ARTICLE DE LA BASE DE CONNAISSANCES

Comment Password Vault protège vos données : chiffrement, code PIN et stockage

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

Vue d'ensemble 4

Résumé 4

Couche 1 : connexion Microsoft 365 et contrôle d'accès OneDrive 5

Couche 2 : chiffrement des entrées dans le navigateur 5

- **Ce qui est chiffré et ce qui ne l'est pas** 6
- **Les coffres-forts existants sont mis à niveau automatiquement** 7

Couche 3 : le code PIN et le coffre-fort verrouillé 8

Verrouillage automatique 9

Limite de tentatives infructueuses 9

Aucune donnée chez Vitextra 10

Usage prévu de Password Vault 10

Recommandations 10

Vue d'ensemble

Password Vault est un gestionnaire de mots de passe personnel pour les pages SharePoint Online et Microsoft Teams. Chaque utilisateur conserve ses propres identifiants dans un seul fichier chiffré, dans son propre OneDrive. Cet article explique, couche par couche, comment les données sont protégées, ce que fait et ne fait pas le code PIN, quelles parties du coffre-fort sont chiffrées et pour quel type d'identifiants Password Vault est conçu. Il s'adresse aux utilisateurs finaux qui veulent comprendre le produit ainsi qu'aux administrateurs et aux responsables de la sécurité qui l'évaluent.

Résumé

Question	Réponse
Où le coffre-fort est-il stocké ?	Dans un seul fichier, *vitextra-password-vault.json*, dans le dossier d'application du OneDrive de l'utilisateur
Qui peut ouvrir le fichier ?	Toute personne qui a accès au OneDrive de l'utilisateur selon les autorisations Microsoft 365 — par défaut, uniquement l'utilisateur
Quelle identité est utilisée ?	L'utilisateur Microsoft 365 connecté, par l'intermédiaire de Microsoft Graph avec l'autorisation déléguée *Files.ReadWrite.AppFolder*
Qu'est-ce qui est chiffré ?	Les champs texte de chaque entrée : nom, nom d'utilisateur, mot de passe, URL, remarques, dossier et étiquettes (AES, dans le navigateur, avec une clé dérivée du code PIN)
À quoi sert le code PIN ?	La clé de chiffrement est dérivée du code PIN à 4 chiffres ; tant que le code PIN n'est pas saisi, le composant WebPart n'affiche aucune entrée
Quand le code PIN est-il redemandé ?	Après 5 minutes sans interaction dans le composant WebPart, et après le

Question	Réponse
	rechargement de la page
Que se passe-t-il après des codes PIN erronés ?	Après 5 codes PIN erronés consécutifs, le coffre-fort est bloqué et ne peut plus qu'être réinitialisé, ce qui efface toutes les entrées
Qu'est-ce qui est envoyé à Vitextra ?	Aucune donnée du coffre-fort ; uniquement les identifiants techniques de la vérification de licence et de la télémétrie d'utilisation

Couche 1 : connexion Microsoft 365 et contrôle d'accès OneDrive

Password Vault n'a ni comptes, ni serveurs, ni bases de données propres. Le composant WebPart s'exécute dans le navigateur de l'utilisateur connecté et lit et écrit le coffre-fort par l'intermédiaire de Microsoft Graph avec l'identité de cet utilisateur. Le fichier est stocké dans le OneDrive de l'utilisateur ; il est donc protégé par les mêmes mécanismes que n'importe quel autre fichier qui s'y trouve : la connexion Microsoft 365 (y compris l'authentification multifacteur et l'accès conditionnel, si votre organisation les utilise), les autorisations OneDrive et les stratégies Microsoft 365 de votre organisation.

Le composant WebPart utilise une seule autorisation déléguée, *Files.ReadWrite.AppFolder*, qui lui permet de travailler uniquement dans le dossier d'application du OneDrive de l'utilisateur connecté. Il ne peut pas ouvrir les autres fichiers de l'utilisateur ni le OneDrive d'un autre utilisateur. Pour plus de détails, consultez KB10454. Autorisation Microsoft Graph Files.ReadWrite.AppFolder : pourquoi Password Vault en a besoin et comment l'approuver.

