WISSENSDATENBANKARTIKEL

Wer Ihre Kennwörter in Password Vault sehen kann

2026 © Vitextra SIA. Alle Rechte vorbehalten.

Haftungsausschluss

Für die Zwecke dieses Haftungsausschlusses:

- **Das Unternehmen** (in diesem Haftungsausschluss entweder als „das Unternehmen“, „wir“, „uns“ oder „unser“ bezeichnet) bezieht sich auf Vitextra SIA, LV-1009 Riga, Matīsa iela 61 – 25.
- **Dokument** verweist auf den Wissensdatenbank-Artikel.
- **Sie** sind die Person, die auf das Dokument zugreift, bzw. das Unternehmen oder eine andere juristische Person, in deren Namen eine solche Person auf das Dokument zugreift oder es nutzt.
- **Die Website** verweist auf Vitextra, zugänglich über https://vitextra.com

Haftungsausschluss

Die in diesem Dokument enthaltenen Informationen dienen nur der allgemeinen Information.

Das Unternehmen übernimmt keine Verantwortung für Fehler oder Auslassungen im Inhalt des Dokuments.

In keinem Fall haftet das Unternehmen für besondere, direkte, indirekte oder zufällige Schäden oder für Schäden jeglicher Art, die sich aus der Nutzung des Inhalts des Dokuments ergeben, unabhängig davon, ob es sich um eine Klage aufgrund von Vertrag, Fahrlässigkeit oder anderen Delikten handelt. Das Unternehmen behält sich das Recht vor, den Inhalt des Dokuments jederzeit und ohne vorherige Ankündigung zu ergänzen, zu streichen oder zu ändern.

Haftungsausschluss für Fehler und Auslassungen

Die in dem Dokument enthaltenen Informationen dienen lediglich als allgemeine Orientierungshilfe zu Fragen von Interesse. Daher können Fehler auftreten, auch wenn das Unternehmen alle Vorsichtsmaßnahmen ergreift, um sicherzustellen, dass der Inhalt des Dokuments aktuell und korrekt ist. Außerdem kann es angesichts der sich ändernden Gesetze, Regeln und Vorschriften zu Verzögerungen, Auslassungen oder Ungenauigkeiten bei den in diesem Dokument enthaltenen Informationen kommen.

Das Unternehmen haftet nicht für etwaige Fehler oder Auslassungen oder für die Ergebnisse, die sich aus der Verwendung dieser Informationen ergeben.

Haftungsausschluss für faire Nutzung

Das Unternehmen darf urheberrechtlich geschütztes Material verwenden, das der Urheberrechtsinhaber nicht ausdrücklich genehmigt hat. Das Unternehmen stellt dieses Material für Kritik, Kommentare, Berichterstattung, Schulung, Wissenschaft oder Forschung zur Verfügung.

Das Unternehmen ist der Ansicht, dass dies eine „faire Nutzung“ von urheberrechtlich geschütztem Material im Sinne von Abschnitt 107 des US-Urheberrechtsgesetzes darstellt.

Wenn Sie urheberrechtlich geschütztes Material aus dem Dokument für Ihre eigenen Zwecke verwenden möchten, die über eine angemessene Nutzung hinausgehen, müssen Sie die Erlaubnis des Urheberrechtsinhabers einholen.

„Benutzung auf eigene Gefahr“ Haftungsausschluss

Alle Informationen in diesem Dokument werden im Ist-Zustand zur Verfügung gestellt, ohne Garantie auf Vollständigkeit, Genauigkeit, Aktualität oder auf die Ergebnisse, die sich aus der Verwendung dieser Informationen ergeben, und ohne jegliche ausdrückliche oder stillschweigende Garantie, einschließlich, aber nicht beschränkt auf Garantien für Leistung, Marktgängigkeit und Eignung für einen bestimmten Zweck.

Das Unternehmen haftet weder Ihnen noch anderen gegenüber für Entscheidungen oder Handlungen, die im Vertrauen auf die Informationen des Dienstes getroffen wurden, noch für Folgeschäden, besondere oder ähnliche Schäden, selbst wenn auf die Möglichkeit solcher Schäden hingewiesen wurde.

Kontaktieren Sie uns

Wenn Sie Fragen zu diesem Haftungsausschluss haben, können Sie uns per E-Mail kontaktieren: support@vitextra.com.

