Evidian

Authentification unique (SSO) d'entreprise mobilité, sécurité et simplicité

Trusted partner for your **Digital Journey**

Sommaire

Ce livre blanc décrit les principales fonctions apportées par le SSO d'entreprise. Il présente également Enterprise SSO, la solution d'authentification unique d'Evidian.

Qu'est-ce que l'authentification unique ?

L'authentification unique (en anglais single sign-on ou SSO) permet à un utilisateur d'accéder à toutes ses applications avec un seul moyen d'authentification. Cela peut être par exemple un mot de passe, un badge sans contact, un certificat sur une carte nationale d'identité, une clé USB cryptographique, un mot de passe à usage unique (OTP) ou votre doigt si vous disposez d'un lecteur biométrique.

Les bénéfices d'un SSO

Typiquement, un SSO nécessite d'installer un logiciel sur votre PC, tablette ou smartphone, qui renseigne les mots de passe des applications à votre place. Ce logiciel n'est pas nécessaire si vous vous contentez de lancer des applications Web ou si vous travaillez en mode 'client léger'. Dans ce cas, le logiciel de SSO réside sur un serveur et renseigne les mots de passe à distance.

Le SSO simplifie la vie des utilisateurs, libère leur temps et leur esprit de la saisie, du changement et même de la connaissance des mots de passe. Evidian a rencontré des entreprises où les utilisateurs devaient connaître une trentaine de mots de passe différents : à présent, zéro ou un seul mot de passe suffit. Le SSO permet également d'augmenter la sécurité et de réduire les coûts. Ces enjeux sont décrits ci-dessous dans la section *«Les trois raisons d'investir dans un SSO d'entreprise»*.

SSO individuel et SSO d'entreprise

Il existe de nombreux outils individuels de SSO, comme les fonctions d'auto-remplissage des navigateurs Web. Mais fournir un SSO aux centaines – voire aux milliers – d'employés d'une entreprise nécessite une approche toute différente. Cela est dû à la nécessité de gérer, contrôler et proposer des moyens d'authentification forte, des fonctions d'administration, de délégation, de mobilité, d'utilisation de tablettes, de continuité d'activité et d'audit indispensables dans les grandes organisations.

C'est pour ces raisons qu'il est conseillé de choisir un outil de SSO qui remplisse l'ensemble des fonctions dont vous aurez besoin de façon satisfaisante : cela doit être un choix d'entreprise.

La solution Enterprise SSO d'Evidian est l'aboutissement de plus de quinze ans d'expérience en gestion des identités et des accès. Plus de 5 millions d'utilisateurs dans le monde accèdent chaque jour à leurs applications avec l'offre d'Evidian. Par exemple, Evidian a équipé les 120.000 postes d'un client répartis sur plusieurs continents en couvrant une grande variété de cas d'usage. Sur la base de ce savoir-faire, ce livre blanc dresse un panel des fonctions de SSO à l'état de l'art.

Quelles sont les alternatives au SSO?

D'autres types de solutions réduisent le nombre de mots de passe que les utilisateurs renseignent au cours de leur journée.

- La synchronisation des mots de passe diffuse le même mot de passe sur toutes les applications. Si le mot de passe de votre messagerie est « abcd », alors le mot de passe sera également « abcd » pour l'application de paye. Avec cette approche, l'utilisateur continue de saisir son mot de passe pour chaque connexion à une application : l'utilisateur a bien un mot de passe unique mais il n'a pas une authentification unique.

De plus, il faut développer pour chaque application un module qui synchronise les mots de passe uniques des utilisateurs.

Ce type de mot de passe unique donne la sensation de facilité d'utilisation mais cela se fait au détriment de la sécurité. En effet, ceci constitue une politique de contrôle du format de mot de passe (PFCP) extrêmement faible. Si le mot de passe *« abcd »* est piraté ou volé sur une application, alors toutes les applications seront compromises.

Cette méthode est souvent utilisée pour synchroniser tous les mots de passe avec le mot de passe Windows du domaine. Il est lui-même parfois requis pour les accès externes, parfois stocké sur un terminal mobile avec un chiffrement faible.

Certaines organisations essaient de synchroniser les mots de passe selon des politiques différentes, suivant les capacités des applications à gérer des mots de passe plus ou moins longs et contenant plus ou moins de caractère spéciaux. Toutefois à l'usage, on constate que l'utilisation de plus de 2 mots de passe pour un grand nombre d'applications avec des changements de mots de passe imposés représente pour l'utilisateur une situation complexe à gérer. Face à cette situation où les mots de passe se retrouvent inscrits sur une note ou dans un fichier, la mise à disposition pour les utilisateurs d'un logiciel de SSO devient une nécessité.

- Avec des « jetons virtuels » de type Kerberos ou SAML, les applications délèguent l'authentification à un module externe.

Cependant, dans la plupart des cas, il faut modifier l'application et la délégation d'accès entre collègues est impossible. De plus, les fonctions de réauthentification en cas d'accès aux applications sensibles et de gestion de postes en mode kiosque ne sont souvent pas présentes.