Comme le coffre-fort est conservé dans le OneDrive de l'utilisateur et non sur la page, chaque utilisateur qui ouvre une page ou un onglet Teams contenant le composant WebPart ne voit que son propre coffre-fort. Placer le composant WebPart sur une page partagée ne partage aucun mot de passe.

Couche 2 : chiffrement des entrées dans le navigateur

Avant l'enregistrement du coffre-fort, Password Vault chiffre les champs texte de

chaque entrée avec AES. Le chiffrement et le déchiffrement ont lieu dans le navigateur de l'utilisateur ; le fichier circule uniquement entre le navigateur et le OneDrive de l'utilisateur, par l'intermédiaire de Microsoft Graph. Par conséquent, les valeurs ne sont jamais stockées ni transférées en texte clair : une personne qui ouvre le fichier voit des chaînes chiffrées au lieu des noms, des noms d'utilisateur et des mots de passe.

La clé de chiffrement est dérivée du code PIN dans le navigateur avec PBKDF2-SHA256 (Web Crypto), à l'aide d'un sel aléatoire de 16 octets et de 600 000 itérations ; un nouveau sel est créé chaque fois qu'un code PIN est défini ou changé. La clé n'est stockée nulle part — ni dans le fichier du coffre-fort, ni dans le stockage du navigateur, ni chez Vitextra. Elle n'existe que dans la mémoire de la page ouverte tant que le coffre-fort est déverrouillé. Pour vérifier un code PIN, le composant WebPart en dérive la clé et déchiffre une valeur de contrôle — un texte connu chiffré avec la clé — que le fichier stocke avec le sel et le nombre d'itérations. Ni le code PIN ni un hachage du code PIN ne sont stockés. Par conséquent, le fichier du coffre-fort seul ne suffit pas pour lire les entrées : le code PIN est nécessaire.

Avertissement

Le code PIN ne comporte que 4 chiffres, soit 10 000 combinaisons possibles. PBKDF2 ralentit délibérément chaque essai, mais une personne qui obtient une copie du fichier de votre coffre-fort pourrait tout de même essayer tous les codes PIN hors ligne, en dehors du composant WebPart : la limite de cinq tentatives ne s'applique qu'à l'intérieur du composant WebPart. Le contrôle d'accès à votre OneDrive reste donc la première ligne de protection. Protégez votre compte Microsoft 365 et ne partagez ni le fichier du coffre-fort ni le dossier qui le contient.

Ce qui est chiffré et ce qui ne l'est pas

Données du fichier du coffre-fort	Chiffrées
Nom de l'entrée	Oui
Nom d'utilisateur	Oui
Mot de passe	Oui
URL	Oui
Remarques	Oui

Données du fichier du coffre-fort	Chiffrées
Dossier	Oui
Étiquettes	Oui
Indicateur de favori (l'étoile)	Non
Identifiants des entrées, dates de création et de modification	Non
Sel, nombre d'itérations et valeur de contrôle (utilisés pour vérifier le code PIN)	Sel et nombre d'itérations : non ; la valeur de contrôle est un texte connu chiffré avec la clé. Le code PIN, son hachage et la clé ne sont pas stockés
ID d'objet Microsoft Entra ID de l'utilisateur	Non
Compteur de tentatives infructueuses de code PIN	Non

Rien n'est écrit dans les listes SharePoint, dans les propriétés du composant WebPart ni dans le stockage du navigateur. La clé et les valeurs déchiffrées n'existent que dans la mémoire de la page ouverte tant que le coffre-fort est déverrouillé.

Les coffres-forts existants sont mis à niveau automatiquement

Les coffres-forts créés avec des versions antérieures de Password Vault utilisent l'ancien format de fichier, dans lequel la clé était dérivée d'un hachage SHA-256 du code PIN stocké dans le fichier et de l'ID d'objet Microsoft Entra ID de l'utilisateur. La première fois que vous saisissez le code PIN correct dans la nouvelle version, le composant WebPart rechiffre toutes les entrées avec une nouvelle clé dérivée avec PBKDF2 et enregistre le coffre-fort au nouveau format. Les entrées et leurs dates de modification sont conservées, et le compteur de tentatives infructueuses est remis à zéro. Vous n'avez rien à faire. Après la mise à niveau, le fichier ne contient plus le hachage du code PIN.

