ARTICLE DE LA BASE DE CONNAISSANCES

Password Vault. Présentation de la solution

2026 © Vitextra SIA. Tous droits réservés.

Clause d'exclusion de responsabilité

Aux fins du présent Avis de non-responsabilité :

- La **Société** (désignée par « la Société », « Nous » ou « Notre » dans le présent Avis de non-responsabilité) désigne Vitextra SIA, Matīsa iela 61-25, Rīga, LV-1009, Latvia.
- Le **Document** désigne l'article de la base de connaissances.
- **Vous** désigne la personne physique qui accède au Document, ou la société ou autre entité juridique pour le compte de laquelle cette personne accède au Document ou l'utilise, selon le cas.
- Le **Site web** désigne Vitextra, accessible à l'adresse https://vitextra.com

Avis de non-responsabilité

Les informations contenues dans le Document sont fournies à titre purement informatif et général.

La Société décline toute responsabilité quant aux erreurs ou omissions dans le contenu du Document.

En aucun cas la Société ne pourra être tenue responsable de dommages spéciaux, directs, indirects, consécutifs ou accessoires, ni de quelque dommage que ce soit, que ce soit dans le cadre d'une action contractuelle, d'une action en négligence ou d'une autre action délictuelle, résultant de l'utilisation du contenu du Document ou en lien avec celle-ci. La Société se réserve le droit d'ajouter, de supprimer ou de modifier le contenu du Document à tout moment et sans préavis.

Avis de non-responsabilité relatif aux erreurs et omissions

Les informations fournies dans le Document sont destinées uniquement à une orientation générale sur des sujets d'intérêt. Par conséquent, des erreurs peuvent survenir, même si la Société prend toutes les précautions pour que le contenu du Document soit à jour et exact. En outre, compte tenu de l'évolution des lois, règles et réglementations, les informations contenues dans le Document peuvent comporter des retards, des omissions ou des inexactitudes.

La Société n'est responsable ni des erreurs ou omissions, ni des résultats obtenus par l'utilisation de ces informations.

Avis de non-responsabilité relatif à l'usage équitable

La Société peut utiliser des contenus protégés par le droit d'auteur que le titulaire des droits n'a pas expressément autorisés. La Société met ces contenus à disposition à des fins de critique, de commentaire, de reportage d'actualité, d'enseignement, d'étude ou de recherche.

La Société estime que cela constitue un « usage équitable » (« fair use ») de ces contenus protégés par le droit d'auteur, au sens de la Section 107 de la loi américaine sur le droit d'auteur (United States Copyright Act).

Si Vous souhaitez utiliser des contenus protégés par le droit d'auteur issus du Document pour Vos propres besoins, au-delà de l'usage équitable, Vous devez obtenir l'autorisation du titulaire des droits d'auteur.

Avis de non-responsabilité « Utilisation à Vos propres risques »

Toutes les informations du Document sont fournies « en l'état », sans garantie d'exhaustivité, d'exactitude, d'actualité ni des résultats obtenus par l'utilisation de ces informations, et sans garantie d'aucune sorte, expresse ou implicite, y compris, mais sans s'y limiter, les garanties de performance, de qualité marchande et d'adéquation à un usage particulier.

La Société ne sera responsable ni envers Vous ni envers quiconque de toute décision prise ou de toute action entreprise sur la base des informations fournies dans le Document, ni de tout dommage consécutif, spécial ou similaire, même si elle a été informée de la possibilité de tels dommages.

Nous contacter

Si Vous avez des questions concernant le présent Avis de non-responsabilité, Vous pouvez Nous contacter par e-mail : support@vitextra.com.

Table des matières

Introduction 4

Fonctionnalités principales 4

Fonctionnement 5

- **Où les entrées sont stockées** 5
- **Chiffrement et code PIN** 6
- **Travailler sur plusieurs appareils** 7

À quoi sert Password Vault 7

Configuration requise 8

Introduction

Les employés accumulent des identifiants pour de nombreux systèmes non couverts par l'authentification unique : portails fournisseurs, extranets partenaires, environnements de test, inscriptions à des conférences, consoles d'équipements. Sans outil dédié, ces identifiants finissent dans des feuilles de calcul, sur des post-it ou dans des brouillons d'e-mails.

