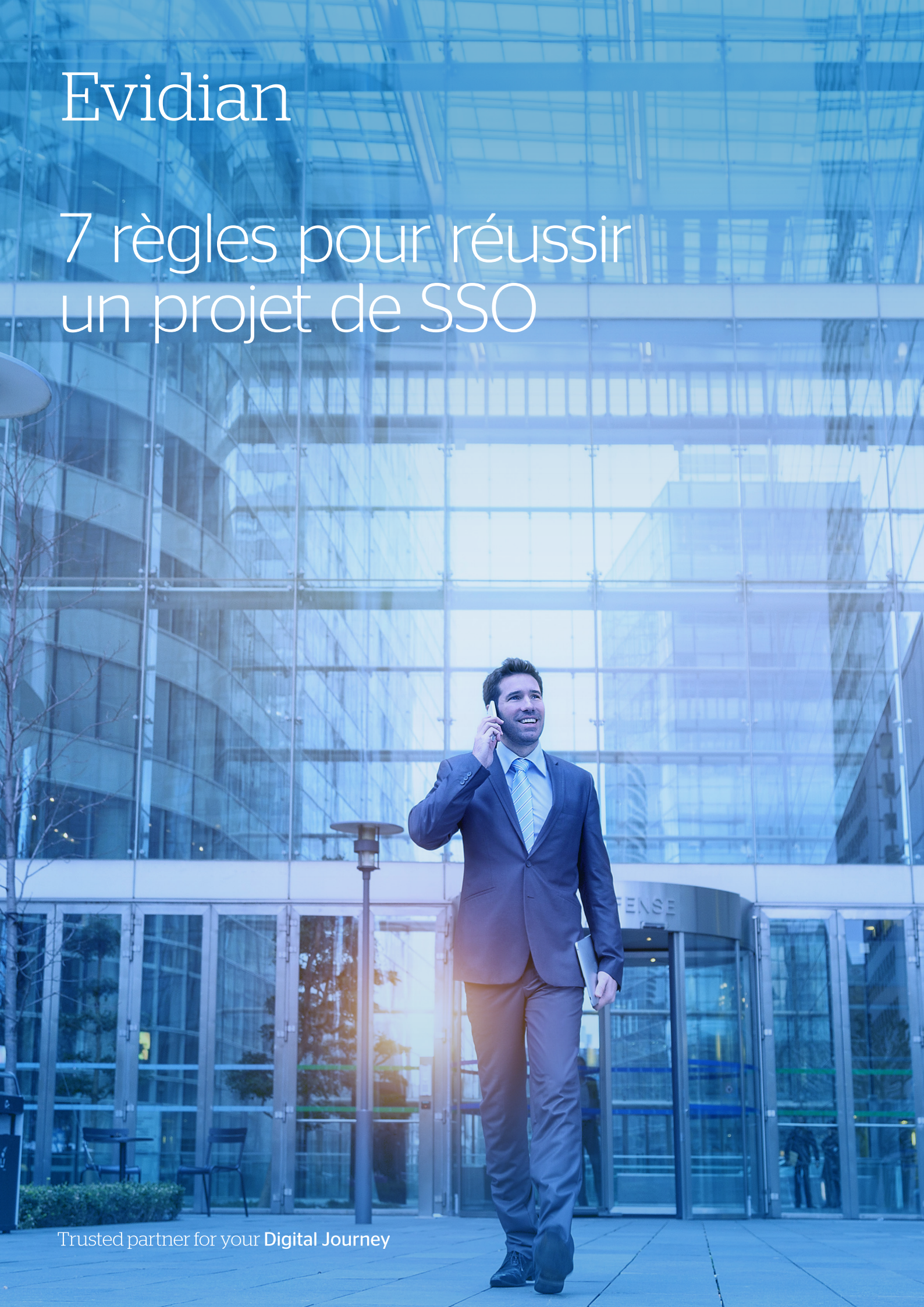
Evidian

7 règles pour réussir un projet de SSO



Trusted partner for your **Digital Journey**

Tables des matières

Basé sur 18 ans d'expérience du Single Sign-On (SSO), ce livre blanc décrit les bonnes pratiques et les pièges à éviter pour un déploiement de SSO réussi.