Pour illustrer ce propos, voici des exemples de situations fréquemment rencontrées :

Risque opérationnel	Situations fréquentes	Single Sign-On Evidian
Mots de passe utilisés pour chacune des applications	Tous identiques au mot de passe Windows	Tous différents et complexes
Dévoilement ou usurpation du mot de passe d'une application	Donne accès à toutes les applications autorisées pour cet utilisateur	Donne accès à cette seule application
Accès interne pour les utilisateurs à des applications sensibles Il s'agit d'applications qui nécessitent un haut niveau de privilèges et ne doivent absolument pas être accessibles si le mot de passe Windows est forcé par le support ou l'administrateur	Le mot de passe Windows donne accès aux applications Pour gérer ce risque, les applications sensibles doivent donc être exclues de la synchronisation **La situation à risque n'est pas gérée**	Niveau d'authentification configurable par application sensible et par utilisateur Si un administrateur réinitialise le mot de passe Windows, alors l'accès à l'application par le SSO sera refusé et l'utilisateur propriétaire sera averti **La situation à risque est gérée de manière globale**
Accès externe pour les utilisateurs équipés d'un appareil mobile pour le mail, l'agenda, les contacts, les notes, la messagerie instantanée	Mot de passe interne du domaine Windows stocké dans la configuration locale du terminal **La situation à risque n'est pas gérée**	Mot de passe différent du mot de passe Windows stocké dans la configuration locale du terminal **La situation à risque est gérée de manière globale**
Accès externe via un terminal mobile – (PC, tablette, ...) en client léger via des fermes « VDI » pour traiter les situations de mobilité L'utilisateur dispose d'une authentification par mot de passe ou par mot de passe unique (OTP)	Mot de passe interne du domaine Windows saisi par l'utilisateur dans le processus de connexion, seul ou combiné à un OTP La situation est à très haut risque car le mot de passe interne du domaine Windows est exposé sur le terminal et sur le réseau externe de l'entreprise **La mobilité induit une situation à haut risque qui freine son adoption**	Mot de passe interne du domaine Windows **non** saisi par l'utilisateur dans le processus de connexion, seul l'OTP est nécessaire Le risque de mots de passe internes du domaine Windows exposés sur le terminal et sur le réseau externe de l'entreprise est éliminé **La mobilité n'induit pas de situation à haut risque**

Note : pour renforcer de manière optimale la sécurité des accès externes d'utilisateurs privilégiés, la solution d'Evidian permet de combiner l'OTP avec un mot de passe différent du mot de passe Windows grâce à l'authentification multi-facteurs.

Les trois raisons d'investir dans un SSO d'entreprise

Les entreprises sont motivées par trois principaux facteurs dans leurs décisions d'investir dans une solution de Single Signe-On.

1 Renforcer la sécurité et respecter les contraintes réglementaires

En intégrant un point de passage obligé entre un utilisateur et ses applications, une organisation peut contrôler les accès de manière efficace.

Pour plus de précisions, reportez-vous à la section *« Renforcer la sécurité : l'authentification forte »*.

2 Réduire les coûts de fonctionnement de l'informatique

En multipliant les mots de passe, souvent pour d'excellentes raisons, la productivité de l'utilisateur baisse et la qualité du travail s'en ressent. De plus, ces « coûts cachés » ont aussi une face visible : jusqu'à 30% des appels au help desk résultent de mots de passe perdus. Cette charge sera considérablement allégée par un SSO, avec un retour sur investissement facile à estimer.

Pour plus de précisions, reportez-vous à la section *« La continuité de service réduit les coûts d'exploitation »*.

3 Ouvrir sans risque l'informatique au monde extérieur

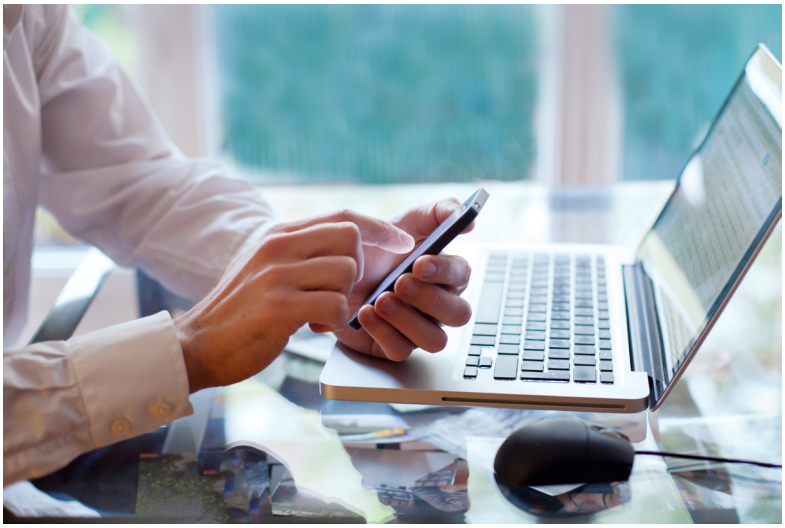
Cette demande est de plus en plus fréquente : l'accès au Web est devenu aisé, mais les employés continuent à avoir des difficultés à accéder de l'extérieur aux applications intranet.

Pour plus de précisions, reportez-vous à la section *« Votre informatique s'ouvre sans risque »*.

La façon de mettre en place l'outil de SSO peut varier en fonction de ces facteurs, même si cet outil est le même dans les trois cas. Bien sûr, certaines entreprises peuvent décider de faire d'une pierre deux coups, et de combler plusieurs besoins à la fois !