Password Vault est un composant WebPart SharePoint Framework qui offre à chaque employé un gestionnaire de mots de passe personnel dans Microsoft 365. Chaque utilisateur tient sa propre liste d'entrées — nom, nom d'utilisateur, mot de passe, URL, remarques, dossier et étiquettes — protégée par un code PIN à 4 chiffres. Les entrées sont stockées chiffrées dans un fichier du OneDrive de l'utilisateur, et non dans des listes SharePoint ni sur les serveurs de Vitextra. Le même composant WebPart peut être placé sur une page SharePoint ou dans Microsoft Teams, et chaque utilisateur voit toujours son propre coffre-fort.

Cet article explique ce que fait le composant WebPart et comment il fonctionne. Pour le placer sur une page, voir KB10438. Comment ajouter le composant WebPart Password Vault à une page et créer votre coffre-fort.

Fonctionnalités principales

Un coffre-fort personnel pour chaque utilisateur. Le composant WebPart affiche le coffre-fort de la personne qui ouvre la page. Le placer sur une page partagée ou dans un canal d'équipe ne partage aucun mot de passe : chaque visiteur ne voit que ses propres entrées.

Protection par code PIN. Lors de la première utilisation, l'utilisateur définit un code PIN à 4 chiffres. Tant que le coffre-fort est verrouillé, le composant WebPart n'affiche aucune entrée, seulement une invite de saisie du code PIN ; une fois le code PIN saisi, toutes les entrées et actions sont disponibles. Voir KB10442. Comment configurer votre code PIN dans Password Vault.

Verrouillage automatique. Une fois le code PIN saisi, le coffre-fort reste déverrouillé tant que l'utilisateur travaille avec lui et se verrouille de nouveau après 5 minutes sans interaction : la liste est masquée et les boîtes de dialogue ouvertes sont fermées. Le rechargement de la page le verrouille également. Voir KB10451. Verrouillage automatique : quand Password Vault demande à nouveau le code PIN.

Des entrées complètes. Chaque entrée comporte un **Nom**, un **Nom d'utilisateur**, un **Mot de passe**, une **URL** facultative qui s'ouvre dans un nouvel onglet, un **Dossier**, des

Étiquettes et des **Remarques**. Voir KB10443. Comment ajouter, modifier et supprimer des entrées dans Password Vault.

Copie en un clic. Le nom d'utilisateur et le mot de passe sont copiés dans le Presse-papiers avec les boutons **Copier dans le Presse-papiers**, si bien que les mots de passe n'ont pas besoin d'être affichés à l'écran. Voir KB10444. Comment afficher et copier un mot de passe ou un nom d'utilisateur dans Password Vault.

Générateur de mots de passe. Le générateur intégré crée des mots de passe aléatoires de 8 à 64 caractères à partir des jeux de caractères choisis par l'utilisateur, à l'aide du générateur de nombres aléatoires cryptographique du navigateur. Voir KB10445. Comment générer un mot de passe robuste avec le générateur de Password Vault.

Indicateur de robustesse. Pendant la saisie d'un mot de passe, une barre en cinq niveaux indique sa robustesse estimée, de *Très faible* à *Très fort*. Voir KB10446. Indicateur de robustesse des mots de passe dans Password Vault : signification des niveaux.

Dossiers, étiquettes et favoris. Les entrées peuvent être regroupées dans des dossiers, marquées d'un nombre quelconque d'étiquettes et ajoutées aux favoris, qui sont toujours affichés en haut de la liste. Voir KB10447. Organiser les entrées avec des dossiers et des étiquettes dans Password Vault et KB10448. Favoris dans Password Vault : garder les entrées fréquemment utilisées en haut de la liste.

Recherche et filtre. La zone **Rechercher** trouve les entrées par nom, nom d'utilisateur, URL, dossier, remarques et étiquettes ; la liste déroulante de filtre restreint la liste aux favoris, à un dossier ou à une étiquette. Voir KB10449. Rechercher et filtrer les entrées dans Password Vault.

