

L'authentification unique.

L'accès des utilisateurs au système d'information de l'entreprise implique aujourd'hui une authentification préalable à l'accès de quasiment toute ressource informatique de l'entreprise. Cette authentification est rendue nécessaire pour assurer la sécurité des accès et respecter les contraintes réglementaires associées. En contrepartie, l'authentification représente une charge supplémentaire pour les administrateurs du système d'information et pour les utilisateurs.

La signature unique (SSO) est une technologie qui permet d'apporter une réponse concrète et pragmatique à ces problématiques. En terme de sécurité, grâce à la signature unique, un utilisateur n'a plus à mémoriser qu'un seul mot de passe maître (ou code PIN en cas d'authentification forte), ce qui rend donc possible le durcissement de la politique de ce mot de passe unique et les politiques de sécurité applicatives (les utilisateurs n'ont désormais plus à connaître ces mots de passe secondaires).

Bénéfices apportés par le SSO :

- **Renforcement de la sécurité :**

La multiplication des applications de l'entreprise entraîne l'augmentation du nombre des mots de passe que les utilisateurs doivent mémoriser. Les conséquences immédiates sont que les mots de passe sont soit délibérément affaiblis (simples, parfois uniques), ou (inclusif !) notés en clair sur des bloc-notes non sécurisés, où quiconque peut les retrouver... et donc usurper une identité !

- **Conformité avec la réglementation :**

Les réglementations actuelles (HIPAA, Sarbanes-Oxley, Bâle II...) touchent un nombre croissant d'organisations. La traçabilité de qui accède à quoi et quand dans le système d'information devient donc une préoccupation majeure pour les responsables sécurité, non seulement pour répondre à ces normes mais aussi pour se doter d'outils permettant de superviser les accès aux ressources.

- **Source d'économies :**

La perte ou l'oubli de credentials représentent une charge non négligeable pour les équipes de support aux utilisateurs. Le temps passé à cette activité est improductif pour le support qui pourrait se consacrer à des tâches plus constructives, et pour les utilisateurs qui sont bloqués sans pouvoir accéder à leur poste de travail.

- **Amélioration de l'ergonomie :**

Les phases d'authentification, de changements de mots de passe représentent, en temps cumulé, une durée non négligeable. La complexité de ces opérations pousse les utilisateurs à minimiser le nombre de ces phases et à ouvrir simultanément plusieurs applications et les suspendre sans les quitter, ce qui augmente la charge des postes de travail des utilisateurs.

Fonctionnalités de SSOX :

- **Support de tous les types d'applications :**

SSOX gère tous les types d'applications :

- Applications Web avec Internet Explorer et Firefox : la configuration est réalisée une seule fois, indépendamment du navigateur ;
- Applications Windows, quel que soit l'environnement de développement utilisé ;

- Applications Java : intégration avec les machines virtuelles Java ;
- Support des Applets Java, Flex ou Flash dans les navigateurs ;
- Support des émulateurs de terminaux d'accès aux grands systèmes (MVS, AS400...) via les HLL API ;
- Support de *putty*, application commune d'accès sécurisé aux systèmes Unix ;
- Accès en environnement distant (Systancia, Citrix, TSE) pour tous les types d'applications cités ci-dessus.

La performance d'un moteur SSO se mesure à sa capacité à intégrer les applications. Fort de ses 10 ans d'expérience dans le domaine, le moteur SSO de Avencis est capable de prendre en compte n'importe quel type d'application, de manière simple, robuste et fiable.

- **Solution non intrusive :**

Les applications ne sont pas modifiées ce qui permet, d'une part, d'éliminer les coûts d'intégration spécifique et, d'autre part, de déployer le SSO progressivement. La prise en compte des applications est réalisée graphiquement, de manière simple et intuitive.

- **Cinématiques complètes :**

SSOX gère toutes les cinématiques de connexion :

- Authentification,
- Echec d'authentification,
- Changement de mot de passe,

- Echec de changement de mot de passe,
 - Changement de mot de passe forcé à la première connexion,
 - Gestion intelligente des échecs de connexion (ex. : Lotus Notes)...
- Le moteur SSO est capable de gérer la durée de validité de mots de passe applicatifs quand l'application ne dispose pas de sa propre politique de sécurité.