01 Déployez un SSO dans votre organisation

02 Etablissez et partagez clairement les objectifs du projet

03 Démontrez que le projet améliore la conformité réglementaire

04 Associez activement les utilisateurs au projet

05 Respectez les procédures et politiques établies

06 Gardez une architecture simple

07 Publiez régulièrement des indicateurs chiffrés

08 Préparez la mise en place de la gestion des identités

09 Le déroulement de votre projet de SSO

10 La Suite logicielle Evidian

Déployez un SSO dans votre organisation

L'authentification unique (en anglais Single Sign-On ou SSO) améliore la productivité des utilisateurs, accroit la sécurité, réduit les coûts de helpdesk et aide à respecter les contraintes légales.

Un projet de SSO d'entreprise ne s'improvise pas. Seule une bonne préparation assure un déploiement rapide, un respect des objectifs et l'adhésion des utilisateurs au projet.

Depuis 1999, Evidian et ses partenaires ont déployé des centaines de projets de SSO. Les enseignements majeurs sont présentés dans ce document. Comme vous le constaterez, au-delà des aspects purement techniques, la plupart de ces règles d'or touchent à l'organisation du projet :

1. Etablissez et partagez clairement les objectifs du projet
2. Démontrez que le projet améliore la conformité réglementaire
3. Associez activement les utilisateurs au projet
4. Respectez les procédures et politiques établies
5. Gardez une architecture simple
6. Publiez régulièrement des indicateurs chiffrés
7. Préparez la mise en place de la gestion des identités

Qu'est-ce que l'authentification unique ?

L'authentification unique vous permet d'accéder à toutes vos applications avec un seul moyen d'authentification. Par exemple un mot de passe, un badge d'entreprise ou votre empreinte.

Les mots de passe des applications seront automatiquement renseignés par l'outil de SSO.

Etablissez et partagez clairement les objectifs du projet

En quelques mots

Les objectifs d'un projet réussi de SSO sont toujours très concrets :

- Réduire les coûts de helpdesk
- Améliorer la productivité des utilisateurs : médecins, vendeurs, traders...
- Améliorer la sécurité des accès aux applications critiques
- Se conformer à des lois et règlementations : confidentialité médicale, PCI DSS ...

Chaque projet de SSO a généralement un ou deux objectifs majeurs, avec des sous-objectifs précis. Il est important de mettre noir sur blanc les résultats concrets attendus.

Ce document d'objectifs du SSO pourra faire l'objet de commentaires formels par les participants au projet, voire d'une décision collégiale. Qu'ils soient externes comme le prestataire de service, mais aussi internes : direction financière, contrôle interne ou directions opérationnelles.

Pourquoi est-ce important ?

Un objectif bien établi, chiffré et une cible réaliste permettent d'avoir l'appui de votre management au cours du projet. Il servira de référence pour les participants. En effet, le but du SSO n'est pas de faire disparaître 100% des mots de passe, mais plutôt de faire disparaître la saisie des mots de passe les plus fréquemment utilisés.

Pour faciliter grandement la mise en place et la participation des utilisateurs au projet, vous assurerez l'adhésion d'une direction, opérationnelle ou non, en travaillant avec elle pour estimer les bénéfices attendus.

Le cas pratique

Une grande banque souhaitait remplacer un SSO sur 80 000 postes. Son objectif concret : remplacer un fournisseur de SSO qui n'était plus supporté par une solution innovante et remplissant toutes les fonctions de la précédente.

Cette banque avait également des prérequis de conformité avec des produits tiers et un besoin de personnalisation du SSO.