Sécurité, réduction des coûts, ouverture : le SSO d'entreprise d'Evidian répond à ces besoins par une architecture modulaire. Les modules fonctionnels peuvent être mis en œuvre par étapes, en apportant à chacune d'elles des fonctions utiles et visibles.

De même, il est possible d'équiper dans un premier temps un seul service et d'étendre par la suite les fonctions au reste de l'entreprise.



Une architecture simple

Les trois architectures du SSO d'entreprise

Le logiciel de SSO présent sur le poste, la tablette ou le smartphone de l'utilisateur renseigne les identifiants et mots de passe à sa place. Mais où le logiciel trouve-t-il ces informations ?

Avec un SSO individuel, les données de SSO sont sur le poste de l'utilisateur. Quelle que soit la méthode de cryptage des données, l'entreprise abandonne le SSO individuel au profit du SSO d'entreprise pour les raisons suivantes :

- le contrôle : il faut pouvoir retirer ou attribuer un accès à distance,
- l'audit : il faut pouvoir analyser les accès pour optimiser les coûts liés à l'utilisation des applications,
- la traçabilité et la mobilité des utilisateurs : changement de poste de travail, utilisation de postes en mode kiosque, de serveurs de présentation, d'appareils mobiles à l'extérieur de l'entreprise.

Sur le marché du SSO d'entreprise, nous rencontrons principalement **trois architectures** permettant de rendre disponibles les informations de SSO telles qu'identifiants, mots de passe et droits d'accès.

1 **Serveur de SSO** : les informations sont stockées sur un serveur, par exemple Novell ou Unix, qu'il faut généralement dédier à cette tâche. Le client sur le PC interroge donc le serveur quand c'est nécessaire. Ce serveur est souvent répliqué en plusieurs instances pour une plus grande disponibilité et capacité, même si des mécanismes de cache sur le PC permettent de pallier une indisponibilité temporaire. Des coûts de démarrage et d'opération doivent donc être pris en compte : serveurs, installation du logiciel, synchronisations périodiques de sa base de compte utilisateurs avec l'annuaire en place dans l'entreprise. Dans une entreprise étendue, le nombre de ces serveurs peut être important, les synchronisations de comptes complexes présentant un risque de cohérence pour la gestion des droits d'accès.

2 ***« Appliance »* de SSO** : il s'agit d'une variante de la solution précédente. Matériels et logiciels sont livrés ensemble. Les coûts de mise en place du logiciel peuvent paraître réduits. Par contre, il n'est pas possible d'installer le logiciel sur un serveur existant, ce qui peut augmenter les coûts de mise en place. Enfin, il est souvent impossible d'ajouter mémoire et disque sur une « appliance », contrairement à un serveur. La solution « appliance » a une capacité limitée, elle nécessite plusieurs instances d'*« appliance »* pour chaque environnement (production, intégration, site de secours), elle introduit un nouveau système d'exploitation, un nouvel annuaire à synchroniser. Comme dans le cas ci-dessus, les synchronisations de comptes complexes présentent un risque de cohérence pour la gestion des droits d'accès. Pour ce qui est de la continuité des accès, ce type de solution peut présenter un risque de SPOF (Single Point Of Failure).

3 **Annuaire de l'entreprise** : les informations de SSO sont tout simplement stockées chiffrées dans l'annuaire qui équipe déjà la plupart des entreprises, garantissant un haut niveau de confidentialité avec un chiffrement non réversible de type AES256. Par exemple : l'annuaire Microsoft Active Directory où sont déclarés les utilisateurs et par lequel ils accèdent à leur session Windows, ou bien son instance applicative Microsoft AD-LDS dans lequel peuvent être stockées des données d'applications associées aux utilisateurs déclarés dans l'Active Directory.

Dans le cas de Microsoft Active Directory, il n'y a donc aucun serveur ni appliance à installer, dans celui de Microsoft AD-LDS on pourra facilement utiliser ou mapper les serveurs sur ceux de Microsoft Active Directory déjà présents. Vos postes sont déjà configurés pour accéder aux informations, puisqu'ils accèdent déjà à l'annuaire.

Les coûts de mise en œuvre, haute disponibilité, continuité d'activité de cette architecture sont considérablement réduits. C'est aussi le cas pour l'évolution dans le temps de la solution qui peut facilement suivre celle des composants de l'infrastructure Active Directory.

Dans une telle architecture, l'annuaire est généralement complété par quelques postes d'administration et une base abritant l'historique des actions (pour l'audit et les rapports). Cette base peut être une base relationnelle déjà présente dans le système d'information. Les stations et la base ne sont pas utilisées lors de l'authentification ou des accès de l'utilisateur aux applications, et donc ne sont pas un point de passage obligé et critique pour le fonctionnement de l'ensemble. Il n'y a donc pas de SPOF dans cette architecture dite *« Annuaire »*, contrairement aux architectures « serveur » et *« Appliance »*.

Evidian Enterprise SSO utilise une architecture basée sur l'annuaire de l'entreprise, permettant des montées en charge sans interruption. Notre expérience dans le domaine démontre que cette solution est la plus simple et la plus rapide à mettre en œuvre, en gardant le niveau de sécurité le plus élevé.

Plusieurs annuaires d'entreprise

Toutes les entreprises ont mis en place des annuaires, mais certaines en ont plusieurs ! Les raisons peuvent être historiques (une entreprise récemment acquise, une filiale indépendante) ou fonctionnelles (les partenaires sont gérés dans une base à part). Cela peut poser problème si un utilisateur se déplace d'un domaine à un autre.

