

Gestion métier de l'authentification multi-facteurs pour toute l'organisation



Evidian Authentication Manager

Sécurisez l'accès à vos postes de travail et serveurs en toute situation. Couvrez tous les scénarios d'authentification, pour un utilisateur accédant à un ou plusieurs PC, ou plusieurs utilisateurs partageant un même PC.

Les mots de passe sont le point faible de nombreuses politiques d'authentification. Les mots de passe Windows simples ou partagés créent un risque d'intrusion, et rendent presque impossible la vérification précise de l'usage des comptes Windows.

L'authentification forte résout ces problèmes en remplaçant les mots de passe par des dispositifs ou de la biométrie. Mais l'authentification forte rencontre des contraintes opérationnelles. Pour déployer et gérer des milliers d'utilisateurs, il faut couvrir tous les cas d'usage - sous peine de gêner le travail des employés.

Fonctions adaptées aux métiers

Les employés d'agence et les commerciaux en magasin utilisent un PC en kiosque et y retrouvent leur propre environnement en quelques secondes sans devoir changer de session Windows. En hôpital, la session de travail d'un médecin le suit quand il effectue son tour de garde.

Les traders et les techniciens de salle de contrôle peuvent ouvrir, verrouiller, déverrouiller ou fermer une grappe de PCs avec une seule authentification multi-facteurs. Et ils peuvent déléguer l'accès à leurs sessions verrouillées, de façon totale ou partielle, permanente ou temporaire.

Simplifiez l'authentification forte multi-facteurs

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

- Gestion de politique d'accès centralisée.
- Profil d'authentification basé sur les groupes.
- Système intégré de gestion de carte (inventaire, émission, liste noire...).
- Audit centralisé de toutes les tentatives d'accès aux ordinateurs.

Avec *Evidian Authentication Manager*, vous n'êtes pas enfermé dans une technologie. Vous déployez la bonne authentification au bon endroit. Votre politique de sécurité est définie en une seule fois - pour tous les modes d'accès.

Réduisez les coûts d'utilisation

Evidian Authentication Manager remplace plusieurs consoles d'administration. Le help desk débloque ou supprime l'accès en quelques secondes, que ce soit par mot de passe Windows, carte à puce, RFID, biométrie ou mot de passe à usage unique (OTP).

Les utilisateurs Windows débloquent leur accès eux-mêmes avec les mots de passe de secours en self-service (SSPR). Cela élimine de nombreux appels au support.

FONCTIONNALITES

Sécurisez des scénarios complexes d'authentification

Evidian Authentication Manager adapte l'utilisation de l'authentification forte aux contraintes métier des utilisateurs, en permettant des scénarios élaborés tels que :

- Basculement de l'accès quand une carte est perdue, oubliée ou ne fonctionne pas.
- Mode kiosque et changement rapide d'utilisateur
- Authentification sur une grappe de PCs avec un seul équipement d'authentification.
- Accès individuel nommé à des comptes Windows génériques.
- Délégation de comptes Windows entre utilisateurs.
- Lien avec le contrôle d'accès physique.

Un large éventail de méthodes d'authentification

La plupart des technologies d'authentification sont supportées :

- Cartes à puce et les clés USB de sécurité, avec ou sans certificat
- Biométrie digitale et veineuse
- Badge radio RFID
- Mot de passe à usage unique
- Questions et réponses
- Login / mot de passe

Gérez le cycle de vie complet de l'authentification

Evidian Authentication Manager vous permet de gérer le cycle de vie des cartes en un seul point. Vous attribuez les cartes et gérez cartes de remplacement, liste noire, données et certificats.

Fonctionnalités métier spécifiques

Vendeurs et employés d'agence partagent un kiosque et obtiennent leur bureau personnel en quelques secondes, sans relancer la session Windows. Quand les médecins font leur ronde, leur session Windows se déplace avec eux dans l'hôpital.

Traders et employés de salle de contrôle accèdent à une grappe de PC par une seule authentification. Ils la verrouillent, déverrouillent, en délèguent tout ou partie, de façon permanente ou temporaire.

Délégation par l'utilisateur

Lorsque les utilisateurs partent en vacances ou doivent s'absenter, *Evidian Authentication Manager* leur permet de déléguer l'accès à leur ordinateur sous le contrôle de la politique de sécurité.

Gestion des comptes partagés

Les utilisateurs peuvent utiliser les comptes Windows génériques en toute sécurité. Ils n'ont pas besoin de connaître les mots de passe et sont identifiés par leur nom.

Un accès de secours ...

Quand *Evidian Authentication Manager* est lancé sur un PC pour la première fois, l'utilisateur choisit des questions et réponses. S'il oublie son moyen d'accès, il obtient ainsi un accès temporaire.

... même hors connexion !

Les utilisateurs mobiles peuvent réinitialiser leur accès même s'ils ne sont pas connectés. Ils répondent aux questions à partir de la fenêtre de login de leur ordinateur portable.

Auditez tous les accès et actions administrative

Des pistes d'audit signées sont stockées dans une base centrale. Analysez-les par point d'accès, application, utilisateur, carte à puce etc. Les données sont exportables vers des outils de SIEM et de rapports.

Intégration dans des solutions IAM d'Evidian

Evidian Authentication Manager fait partie des solutions de gestion des identités et des accès d'Evidian. Vos cycles de vie d'authentification et d'identité convergent.

- Avec *Evidian Enterprise SSO*, lancez vos applications sans mot de passe supplémentaire.
- Avec *Evidian Web Access Manager*, accédez en toute sécurité aux applications Web depuis tout navigateur, sans se ré-authentifier.

Utilisez l'infrastructure existante

Evidian Authentication Manager utilise votre base LDAP ou Active Directory. Les utilisateurs ne sont pas dupliqués.

Toutes les données de sécurité y sont cryptées et stockées ; il n'y a pas de boîtier à installer. Vous pouvez commencer dans un département et étendre ensuite *Evidian Authentication Manager* à des milliers d'utilisateurs.

Evidian Authentication Manager fonctionne sur la plupart des versions Microsoft Windows, Terminal Server et Citrix XenApp .

© 2008-2011 Evidian

Evidian est une marque déposée, propriété d'Evidian, société anonyme immatriculée à Versailles, RCS B422 689 208. Tous les produits, noms, marques et autres éléments, cités dans ce document appartiennent à leurs propriétaires respectifs et peuvent être protégés au titre des lois et règlements régissant la propriété intellectuelle. Evidian se réserve le droit de modifier les caractéristiques de ses produits sans avis préalable.

Pour plus d'information, visitez notre site Web : www.evidian.fr ou contactez nous : info@evidian.com

Evidian - rue Jean Jaurès B.P.68 - 78340 Les Clayes sous Bois - France - Tél. : +33 (0)1 30 80 37 00 - Fax : +33 (0)1 30 80 37 10.

Cette brochure est imprimée sur un papier composé de 40 % de fibres éco-certifiées, issues d'une gestion forestière durable, et de 60 % de fibres recyclées, en application des règles environnementales (ISO 14001).