Inhaltsverzeichnis

Überblick 4

Können Kollegen, die dieselbe Seite öffnen, meine Kennwörter sehen? 4

Können Mitglieder eines Teams-Kanals meine Kennwörter sehen? 4

Können Seitenbesitzer oder Websiteadministratoren meine Kennwörter sehen? 5

Können Microsoft-365- oder OneDrive-Administratoren meine Kennwörter sehen? 5

Können andere Apps in meiner Organisation auf die Tresordatei zugreifen? 6

Kann Vitextra meine Kennwörter sehen? 6

Was kann jemand an meinem nicht gesperrten Computer sehen? 6

Kann ich einen Eintrag absichtlich mit einem Kollegen teilen? 8

Verwandte Artikel 8

Begriffe 9

Überblick

Password Vault speichert die Einträge jedes Benutzers in einer verschlüsselten Datei, *json*, im App-Ordner des eigenen OneDrive dieses Benutzers. Wer Ihre Einträge sehen kann, hängt daher davon ab, wer auf Ihr OneDrive zugreifen kann und wer Ihren angemeldeten Computer verwenden kann – nicht davon, wer die Seite öffnen kann. Die folgenden Antworten gehen die typischen Fälle durch.

Wer	Kann Ihre Einträge sehen?
Kollegen, die dieselbe Seite öffnen	Nein – sie sehen ihre eigenen Tresore
Mitglieder eines Teams-Kanals mit einer Password-Vault-Registerkarte	Nein – jedes Mitglied sieht seinen eigenen Tresor
Seitenbesitzer und Websiteadministratoren	Nein – auf der Seite oder der **Website** wird nichts gespeichert
Microsoft-365- / OneDrive-Administratoren	Sie können wie auf jede andere Datei in Ihrem OneDrive auf die Datei zugreifen, die Einträge aber ohne die PIN nicht lesen; mit einer Kopie der Datei könnten sie offline alle 10.000 PINs ausprobieren
Vitextra	Nein – Vitextra erhält keine Tresordaten
Jemand an Ihrem nicht gesperrten Computer	Bei gesperrtem Tresor nichts – nicht einmal die Namen der Einträge; alles, solange der Tresor entsperrt ist

Können Kollegen, die dieselbe Seite öffnen, meine Kennwörter sehen?

Nein. Das **Webpart** öffnet immer den Tresor der angemeldeten Person. Wenn zehn Kollegen dieselbe SharePoint-Seite öffnen, sieht jeder von ihnen nur seine eigenen Einträge, gelesen aus seinem eigenen OneDrive. Das Platzieren von Password Vault auf einer gemeinsam genutzten Seite gibt keine Kennwörter frei.

Können Mitglieder eines Teams-Kanals meine Kennwörter sehen?

Nein. Eine Password-Vault-Registerkarte in einem Teams-Kanal funktioniert wie das Webpart auf einer Seite: Jedes Kanalmitglied, das die Registerkarte öffnet, sieht seinen eigenen Tresor. Es ist derselbe Tresor, den das Mitglied auf SharePoint-Seiten und in der persönlichen App sieht.

Können Seitenbesitzer oder Websiteadministratoren meine Kennwörter sehen?

Nein. Password Vault speichert nichts in SharePoint-Listen, -Bibliotheken oder den Webpart-Eigenschaften; die Seite enthält nur das Webpart und seinen Titel. Der Besitz einer Seite oder Website oder die Rolle eines Websitesammlungsadministrators gewährt keinen Zugriff auf die Tresordateien der Personen, die es verwenden.

Können Microsoft-365- oder OneDrive-Administratoren meine Kennwörter sehen?

Password Vault hat keine Verwaltungskonsole: Administratoren können Tresore über das Produkt weder anzeigen, verwalten, entsperren noch wiederherstellen.

