Devolutions

Password Hub Business

FICHE TECHNIQUE

SOLUTION DE GESTION DE MOTS DE PASSE POUR LES ENTREPRISES

INTRODUCTION

La gestion des mots de passe devient un vrai cauchemar et un important enjeu de sécurité pour les départements de TI et les entreprises dans le monde entier. Les accès privilégiés aux ressources clés sont protégés par des mots de passe partagés. Cette pratique rend les ressources vulnérables aux fuites de données et aux attaques de l'intérieur si les mots de passe ne sont pas gérés adéquatement. La majorité des professionnels des TI doit accomplir des tâches complexes, dont sécuriser des mots de passe. Le principal défi est de trouver un juste équilibre entre la sécurité et l'accessibilité. En effet, les mots de passe privilégiés des administrateurs et des utilisateurs doivent être stockés à un emplacement chiffré et sécurisé, sans compromettre l'expérience utilisateur.

Heureusement, Devolutions offre Password Hub Business, une solution complète de gestion de mots de passe non seulement conçue pour les départements de TI, mais aussi pour l'ensemble des entreprises. Ainsi, les administrateurs et les utilisateurs peuvent accéder aux mots de passe privilégiés stockés dans leur base de données chiffrée à partir de notre application Web.

Selon les permissions définies par l'administrateur à l'aide de notre système de contrôle d'accès basé sur les rôles, l'utilisateur peut se connecter aux sessions ou aux sites Web appropriés sans avoir à saisir, ni à voir, les informations d'identification. Puis, chaque entrée ou action dans une session sont journalisées à des fins d'audit et de conformité.

CONFIGURATION MINIMALE DU SYSTÈME

Les applications de Password Hub Business requièrent l'accès à Internet en tout temps. Elles comprennent une interface Web, des applications Bureau et des applications mobiles et un module PowerShell.

Interface Web

- Google
- Firefox
- Opera
- Safari
- Edge

Module PowerShell

- Windows 7 +
- Windows Server 2008 R2 +
- macOS 10.13 +
- RHEL / CentOS 7+, Fedora 29+, Debian 9+, Ubuntu 16.04+, openSUSE 15+, Alpine Linux 3.8+

Applications mobiles

- Android Marshmallow
- iOS 10

Spécifications relatives à la sécurité

Hôte	Microsoft Azure basé sur la région sélectionnée par l'utilisateur au moment de la création
Protection des données	• Données sensibles chiffrées par une clé AES 256 GCM • Clés de chiffrement protégées par la technologie Key Vault de Microsoft avec RSA 4096 • Niveau additionnel de chiffrement pour les données au repos en utilisant la technologie Transparent Data Encryption de Microsoft.
Transmission des données	• Données transmises par TLS
Modes d'authentification	Compte Devolutions • Nom d'utilisateur/Mot de passe • OAuth2 via JWS, avec la prise en charge d'OpenID
Authentification à deux facteurs	Dans le compte Devolutions : • Authenticator – Notification poussée sur mobile – Devolutions Authenticator • Application Authenticator : - Devolutions Authenticator (Android ou iOS) - Google Authenticator - Microsoft Authenticator - Authy • Courriel • SMS
Contrôle des accès	• Permissions basées sur les rôles dans les coffres partagés • Par coffre d'utilisateur
Surveillance	• Journaux des activités • Journaux et historique par entrée • Journaux administratifs
Conformité	SOC2 de Type II (Vous retrouverez le rapport SOC 2 sous l'onglet Sécurité en cliquant sur le lien suivant.)

Devolutions | CONTROL THE IT CHAOS

Pour plus d'informations, veuillez visiter notre site Web au **https://devolutions.net/fr**