



swSSO v0.95
Guide d'administration

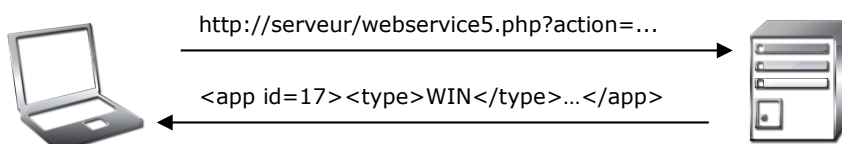
Contenu du document

1. Installation.....	3
1.1. Principe général de fonctionnement.....	3
1.2. Stratégie de déploiement.....	3
1.3. Matrice de compatibilité client / serveur.....	3
1.4. Déploiement du client swSSO.....	4
1.5. Fichier de configuration swsso.ini – section [swSSO].....	4
1.6. Fichier d’aide en ligne.....	6
1.7. Mise en place d’un serveur de configuration en interne.....	7
2. Scénario collaboratif, faiblement ou fortement administré.....	8
2.1. Introduction.....	8
2.2. Scénario collaboratif.....	8
2.3. Scénario faiblement administré.....	9
2.4. Scénario fortement administré.....	9
2.5. Informations sur la gestion des configurations.....	9
3. Configuration du client swSSO (base de registre).....	11
3.1. Adresse du serveur et options de synchronisation client-serveur.....	11
3.2. Exclusion de fenêtres	13
3.3. Politique de mot de passe.....	13
3.4. Bridage de l’interface graphique de configuration.....	14
3.5. Personnalisation des messages d’erreur.....	16
3.6. Logs.....	17
3.7. Traces.....	18
4. Supervision et exploitation du serveur.....	19
4.1. Supervision.....	19
4.2. Exploitation.....	19
4.3. Restriction d’accès à l’IHM du serveur de configuration.....	21
4.4. Logs et statistiques.....	21
4.5. Chiffrement des données sensibles en base	22

1. Installation

1.1. Principe général de fonctionnement

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



1.2. Stratégie de déploiement

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

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

Remarque : l'utilisation du serveur de configuration public est fortement déconseillée, la confidentialité, l'intégrité et la disponibilité des informations hébergées sur ce serveur ne pouvant aucunement être garantie.

1.3. Matrice de compatibilité client / serveur

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

Version client (swsso.exe)	Version serveur	Commentaire
0.88	webservice2.php	Mode de fonctionnement nominal
0.89 et 0.90	webservice3.php	Mode de fonctionnement nominal
	webservice2.php	Dans ce cas les évolutions #77 (simulation de frappe clavier) et #96 (centralisation des noms des configurations) ne sont pas disponibles
0.91 à 0.93	webservice4.php	Mode de fonctionnement nominal
0.94+	Webservice5.php	Mode de fonctionnement nominal

1.4. Déploiement du client swSSO

Vous pouvez déployer :

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

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

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

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

Valeurs pouvant être prédéfinies pour le déploiement :

Nom de la valeur	Défaut	Description
sessionLock	NO	YES = verrouille swSSO lorsque la session Windows est verrouillée.
internetCheckVersion	YES	YES = vérifie au lancement si une nouvelle version est disponible.
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.

Nom de la valeur	Défaut	Description
x,y,cx,cy	-	Position (x,y) et dimension (cx,cy) de la fenêtre de gestion des applications et sites. Par défaut la fenêtre est affichée en base à droite de l'écran et mesure 667x480 pixels.
x2,y2,cx2,cy2	-	Position (x2,y2) et dimension (cx2,cy2) de la fenêtre de lancement d'application. Par défaut la fenêtre est affichée en base à droite de l'écran et mesure 384x549 pixels. Disponible à partir de la version v0.91.
LaunchTopMost	NO	YES = la fenêtre de lancement d'applications s'affiche au premier plan et ne peut pas être recouverte par une autre fenêtre. Disponible à partir de la version v0.91.
parseWindowsOnStart	YES	NO = les fenêtres déjà ouvertes au moment du lancement de swSSO ne seront jamais traitées Disponible à partir de la version v0.93.
domainId	1	Identifiant du domaine de rattachement de l'utilisateur Disponible à partir de la version v0.94.
DomainLabel	Commun	Libellé du domaine de rattachement de l'utilisateur Disponible à partir de la version v0.94.