SharePoint et Microsoft Teams. Le composant WebPart fonctionne sur les pages SharePoint Online modernes, comme onglet de canal Teams et comme application personnelle Teams **Passwords**. C'est partout le même coffre-fort. Voir KB10457. Comment ajouter Password Vault à Microsoft Teams.

Thème et langue. Le composant WebPart suit le thème du site, y compris les arrière-plans de section, ainsi que la police du site. Son interface est traduite dans les langues de SharePoint et suit la langue de SharePoint ou de Teams. Dans une colonne étroite (moins de 500 pixels de large), la liste passe à une disposition compacte.

Fonctionnement

Où les entrées sont stockées

Le coffre-fort de chaque utilisateur est un fichier unique, `vitextra-password-vault.json`, situé dans le dossier d'application du OneDrive de cet utilisateur. Le composant WebPart lit et écrit ce fichier via Microsoft Graph au nom de l'utilisateur connecté. Rien n'est stocké dans des listes SharePoint, dans les propriétés du composant WebPart ni sur les serveurs de Vitextra.

Comme le coffre-fort se trouve dans le OneDrive de l'utilisateur et non sur la page, le même coffre-fort apparaît sur chaque page, chaque site et chaque onglet Teams où le composant WebPart est placé. Si le composant WebPart ne trouve aucun fichier de coffre-fort pour l'utilisateur, il en crée un vide et invite l'utilisateur à configurer un code PIN. Détails : KB10453. Où Password Vault stocke vos mots de passe : le dossier d'application OneDrive.

Chiffrement et code PIN

Le nom, le nom d'utilisateur, le mot de passe, l'URL, les remarques, le dossier et les étiquettes de chaque entrée sont chiffrés avec AES dans le navigateur de l'utilisateur avant l'enregistrement du fichier. La clé de chiffrement est dérivée du code PIN avec PBKDF2-SHA256 (un sel aléatoire par coffre-fort, 600 000 itérations) ; elle n'est stockée nulle part et n'existe que dans la mémoire de la page ouverte tant que le coffre-fort est déverrouillé. Le fichier du coffre-fort seul ne suffit donc pas pour lire les entrées. Le fichier ne circule qu'entre le navigateur et le OneDrive de l'utilisateur, et son accès est régi par les autorisations de Microsoft 365 et de OneDrive, comme pour tout autre fichier du OneDrive de l'utilisateur.

Le code PIN ouvre le coffre-fort. Tant que le coffre-fort est verrouillé, le composant WebPart n'affiche aucune entrée — pas même leurs noms —, mais seulement l'invite **Entrez le code PIN** avec quatre cases dans lesquelles les chiffres sont masqués. Gardez à l'esprit qu'un code PIN ne comporte que 4 chiffres (10 000 combinaisons) : PBKDF2 ralentit volontairement chaque tentative, mais une personne qui obtient une copie du fichier pourrait tout de même essayer tous les codes PIN hors connexion, car la limite de 5 tentatives ne s'applique qu'à l'intérieur du composant WebPart. Le contrôle d'accès à OneDrive reste donc la première ligne de protection. Pour une description complète, voir KB10452. Comment Password Vault protège vos données : chiffrement, code PIN et stockage et KB10456. Qui peut voir vos mots de passe dans Password Vault.

Avertissement

Un code PIN oublié ne peut être ni récupéré ni réinitialisé — ni par l'utilisateur, ni par un administrateur, ni par Vitextra. Après 5 codes PIN incorrects consécutifs, le coffre-fort est bloqué, et la seule façon de l'utiliser à nouveau est **Réinitialiser**, qui efface toutes les entrées. Conservez votre code PIN en lieu sûr et gardez aussi vos identifiants importants à un autre endroit approuvé par votre organisation. Voir KB10455. Tentatives de code PIN incorrect dans Password Vault : que se passe-t-il après cinq échecs et KB10460. J'ai oublié mon code PIN dans Password Vault : quelles sont mes options ?.