Remarque

La mise à niveau ne modifie que le fichier actuel du coffre-fort. Les versions antérieures du fichier que OneDrive conserve dans son historique des versions ou dans sa corbeille, ainsi que les copies dans les sauvegardes, restent à l'ancien format, dans lequel les entrées pouvaient être déchiffrées à partir du fichier lui-même, sans le code PIN. Les personnes qui peuvent les ouvrir sont déterminées par le contrôle d'accès OneDrive et par les paramètres de rétention et de sauvegarde de votre organisation.

Couche 3 : le code PIN et le coffre-fort verrouillé

Le code PIN est un code à 4 chiffres que l'utilisateur définit lors de la création du coffre-fort (voir KB10442. Comment configurer votre code PIN dans Password Vault). Il n'est nécessaire qu'une fois, pour ouvrir le coffre-fort : le composant WebPart le vérifie dès que le quatrième chiffre est saisi. Jusque-là, le coffre-fort est verrouillé et le composant WebPart n'affiche aucune entrée — pas même leurs noms. Au lieu de la liste, il affiche l'invite **Entrez le code PIN** avec « Entrez votre code PIN pour continuer » et quatre cases de chiffres, et la barre d'outils ne propose que le bouton **Actualiser**.

Action	Disponible tant que le coffre-fort est verrouillé
Consulter la liste avec le nom, le nom d'utilisateur, l'URL, le dossier, les étiquettes et les remarques des entrées	Non — la liste est masquée
Afficher un mot de passe (bouton en forme d'œil) ou **Copier dans le Presse-papiers** pour un mot de passe ou un nom d'utilisateur	Non
Nouvel élément, **Modifier**, **Supprimer**	Non
Changer le code PIN (l'engrenage **Configuration**)	Non
Ajouter aux favoris / **Retirer des favoris**	Non
Rechercher et filtre	Non
Actualiser	Oui

Après le code PIN correct, le coffre-fort est déverrouillé et toutes ces actions fonctionnent directement, sans redemander le code PIN, jusqu'à ce que le coffre-fort se verrouille.

Avertissement

Tant que le coffre-fort est déverrouillé, tout son contenu — y compris les mots de passe — peut être affiché et copié par toute personne qui utilise votre ordinateur, jusqu'à ce que le coffre-fort se verrouille à nouveau. Verrouillez votre ordinateur chaque fois que vous vous en éloignez.

Dans l'invite **Entrez le code PIN**, les chiffres sont masqués pendant la saisie. Sur les écrans **Configurer le code PIN** et **Changer le code PIN**, ils sont visibles : définissez ou changez donc votre code PIN là où personne ne peut voir votre écran.

Verrouillage automatique

Après le chargement de la page, le coffre-fort est verrouillé : aucune entrée n'est affichée, uniquement l'invite **Entrez le code PIN**. Après un code PIN correct, le coffre-fort s'ouvre et reste déverrouillé pendant que vous travaillez. Lorsqu'aucun clic ni aucune frappe de touche n'a eu lieu dans le composant WebPart pendant **5 minutes** (l'activité sur l'écran **Changer le code PIN** compte également), le coffre-fort se verrouille à nouveau : la liste disparaît, les mots de passe affichés sont masqués, la clé est supprimée de la mémoire, et toutes les boîtes de dialogue ouvertes (**Nouvel élément**, **Modifier les propriétés**, la confirmation de suppression) sont fermées sans enregistrement. Le rechargement de la page verrouille également le coffre-fort, car l'état déverrouillé n'existe que dans la page ouverte. Consultez KB10451. Verrouillage automatique : quand Password Vault demande à nouveau le code PIN.