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

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

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

Nom de la valeur	Description
version	Version du fichier de configuration. Valeur inscrite automatiquement à la création du fichier. Ne pas modifier cette valeur.
pwdProtection	ENCRYPTED : les mots de passe sont chiffrés par une clé dérivant du mot de passe maître de l'utilisateur. ENCODED : les mots de passe sont simplement brouillés : ils n'apparaissent pas en clair dans le fichier, mais ne sont pas protégés (tout utilisateur récupérant le fichier swsso.ini peut visualiser les mots de passe). NONE : les mots de passe sont en clairs dans le .ini.
pwdValue	Mot de passe maître.

Nom de la valeur	Description
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 lesquels 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. Disponible 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 passe.
lastConfigUpdate	Date de dernière vérification des configurations sur le serveur (format : AAAAMMJJHHMMSS)

1.6. Fichier d'aide en ligne

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

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

- swSSO.chm,
- swSSO v0.95 - Manuel utilisateur.pdf,
- swSSO.pdf,
- La page « manuel utilisateur » du site www.swsso.fr.

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

Pré-requis :

- PHP5
- MySQL5

Installation du service Web :

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

Création de la base de données :

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

Création des tables :

- Créer les tables à l'aide des scripts : creation_table_categ.sql, creation_table_config.sql, creation_table_domains.sql, creation_table_logs.sql et creation_table_stats.sql.
Remarque : la création des tables de logs et de statistiques est optionnelle. Si vous ne souhaitez pas les créer, vous devez cependant modifier la configuration dans le fichier variable.php (voir §4.4).

Attention, si vous souhaitez chiffrer les valeurs sensibles en base de données, vous devez utiliser le script creation_table_config_chiffrement.sql au lieu de creation_table_config.sql. Référez-vous au §4.5 pour plus d'informations.

- Modifier le fichier variables.php pour spécifier les éléments suivants :

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

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

Vérification de l'installation :

- Lancer la requête suivante depuis un navigateur :

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

L'affichage doit être le suivant :

```
ALIVE
```

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

2. Scénario collaboratif, faiblement ou fortement administré

2.1. Introduction

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

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

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

Selon leur nature, les paramètres doivent être définis :

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

2.2. Scénario collaboratif

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

Pour implémenter ce scénario, vous devez :

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

2.3. Scénario faiblement administré

Pour implémenter ce scénario, vous devez :

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

2.4. Scénario fortement administré

Pour implémenter ce scénario, vous devez :

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

2.5. Informations sur la gestion des configurations

Applications

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

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

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

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

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

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

Catégories

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

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

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

Domaines

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

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

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

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

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

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

3. Configuration du client swSSO (base de registre)

3.1. Adresse du serveur et options de synchronisation client-serveur

HKEY_LOCAL_MACHINE\SOFTWARE\swSSO\EnterpriseOptions

Nom de la valeur	Type	Défaut	Description
ServerAddress	Chaîne	www.swsso.fr	Adresse du serveur de configuration.
WebServiceAddress	Chaîne	/server/ webservice5.php	Chemin relatif du webservice de configuration
CategoryManagement	DWORD	0	Active (1) / Désactive (0) la gestion des catégories sur le serveur. Si activé, les identifiants et libellés des catégories sont stockés sur le serveur : ainsi, les configurations récupérées par les utilisateurs sont stockées dans la catégorie définie lors de la création de la configuration. Disponible à partir de la version v0.91.
GetAllConfigsAtFirstStart	DWORD	0	Propose (1) / ne propose pas (0) à l'utilisateur de récupérer toutes les configurations disponibles sur le serveur au premier lancement de swSSO. Remarque : si DisplayConfigsNotifications=1, GetAllConfigsAtFirstStart=1 ne propose pas mais impose silencieusement la récupération des configurations. Attention, cette valeur doit être placée à 1 si vous souhaitez que le choix du domaine soit proposé à l'utilisateur au 1er lancement. Disponible à partir de la version v0.91.
GetNewConfigsAtStart	DWORD	0	A chaque lancement de swSSO, récupère (1) / ne récupère pas (0) les nouvelles configurations ajoutées sur le serveur depuis le dernier lancement de swSSO. Disponible à partir de la version v0.91.

