ARTICLE DE LA BASE DE CONNAISSANCES

Qui peut voir vos mots de passe dans Password Vault

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

Les collègues qui ouvrent la même page peuvent-ils voir mes mots de passe ? 4

Les membres d'un canal Teams peuvent-ils voir mes mots de passe ? 5

Les propriétaires de pages ou les administrateurs de sites peuvent-ils voir mes mots de passe ? 5

Les administrateurs Microsoft 365 ou OneDrive peuvent-ils voir mes mots de passe ? 5

D'autres applications de mon organisation peuvent-elles accéder au fichier du coffre-fort ? 6

Vitextra peut-il voir mes mots de passe ? 6

Que peut voir une personne devant mon ordinateur déverrouillé ? 6

Puis-je partager volontairement une entrée avec un collègue ? 7

Articles connexes 8

Vue d'ensemble

Password Vault stocke les entrées de chaque utilisateur dans un seul fichier chiffré, *vitextra-password-vault.json*, dans le dossier d'application du propre OneDrive de cet utilisateur. Les personnes qui peuvent voir vos entrées dépendent donc de qui peut accéder à votre OneDrive et de qui peut utiliser votre ordinateur sur lequel vous êtes connecté — et non de qui peut ouvrir la page. Les réponses ci-dessous passent en revue les cas typiques.

Qui	Peut voir vos entrées ?
Les collègues qui ouvrent la même page	Non — ils voient leur propre coffre-fort
Les membres d'un canal Teams contenant un onglet Password Vault	Non — chaque membre voit son propre coffre-fort
Les propriétaires de pages et les administrateurs de sites	Non — rien n'est stocké sur la page ni sur le site
Les administrateurs Microsoft 365 / OneDrive	Ils peuvent accéder au fichier comme à n'importe quel autre fichier de votre OneDrive, mais ne peuvent pas lire les entrées sans le code PIN ; avec une copie du fichier, ils pourraient essayer les 10 000 codes PIN hors ligne
Vitextra	Non — Vitextra ne reçoit aucune donnée du coffre-fort
Une personne devant votre ordinateur déverrouillé	Sans le code PIN, rien — pas même les noms des entrées ; tout, tant que le coffre-fort est déverrouillé

Les collègues qui ouvrent la même page peuvent-ils voir mes mots de passe ?

Non. Le composant WebPart ouvre toujours le coffre-fort de la personne connectée. Si dix collègues ouvrent la même page SharePoint, chacun d'eux ne voit que ses propres entrées, lues depuis son propre OneDrive. Placer Password Vault sur une page partagée ne partage aucun mot de passe.

Les membres d'un canal Teams peuvent-ils voir mes mots de passe ?

Non. Un onglet Password Vault dans un canal Teams fonctionne comme le composant WebPart sur une page : chaque membre du canal qui ouvre l'onglet voit son propre coffre-fort. Il s'agit du même coffre-fort que celui que ce membre voit sur les pages SharePoint et dans l'application personnelle. Consultez KB10457. Comment ajouter Password Vault à Microsoft Teams.

Les propriétaires de pages ou les administrateurs de sites peuvent-ils voir mes mots de passe ?

Non. Password Vault ne stocke rien dans les listes, les bibliothèques SharePoint ni les propriétés du composant WebPart ; la page ne contient que le composant WebPart et son titre. Être propriétaire d'une page ou d'un site, ou administrateur de collection de sites, ne donne aucun accès aux fichiers de coffre-fort des personnes qui l'utilisent.

Les administrateurs Microsoft 365 ou OneDrive peuvent-ils voir mes mots de passe ?

Password Vault n'a pas de console d'administration : les administrateurs ne peuvent pas consulter, gérer, déverrouiller ni récupérer des coffres-forts au moyen du produit.

Le fichier du coffre-fort lui-même est un fichier ordinaire de votre OneDrive, protégé par le contrôle d'accès de Microsoft 365 et de OneDrive. Comme n'importe quel autre fichier de votre OneDrive, il est accessible aux administrateurs qui disposent d'un accès à votre OneDrive, ou qui s'en attribuent un, conformément aux stratégies de votre organisation — par exemple lors d'une enquête, au moyen d'outils de conformité ou lorsque le OneDrive d'un employé qui a quitté l'organisation est transféré. Les champs de ses entrées sont chiffrés avec une clé dérivée de votre code PIN et qui n'est pas stockée dans le fichier ; l'accès au fichier seul ne permet donc pas à un administrateur de lire vos entrées. Toutefois, le code PIN ne comporte que 4 chiffres : une personne ayant accès au fichier pourrait le copier et essayer les 10 000 codes PIN hors ligne. PBKDF2 ralentit chaque essai, et la limite de cinq tentatives ne s'applique qu'à l'intérieur du composant WebPart.