Die Tresordatei selbst ist eine gewöhnliche Datei in Ihrem OneDrive und durch die Zugriffssteuerung von **Microsoft 365** und OneDrive geschützt. Wie auf jede andere Datei in Ihrem OneDrive können Administratoren auf sie zugreifen, die gemäß den Richtlinien Ihrer Organisation Zugriff auf Ihr OneDrive haben oder sich diesen verschaffen – zum Beispiel im Rahmen einer Untersuchung, über Compliancetools oder wenn das OneDrive eines ausgeschiedenen Mitarbeiters übergeben wird. Ihre Eintragsfelder sind mit einem Schlüssel verschlüsselt, der aus Ihrer PIN abgeleitet und nicht in der Datei gespeichert wird, sodass der Zugriff auf die Datei allein einem Administrator nicht ermöglicht, Ihre Einträge zu lesen. Die PIN hat jedoch nur 4 Ziffern: Wer Zugriff auf die Datei hat, könnte sie kopieren und offline alle 10.000 PINs ausprobieren. PBKDF2 verlangsamt jeden Rateversuch, und die Begrenzung auf fünf Versuche gilt nur innerhalb des Webparts.

Warnung

Gegen jemanden, der an einer Kopie der Datei alle PINs ausprobiert, bietet eine 4-stellige PIN nur begrenzten Schutz; die OneDrive-Zugriffssteuerung bleibt daher die erste Schutzlinie. Password Vault ist für persönliche, alltägliche Anmeldeinformationen gedacht. Für Administratorkonten, Dienstkonten und andere hochprivilegierte oder gemeinsam genutzte Anmeldeinformationen befolgen Sie die Richtlinie Ihrer Organisation. Siehe KB10452. Wie Password Vault Ihre Daten schützt: Verschlüsselung, PIN und Speicherung.

Können andere Apps in meiner Organisation auf die Tresordatei zugreifen?

Der Tresor wird über die Microsoft-Graph-Berechtigung *Files.ReadWrite.AppFolder* gespeichert. In **SharePoint Online** wird diese Berechtigung einer einzigen Anwendung erteilt, die alle SharePoint-Framework-Lösungen im Mandanten gemeinsam nutzen. Daher arbeiten andere in Ihrer Organisation bereitgestellte SPFx-Lösungen, die dieselbe Berechtigung verwenden, im Namen des angemeldeten Benutzers mit demselben App-Ordner. Eine solche Lösung könnte die Tresordatei lesen oder ändern; die Einträge darin sind mit einem aus Ihrer PIN abgeleiteten Schlüssel verschlüsselt, mit der im vorherigen Abschnitt beschriebenen Einschränkung. Administratoren sollten nur SPFx-Lösungen bereitstellen, denen sie vertrauen. Siehe KB10454. Microsoft-Graph-Berechtigung Files.ReadWrite.AppFolder: Warum Password Vault sie benötigt und wie Sie sie genehmigen.

Kann Vitextra meine Kennwörter sehen?

Nein. Ver- und Entschlüsselung finden in Ihrem Browser statt, und die Tresordatei wird nur zwischen Ihrem Browser und Ihrem OneDrive übertragen. Vitextra empfängt, speichert und sichert weder Tresordaten noch Ihre PIN oder den daraus abgeleiteten Schlüssel. Das Webpart sendet an Vitextra nur die technischen Bezeichner der Lizenzprüfung und der Nutzungstelemetrie; siehe KB10363. Wo Vitextra-Produkte Ihre Daten speichern: Datenschutz, Datenresidenz und DSGVO.

Was kann jemand an meinem nicht gesperrten Computer sehen?

Jeder, der Ihren Browser verwenden kann, während Sie bei Microsoft 365 angemeldet sind, kann eine Seite mit Password Vault öffnen. **Solange der Tresor gesperrt ist,** sieht

diese Person ohne PIN überhaupt keine Einträge – nicht einmal ihre Namen:

- statt der **Liste** zeigt das Webpart nur die Eingabeaufforderung **PIN eingeben**, und die Symbolleiste bietet nur die Schaltfläche **Aktualisieren**;
- Kennwörter, Benutzernamen, URLs, Ordner, Tags und Hinweise werden nicht angezeigt, und **Neues Element**, **PIN ändern**, **Suchen**, der Filter und die Favoriten sind nicht verfügbar;
- die Person kann PINs eingeben, und jede falsche PIN zählt zur Begrenzung auf fünf Versuche (siehe unten).

Sobald die korrekte PIN eingegeben wurde, funktioniert jede Aktion – Anzeigen und Kopieren von Kennwörtern, **Neues Element**, **Bearbeiten**, **Entfernen** und **PIN ändern** – ohne erneute Abfrage der PIN.