Dans ce cas, Evidian propose une solution de synchronisation d'annuaires : les informations les plus fiables sont obtenues depuis l'endroit adéquat et il est possible de bâtir ainsi un annuaire central. De cette façon, un utilisateur déclaré dans les bases des ressources humaines sera très rapidement opérationnel dans l'ensemble de l'entreprise.

Une architecture basée sur l'annuaire existant de l'entreprise est donc une solution à la fois simple, facile à maintenir et rapidement déployée.

MES CRITERES

- La solution de SSO impose-t-elle de déployer de nouveaux serveurs ou des appliances dans mon entreprise ?
- Est-ce un problème si mes utilisateurs sont référencés dans plusieurs bases, fichiers et annuaires ?

Pour une grande entreprise disposant d'entités ayant chacune son propre annuaire et sans relation d'approbation, le service de SSO commun à toutes les entités peut être déployé sans remettre en cause ce principe de gouvernance. Cette architecture est basée sur la mise en place d'un annuaire commun facilement déployé. Chaque utilisateur s'authentifie dans le domaine de sa propre entité et bénéfice du service de SSO mis à disposition à partir de l'annuaire commun.

MES CRITERES

- La solution de SSO impose-t-elle de déployer des solutions d'approbation entre les domaines de mon entreprise ?
- Pour bénéficier d'un SSO partagé par toutes mes entités, est-ce un problème si mes utilisateurs s'authentifient dans leur domaine et si ces domaines ne disposent pas de relations d'approbation ?

Une gestion qui devient naturelle

Un SSO pour que la sécurité devienne naturelle

Avec un Single Sign-On d'entreprise bien conçu, votre politique de sécurité n'est plus une contrainte pour vos utilisateurs. Ils lancent les applications auxquelles ils ont droit, sans avoir à retenir ni gérer leurs mots de passe. Ainsi, les employés obéissent naturellement à la politique de sécurité.

Le SSO se charge de l'ensemble des opérations concernant les mots de passe. Il peut même les changer automatiquement, sans que l'utilisateur intervienne. Vous pouvez faire en sorte que l'utilisateur ignore le mot de passe d'une application sensible : il lui sera donc impossible de révéler ce mot de passe, de le dévoiler à un tiers ou de l'utiliser frauduleusement en-dehors de l'entreprise.

Le SSO vous permet d'exiger une nouvelle authentification par l'utilisateur afin d'autoriser l'accès à une application spécifique.

À partir d'une console de gestion centrale, vous décidez qui a accès à quelle application.

Bien sûr, avec des milliers d'employés et des centaines d'applications, il n'est pas question d'attribuer des accès un par un ! De façon bien plus simple, l'administrateur indique quel groupe d'utilisateurs a accès à quel groupe d'applications, et éventuellement à partir de quelles stations.

Par exemple :

- Les applications de back-office ne doivent jamais être utilisées depuis une station de trading.
- Les stations de R&D ne sont accessibles qu'après une authentification biométrique.
- L'application SAGE ne peut être utilisée que par le département finance.

MES CRITERES

- Peut-on restreindre l'accès à une application en fonction du métier de l'utilisateur, mais aussi de l'endroit où l'application est lancée ?

Gérer les mots de passe naturellement

Avec Evidian Enterprise SSO, vous pouvez faire respecter une politique de mots de passe stricte (par exemple au moins deux chiffres dont un en tête, plus de dix caractères etc.). Cette politique est différente pour chaque application, même si l'application elle-même est plus permissive.

Cela est possible car toutes les opérations se passent sous le contrôle du SSO. En conséquence les mots de passe peuvent être différents pour chaque application. Des exceptions sont possibles et certaines applications peuvent, sans difficulté, être déclarées comme utilisant le mot de passe de la session Windows de l'utilisateur.

Mais que se passe-t-il si un employé souhaite qu'un collègue le remplace pendant une absence ? Auparavant, il lui révélait son identifiant et son mot de passe, avec tous les risques en termes de sécurité et d'audit que cela comporte.

Au contraire, Evidian Enterprise SSO permet à un employé de déléguer l'accès de façon temporaire à un collègue. Il ne peut bien sûr le faire que si vous avez autorisé cette éventualité. L'historique des accès est également conservé, ce qui permet de distinguer quelles opérations ont été effectuées par quelle personne.

MES CRITERES

- La solution de SSO permet-elle à un employé de déléguer lui-même l'accès à une application de façon temporaire, par exemple pendant un congé ?

Renforcer la sécurité : l'authentification forte

La combinaison nom d'utilisateur/mot de passe est la méthode d'accès la plus courante, en particulier dans les environnements Microsoft. Toutefois, ce *« sésame ouvre-toi »* universel n'est souvent pas suffisant pour la protection de ressources sensibles. Un mot de passe prouve-t-il que la personne qui se connecte est vraiment la personne qu'elle prétend être ?

C'est pourquoi l'on choisit parfois de renforcer le Single Sign-On avec des méthodes d'authentification forte.

Celles-ci peuvent être déployées sur tout ou partie des postes de travail. Il est courant de protéger certains postes et certaines applications sensibles.