Evidian et le prestataire intégrateur ont donc déployé rapidement un SSO complet d'entreprise pour la majorité des applications. Puis des développements supplémentaires ont été nécessaires pour des applications spécifiques ainsi que pour la personnalisation de la solution pour la banque.

Démontrez que le projet améliore la conformité réglementaire

En quelques mots

EMême si l'objectif principal du SSO est opérationnel – productivité ou réduction des coûts par exemple – il peut être utile de contacter le service de contrôle interne. Un SSO peut permettre à l'entreprise d'atteindre des objectifs de conformité réglementaire, de simplifier des procédures de contrôle existantes et de simplifier les audits.

La plupart des lois et règlementations visent à améliorer l'intégrité, la confidentialité ou la disponibilité de l'informatique.

- **Intégrité :** le SSO restreint l'accès aux ressources critiques, financières par exemple, aux personnes dont le rôle l'exige. Il peut également détecter les comptes inutilisés.
- **Confidentialité :** les applications gérant les données personnelles (dossiers médicaux, numéros de carte bancaire) sont protégées par le SSO. Les logs d'accès sont conservés en un point central.
- **Disponibilité :** en cas d'oubli de mot de passe, les PC et applications restent disponibles grâce à un accès de secours par question-réponse ou par OTP fourni à l'utilisateur par e-mail, SMS ou via l'application dédiée QRentry. De plus, si le SSO utilise les annuaires existants, il est facilement inclus dans un plan de secours.

Pourquoi est-ce important ?

Le contrôle interne doit être impliqué dans le projet, même à titre consultatif, car il apporte une crédibilité supplémentaire à cet effort et valorise le SSO.

Par ailleurs, en apportant très tôt son opinion au projet de déploiement, le contrôle interne peut donner des conseils d'implémentation qui seront utiles par la suite. La façon dont un SSO est mis en place pourra faciliter son travail de contrôle. Cela permettra également de trouver des sponsors.

La conformité réglementaire est donc un objectif primordial qui doit être mis en avant par le management, car ses conséquences sont importantes pour l'entreprise.

Le cas pratique

Une grande entreprise de télécommunications souhaitait mettre en place un SSO pour rendre ses utilisateurs plus productifs et se conformer à la loi Sarbanes-Oxley. Cette loi américaine a pour but d'assurer l'intégrité du rapport financier.

Lors de la préparation du projet, Evidian et son partenaire local ont consulté le service de contrôle interne du client, mais aussi des auditeurs externes. Cette revue a révélé des besoins non identifiés au départ. Par exemple, la vérification de procédures de contrôle se fait en consultant les données consolidées sur les accès. Les auditeurs ont donc exigé que ces données de SSO ne soient pas altérées, et leur origine systématiquement documentée et archivée.

Enfin, le projet a rédigé des procédures pour vérifier les informations collectées. Cela a permis d'accélérer de plusieurs jours les audits annuels des procédures d'accès.

Associez activement les utilisateurs au projet

En quelques mots

Les employés sont les principaux concernés par le SSO. Il est donc très important de recueillir leur avis, et d'en tenir compte dans le déploiement. Il ne suffit pas d'interroger leur hiérarchie !

Il faut donc identifier les catégories d'employés les plus influentes. Ils peuvent être méfiants face à une nouveauté comme le SSO – mais deviendront moteurs une fois convaincus. Toutes leurs remarques permettront d'anticiper les réticences au déploiement.

- Identifiez les profils et individus auxquels le SSO apportera le plus
- Faites des réunions régulières d'utilisateurs pilotes, avec démonstrations
- Proposez-leur de tester le SSO ainsi que des fonctionnalités en avant-première, comme la délégation de comptes partagés
- Démontrez-leur que leurs habitudes de travail ne changeront pas
- Présentez-leur les avantages en termes « métier » – et non techniques.

Pourquoi est-ce important ?

Une fois adeptes du SSO, les utilisateurs se rendront compte du confort d'utilisation qu'il peut leur apporter. Ils n'auront plus à se rappeler aucun de leurs mots de passe et deviendront alors promoteurs du projet.

