | --- |
| Nom de la valeur | Type | Défaut | Description |
| Filename | Chaîne | - | Chemin complet du fichier trace |
| Filesize | DWORD | 20 | Taille max. en Mo (fichier tournant) |
| Level | DWORD | - | 0 ou non défini : pas de traces  1 : erreurs seulement  3 : 1 + entrée/sorties de fonctions  4 : 3 + informations  5 : 4 + debug |

## Gestion des erreurs en cours de transchiffrement

Lorsque le web service de resynchronisation a bien fonctionné et retourné à swSSO les éléments nécessaire à la suite de la procédure de secours, mais qu'une entrée du .ini est corrompue et/ou qu’elle ne peut pas être transchiffrée, les autres entrées sont traitées et un message en fin d'opération indique le nombre d'entrées en erreur.

Un fichier de log portant le nom du .ini mais avec l'extension .err est créé dans le même dossier et indique précisément les erreurs de tranchiffrement (configurations concernées et champ en erreur : identifiant et/ou mot de passe).

Par ailleurs, les configurations en erreur sont marquées d'un rond noir dans la fenêtre de gestion des sites et applications. Si l'utilisateur renseigne un identifiant ou un mot de passe pour une configuration en erreur, elle reprend son statut précédent (vert pour activée, rouge pour désactivée).

# 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 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 (la combinaison de touches permettant de faire le collage est configurable, voir plus loin) :



1. 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 copier ce nouveau mot de passe et le coller facilement dans les champs de saisie 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 :



1. 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)

La configuration de la combinaison de touches et du message associés est obligatoire. Elle se fait sous la clé HKLM\SOFTWARE\swSSO\HotKey

| Nom de la valeur | Type | Défaut | Description |
| --- | --- | --- | --- |
| PastePwd\_Alt | DWORD | - | 1 si la combinaison de touches contient ALT |
| PastePwd\_Ctrl | DWORD | - | 1 si la combinaison de touches contient CTRL |
| PastePwd\_Key | DWORD | - | Touche (voir liste plus loin) |
| PastePwd\_Shift | DWORD | - | 1 si la combinaison de touches contient SHIFT |
| PastePwd\_Text | Chaine | - | Texte affiché dans les fenêtres pour présenter la combinaison de touches.  Exemple : CTRL + M |
| PastePwd\_Win | DWORD | - | 1 si la combinaison de touches contient la touche Windows |

Les codes de touche à utiliser pour la valeur PastePwd\_Key sont les « virtual key codes » décrits ici :

<http://msdn.microsoft.com/en-us/library/windows/desktop/dd375731(v=vs.85).aspx>

# Traces

Les traces peuvent être utiles pour investiguer les problèmes que vous rencontreriez avec swSSO. A partir de la version 1.11, il n'y a plus qu'une seule et unique version de chaque module, la version debug des modules n'est plus publiée.

Les traces sont activables par configuration en base de registre module par module (à l'exception du module swSSORecoverDll pour lequel la configuration des traces se fait dans le fichier swSSORecoverDll.ini comme décrit au §8.6).

Le tableau ci-dessous indique le nom de la clé à créer pour configurer les traces de chaque modules, sous la clé **HKEY\_LOCAL\_MACHINE\SOFTWARE\(Wow6432Node\)swSSO**

|  |  |
| --- | --- |
| Module | Clé |
| swSSO | Trace |
| swSSOCM | TraceCM |
| swSSOGenKey | TraceGenKey |
| swSSOHotKey | TraceHotKey |
| swSSOMigration | TraceMigration |
| swSSORecover | TraceRecover |
| swSSORecoverSvc | TraceRecoverSvc |
| swSSOSVC | TraceSVC |

Dans chaque clé, créer les valeurs suivantes. Les valeurs FileName et Level sont obligatoires, si elles ne sont pas définies aucune trace ne sera générée pour ce module.

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