Limite de tentatives infructueuses

Chaque code PIN erroné affiche « Le code PIN est incorrect » et le nombre de **Tentatives restantes**. Le compteur est stocké dans le fichier du coffre-fort et est toujours incrémenté à partir de la version la plus récente du fichier : les tentatives effectuées sur différents appareils et différentes pages s'additionnent de manière fiable. La ligne **Tentatives restantes** est affichée dans l'invite **Entrez le code PIN** dès que des tentatives erronées antérieures existent, y compris après un rechargement ou sur un autre appareil. Le compteur ne se réinitialise pas avec le temps — seul un code PIN correct le remet à zéro. Après **5** codes PIN erronés consécutifs, le coffre-fort est

bloqué : le composant WebPart n'affiche plus que l'écran **Réinitialiser**, et la réinitialisation efface toutes les entrées et le code PIN. Consultez KB10455. Tentatives de code PIN incorrect dans Password Vault : que se passe-t-il après cinq échecs.

Avertissement

Un code PIN oublié ne peut être ni récupéré ni réinitialisé, ni par vous, ni par votre administrateur, ni par Vitextra. Notez votre code PIN en lieu sûr et conservez également les identifiants importants dans un autre emplacement approuvé par votre organisation. Consultez KB10460. J'ai oublié mon code PIN dans Password Vault : quelles sont mes options ?.

Aucune donnée chez Vitextra

Vitextra ne reçoit, ne stocke ni ne sauvegarde aucune donnée du coffre-fort. Les seules requêtes du composant WebPart vers les services Vitextra sont la vérification de licence et la télémétrie d'utilisation avec des identifiants techniques. Pour la liste complète, consultez KB10363. Où les produits Vitextra stockent vos données : confidentialité, résidence des données et RGPD.

Usage prévu de Password Vault

Password Vault est conçu comme un emplacement pratique et personnel pour les identifiants du quotidien — connexions à des portails web, à des systèmes de partenaires, comptes de test et entrées similaires qu'un utilisateur conserverait sinon dans un carnet ou un fichier texte. Sa protection associe le contrôle d'accès Microsoft 365 et le chiffrement des valeurs stockées avec une clé dérivée d'un code PIN à 4 chiffres.

Ce n'est pas un système de gestion des accès privilégiés : il n'offre ni partage entre utilisateurs, ni récupération par un administrateur, ni journal d'audit propre, ni mot de passe principal à haut niveau de robustesse. Pour les comptes d'administrateur, les comptes de service, les identifiants partagés par une équipe et les autres secrets hautement privilégiés, suivez la stratégie de votre organisation et utilisez les outils qu'elle prescrit. Pour une comparaison avec d'autres approches, consultez KB10440. Password Vault, gestionnaires de mots de passe des navigateurs ou gestionnaires de mots de passe d'entreprise : lequel choisir.

Recommandations

- Protégez votre compte Microsoft 365 : le coffre-fort n'est pas plus sûr que le compte

propriétaire du OneDrive.
- Choisissez un code PIN difficile à deviner (évitez *0000*, *1234* ou votre année de naissance) et conservez-le en lieu sûr.
- Ne partagez pas et ne copiez pas le fichier du coffre-fort : une personne disposant d'une copie pourrait essayer les 10 000 codes PIN hors ligne.
- Verrouillez votre ordinateur lorsque vous vous en éloignez, même pour peu de temps.
- Un mot de passe copié reste dans le Presse-papiers jusqu'à ce que vous copiiez autre chose ; videz le Presse-papiers après utilisation sur les ordinateurs partagés.
- Si vous utilisez le coffre-fort sur plusieurs appareils ou onglets, les modifications sont combinées automatiquement ; cliquez sur **Actualiser** pour voir les modifications effectuées ailleurs (voir KB10453. Où Password Vault stocke vos mots de passe : le dossier d'application OneDrive).
- Ne stockez que les identifiants que votre organisation vous autorise à conserver dans un gestionnaire de mots de passe personnel.

Conseil

Pour savoir exactement qui peut et qui ne peut pas voir vos entrées, consultez KB10456. Qui peut voir vos mots de passe dans Password Vault.