De plus, les remarques d'utilisateurs permettent de découvrir et régler à l'avance des points bloquants. Par exemple, une application critique à prendre en compte, des exigences locales, ou des besoins non identifiés au départ.

Le cas pratique

Un groupement hospitalier de 100.000 utilisateurs souhaitait fournir une authentification unique à ses personnels soignants. Dans un espace hospitalier, le temps perdu à renseigner les mots de passe a un impact sur la qualité des soins. Un SSO réalisé avec la carte de personnel de santé permet aux personnels soignants de mieux se consacrer aux patients.

L'équipe projet a réalisé plusieurs démonstrations auprès des représentants du personnel soignant et a effectué un test dans un service. Elle a constaté que les médecins, dont certains voyaient l'informatique comme une contrainte, souhaitaient que le système soit le plus discret possible. Par contre, ils appréciaient l'accélération des lancements des applications, et le fait que ces accès étaient archivés. De même, les infirmiers se sont rapidement adaptés à l'accès SSO sur un PC partagé.

Cependant, dans le service des urgences, les médecins ont rejeté l'usage systématique de la carte à microprocesseur pour s'authentifier. Cela nuisait à la rapidité d'accès. La solution a été d'adopter une politique de sécurité spécifique dans l'enceinte des urgences, basée sur un délai de grâce et l'itinérance de session. Comme l'accès à ce service est physiquement contrôlé par carte, il a été possible d'allier rapidité et sécurité.

Respectez les procédures et politiques établies

En quelques mots

Un SSO n'est pas seulement un « projet technique » : il améliore la vie quotidienne des utilisateurs et les processus des organisations.

Les utilisateurs doivent être impliqués dans le projet de SSO afin d'anticiper des changements nécessaires et éviter que des managers découvrent qu'ils doivent modifier leurs procédures pour prendre en compte le SSO. Par exemple, la façon dont ils autorisent leurs employés à accéder aux applications peut changer.

Vous devez donc vous assurer que ces changements soient réduits au minimum, et les anticiper quand ils sont inévitables. Mieux encore, permettez à chaque organisation de planifier progressivement certaines étapes en fonction de ses impératifs propres.

Pourquoi est-ce important ?

Un déploiement bien préparé, en faisant participer les responsables de sites ou de divisions, met toutes les chances de votre côté.

La réticence des managers n'est généralement pas une question d'inertie : les priorités et le calendrier ne sont pas les mêmes pour tous. Par exemple, les financiers ou les commerciaux évitent d'installer de nouveaux outils en phase de clôture.

Même si le SSO simplifie les procédures – un seul écran gère l'accès à toutes les applications – il faut former les administrateurs locaux. En effet, lorsqu'une procédure existe pour des raisons légales, elle est certainement documentée et auditée - la changer aura un coût.

Le cas pratique

Une société industrielle souhaitait déployer un SSO sur plus de 70.000 postes. Les responsables de divisions et sites adhéraient au projet de SSO. Cependant, il est vite apparu que chacun avait des priorités différentes et des particularités de mise en œuvre.

Peu de responsables acceptaient de changer la façon dont ils géraient l'accès à leurs applications. Des applications comme mySAP devaient subir des tests avant d'être intégrées au SSO – la conformité aux lois sur la sécurité financière l'exigeait.

La solution : définir, pour chaque site et organisation, 10 à 20 applications « de base » à intégrer immédiatement au SSO. Les applications comme mySAP en étaient exclues dans un premier temps, pour respecter le rythme des organisations. La décision de « passer en mode SSO » est prise par chaque division.

De même, le SSO ne modifie pas forcément l'administration des accès. Dans une première phase, il se contente d'automatiser l'accès aux comptes déjà créés. Le déploiement du SSO s'est donc fait sans heurts. Chaque organisation restait libre de son calendrier et de ses choix : quelles applications intégrer, quand le faire et comment gérer les droits d'accès.