Nom de la valeur	Type	Défaut	Description
GetModifiedConfigsAtStart	DWORD	0	A chaque lancement de swSSO, récupère (1) / ne récupère pas (0) les configurations modifiées sur le serveur depuis le dernier lancement de swSSO. Disponible à partir de la version v0.91.
DisableArchivedConfigsAtStart	DWORD	0	A chaque lancement de swSSO, désactive (1) / ne désactive pas (0) les configurations archivées sur le serveur depuis le dernier lancement de swSSO. Disponible à partir de la version v0.91.
AllowManagedConfigsDeletion	DWORD	1	Autorise (1) / interdit (0) la suppression des configurations récupérées depuis le serveur ou uploadées vers le serveur. Disponible à partir de la version v0.91.
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 accède à l'application, une configuration est activée et que le login/mdp n'est pas connu pour cette application, une fenêtre de saisie demande les informations manquantes à l'utilisateur, puis le SSO est réalisé. Disponible à partir de la version v0.91.
DisplayConfigsNotifications	DWORD	1	Affiche (1) / n'affiche pas (0) les messages de notification d'ajout / modification / suppression des configurations au démarrage. Disponible à partir de la version v0.92.

3.2. Exclusion de fenêtres

HKEY_LOCAL_MACHINE\SOFTWARE\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 (10 maximum, numérotés de 0 à 9) à exclure :

Nom de la valeur	Type	Description
0	Chaîne	Titre de la 1 ^{ère} fenêtre à exclure
...
9	Chaîne	Titre de la 10 ^{ème} fenêtre à exclure

3.3. Politique de mot de passe

HKEY_LOCAL_MACHINE\SOFTWARE\swSSO>PasswordPolicy :

Nom de la valeur	Type	Défaut	Description
MinLength	DWORD	0	Nombre minimum de caractères
MinLetters	DWORD	0	Nombre minimum de lettres (a-z / A-Z)
MinNumbers	DWORD	0	Nombre minimum de chiffres (0-9)
MinSpecialChars	DWORD	0	Nombre minimum de caractères spéciaux (tous caractères autres que lettres et chiffres)
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.)
MinUpperCase	DWORD	0	Nombre minimum de minuscules (a-z)
MinLowerCase	DWORD	0	Nombre minimum de majuscules (A-Z)
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.

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

3.4. Bridage de l'interface graphique de configuration

HKEY_LOCAL_MACHINE\SOFTWARE\swSSO\GlobalPolicy :

Nom de la valeur	Type	Défaut	Description
ShowOptions	DWORD	1	Affiche (1) / masque (0) l'onglet Options dans la fenêtre de propriétés.
ViewConfigFilePath	DWORD	1	Affiche (1) / masque (0) le chemin complet du fichier swsso.ini dans l'onglet "A propos"
OpenConfigFile	DWORD	1	Affiche (1) / masque (0) le bouton Ouvrir dans l'onglet "A propos"
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"
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..."