Par exemple :

- Stations de travail du top management
- Stations de travail des conseillers clientèle en agence
- Accès par des médecins aux dossiers des patients
- Ouverture de session sur les postes kiosque pour les infirmières
- PCs portables sensibles de commerciaux et de la R&D
- PCs portables de cabinet d'audit très mobiles
- Session des postes kiosques sur les chaînes de fabrication avec carte à certificat
- Postes de vidéo surveillance et d'accès à des données personnelles
- Opérateur disposant de droits d'accès aux *« fadettes »*, *« tickets d'appel »* chez un opérateur télécom
- Personnel soignant se déplaçant et accédant aux PCs en mode kiosque en présentant son badge sans contact et retrouvant sa session de travail dans l'état où il l'avait laissée
- Trader du *« front office »* ouvrant simultanément toutes les sessions Windows sur ses stations de travail avec un seul dispositif matériel d'authentification sur la grappe de stations.

Ainsi, Evidian rencontre couramment les types d'authentification forte suivants :

TYPE	EXEMPLES D'UTILISATEURS	EXEMPLE DE SOLUTIONS
Carte ou Token USB avec certificats provenant d'une infrastructure à clés publiques locale ou nationale	Hôpitaux Industrie Finances Gouvernement Ministères	Cartes de santé CPS (France), NHS (UK) ou UZI-pas (Pays-Bas) Carte agents local, fédéral, gouvernemental ou (PIV, EAS-ECC,...) Badge Corporate Carte d'identité eID (Belgique)
Biométrie	Hôpitaux Industries Finances	Lecteur d'empreintes digitales Biométrie veineuse
Mot de passe à usage unique	Assurances Banques Industries	Calculette Token logiciel sur téléphone ou smartphone
Carte *«confidentiel défense»*	Défense	Carte sécurisée multifonction
Badges sans contact Badge radio	Hôpitaux Distribution	Technologie RFID
Badge bi technologies « contact et sans contact »	Hôpitaux	Cartes de santé CPS (France), NHS (UK) ou UZI-pas (Pays-Bas) Carte agents gouvernemental ou fédéral (PIV, EAS-ECC, ...) Badge Corporate Carte d'identité eID (Belgique)
Objet connecté	Industrie	Bracelet bluetooth

Evidian Enterprise SSO est compatible avec la grande variété des méthodes d'authentification forte présentées ci-dessus. Les solutions d'Evidian permettent de gérer ces équipements sur toute une entreprise : attribution de cartes à puce et tokens USB, prêts, mise en liste noire, personnalisation de badges, etc. La sécurité des accès est ainsi renforcée pour certaines catégories d'utilisateurs.

MES CRITERES

- La solution de SSO est-elle compatible avec l'authentification forte que j'ai choisie ?
- Puis-je interdire à une application d'être exécutée sur un poste qui n'est pas protégé par l'authentification forte ?
- Est-il possible de supporter simultanément plusieurs méthodes d'authentification en fonction des profils d'utilisateurs ou des postes de travail ?
- L'authentification et le SSO couvrent-t-ils bien les cas d'usage propres à mes métiers ?

La continuité de service réduit les coûts d'exploitation

Un outil de SSO bien conçu permet de réduire les coûts d'exploitation. Certains de ces coûts sont difficiles à évaluer, puisqu'ils touchent à la productivité des utilisateurs. Néanmoins, d'autres économies sont plus facilement mesurables : elles concernent la charge du help desk.

Evidian Enterprise SSO prend en charge la contrainte des mots de passe applicatifs, évitant ainsi les oublis ou blocages de comptes. Les appels au help desk de ce type baissent jusqu'à 30%, car les utilisateurs n'ont plus besoin de retenir les mots de passe des applications.

Cependant, il reste à traiter les oublis de mot de passe ou les pertes de carte d'accès. Par exemple, que se passe-t-il si un commercial constate dans un hôtel que sa carte à puce ne fonctionne plus ? Evidian Enterprise SSO, avec son module **Self-Service Password Request (SSPR),** permet de débloquer son accès. Il est inutile pour cela d'être connecté au réseau.

Grace au module **SSPR** d'Evidian, l'entreprise peut choisir d'utiliser la procédure adaptée à son besoin. Par exemple, le module SSPR peut être configuré de manière à ce que l'utilisateur réponde à trois questions au lancement initial du SSO sur son poste. S'il oublie son mot de passe ou perd sa carte d'accès, il répondra aux questions prédéfinies et réinitialisera son mot de passe. Ainsi, un accès perdu ne bloque pas l'utilisateur.

Evidian propose également **QRentry**, un mode de secours sans Questions - Réponses avec une authentification forte toujours disponible.

Avec **Evidian QRentry**, les utilisateurs se connectent à leurs sessions Windows en scannant un QR Code avec leur smartphone et en entrant le code fourni par le smartphone. Cet accès est toujours disponible en mode connecté et non connecté même avec un smartphone sans connexion réseau. Ainsi l'utilisateur dispose d'un générateur de mot de passe à usage unique (OTP) à partir de son smartphone.

Evidian QRentry est le complément idéal des déploiements d'authentification, qui génèrent des appels *« mot de passe oublié »*, *« carte perdue »* ou *« biométrie inopérante »*. Le nombre d'appels au help desk baisse drastiquement – il n'y a rien à mémoriser. Un utilisateur peut débloquer lui-même son accès à Windows, même si le help desk est injoignable.