Gardez une architecture simple

En quelques mots

Un projet a plus de chance de réussir si son coût est réduit et s'il s'intègre bien dans l'informatique existante. Il faut donc utiliser une architecture aussi simple que possible. Sachez que la solution de SSO elle-même n'est qu'une partie de l'équation. Il faut aussi disposer d'une liste fiable – et mise à jour – des utilisateurs. Et pour que chaque utilisateur travaille sans incident, les informations de SSO stockées sous l'identité de chaque utilisateur (mots de passe chiffrés, liste des applications autorisées...) doivent résider dans chaque site principal.

Néanmoins, ces exigences n'entraînent pas nécessairement une complexité de la solution. En réutilisant les annuaires, serveurs et ressources réseau déjà en place, le projet peut réaliser des économies importantes à l'installation et à l'usage.

Pourquoi est-ce important ?

Maîtriser le coût et la complexité d'un projet contribue à sa réussite. Vous pourrez démontrer plus facilement un retour sur investissement rapide.

Ainsi, votre entreprise possède certainement déjà un référentiel des identités – par exemple l'annuaire LDAP existant. Autant utiliser nativement cette ressource. Vous profiterez ainsi des procédures existantes de mise à jour des utilisateurs.

De la même façon, les « appliances » permettent des déploiements rapides sur quelques centaines d'utilisateurs. Cependant, si votre entreprise est organisée en plusieurs sites, vous risquez de multiplier ces appliances et le support associé. En utilisant plutôt des bases locales existantes, vous conservez la logistique et les compétences actuelles

Le cas pratique

Un groupement hospitalier souhaitait équiper de SSO ses 5000 personnels soignants et administratifs. Ses objectifs : baisse des coûts du helpdesk et accès sécurisé par carte du personnel soignant. Bien entendu, la continuité de service est primordiale en milieu hospitalier.

Une solution de SSO avec des appliances était en phase de déploiement. Cependant, du fait du volume et de la complexité de son organisation, l'hôpital a constaté des insuffisances de performance et de fiabilité. En prenant en compte maintenance et remplacement, le coût d'usage était plus élevé que prévu, et la haute disponibilité non assurée.

L'hôpital a donc préféré s'appuyer sur l'annuaire Active Directory existant. En effet, cet annuaire peut abriter lui-même les données de SSO. Aucun nouveau matériel n'a été nécessaire. Les données de SSO sont ainsi disponibles sur chaque site, proches des utilisateurs ; le SSO est donc plus rapide. La haute disponibilité du SSO est celle de l'annuaire. De plus, les plans de secours et procédures de sauvegarde existent déjà : ce sont ceux qui sont en place pour l'annuaire.

Publiez régulièrement des indicateurs chiffrés

En quelques mots

Tout au long de votre projet, le SSO publie des rapports de déploiement et d'exploitation. La visibilité du SSO dépassant le cadre de l'informatique, ces rapports sont compréhensibles pour des non-techniciens, et contiennent des indicateurs parlant :

- Nombre de PCs sur lesquels le SSO est installé, d'utilisateurs concernés
- Volume d'appels au helpdesk, de problèmes résolus
- Taille et portée des données d'audit collectées, fonctions de sécurité activées
- Indices de satisfaction des utilisateurs (via des enquêtes)
- Quantité de comptes applicatifs déclarés, au total et par utilisateur
- Nombre d'applications prises en compte par le SSO
- Nombre de logins « automatisés » avec estimation du temps gagné

Les points plus techniques sont bien sûr importants, mais ces rapports sont des outils de communication autant que de suivi. Dans bien des cas, un outil d'audit automatisé recueille les indicateurs. Cela facilite le travail d'analyse et d'optimisation. Ainsi, il est généralement facile de démontrer le retour sur investissement rapide du SSO.

Pourquoi est-ce important ?

Ces rapports rendent visible la progression du projet. Comme nous l'avons vu, vous devrez obtenir la confiance de responsables opérationnels, financiers, auditeurs... Ils attendent des résultats objectifs : fournissez-les clairement.