Was sichtbar ist, solange der Tresor gesperrt ist

Nachdem Sie die PIN eingegeben haben, bleibt der Tresor entsperrt, solange die Seite geöffnet ist und verwendet wird: Jeder am Computer kann Kennwörter anzeigen und kopieren und Einträge ändern, bis die automatische Sperre nach **5 Minuten** ohne Interaktion greift (siehe KB10451. Automatische Sperre: Wann Password Vault erneut nach der PIN fragt). Ein von Ihnen kopiertes Kennwort bleibt außerdem in der Zwischenablage, bis etwas anderes kopiert wird. Als Aktivität gelten Interaktionen innerhalb des Webparts; Aktionen an anderer Stelle der Seite starten den Timer nicht neu.

Jemand, der die PIN nicht kennt, kann auch falsche PINs eingeben. Fünf falsche PINs in Folge blockieren den Tresor, und der einzige Ausweg ist ein Zurücksetzen, das alle Einträge löscht (siehe KB10455. Falsche PIN-Eingaben in Password Vault: Was nach fünf Fehlversuchen passiert).

Die fünfte falsche PIN sperrt den Zugriff, löscht aber keine Einträge automatisch. Zum Löschen müssen Sie **Zurücksetzen** bestätigen und der leere Tresor muss erfolgreich gespeichert werden. Fehlversuche werden erst nach dem Speichern des Zählers in OneDrive mit anderen Seiten und Geräten geteilt; schlägt dies fehl, gilt die Erhöhung nur in der geöffneten Sitzung.

Tipp

Sperren Sie Ihren Computer jedes Mal, wenn Sie ihn verlassen, und legen Sie Ihre PIN dort fest oder ändern Sie sie dort, wo niemand den Bildschirm sehen kann: Auf den Bildschirmen **PIN einrichten** und **PIN ändern** sind die Ziffern während der Eingabe sichtbar (in der Eingabeaufforderung **PIN eingeben** werden sie maskiert).

Kann ich einen Eintrag absichtlich mit einem Kollegen teilen?

Nein. Password Vault ist ein persönlicher Tresor: Es gibt keine freigegebenen Einträge, freigegebenen Ordner oder Teamtresore. Für Anmeldeinformationen, die ein Team gemeinsam nutzen muss, befolgen Sie die Richtlinie Ihrer Organisation.

Verwandte Artikel

- KB10453. Wo Password Vault Ihre Kennwörter speichert: Der App-Ordner in OneDrive
- KB10452. Wie Password Vault Ihre Daten schützt: Verschlüsselung, PIN und Speicherung
- KB10439. Password Vault: Häufig gestellte Fragen

Begriffe

Liste
Eine Liste ist eine Speichereinheit in SharePoint. Eine Liste kann Spalten unterschiedlicher Typen, Inhaltstypen und Ansichten enthalten. Eine Dokumentbibliothek ist ein spezieller Listentyp und erbt daher die Funktionalität einer Liste.

Microsoft 365
Microsoft 365 ist ein cloudbasierter Abonnementdienst, der Produktivitäts-Apps wie Word, Excel, PowerPoint und Outlook mit Clouddiensten wie SharePoint, OneDrive, Teams und Exchange Online sowie mit erweiterten Sicherheits- und Geräteverwaltungsfunktionen kombiniert.

SharePoint Online
Die Cloudversion von SharePoint, einer webbasierten Zusammenarbeitsplattform in Microsoft 365, die umfangreiche Funktionen zum Speichern, Freigeben und Verwalten der digitalen Informationen, Inhalte und des Wissens einer Organisation bietet.

Webpart
Ein Webpart ist ein grundlegender Baustein für Funktionalität oder Inhalte, der auf einer SharePoint-Seite platziert wird. Einige Webparts unterstützen Anpassungen, z. B. das Konfigurieren des Webparts oder das Ändern seines Erscheinungsbilds.

Website
Eine SharePoint-Website ist ein Container für Informationen innerhalb der SharePoint-Plattform. Websites bieten in der Regel Funktionen wie Dokumentbibliotheken, Listen, Kalender, Diskussionsforen und Workflows und erleichtern so die Zusammenarbeit, Kommunikation und Dokumentverwaltung innerhalb von Teams oder abteilungsübergreifend. Websites können angepasst und konfiguriert werden, um die spezifischen Anforderungen und Workflows einer Organisation zu erfüllen.