MES CRITERES

- Mes utilisateurs pourront-ils réinitialiser leur mot de passe sans appeler le help desk ?
- Est-il possible de réinitialiser un mot de passe sans être connecté au réseau ?
- La solution SSO assure-t-elle la continuité des accès des utilisateurs en cas de défaillance de l'authentification forte ?

Comment intégrer une de vos applications au SSO ?

Le SSO se substitue à l'utilisateur et renseigne ses identifiants et mots de passe à sa place. Pour cela, le logiciel de SSO doit reconnaître la fenêtre de login du logiciel, mais aussi celle de changement de mot de passe, ou d'annonce de mot de passe incorrect. Ce travail d'apprentissage est réalisé une fois pour toutes dans l'entreprise, puis répercuté sur les PCs et stations mobiles des employés à travers l'annuaire d'entreprise.

Il est généralement facile d'effectuer ce travail pour les applications Windows qui ont été « développées » suivant les recommandations de Microsoft. Cependant, il ne faut pas oublier vos applications moins classiques :

- Applications internes développées il y a de très nombreuses années
- Applications mainframe en mode « émulation de terminal »
- Packages avec particularités d'interface telles que OWA, Office 365, SAP et Notes
- Applications ou applettes Java
- Sites et portails web à travers Internet Explorer, Chrome ou Firefox.

Comment vous assurer que le logiciel de SSO saura intégrer vos applications, même les plus *« exotiques »* ? Il est souvent prudent de demander un essai de la solution sur votre site, accompagné de l'intégration des applications les plus critiques.

Evidian Enterprise SSO permet d'intégrer la plupart des applications en quelques clics. Vous lancez l'application et pointez la souris sur les champs *« identifiant »*, *« mot de passe »* etc. Par la suite, l'application sera reconnue partout dans l'entreprise. Des versions d'applications Lotus Notes, SAP ou navigateurs sont traitées nativement et un outil graphique de scripts est disponible.

MES CRITERES

- La solution de SSO permettra-elle d'intégrer simplement mes applications, ou nécessite-t-elle de la programmation ?

L'administration du SSO au quotidien

Si la solution de SSO permet de réelles économies, elle ne doit pas à l'inverse générer autant de coûts d'administration ! Ainsi, quand on dépasse plusieurs dizaines d'utilisateurs, il n'est plus question d'attribuer des droits individuellement. Il doit être extrêmement facile de gérer les droits d'un utilisateur arrivant, changeant de fonction et quittant l'entreprise.

De même, si des applications sont 'découvertes' dans l'entreprise pendant le déploiement, il faudra les intégrer rapidement elles aussi. Et comme l'utilisateur peut ignorer les mots de passe de ses applications critiques, comment fait-il pour déléguer ses accès sans encombrer le help desk en période de vacances ?

Pour se rendre compte de la charge d'administration quotidienne d'un outil de SSO, le mieux est de demander une évaluation sur site. Pendant quelques jours, vous pourrez tester des scénarios d'administration. Vous vous rendrez compte si les profils des personnes choisies sont adéquats, et vous estimerez le volume de travail.
Evidian a incorporé dans Enterprise SSO de nombreuses facilités d'administration. Fruits de plus de quinze ans d'expérience, l'ergonomie et les fonctions ont été affinées pour rendre les administrateurs efficaces dans cette tâche. Par exemple :

- Lorsque l'utilisateur s'absente, il délègue lui-même ses accès à son remplaçant avant son départ, sans dévoiler ses mots de passe.
- Des gestionnaires locaux intègrent leurs propres applications et gèrent les accès de leurs équipes.
- Des rôles d'administration couvrent les applications, les cartes, les mots de passe, l'audit etc.
- Quand un administrateur change de fonction, ses droits sont facilement transférés ou délégués.
- Si nécessaire, les équipes applicatives peuvent disposer d'un outil de simulation et de diagnostic qui leur permettent de valider le bon fonctionnement de la configuration établie avec leur application.

MES CRITERES

- Quelle sera la charge quotidienne de gestion de la solution de SSO ?

Votre informatique s'ouvre sans risque

L'ouverture aux usages des appareils mobiles

Quand les usages imposent l'utilisation d'appareils mobiles iOS ou Android, en parallèle ou en remplacement des PCs pour accéder aux applications intranet ou dans le Cloud, comment disposer de ses mots de passe et notes personnelles ?

Les fonctions de SSO doivent permettre d'accéder à ses applications, de n'importe quel terminal (PC, tablettes, smartphone, client léger, poste virtualisé) en toute sécurité.

Evidian met à disposition de ses clients **Entreprise SSO pour les mobiles,** celui-ci partage en toute sécurité les mêmes informations protégées, mots de passe ou notes personnelles, quel que soit le terminal utilisé.

MES CRITERES

- Si le SSO du poste de travail a changé le mot de passe d'une application à l'insu de l'utilisateur, ce dernier y accédera-t-il toujours à partir de sa tablette iOS ou Android ?

L'ouverture au monde extérieur

Quand un de vos employés se déplace à l'extérieur, est-il obligé d'utiliser un PC spécialement configuré pour utiliser les applications intranet ? Pourtant, des fonctions de SSO peuvent lui permettre d'accéder à ses applications web internes, de n'importe quel navigateur (cybercafé, site client par exemple) et en toute sécurité.