N'oubliez pas qu'un déploiement se passe beaucoup mieux avec la participation active des départements concernés. Une fois les premiers sites et services déployés, les rapports et chiffres concrets serviront à convaincre les suivants. Lorsque le déploiement du SSO sera terminé, vous aurez acquis un capital de crédibilité qui accélèrera des phases ultérieures, ou d'autres projets.

Le cas pratique

Dans la filiale française d'une banque internationale, la direction sécurité a constaté que la multiplication des mots de passe créait des trous de sécurité et mécontentait les 1200 employés. Elle a donc lancé un projet de SSO avec biométrie. Pour obtenir le feu vert, un argument important a été la baisse attendue du coût de helpdesk.

Les rapports d'utilisation de la biométrie ont permis d'identifier les bons et les mauvais élèves. Pour les bons élèves, ceux ayant activés la biométrie, le rapport a permis de vérifier que les faux rejets étaient peu nombreux. Pour les mauvais élèves, ceux n'ayant pas activé la biométrie, le rapport a permis d'envoyer des e-mails de relance pour leur rappeler la nouvelle politique d'authentification.

Grâce à ce suivi, la nouvelle politique d'authentification a pu être mise en place rapidement avec succès. Les enseignements pratiques et chiffrés ont également contribué à convaincre la maison mère de généraliser la nouvelle politique à l'international.

Préparez la mise en place de la gestion des identités

En quelques mots

A la fin d'un projet de SSO, il est utile de faire un bilan sur l'atteinte des objectifs. Certains points en suspens, comme l'authentification forte ou la prise en compte de nouvelles applications, pourront faire l'objet de projets ultérieurs.

Evidian a constaté que les projets de SSO sont une excellente première étape pour des projets plus ambitieux de gestion des identités. En effet, vous disposerez au bout de quelques mois d'une source d'information précieuse : vous savez quels comptes applicatifs sont réellement utilisés, et par qui.

Cet état permet aussi de détecter les comptes dormants (comptes déclarés dans l'application qui ne sont associés à aucun utilisateur). Ces comptes peuvent alors être supprimés ou désactivés et ainsi permettre une diminution du coût des licences.

Pourquoi est-ce important ?

Un projet de SSO réussi est l'occasion de proposer de prochaines étapes vers la gestion des identités et des accès (IAM). La raison est simple. Comme vous connaissez à présent l'usage réel des applications, vous pouvez définir une politique de sécurité réaliste. De plus, avant de l'imposer, vous pouvez prédire quels en seront les résultats.

De la même façon, vous pourrez mettre en œuvre le « provisionnement » des comptes, à savoir leur mise à jour automatisée, sous le contrôle d'un circuit d'approbation. Les mots de passe de ces comptes seront transmis au SSO.

Ainsi, les utilisateurs respecteront naturellement la politique de sécurité. Leurs comptes seront créés et supprimés automatiquement en fonction de leur parcours dans l'entreprise.

Le cas pratique

Une grande société ferroviaire européenne souhaitait mettre en place une politique de sécurité pour gérer les comptes de plus de 150.000 utilisateurs sur 80 applications, soit plus d'un million de comptes applicatifs.

Elle a donc démarré un inventaire de ces comptes, mais cela s'est révélé à la fois utopique et coûteux. D'une part la collecte était plus difficile que prévu, mais surtout, comment savoir qui utilise le compte « sch002 » : un employé, toute une équipe, personne ? La société a rapidement réalisé que continuer dans cette voie coûterait des milliers d'heures d'efforts.

La société a donc préféré réaliser automatiquement un inventaire des comptes réellement utilisés. Pour cela, elle s'est basée sur le client de SSO d'Evidian. Pendant 3 mois, elle a ainsi accumulé sans effort des informations sur l'usage réel de l'informatique. Chaque fois qu'un utilisateur utilisait un compte, cette information était historiée dans une base centrale. Dans un second temps, la société a recoupé cette base avec la liste des comptes déclarés dans les applications. Cela lui a permis d'éliminer les comptes obsolètes, et de bâtir sa politique de sécurité sur une fondation concrète. C'est sur ces fondations qu'un futur projet de gestion des identités et des accès pourra être élaboré.

