ARTICLE DE LA BASE DE CONNAISSANCES

Password Vault, gestionnaires de mots de passe des navigateurs ou gestionnaires de mots de passe d'entreprise : lequel choisir

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

Password Vault en bref 4

Comparaison en un coup d'œil 5

Quand Password Vault est un bon choix 6

Quand un gestionnaire de mots de passe de navigateur est un bon choix 6

Quand un gestionnaire de mots de passe d'entreprise est un bon choix 7

Utiliser les outils côte à côte 7

Questions à se poser avant de décider 8

Vue d'ensemble

Les organisations qui veulent que leurs employés cessent de conserver leurs mots de passe dans des feuilles de calcul et des notes envisagent généralement trois types d'outils :

- **Les gestionnaires de mots de passe des navigateurs** — le stockage de mots de passe intégré aux navigateurs web, qui enregistre les identifiants lorsque l'utilisateur se connecte à des sites web.
- **Les gestionnaires de mots de passe d'entreprise** — des produits dédiés, généralement dotés de leur propre service, d'applications clientes et d'extensions de navigateur, conçus pour la gestion des identifiants à l'échelle de l'organisation.
- **Password Vault** — un composant WebPart SharePoint Framework de Vitextra qui offre à chaque employé un coffre-fort personnel léger dans Microsoft 365 (SharePoint Online et Microsoft Teams).

Ces outils répondent à des problèmes différents. Cet article décrit les caractéristiques générales de chaque catégorie afin que vous puissiez déterminer laquelle correspond à un besoin donné. Les produits d'une même catégorie diffèrent les uns des autres ; vérifiez donc les spécificités de tout produit envisagé au regard de vos propres exigences.

Password Vault en bref

Password Vault stocke les entrées de chaque utilisateur, chiffrées, dans un fichier du OneDrive de cet utilisateur et les affiche dans un composant WebPart sur une page SharePoint ou dans Teams. L'accès à l'intérieur du composant WebPart est protégé par un code PIN à 4 chiffres, dont est dérivée la clé de chiffrement ; tant que le coffre-fort est verrouillé, aucune entrée n'est affichée, et il se verrouille automatiquement après 5 minutes sans interaction. Comme un code PIN ne comporte que 4 chiffres, le contrôle d'accès à OneDrive reste la première ligne de protection du fichier. Il comprend un générateur de mots de passe, un indicateur de robustesse, des dossiers, des étiquettes, des favoris et une recherche. Pour plus de détails, voir KB10437. Password Vault. Présentation de la solution.

Ce qu'il ne fait **pas** est tout aussi important :

- pas de remplissage automatique des formulaires de connexion ni d'extension de navigateur — les identifiants sont copiés avec **Copier dans le Presse-papiers** ;
- pas de partage d'entrées ni de coffres-forts d'équipe ;
- pas de console d'administration ni de récupération d'un code PIN oublié — après 5 codes PIN incorrects, la seule option est de réinitialiser le coffre-fort, ce qui efface

toutes les entrées ;
- pas d'exportation ni d'importation.

Comparaison en un coup d'œil

La colonne Password Vault décrit le produit ; les deux autres colonnes décrivent ce qui est typique de la catégorie.

Aspect	**Password Vault**	**Gestionnaires de mots de passe des navigateurs (typique)**	**Gestionnaires de mots de passe d'entreprise (typique)**
Objectif	Identifiants personnels d'un employé, dans Microsoft 365	Confort personnel lors de la navigation	Gestion des identifiants à l'échelle de l'organisation
Lieu de conservation des données	Fichier chiffré dans le OneDrive de l'utilisateur	Dans le profil du navigateur, souvent synchronisé via le compte de l'éditeur du navigateur	Dans le service du produit ou dans une infrastructure exploitée par l'organisation
Accès	Page SharePoint ou Microsoft Teams, avec le compte professionnel et un code PIN à 4 chiffres	Le navigateur dans lequel le profil est connecté	Applications clientes, extensions de navigateur et accès web du produit
Remplissage automatique des formulaires de connexion	Non	Oui	Généralement oui
Partage avec des collègues	Non	Limité ou inexistant dans un contexte professionnel	Généralement oui, avec des dossiers ou coffres-forts partagés
Administration, stratégies, audit	Non ; uniquement le déploiement et	Dépend des options de gestion	Généralement étendus