Cela est souvent extrêmement utile. Des clients d'Evidian utilisent cette fonction pour rendre leurs employés réellement autonomes : commerciaux en déplacement, policiers en mission, ingénieurs sur un chantier à l'étranger etc.

Certaines solutions de SSO considèrent les accès web comme un ajout peu intégré : les parties « web » et « intranet » échangent donc mal certaines informations de SSO.

A l'inverse, Evidian Enterprise SSO partage en toute sécurité les mêmes informations protégées, quel que soit le mode d'accès.

MES CRITERES

- Si le SSO du poste de travail a changé le mot de passe d'une application à l'insu de l'utilisateur, ce dernier y accédera-t-il toujours normalement de l'extérieur avec un simple navigateur et de façon sécurisée ?
- Dans ce cas, comment ne pas propager des mots de passe internes à mon organisation entre son navigateur externe et la passerelle d'accès sécurisé de mon système d'information ?
- Si mes partenaires doivent accéder avec un simple navigateur à mon service unifié de prise de commandes, comptes clients, offres spéciales, alors comment l'authentifier par un mot de passe à usage unique et comment lui donner cette vue unifiée et sécurisée ?

La montée en charge

Pour le moment, vous souhaitez équiper uniquement votre service ou un seul site de votre entreprise avec un SSO. Il est toutefois prudent d'anticiper le moment où le SSO sera étendu au reste de votre entreprise, même si cette échéance est encore lointaine. Il vous faut donc choisir un SSO capable de monter en charge, sous peine de devoir changer de solution le moment venu, avec les difficultés de migration de mots de passe que cela impose.

Pour certains produits de SSO capables de satisfaire quelques centaines d'utilisateurs, la montée en charge est une vraie question. Comment partager les données pour que les utilisateurs soient mobiles sur plusieurs pays ? Faut-il former un administrateur par site, voire par service ? La technologie de base change-t-elle ? Doit-on installer des matériels dédiés à de nombreux endroits ?

Evidian Enterprise SSO a été déployé dans des entreprises avec plus de 100,000 utilisateurs. La solution peut être facilement étendue : la même technologie simple, basée sur l'annuaire de l'entreprise, est utilisée pour des clients de quelques centaines ou de plusieurs dizaines de milliers d'utilisateurs.

MES CRITERES

- La solution de SSO a-t-elle démontré qu'elle pouvait être déployée sur des dizaines de milliers d'utilisateurs ?

Intégration avec la gestion des identités et des accès

Evidian a constaté que le SSO est souvent un prélude à une gestion plus ambitieuse des identités et des accès. En effet, la politique d'accès pourra être définie de façon rigoureuse, validée selon un processus strict et régulièrement auditée. Elle sera ensuite respectée naturellement par les employés grâce aux mécanismes de SSO existant.

Et ce n'est pas tout : puisque le SSO fournit des informations sur l'usage réel des applications, il est possible d'auditer en permanence le respect de la politique de sécurité. Enfin, les comptes peuvent être mis à jour automatiquement dans les applications, l'utilisateur étant ainsi immédiatement opérationnel.

Evidian Enterprise SSO fait partie de la solution de gestion des identités et des accès IAM Suite d'Evidian. Ainsi, il peut être connecté à **Evidian Identity & Access Manager** pour automatiser la gestion des mots de passe, ou transmettre la liste des accès réels pour auditer et affiner la politique de sécurité.

Ne distribuez plus les mots de passe aux utilisateurs : en coordination avec la gestion des identités de l'entreprise, un module de provisionnement ou un workflow peuvent synchroniser les comptes applicatifs avec le SSO.

MES CRITERES

- La solution de SSO pourra-t-elle être étendue par la suite, en intégrant la gestion des accès par les rôles ou le provisionnement ?

Evidian : ensemble des fonctions de gestion des accès

Evidian Enterprise SSO permet de déployer rapidement une solution efficace d'authentification unique. Les utilisateurs accèdent à leurs applications plus facilement et avec une sécurité accrue. Sur cette base, vous pouvez ajouter des outils afin d'obtenir une authentification forte et des fonctions complémentaires d'administration :

- **Accès rapide à l'authentification unique** avec une connexion directe sur les applications, disponible sur PC, tablettes et smartphones.

  Les clients Enterprise SSO pour Windows et pour Mobiles offrent des fonctions d'authentification unique telles que l'administration des règles d'accès et de mots de passe, la délégation, la réauthentification, l'authentification multi-niveaux, la révélation des mots de passe, la gestion d'un coffre-fort électronique et la collecte d'audits.
  Accès SSO depuis Internet avec un client léger ou une tablette équipée uniquement d'un navigateur standard. Mobile E-SSO permet aux utilisateurs de se connecter via un serveur SSO à leurs applications à partir de n'importe quel navigateur Internet, en toute sécurité. Dans un grand nombre de cas, Mobile E-SSO permet de s'authentifier avec un mot de passe à usage unique (OTP) sans que l'utilisateur ne saisisse le mot de passe du domaine Windows et sans que les mots de passe internes à l'entreprise ne transitent entre la station de l'utilisateur et le point d'accès au réseau interne à l'entreprise.

- **Accès aux procédures de continuité d'activité**

  Enterprise SSO Web portal permet à votre organisation, en cas de nécessité, de disposer de procédures de délégation et de révélation des mots de passe depuis un portail web.

