EVIDEN

Gestion des identités et des accès d'Eviden

Self-Service password reset

Une mesure de sécurité unique ne convient pas à toutes les situations

Un seul appel au support technique pour une réinitialisation de mot de passe coûte environ 15 euros et nécessite du temps (environ 20 minutes). Entre trois et quatre réinitialisations de mots de passe par employé et par an sont réalisées (selon le Gartner Research - Note T-15-6454). La réinitialisation du mot de passe Windows par l'utilisateur lui-même (Self-Service Password Reset) réduit ce coût et permet à votre support technique de se consacrer à d'autres tâches.



Eviden Self-Service Password Reset (SSPR) offre plusieurs méthodes d'authentification différentes. Depuis un portail web ou depuis leur poste de travail, les utilisateurs peuvent réinitialiser leurs mots de passe Windows en toute sécurité sans contacter le support technique. Eviden Self-Service Password Reset est également disponible en mode non connecté au réseau.

Eviden Self-Service Password Reset identifie l'utilisateur avec différents moyens: questions et réponses, scan d'un QR code, code de confirmation envoyé par e-mail ou SMS qui, par la suite, exécute la réinitialisation d'un nouveau mot de passe ou génère un mot de passe temporaire (TPA).

Les fonctionnalités d'Eviden Self- Service Password Reset permettent aux utilisateurs de changer leur mot de passe Windows en toute sécurité (connexion au réseau, connexion à Windows), qu'ils soient connectés ou non au réseau. La solution fournit une gamme étendue de méthodes d'authentification et des traces d'audit complètes pour démontrer l'implémentation de la politique de mot de passe.

Eviden Self-Service password reset

Les fonctionnalités de gestion des mots de passe primaires d'Eviden gèrent l'expiration et la réinitialisation du mot de passe Windows selon la politique de mot de passe.

Des notifications par e-mail sont envoyées avant l'expiration du mot de passe pour aider l'utilisateur à gérer son mot de passe Windows et lorsque ce-dernier est modifié.

Une gamme étendue de méthodes d'authentification utilisant le Self-Servic Password Reset:

- Répondez à des questions prédéfinies avec ou sans réseau de disponible et sans avoir à contacter le support technique.
- Scannez un QR code avec l'app QRentry avec ou sans réseau de disponible et sans avoir à contacter le support technique (le mobile ne requiert aucune connexion réseau).
- Utilisez un mot de passe unique envoyé par e-mail sans impliquer le support technique (réseau requis).
- Utilisez un mot de passe unique envoyé par SMS sans impliquer le support technique (réseau requis).
- La sécurité peut être renforcée en utilisant un mécanisme de challenge-réponse lorsque la réinitialisation du mot de passe est utilisée hors-ligne par exemple.

Application d'une politique de mot de passe forte grâce à Eviden Self-Service Password Reset

Eviden SSPR peut faire appliquer une politique de mot de passe forte pour la connexion au réseau. Vous pouvez définir le format du mot de passe pour la connexion au réseau, comme le type de caractères ainsi que leur position, leur nombre minimum et maximum, etc.

Cette politique peut être différente selon la personne qui réinitialise le mot de passe Windows.

Traces d'audit complètes des accès au réseau et des modifications de mot du passe avec Eviden Self-Service Password Reset

La solution fournit des traces d'audit complètes sur QUI accède à QUOI, QUAND et depuis OÙ. Des rapports basés sur ces traces d'audit peuvent être générés.

Ces rapports peuvent aider à démontrer l'efficacité de l'implémentation de votre politique de changement de mot de passe. Ils peuvent également démontrer le retour sur investissement.

Les fonctionnalités de reporting peuvent également être utilisées pour détecter des comptes pour lesquels le mot de passe Windows n'a pas été changé depuis un certain temps (compte Windows dangereux/inutiles).

Utilisez l'infrastructure LDAP/Active Directory existante de votre entreprise

Eviden SSPR s'appuie sur votre Active Directory existant. Vous n'avez donc pas besoin de synchroniser les identités; une fois que le SSPR est installé, tous les utilisateurs peuvent en bénéficier.

Toutes les données de sécurité Eviden sont chiffrées et stockées dans votre annuaire d'entreprise : Active Directory ou AD LDS.

Depuis l'écran d'authentification et un portail Web

Le service autonome de réinitialisation de mot de passe Windows d'Eviden est disponible depuis le portail Web et depuis l'écran d'authentification du poste de travail de l'utilisateur.

La solution est facile à déployer et est compatible avec l'infogérance. Elle s'intègre parfaitement dans les environnements de travail numériques avec une large gamme de terminaux et d'infrastructures VDI (Citrix XenApp, Windows RDS et VMware.

Vérification d'identité

Un mécanisme de questions & réponses peut également être utilisé pour identifier l'utilisateur.

Depuis le portail Web, les utilisateurs peuvent générer un code unique qui peut être vérifié par un administrateur.

