Evidian

Authentication Manager orientation métier prêt à l'emploi

Une authentification multi-facteurs orientée métier

Sécurise l'accès à vos PC et vos serveurs en toute situation. Offre tous les scénarios d'authentification, pour un utilisateur accédant à un ou plusieurs PC, ou plusieurs utilisateurs partageant un même PC.

Le mot de passe Windows est un maillon faible des politiques d'authentification. Il est trop simple ou partagé entre utilisateurs, ce qui constitue un risque d'intrusion, et rend quasiment impossible un audit précis de l'usage des comptes Windows.

Une authentification forte répond à ces problèmes en remplaçant le mot de passe par un dispositif d'authentification physique ou de la biométrie. En pratique, l'authentification forte se heurte à des contraintes opérationnelles : pour déployer et gérer des milliers d'utilisateurs, vous devez couvrir tous les cas d'usage, sans perturber vos employés dans leurs tâches journalières.

Fonctionnalités adaptées aux métiers

Avec Authentication Manager, les employés d'agence ou de magasin partagent un même PC et basculent en quelques secondes vers leur environnement de travail sans changement de session Windows.

Lors de leur visite auprès des patients, les médecins retrouvent aisément la même session Windows sur les différents postes de l'hôpital.

Depuis un seul PC, les traders et les superviseurs des salles de contrôle peuvent ouvrir, verrouiller, déverrouiller ou fermer un groupe de PC avec n'importe quel moyen d'authentification.

Un employé peut déléguer de manière permanente ou temporaire l'accès à ses sessions verrouillées pour un ou plusieurs PC. Le verrouillage pouvant être transparent pour permettre la visualisation.

Simplification du déploiement de l'authentification multi-facteurs

Evidian Authentication Manager simplifie le déploiement et la gestion de l'authentification forte au quotidien :

- gestion centralisée de la politique d'accès
- profil d'authentification basé sur les groupes
- gestion de cartes (assignation, inventaire, liste noire...)
- audit centralisé de l'ensemble des tentatives d'accès aux PC.

En choisissant Evidian Authentication Manager, vous n'êtes pas lié à une technologie. Vous déployez la bonne authentification au bon endroit. Votre politique d'authentification est définie centralement, quel que soit la méthode d'authentification.

Réduction des coûts d'utilisation

Grâce à Authentication Manager, l'équipe du support technique peut déverrouiller ou interdire immédiatement l'accès quel que soit le moyen d'authentification (mot de passe, carte à puce, badge RFID, biométrie, mot de passe à usage unique (OTP)...) depuis une console unique.

De plus, les utilisateurs peuvent déverrouiller de manière autonome leur accès Windows en utilisant des questions/réponses (SSPR). Cela réduit les nombreuses demandes de déblocage au support technique.

Exploitation de l'infrastructure existante

Evidian Authentication Manager s'appuie sur votre annuaire LDAP ou Active Directory où seront stockées de manière chiffrée les données de sécurité : les utilisateurs ne sont pas dupliqués et aucun autre équipement n'est nécessaire.

Authentification par Microsoft smart card logon

Evidian Authentication Manager est entièrement compatible avec le smart card logon et peut vous faire bénéficier de procédures d'accès de secours efficaces.

Intégration du client léger IGEL

Evidian Authentication Manager et IGEL simplifient, accélèrent et sécurisent l'authentification aux clients légers. Les utilisateurs peuvent accéder à des clients légers sous Linux avec un badge RFID ou une carte à puce.

Les employés déjà authentifiés peuvent accéder à leur session (Citrix XenApp et Microsoft RDS) rapidement et en toute sécurité à n'importe quel client léger durant la journée, et ceci en présentant simplement leur badge RFID ou en insérant leur carte à puce.

Facilité de déploiement

Commencez par un seul service puis étendez Authentication Manager à des milliers d'utilisateurs. Evidian Authentication Manager est compatible avec les environnements suivants : Microsoft Windows, Citrix XenApp et Windows Terminal Serve

FRANCE CYBER SECURITY

Trusted partner for your **Digital Journey**

Atos

Orientation métier – Prêt à l'emploi

Compatible avec une vaste gamme de méthodes d'authentification

Evidian Authentication Manager est compatible avec la plupart des technologies d'authentification :

- cartes à puces avec ou sans certificats
- biométrie digitale ou veineuse
- badges radio (RFID)
- mot de passe à usage unique (OTP)
- questions / réponses
- identifiant / mot de passe.

Gestion du cycle de vie de l'authentification

Evidian Authentication Manager inclut des fonctionnalités de gestion de cartes vous permettant de gérer de manière centralisée le cycle de vie du dispositif. Vous pouvez émettre, prêter, suspendre ou mettre en liste noire une carte. Lors de l'assignation ou de la mise en liste noire, vous pouvez émettre ou révoquer les certificats liés à l'utilisateur.

Délégation initiée par l'utilisateur

Encadrés par la politique de sécurité, lorsque des utilisateurs prévoient de s'absenter, Evidian Authentication Manager leur permet de déléguer l'accès à leur PC.

Gestion des comptes partagés

Les utilisateurs peuvent utiliser des comptes Windows génériques en toute sécurité. Ils n'ont pas besoin de connaître les mots de passe ; les évènements d'audit contiennent leur identité et non celle du compte générique.

Accès de secours depuis l'écran de connexion Windows

La fonctionnalité Self Service Password Request (SSPR) réduit les coûts d'utilisation en autorisant les utilisateurs à réinitialiser leur mot de passe de manière autonome. En complément, un challenge fourni par le support technique peut être nécessaire. Si les utilisateurs oublient leur moyen d'authentification, ils doivent répondre à des questions personnelles, pour pouvoir réinitialiser leur mot de passe ou accéder à leur session Windows.