Aspect	**Password Vault**	**Gestionnaires de mots de passe des navigateurs (typique)**	**Gestionnaires de mots de passe d'entreprise (typique)**
	l'autorisation Graph	du navigateur	
Récupération d'un accès perdu	Aucune ; la réinitialisation efface le coffre-fort	Dépend du compte du navigateur	Propose généralement des options de récupération pour les administrateurs ou les utilisateurs
Déploiement	Un package SPFx et une autorisation Graph ; aucun logiciel client supplémentaire	Déjà présent dans le navigateur	Un produit distinct à déployer, configurer et licencier par utilisateur
Modèle de coût typique	Licence par locataire	Inclus avec le navigateur	Généralement un abonnement par utilisateur

Quand Password Vault est un bon choix

- Les employés ont besoin d'un endroit pour **leurs propres** identifiants professionnels — portails fournisseurs, extranets partenaires, systèmes de test, consoles d'équipements — et l'organisation souhaite que cet endroit se trouve dans Microsoft 365 plutôt que dans des outils ou fichiers personnels.
- L'organisation préfère que les données restent dans **son propre locataire** (le OneDrive de chaque utilisateur) et non chez un service tiers supplémentaire.
- Un outil simple qui fonctionne sur une page SharePoint et dans Teams sans installer d'extensions ni de logiciel client compte davantage que le remplissage automatique.
- Les identifiants ne sont pas partagés, et leur perte en cas d'oubli du code PIN est acceptable, car ils peuvent être rétablis depuis leur source (par exemple via la procédure « mot de passe oublié » du service concerné).

Quand un gestionnaire de mots de passe de navigateur est

un bon choix

- Le besoin principal est le confort : enregistrer et remplir automatiquement les mots de passe des sites web pendant la navigation.
- Les utilisateurs travaillent principalement dans un seul navigateur et la politique de l'organisation autorise à y stocker des identifiants professionnels.

N'oubliez pas qu'un gestionnaire de mots de passe de navigateur stocke les identifiants dans le profil du navigateur : ce qui est disponible dépend donc du navigateur et du compte avec lequel l'utilisateur est connecté, ainsi que de la façon dont l'organisation gère les navigateurs.

Quand un gestionnaire de mots de passe d'entreprise est un bon choix

- Les identifiants doivent être **partagés** au sein des équipes, par exemple des comptes de service ou des boîtes aux lettres partagées.
- L'organisation a besoin de **stratégies, de pistes d'audit, de révisions d'accès et de procédures de récupération** centralisées.
- Des comptes d'administration **hautement privilégiés** doivent être gérés — souvent en combinaison avec une gestion des accès privilégiés.
- Le remplissage automatique est requis dans les navigateurs, les applications de bureau et les applications mobiles.

Ces fonctionnalités s'accompagnent d'un produit distinct à déployer, à configurer, à enseigner aux utilisateurs et à licencier, généralement par utilisateur.

Avertissement

Password Vault est conçu pour les identifiants personnels. Il ne remplace pas une solution qui gère des comptes partagés ou hautement privilégiés. Pour de tels comptes, suivez la politique de sécurité de votre organisation.

Utiliser les outils côte à côte

Ces catégories ne s'excluent pas mutuellement. Une organisation peut exploiter un gestionnaire de mots de passe d'entreprise pour l'informatique et les comptes partagés, et proposer Password Vault à tous les employés comme espace personnel simple pour leurs autres identifiants professionnels — ou autoriser le stockage dans le navigateur pour les sites web à faible risque. L'essentiel est une politique claire qui

indique quel type d'identifiant va où.

Remarque

Password Vault ne propose ni importation ni exportation : faire entrer ou sortir des entrées implique de les ajouter une par une. Faites votre choix avant que les employés ne commencent à remplir leurs coffres-forts.

Questions à se poser avant de décider

1 Les identifiants doivent-ils être partagés, ou sont-ils strictement personnels ?
2 Le remplissage automatique des formulaires de connexion est-il requis ?
3 Où les données chiffrées peuvent-elles être stockées — dans votre locataire Microsoft 365, dans le compte d'un éditeur de navigateur ou dans un service tiers ?
4 Avez-vous besoin d'une récupération par l'administrateur, de stratégies et d'un audit ?
5 Que pouvez-vous déployer : un composant WebPart SPFx, ou un logiciel client et des extensions sur chaque appareil ?
6 Qu'advient-il des identifiants si un utilisateur perd l'accès — peuvent-ils être rétablis depuis le système source ?

Conseil

Pour savoir comment Password Vault protège les données et qui peut y accéder, lisez KB10452. Comment Password Vault protège vos données : chiffrement, code PIN et stockage et KB10456. Qui peut voir vos mots de passe dans Password Vault. Pour l'essayer, voir KB10438. Comment ajouter le composant WebPart Password Vault à une page et créer votre coffre-fort.