En activant les vérifications par OTP via le mobile, les SMS et les e-mails pour les vérifications d'identités, les organisations peuvent accroitre le taux d'adoption du Self-Service Password Reset par les utilisateurs de 98%.

3 raisons de gérer les mots de passe avec Eviden Self-Service Password Reset:



Déchargez votre support technique des réinitialisations de mots de passe



Totalement intégré à votre environnement Microsoft, avec une interface intuitive pour les utilisateurs



Facilitez le déploiement de l'authentification multi-facteurs en offrant une solution de secours simple et conviviale.

Fonctionnalités principales d'Eviden Enterprise SSO (E-SSO)

Une solution non intrusive

Aucune de vos applications n'aura besoin d'être modifiée. Eviden Enterprise SSO active l'authentification unique pour de nombreux types d'application : Windows, Web, console virtuelle, etc.

Une solution universelle

Eviden Enterprise SSO s'exécute depuis un poste de travail Windows, mac OS, Android, iOS, un smartphone, une tablette, un serveur, un environnement virtuel comme Citrix ou Microsoft et une machine virtuelle telle que zéro client ou un client léger. Le coffre-fort personnel, les informations d'authentification, les notes personnelles et l'authentification unique restent sécurisées en permanence et l'utilisateur peut toujours y accéder depuis n'importe quel terminal.

Accès sans mot de passe à vos applications mobiles

Eviden élargit son offre d'authentification unique pour les entreprises grâce à Eviden Enterprise SSO pour appareils mobiles : Eviden fournit désormais une solution SSO pour Android et iOS. Enterprise SSO pour appareils mobiles saisit automatiquement les mots de passe des applications à votre place et stocke vos notes personnelles et mots de passe en toute sécurité dans votre coffre-fort numérique. Ces informations sont stockées de manière sécurisées

sur-site ou dans un Cloud et sont accessibles depuis votre poste de travail et vos appareils mobiles.

Transformez votre appareil mobile en un moyen d'authentification forte

Après avoir activé votre appareil mobile avec un QR Code, il devient un point d'accès sécurisé au réseau d'entreprise. L'authentification depuis votre appareil mobile vous donne alors accès à vos applications en toute sécurité.

Déploiement simple dans votre infrastructure existante

Eviden Enterprise SSO collecte les mots de passe utilisateurs, il est donc inutile de les redéfinir. Il peut également être associé à un système de provisionnement existant. Vous pouvez commencer par un seul service puis déployer le SSO sur des milliers d'appareils par la suite.

Eviden Enterprise SSO est basé sur les annuaires suivants : LDAP, Active Directory ou AD LDS. Aucun autre équipement n'est nécessaire.

Élimination des mots de passe pour les utilisateurs itinérants

Les utilisateurs, qu'ils soient internes ou externes, accèdent souvent à distance à des applications dans un environnement virtuel. Avec Eviden Enterprise SSO, ces utilisateurs n'ont plus besoin de mémoriser ni de taper leurs mots de passe pour accéder à ces applications virtualisées.

Eviden Enterprise SSO est certifié Citrix- Ready. Vous trouverez la liste complète des certifications sur le site Web d'Eviden.

Optimisation des accès distants pour le BYOD (Bring Your Own Device) et les appareils non gérés

Avec Web Access Manager, l'authentification unique est étendue aux appareils non gérés. Cela vous évite de devoir installer des agents sur des appareils et de révéler les mots de passe des applications à l'extérieur de votre réseau d'entreprise. De plus, cela permet aux ordinateurs, tablettes et smartphones qui accèdent aux applications dans le Cloud d'utiliser la fédération d'identité à travers les protocoles standards comme SAMLv2, OpenIDConnect/OAUTH.

Authentification forte

Eviden Authentication Manager renforce et gère l'authentification forte pour Windows grâce à des cartes à puces ou des jetons USB chiffrés, des mots de passe à usage unique (OTP), la biométrie, les badges RFID, les smartphones avec QRentry, etc.

Self-Service Password Reset

La fonction de demande du mot de passe par l'utilisateur (SSPR) permet aux utilisateurs qui ont oublié leur mot de passe Windows ou leur carte d'accès de déverrouiller leurs accès - même sans réseau, avec ou sans l'aide du support technique.

Accès d'urgence à la session Windows

Avec la demande du mot de passe par l'utilisateur, les utilisateurs peuvent débloquer eux-mêmes leurs accès avec une procédure d'urgence, disponible en ligne et hors ligne.

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. Ils y accèdent en présentant leur badge RFID ou en insérant une carte à puce.

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.

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

Vous pouvez surveiller les tentatives d'accès aux applications et PC. Tous les accès sont audités par nom, y compris les accès aux comptes Windows et aux applications génériques. Cela vous permet de vérifier que votre politique d'accès est respectée et remplit ses objectifs.

Connect with us

eviden.com

Eviden is a registered trademark © Copyright 2026, Eviden SAS – All rights reserved.