Nom de la valeur	Type	Défaut	Description
ManualPutConfigOption	DWORD	1	Autorise (1) / interdit (0) la modification de l'option "Sur demande, mettre à disposition mes informations de configuration..." Disponible à partir de la version v0.89.
ProxyOption	DWORD	1	Autorise (1) / interdit (0) la modification des paramètres proxy
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.
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.
PasswordChoiceLevel	DWORD	1	Définit les options autorisées dans la fenêtre de bienvenue swSSO (celle qui est affichée au premier lancement) : 1 : tout est autorisé 2 : le choix "mots de passe non chiffrés" est interdit 3 : seul le choix "définir un mot de passe maître" est autorisé (dans ce cas, une fenêtre simplifiée est affichée)
ViewApplicationConfig	DWORD	1	Affiche (1) / masque (0) les onglets "Configuration" et "Champs complémentaires" de la fenêtre "Gestion des sites et applications". Disponible à partir de la version v0.86.
ModifyApplicationConfig	DWORD	1	Autorise (1) / interdit (0) la modification des paramètres affichés dans les onglets "Configuration" et "Champs complémentaires" de la fenêtre "Gestion des sites et applications". Disponible à partir de la version v0.86.
ShowChangeCategIdsMenu	DWORD	1	Montre (1) / cache (0) le menu contextuel « Identifiants et mot de passe » sur les catégories. Ce menu permet de modifier d'un coup un ou plusieurs identifiants et/ou le mot de passe de toutes les applications d'une catégorie. Disponible à partir de la version 0.91.
ShowLaunchAppMenu	DWORD	1	Montre (1) / cache (0) les menus et les champs liés au lancement d'applications depuis swSSO. Cela concerne le menu clic-droit sur l'icône swSSO, le menu contextuel des applications dans la fenêtre « Gestion des sites et applications » ainsi que le champ « Lancement » et le bouton « Parcourir » de cette même fenêtre. Disponible à partir de la version v0.91.

Nom de la valeur	Type	Défaut	Description
ShowAddAppMenu	DWORD	1	Montre (1) / cache (0) le menu « Ajouter cette application ». Disponible à partir de la version v0.92.

3.5. Personnalisation des messages d'erreur

HKEY_LOCAL_MACHINE\SOFTWARE\swSSO\EnterpriseOptions

Nom de la valeur	Type	Défaut	Description
ErrorMessageIniFile	Chaîne	->	Message affiché lorsque la lecture du fichier swsso.ini échoue au démarrage de swSSO. Message par défaut : « 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. Message par défaut : « Impossible de joindre le serveur swSSO. Veuillez vérifier votre configuration proxy (menu Propriétés, onglet Options). »
ErrorMessageConfigNotFound	Chaîne	->	Message affiché lorsque la configuration demandée par l'utilisateur (menu « Ajouter cette application ») n'existe pas sur le serveur. Message par défaut : « La configuration pour ce site n'a pas été trouvée. Voulez-vous la faire manuellement ? » Remarque : si vous personnalisez ce message, les boutons Oui / Non présentés avec le message par défaut sont remplacés par un bouton OK. Le message devient donc simplement informatif.

3.6. Logs

Vous pouvez configurer swSSO pour tracer les événements principaux dans un fichier texte ou dans le journal d'événements de Windows. La liste des événements tracés dans la version actuelle sont :

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 complète du serveur>)
15	Information	Mise a jour des configurations : <X> ajouts, <Y> modifications, <Z> désactivations

La configuration se fait sous la clé :

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.