- **Politiques avancées de mots de passe :**

SSOX gère des politiques de mots de passe pour chaque application. Lors du changement de mot de passe, le nouveau mot de passe peut être demandé à l'utilisateur ou généré aléatoirement par SSOX suivant un modèle paramétrable.

- **Support des environnements Windows 32 et 64 bits :**

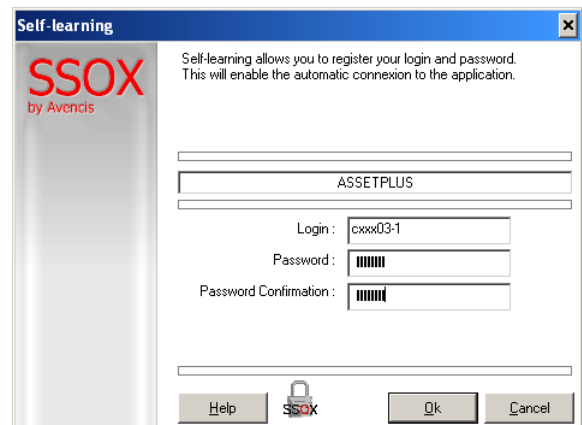
SSOX supporte les environnements Windows 32 bits (Windows 2000 / XP / XP Embedded / Vista / Seven / 2003 et R2 / 2008) et 64 bits (Vista / Seven / 2008R2)

Expérience utilisateur :

- **Lancement des applications par le panel :**

L'utilisateur peut lancer ses applications directement via le panel SSOX, d'un simple clic :

Lorsque SSOX ne connaît pas les crédeniels de l'utilisateur, il les demande automatiquement à l'utilisateur lors de la première connexion à l'application.



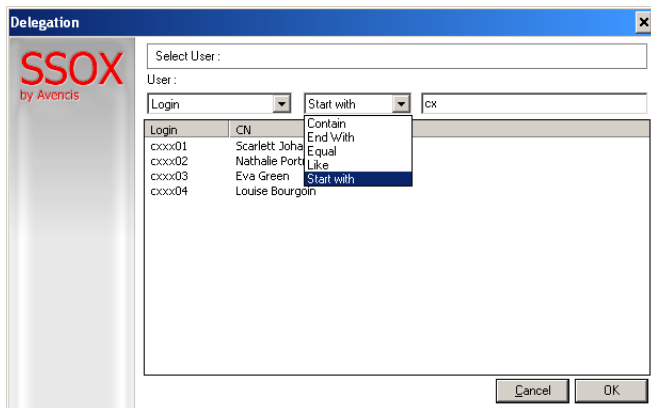
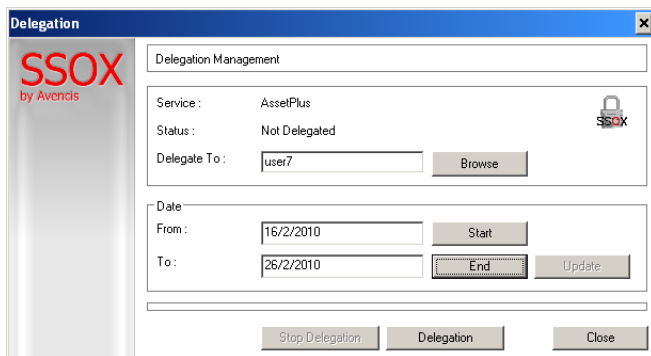
- **Personnalisation des interfaces :**

Toutes les interfaces utilisateurs peuvent être personnalisées, graphiquement et textuellement, pour adopter le lexique des métiers des utilisateurs.

- **Auto-apprentissage :**

- **Délégation**

L'utilisateur peut déléguer, s'il y est autorisé, certains de ses comptes applicatifs à d'autres utilisateurs. L'utilisateur peut, en option, définir une date de début et une date de fin pour cette délégation.



Au moment de l'authentification dans l'application dont le compte a été délégué, l'utilisateur qui reçoit la délégation pourra choisir entre l'utilisation de son compte propre et le compte qui lui a été délégué. Les audits permettent de tracer l'utilisation de comptes délégués et de savoir quel utilisateur réel a utilisé quel compte applicatif.

- **Comptes Multiples :**

Pour chaque application, un utilisateur peut disposer de comptes multiples (ex. : compte utilisateur, compte d'administration...) Lors de l'authentification, l'utilisateur pourra choisir le compte qu'il souhaite utiliser. Si l'utilisateur ne dispose que d'un compte, l'authentification sera automatique.