- **Accès au plan blanc**, Enterprise SSO Web portal permet à votre organisation, en cas de nécessité, de transmettre par email leurs informations d'authentification aux applications et mots de passe.

  Gestion de l'authentification Windows et de l'authentification forte, Authentication Manager simplifie l'utilisation des méthodes d'authentification de l'utilisateur pour accéder à sa session Windows avec le niveau de sécurité attendu. Ces méthodes sont : les cartes cryptographiques avec ou sans PKI au format badge et clés USB, l'utilisation des certificats, les badges sans contact « RFID », la biométrie, les mots de passe à usage unique (OTP) générés par des mécanismes logiciels et matériels.

- **Accès d'urgence** à la session Windows et à la gestion de son mot de passe

  Avec le Self-Service Password Request, les utilisateurs gèrent eux-mêmes les procédures d'accès de secours à leur session : la réinitialisation de leur mot de passe du domaine, le déblocage de leur PIN, l'ouverture de la session Windows sans changement du mot de passe du domaine. Cette procédure est basée sur un mécanisme de questions/réponses, elle est utilisable à partir de la fenêtre de login Windows du poste de travail de l'utilisateur et à partir d'une page Web du portail mis à disposition pour le changement du mot de passe du domaine et le déblocage du compte.

- **Mode kiosque** sur une station de travail

  Le module Session Management permet à des employés de partager une station de travail en mode kiosque sans redémarrer la session Windows. Ce module sait parquer la session en cours d'un premier utilisateur et démarrer ou reprendre la session d'un second utilisateur. Le changement d'utilisateur se fait donc en quelques secondes.

- **Authentification forte** par l'application Evidian **QRentry**

  QRentry permet à l'utilisateur de transformer son smartphone en moyen d'authentification forte protégé par le PIN de l'appareil. Cette application permet de gérer et d'authentifier le smartphone comme un point d'accès protégé par un certificat avec un mécanisme de clé privée et clé publique. C'est la solution idéale pour disposer d'un accès d'urgence à la session Windows sans utiliser les mécanismes de questions/réponses. En mode connecté, l'utilisateur a juste à valider une notification pour s'authentifier.

- **Mode cluster** pour ouvrir **N** sessions simultanément

  Avec le mode Cluster, les employés peuvent utiliser plusieurs PCs simultanément (par exemple les traders en salle de marchés ou l'équipe de surveillance d'usine). Une seule authentification débloque l'ensemble des PCs d'un utilisateur. Les mécanismes de délégation et de détachement de PCs entre utilisateurs sont nativement gérés par ce mode.

- **Reporting**

  Enfin des outils de reporting génèrent des rapports sur les événements d'administration, d'authentification et de connexion aux applications cibles.

Environnements supportés

- Le client de SSO est disponible pour des versions supportées d'iOS, Android, Windows, Mac OS, Citrix, VMware et Terminal Server.
- La plupart des applications Windows, HTML ou Java sont configurées par simple « glisser-déplacer ». Les particularités de certaines applications sont supportées en standard ou par configuration graphique.
- L'annuaire contenant les utilisateurs et la politique de sécurité peut être situé sur des versions supportées d'Active Directory ou d'autres annuaires LDAP.
- Les événements d'audit sont stockés dans une base relationnelle.
- Les rapports sont générés dans différents formats dont PDF.

La suite logicielle d'Evidian

Notre solution IAM est reconnue par les clients et les analystes pour sa complétude. En effet, elle offre les composants suivants, pouvant être déployés indépendamment ou intégrés nativement :

Evidian Identity & Access Manager

permet la gouvernance des autorisations et une gestion complète du cycle de vie des identités et des accès aux services, pilotée par une politique de sécurité et ses workflows d'approbation.

Evidian Web Access Manager

fédère des accès aux applications web, sécurise l'accès des utilisateurs mobiles et remplace l'ensemble des mots de passe des utilisateurs par un mode d'authentification unique et forte.

Evidian Enterprise SSO

gère l'accès aux applications d'entreprise et personnelles sur les postes de travail ainsi que sur les terminaux mobiles, évite à l'utilisateur de mémoriser et saisir les mots de passe.

Evidian Authentication Manager

offre l'authentification forte sur les postes de travail et terminaux mobiles : carte ou token avec certificat, carte sans contact, biométrie, mot de passe à usage unique.

Evidian SafeKit

apporte la haute disponibilité et le partage de charge aux applications.

16/02/2018 : Visa de sécurité ANSSI (CSPN) pour Evidian Enterprise SSO v. 8.06PL5 b5386.30
(https://www.ssi.gouv.fr/entreprise/certification_cspn/evidian-enterprise-sso-v-8-06pl5-b5386-30/)

À propos d'Evidian

Evidian est la suite logicielle de gestion des identités et des accès (IAM), d'Eviden.

Evidian IAM est le leader européen des logiciels de gestion des identités et des accès, avec une présence en pleine croissance en dehors du continent européen et notamment aux Etats-Unis et au Japon.

Plus de 5.000.000 d'utilisateurs dans plus de 900 organisations dans le monde entier se connectent tous les jours à leur entreprise et gèrent leurs droits d'accès avec les solutions de gestion des identités et des accès d'Evidian.

For more information: **Evidian.com**

CT_180622_EM_WP-AUTHENTIFICATION-UNIQUE-SSO-ENTERPRISE-FR