Lorsque les utilisateurs réinitialisent leur mot de passe avec cette fonctionnalité, ce mot de passe peut être :

- un mot de passe temporaire : autorisé pour une durée déterminée
- un mot de passe valide uniquement sur le PC où la réinitialisation a été demandée
- le nouveau mot de passe de l'utilisateur.

… Même hors connexion!

Le personnel itinérant peut réinitialiser son accès depuis son PC même s'il n'est pas connecté au réseau d'entreprise.

En tant qu'alternative aux questions-réponses, QRentry peut également être utilisé comme un accès de secours.

Accès de secours depuis le portail Web

Tout comme sur leur poste de travail, les utilisateurs peuvent se connecter au portail Web Authentication Manager pour répondre aux questions ou activer l'accès de secours.

Le portail Web peut également servir à réinitialiser leur mot de passe avec :

- un code de confirmation envoyé à l'utilisateur par e-mail ou SMS
- QRentry comme moyen d'authentification
- un captcha peut être configuré pour renforcer l'accès à la sécurité de la procédure d'accès de secours.

Module avancé de rapports

Evidian Authentication Manager contient un module de rapports vous permettant de générer des tableaux de bord sur des indicateurs clés tel que : l'activité, un aperçu instantané, le risque, la surveillance et des indicateurs clés de performance. Seuls les utilisateurs autorisés peuvent télécharger ces rapports.

Vérification de la conformité de votre système d'information avec les lois et réglementations en vigueur

Les traces d'audit liées aux accès et aux actions d'administration sont stockées dans une base de données centrale.

Authentication Manager vous aide à vous conformer aux obligations légales et règlementaires comme la loi Sarbanes – Oxley, les décrets sur la confidentialité médicale, la norme PCI DSS ou encore les lois sur l'intégrité financière.

Vous pouvez surveiller les tentatives d'accès aux PC. Les évènements d'audit contiennent les informations d'identification des utilisateurs. Cela vous permet de vérifier que votre politique d'accès est respectée et remplit ses objectifs.

Intégration avec ActiveSync

Evidian Web Access Manager peut contrôler les accès des appareils mobiles au système de messagerie électronique en utilisant le protocole ActiveSync sans que le mot de passe Windows ne soit nécessaire sur l'appareil. Pour se faire, Evidian Web Access Manager utilise le mot de passe Windows fourni par Evidian Authentication Manager pour s'authentifier sur le serveur de messagerie. L'association d'Evidian Authentication Manager et Web Access Manager vous permet d'offrir l'accès aux serveurs de messagerie sans exposer les mots de passe Windows à l'extérieur de l'entreprise.

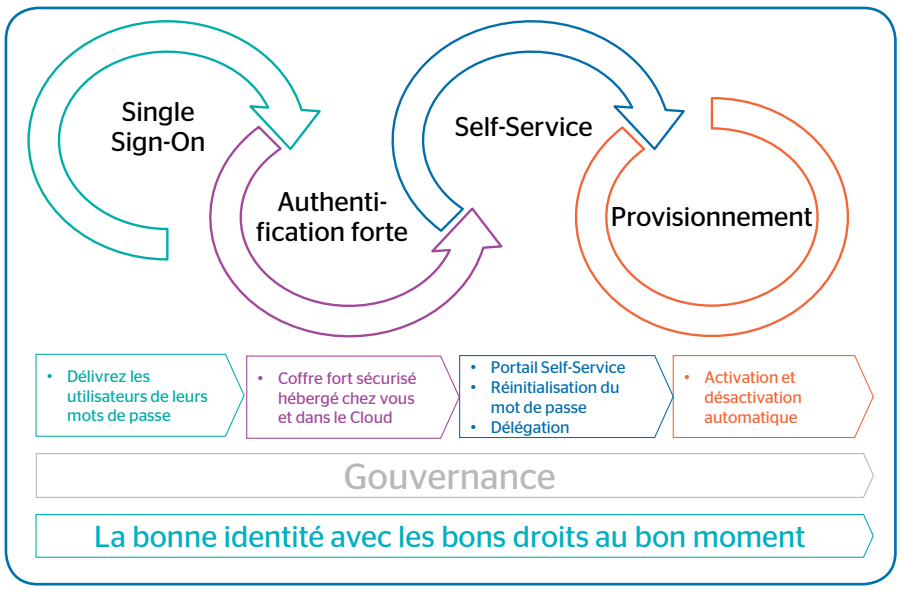
Intégration aux solutions IAM d'Evidian

Evidian Authentication Manager fait partie de la solution de gestion des identités et des accès Identity and Access Manager (IAM) d'Evidian.

- Avec Evidian Enterprise SSO, vous accédez à vos applications sans avoir à mémoriser un mot de passe
- Avec Evidian Web Access Manager, les utilisateurs accèdent sans avoir à se ré-authentifier à leurs applications Web depuis n'importe quel navigateur en toute sécurité
- Des workflows d'approbation associés à une politique de sécurité permettent à Evidian Identity & Access Manager de gérer les identités et les accès

Authentification forte par QR Code

Avec Evidian QRentry, les utilisateurs s'authentifient à Windows simplement en scannant un QR Code avec leur appareil mobile. Cet accès est disponible si vous êtes connecté ou non au réseau d'entreprise.



Find out more about us
evidian.com

CT_180618_LPM_Fs-Evidian_Authentification_manager_fr2