Le déroulement de votre projet de SSO

Chaque projet de SSO est différent, mais tous suivent généralement le même cheminement. Notez que pour un déploiement sur plus d'une centaine de postes, il est préférable de s'appuyer sur un prestataire intégrateur.

1. La maquette

vant de choisir un fournisseur, exigez de tester son produit sur quelques PCs et des applications représentatives. Observez la prestation : l'installation est-elle facile, peut-on facilement intégrer les applications, qu'en sera-t-il en grandeur nature?

2. La planification

Mettez par écrit les objectifs chiffrés et fonctionnels. Faites un bilan des interlocuteurs internes avec le prestataire intégrateur, et sélectionnez des représentants des utilisateurs. Réalisez un inventaire des sites, applications à intégrer et exigences spécifiques. Vous en tirerez un calendrier prévisionnel.

3. Le pilote

Cette étape est importante – choisissez un service représentatif. Par exemple, testez le produit sur 100 utilisateurs pendant 30 jours. Profitez de cette étape pour configurer le SSO sur les applications les plus courantes. N'omettez pas de faire un bilan détaillé et d'en tirer des leçons pour le déploiement général.

4. Le déploiement

Dans un premier temps, vous devez vous assurer que vous disposez d'un annuaire complet et fiable des utilisateurs. Si ce n'est pas le cas, des outils permettent de bâtir et maintenir à jour cette source d'information. Dans un second temps, l'installation du client de SSO sur les PCs se fera par phase, par exemple service par service. Informez clairement les utilisateurs au préalable, voire proposez des formations pour certains d'entre eux. Laissez le temps au helpdesk de répondre aux questions inévitables avant de passer au service suivant. Lors du déploiement, fournissez régulièrement des rapports factuels aux responsables hiérarchiques. Ils doivent constater la progression du projet et les résultats obtenus.

5. Le bilan

A la fin du projet, faites le bilan du déploiement. Les points restant à traiter doivent être identifiés et faire l'objet de plans d'action.

Ce sera l'occasion de prévoir les phases suivantes, comme la gestion des politiques d'accès ou le provisionnement des comptes des applications.

La Suite logicielle Evidian

Nous proposons à nos clients une offre complète, intégrée et modulaire leur permettant une gestion des identités numériques et une gouvernance des accès compatibles avec leurs politiques de sécurité et les exigences réglementaires.

Notre approche sectorielle offre aux organisations une mise en place de nos solutions adaptées au métier de chacun.

Notre suite logicielle est reconnue par les clients et les analystes pour sa complétude. Elle offre les composants suivants, pouvant être déployés indépendamment ou de manière combinée :

- **Evidian Identity Governance & Administration (IGA)** 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. IGA gère es quatre piliers du marché de la gouvernance des identités et des accès : Identités, Politique, Processus & Accès. Avec IGA, les utilisateurs obtiennent, en temps et en heure, les accès aux seules ressources dont ils ont besoin, avec les droits appropriés et pour des raisons métier légitimes.
- **Evidian Web Access Manager (WAM)** fédère des accès aux applications web, sécurise l'accès des utilisateurs. En effet, les utilisateurs mobiles et partenaires doivent accéder à leur messagerie ou aux applications d'entreprise en toute sécurité. WAM permet de gérer l'accès aux applications web et de remplacer l'ensemble des mots de passe des utilisateurs par un mode d'authentification unique et ce sans aucune modification des applications.
- **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.

Pour plus d'informations, consultez : **evidian.com**

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.

Pour plus d'information : **Evidian.com**

CT_180622_EM_WP-7-RULES-SUCCESSFUL-SSO-FR