Remarque

Les coffres-forts créés avec une version antérieure du composant WebPart sont migrés automatiquement vers le nouveau chiffrement la première fois que l'utilisateur saisit le bon code PIN ; les entrées et leurs dates de modification sont conservées. Les versions plus anciennes du composant WebPart ne peuvent pas ouvrir un coffre-fort migré : les administrateurs doivent donc mettre à jour Password Vault dans chaque catalogue d'applications du locataire. Voir KB10050. Comment mettre à jour une solution Vitextra SPFx dans SharePoint Online et KB10361. Catalogue d'applications du locataire ou de la collection de sites : où déployer les applications Vitextra.

Travailler sur plusieurs appareils

Chaque enregistrement est comparé à la version du fichier du coffre-fort à partir de laquelle il a été préparé. Si le coffre-fort a été enregistré ailleurs entre-temps — sur un autre appareil ou dans un autre onglet du navigateur —, le composant WebPart charge le fichier le plus récent et y applique la modification, de sorte que les modifications effectuées ailleurs ne sont pas écrasées. Une modification enregistrée sur un appareil apparaît sur un autre après un clic sur **Actualiser**, après l'enregistrement suivant ou après le déverrouillage sur cet appareil. Si le code PIN a été changé sur un autre appareil, la page ouverte se verrouille d'elle-même dès qu'elle le détecte et demande le nouveau code PIN.

À quoi sert Password Vault

Password Vault est un coffre-fort **personnel** léger. Son périmètre est volontairement restreint :

- Les entrées ne peuvent pas être partagées avec des collègues ; il n'existe pas de coffres-forts d'équipe ou partagés.
- Il n'y a ni extension de navigateur ni remplissage automatique des formulaires de connexion ; les identifiants sont copiés depuis le composant WebPart.
- Les administrateurs ne disposent d'aucune console pour gérer, consulter ou récupérer les coffres-forts des utilisateurs.
- Il n'y a ni exportation ni importation d'entrées.

Pour une comparaison avec d'autres types de gestionnaires de mots de passe, voir KB10440. Password Vault, gestionnaires de mots de passe des navigateurs ou gestionnaires de mots de passe d'entreprise : lequel choisir.

Remarque

Password Vault est destiné aux identifiants personnels. Pour les comptes d'administration hautement privilégiés et les identifiants qu'une équipe doit partager, suivez la politique de sécurité de votre organisation.

Configuration requise

- Microsoft 365 avec SharePoint Online ; pages modernes. Le composant WebPart n'est pas disponible pour SharePoint Server.
- Chaque utilisateur doit disposer d'un OneDrive dans le locataire, car le coffre-fort y est stocké.
- Le package est déployé depuis le catalogue d'applications comme tout produit Vitextra ; le déploiement à l'échelle du locataire est pris en charge. Voir KB10035. Comment installer un produit Vitextra dans SharePoint Online.
- Un administrateur doit approuver l'autorisation déléguée Microsoft Graph `Files.ReadWrite.AppFolder`, qui permet au composant WebPart de lire et d'écrire uniquement dans son propre dossier d'application du OneDrive de l'utilisateur. Voir KB10454. Autorisation Microsoft Graph Files.ReadWrite.AppFolder : pourquoi Password Vault en a besoin et comment l'approuver et KB10360. Comment approuver les autorisations d'API Microsoft Graph pour les solutions Vitextra dans le Centre d'administration SharePoint.
- Aucune autorisation sur des listes SharePoint n'est nécessaire : tout utilisateur qui peut ouvrir la page peut utiliser son propre coffre-fort.
- La licence est accordée par locataire. Lorsque la licence expire, le composant WebPart affiche *Nous espérons que vous avez apprécié votre version d'évaluation gratuite. Achetez une licence maintenant pour continuer à utiliser l'application.* à la place du coffre-fort jusqu'au renouvellement de la licence ; les fichiers des coffres-forts dans OneDrive ne sont pas modifiés. Voir KB10206. Licences et compte Vitextra

: acheter et activer une licence et KB10364. Que se passe-t-il à l'expiration de votre version d'évaluation ou de votre abonnement Vitextra.

Conseil

Les nouveaux utilisateurs peuvent commencer par KB10441. Password Vault : guide rapide pour les utilisateurs finaux. Les réponses aux questions courantes sont réunies dans KB10439. Password Vault : questions fréquentes.