Avertissement

Face à une personne qui essaie tous les codes PIN sur une copie du fichier, un code PIN à 4 chiffres n'offre qu'une protection limitée ; le contrôle d'accès OneDrive reste donc la première ligne de protection. Password Vault est destiné aux identifiants personnels du quotidien. Pour les comptes d'administrateur, les comptes de service et les autres identifiants hautement privilégiés ou partagés, suivez la stratégie de votre organisation. Consultez KB10452. Comment Password Vault protège vos données : chiffrement, code PIN et stockage.

D'autres applications de mon organisation peuvent-elles accéder au fichier du coffre-fort ?

Le coffre-fort est enregistré au moyen de l'autorisation Microsoft Graph *Files.ReadWrite.AppFolder*. Dans SharePoint Online, cette autorisation est accordée à une seule application partagée par toutes les solutions SharePoint Framework du locataire ; les autres solutions SPFx déployées dans votre organisation qui utilisent la même autorisation travaillent donc avec le même dossier d'application pour le compte de l'utilisateur connecté. Une telle solution pourrait lire ou modifier le fichier du coffre-fort ; les entrées qu'il contient sont chiffrées avec une clé dérivée de votre code PIN, avec la limite décrite dans la section précédente. Les administrateurs ne doivent déployer que des solutions SPFx auxquelles ils font confiance. Consultez KB10454. Autorisation Microsoft Graph Files.ReadWrite.AppFolder : pourquoi Password Vault en a besoin et comment l'approuver.

Vitextra peut-il voir mes mots de passe ?

Non. Le chiffrement et le déchiffrement ont lieu dans votre navigateur, et le fichier du coffre-fort est transféré uniquement entre votre navigateur et votre OneDrive. Vitextra ne reçoit, ne stocke ni ne sauvegarde aucune donnée du coffre-fort, ni votre code PIN ni la clé qui en est dérivée. Le composant WebPart n'envoie à Vitextra que les identifiants techniques de la vérification de licence et de la télémétrie d'utilisation ; consultez KB10363. Où les produits Vitextra stockent vos données : confidentialité, résidence des données et RGPD.

Que peut voir une personne devant mon ordinateur déverrouillé ?

Toute personne qui peut utiliser votre navigateur pendant que vous êtes connecté à

Microsoft 365 peut ouvrir une page contenant Password Vault. **Sans le code PIN**, cette personne ne voit aucune entrée — pas même leurs noms :

- au lieu de la liste, le composant WebPart n'affiche que l'invite **Entrez le code PIN**, et la barre d'outils ne propose que le bouton **Actualiser** ;
- les mots de passe, noms d'utilisateur, URL, dossiers, étiquettes et remarques ne sont pas affichés, et **Nouvel élément**, **Changer le code PIN**, **Rechercher**, le filtre et les favoris ne sont pas disponibles ;
- la personne peut saisir des codes PIN, et chaque code PIN erroné compte dans la limite de cinq (voir ci-dessous).

Une fois le code PIN correct saisi, chaque action — afficher et copier des mots de passe, **Nouvel élément**, **Modifier**, **Supprimer** et **Changer le code PIN** — fonctionne sans redemander le code PIN.

Après que vous avez saisi le code PIN, le coffre-fort reste déverrouillé tant que la page est ouverte et utilisée : toute personne devant l'ordinateur peut afficher et copier des mots de passe et modifier des entrées jusqu'à ce que le verrouillage automatique s'applique après **5 minutes** sans interaction (voir KB10451. Verrouillage automatique : quand Password Vault demande à nouveau le code PIN). Un mot de passe que vous avez copié reste également dans le Presse-papiers jusqu'à ce que quelque chose d'autre soit copié.

Une personne qui ne connaît pas le code PIN peut également saisir des codes PIN erronés. Cinq codes PIN erronés consécutifs bloquent le coffre-fort, et la seule issue est une réinitialisation qui efface toutes les entrées (voir KB10455. Tentatives de code PIN incorrect dans Password Vault : que se passe-t-il après cinq échecs).

Conseil

Verrouillez votre ordinateur chaque fois que vous vous en éloignez, et définissez ou changez votre code PIN là où personne ne peut voir l'écran : sur les écrans **Configurer le code PIN** et **Changer le code PIN**, les chiffres sont visibles pendant la saisie (dans l'invite **Entrez le code PIN**, ils sont masqués).

Puis-je partager volontairement une entrée avec un collègue ?

Non. Password Vault est un coffre-fort personnel : il n'existe ni entrées partagées, ni dossiers partagés, ni coffres-forts d'équipe. Pour les identifiants qu'une équipe doit partager, suivez la stratégie de votre organisation.

Articles connexes

- KB10453. Où Password Vault stocke vos mots de passe : le dossier d'application OneDrive
- KB10452. Comment Password Vault protège vos données : chiffrement, code PIN et stockage
- KB10439. Password Vault : questions fréquentes