- **Conteneurs Partagés :**

L'utilisation de conteneurs partagés permet de définir un ou plusieurs comptes partagés par plusieurs utilisateurs. Un cas d'usage fréquent est l'utilisation partagée de comptes d'administration. Le conteneur partagé est stocké dans l'annuaire. Lorsqu'un mot de passe est modifié, il est immédiatement modifié pour tous les utilisateurs utilisant ce conteneur partagé. L'utilisateur peut ne pas connaître le mot de passe applicatif du compte.

Les audits permettent de tracer l'utilisation de comptes partagés et de savoir quel utilisateur réel a utilisé quel compte applicatif.

- **Signature :**

L'accès à des applications dites sensibles peut être soumis à une demande de réauthentification de l'utilisateur avant d'effectuer les actions du SSO.

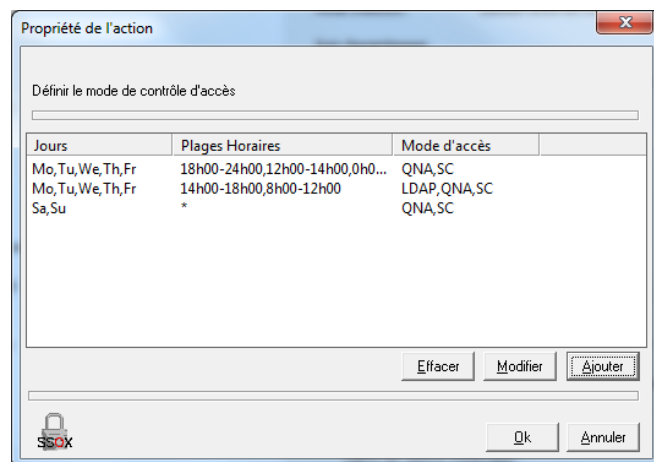
Le mode de réauthentification utilisé dépend de la manière dont l'utilisateur s'est authentifié, la même authentification lui étant redemandée (code PIN, mot de passe, Questions/Réponses, OTP ...)

- **Contrôle d'accès applicatif :**

Le contrôle d'accès permet de définir dans quelles conditions l'utilisateur peut accéder à une application. Ces conditions incluent :

- Des modes d'authentification ;
- Des plages horaires et des jours de la semaine ;
- Des règles spécifiques.

Si l'utilisateur ne possède pas le mode d'authentification requis, il lui est demandé de se « sur authentifier » avec l'un des modes d'authentification compatibles avec les règles de contrôle d'accès définies.



- **Alimentation par une solution de gestion des habilitations :**

Les créden-tiels des utilisateurs peuvent être provisionnés automatiquement par un module externe de gestion des habilitations. Dans ce cas, l'utilisateur n'a jamais besoin de connaître ses créden-tiels applicatifs.

Configuration des applications :

- **Configuration des applications :**

La configuration des applications est réalisée par une interface entièrement graphique qui permet de configurer, via des assistants, les différentes cinématiques (authentification, échec, changement de mot de passe,...).

- **Distribution des cinématiques SSO :**

Les cinématiques SSO sont stockées dans l'annuaire, peuvent être groupées et sont téléchargées automatiquement sur les postes de travail, par le moteur SSO, lors de leur mise à jour dans l'annuaire.

Haute disponibilité :

- **Support des annuaires AD/ADAM/LDAP :**

Le conteneur SSO de chaque utilisateur est stocké dans l'annuaire pour être disponible quel que soit le poste sur lequel l'utilisateur se connecte.

- **Synchronisation multi-maîtres :**

Le conteneur SSO est synchronisé entre l'annuaire et un cache local sur le poste pour assurer la continuité de service en cas d'absence de connexion avec l'annuaire. Cette synchronisation est dite "multi-maîtres".

- **Administration centralisée et déléguable :**

L'administration de la solution SSOX est réalisée à travers une interface web dont l'accès est contrôlé par des profils qui déterminent les privilèges d'accès (fonction et portée). Ces profils permettent de déléguer simplement tout ou partie des tâches d'administration à des administrateurs secondaires.

- **Chiffrement :**

Le conteneur SSO de l'utilisateur est stocké chiffré sur le poste de travail et dans l'annuaire. Il est échangé chiffré sur le réseau et déchiffré à la demande sur le poste de travail.