3.7. Traces

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

HKEY_LOCAL_MACHINE\SOFTWARE\swSSO\Trace

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

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

4. Supervision et exploitation du serveur

4.1. Supervision

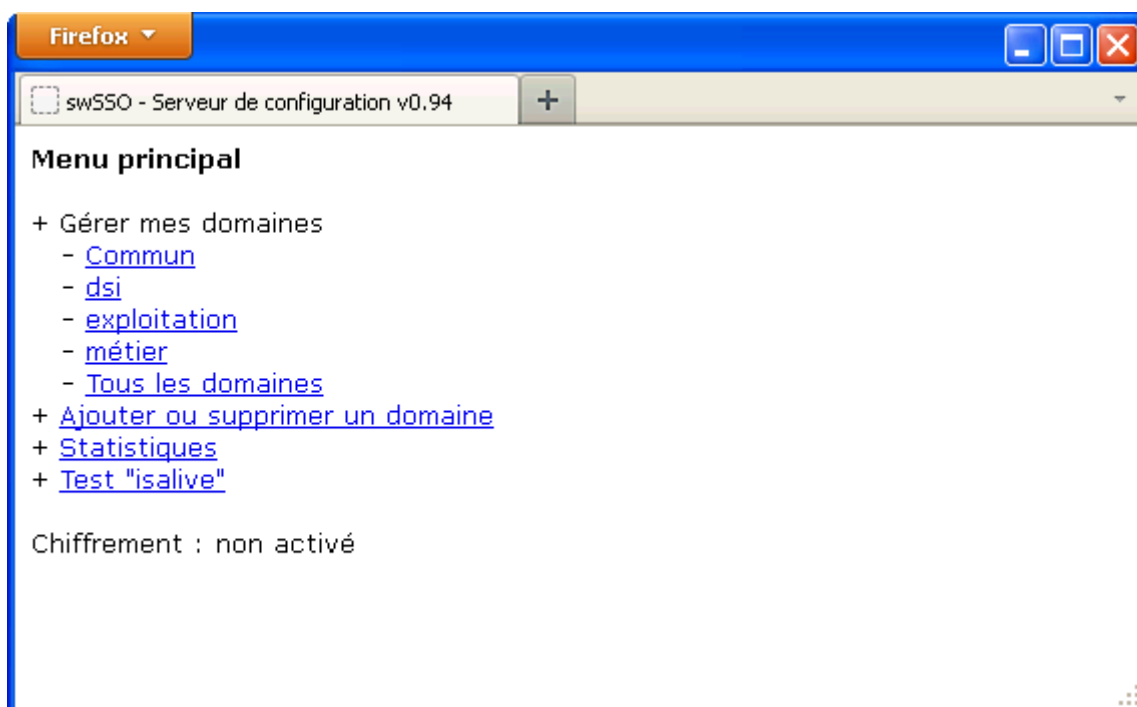
Pour vérifier que le serveur de configuration est opérationnel, il suffit de solliciter le test de vie du serveur avec l'URL suivante :

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

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

4.2. Exploitation

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



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

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



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

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

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

```
/*-----  
OPTIONS  
-----*/  
  
define("_SHOWMENU_", "TRUE"); // TRUE|FALSE (affichage menu autorise / interdit)  
define("_MENUSUFFIX_", "xxx"); // "protection" de l'URL presentant le menu  
define("_READSUFFIX_", "yyy"); // "protection" des URLs permettant la lecture  
                                de la base  
define("_WRITESUFFIX_", "zzz"); // "protection" des URLs permettant la  
                                modification de la base
```

Explication :

- `_SHOWMENU_` : en attribuant la valeur FALSE, vous désactivez l'affichage du menu. Un utilisateur appelant l'URL `http://<adresse sur serveur/webService5.php?action=menu` ne verra plus le menu, mais un message indiquant que le menu n'est pas activé.
- `_MENUSUFFIX_` : protège l'URL menu (voir ci-dessous).
- `_READSUFFIX_` : protège les URLs `showall`, `showold`, `showlogs` et `showcategories` (voir ci-dessous).
- `_WRITESUFFIX_` : protège les URLs `deletelogs`, `archiveconfig`, `deleteconfig` et `deletecateg` (voir ci-dessous).

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

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

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

au lieu de :

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

4.4. Logs et statistiques

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

```
/*-----  
OPTIONS  
-----*/  
  
define("_LOGS_", "TRUE"); // TRUE | FALSE (génère des logs a chaque getConfig)  
define("_STATS_", "TRUE"); // TRUE | FALSE (incrémente un compteur a chaque  
getConfigVersion)
```

4.5. Chiffrement des données sensibles en base

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

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

```
/*-----  
CHIFFREMENT DES COLONNES titre, url, szName et szFullPathName  
-----*/  
define("_ENCRYPT_", "FALSE");          // TRUE | FALSE (chiffre / ne chiffre pas)  
define("_AESPWD_", "my password");    // Mot de passe pour chiffrement
```

Si vous souhaitez activer le chiffrement, vous devez :

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

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

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

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