vitextra

WISSENSDATENBANKARTIKEL

Wie Password Vault Ihre Daten schützt: Verschlüsselung, PIN und Speicherung

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

Zusammenfassung 4

Schicht 1: Microsoft-365-Anmeldung und OneDrive-Zugriffssteuerung 5

Schicht 2: Verschlüsselung der Einträge im Browser 5

- **Was verschlüsselt wird und was nicht** 6
- **Bestehende Tresore werden automatisch umgestellt** 7

Schicht 3: Die PIN und der gesperrte Tresor 8

Automatische Sperre 9

Begrenzung der Fehlversuche 9

Keine Daten bei Vitextra 10

Wofür Password Vault gedacht ist 10

Empfehlungen 11

Begriffe 12

Überblick

Password Vault ist ein persönlicher Kennwortmanager für SharePoint-Online-Seiten und **Microsoft Teams**. Jeder Benutzer bewahrt seine eigenen Anmeldeinformationen in einer einzigen verschlüsselten Datei in seinem eigenen OneDrive auf. Dieser Artikel erklärt Schicht für Schicht, wie die Daten geschützt sind, was die PIN leistet und was nicht, welche Teile des Tresors verschlüsselt werden und für welche Anmeldeinformationen Password Vault gedacht ist. Er richtet sich an Endbenutzer, die das Produkt verstehen möchten, sowie an Administratoren und Sicherheitsbeauftragte, die es prüfen.

Zusammenfassung

Frage	Antwort
Wo wird der Tresor gespeichert?	In einer Datei, `vitextra-password-vault.json`, im App-Ordner des eigenen OneDrive des Benutzers
Wer kann die Datei öffnen?	Wer gemäß den Microsoft-365-Berechtigungen Zugriff auf das OneDrive des Benutzers hat – standardmäßig nur der Benutzer selbst
Welche Identität wird verwendet?	Der angemeldete Microsoft-365-Benutzer, über **Microsoft Graph** mit der delegierten Berechtigung *Files.ReadWrite.AppFolder*
Was wird verschlüsselt?	Die Textfelder jedes Eintrags: Name, Benutzername, Kennwort, URL, Hinweise, Ordner und Tags (AES, im Browser, mit einem aus der PIN abgeleiteten Schlüssel)
Was leistet die PIN?	Der Verschlüsselungsschlüssel wird aus der 4-stelligen PIN abgeleitet; bis die PIN eingegeben ist, zeigt das **Webpart** überhaupt keine Einträge an
Wann wird die PIN erneut abgefragt?	Nach 5 Minuten ohne Interaktion im Webpart und nach dem Neuladen der

Frage	Antwort
	Seite
Was passiert nach falschen PINs?	Nach 5 falschen PINs in Folge wird der Tresor blockiert und kann nur noch zurückgesetzt werden, wodurch alle Einträge gelöscht werden
Was wird an Vitextra gesendet?	Keine Tresordaten; nur die technischen Bezeichner der Lizenzprüfung und der Nutzungstelemetrie

Schicht 1: Microsoft-365-Anmeldung und OneDrive-Zugriffssteuerung

Password Vault hat keine eigenen Konten, Server oder Datenbanken. Das Webpart läuft im Browser des angemeldeten Benutzers und liest und schreibt den Tresor über Microsoft Graph mit der Identität dieses Benutzers. Die Datei wird im eigenen OneDrive des Benutzers gespeichert und ist daher durch dieselben Mechanismen geschützt wie jede andere Datei dort: die Microsoft-365-Anmeldung (einschließlich mehrstufiger Authentifizierung und bedingten Zugriffs, sofern Ihre Organisation diese verwendet), die OneDrive-Berechtigungen und die Microsoft-365-Richtlinien Ihrer Organisation.

Password Vault fordert die delegierte Berechtigung *Files.ReadWrite.AppFolder* für den App-Ordner des angemeldeten Benutzers an. Diese Berechtigung gewährt keinen Zugriff auf dessen übrige Dateien oder das OneDrive eines anderen Benutzers. SPFx-Lösungen verwenden eine gemeinsame Anwendungsidentität; Administratoren müssen daher auch deren weitere Berechtigungen berücksichtigen. KB10454. Microsoft-Graph-Berechtigung Files.ReadWrite.AppFolder: Warum Password Vault sie benötigt und wie Sie sie genehmigen

Da der Tresor im OneDrive des Benutzers und nicht auf der Seite liegt, sieht jeder Benutzer, der eine Seite oder eine **Teams-Registerkarte** mit dem Webpart öffnet, nur seinen eigenen Tresor. Das Platzieren des Webparts auf einer gemeinsam genutzten Seite gibt keine Kennwörter frei.

Schicht 2: Verschlüsselung der Einträge im Browser

Bevor der Tresor gespeichert wird, verschlüsselt Password Vault die Textfelder jedes

Eintrags mit AES. Ver- und Entschlüsselung finden im Browser des Benutzers statt; die Datei wird nur zwischen dem Browser und dem OneDrive des Benutzers über Microsoft Graph übertragen. Dadurch werden die Werte nie als Klartext gespeichert oder übertragen: Wer die Datei öffnet, sieht verschlüsselte Zeichenfolgen statt Namen, Benutzernamen und Kennwörtern.

Der Verschlüsselungsschlüssel wird im Browser mit PBKDF2-SHA256 (Web Crypto) aus der PIN abgeleitet, mit einem zufälligen Salt von 16 Byte und 600.000 Iterationen; bei jedem Festlegen oder Ändern einer PIN wird ein neuer Salt erzeugt. Der Schlüssel wird nirgends gespeichert – weder in der Tresordatei noch im Browserspeicher noch bei Vitextra. Er existiert nur im Arbeitsspeicher der geöffneten Seite, solange der Tresor entsperrt ist. Um eine PIN zu prüfen, leitet das Webpart aus ihr den Schlüssel ab und entschlüsselt einen Prüfwert – einen bekannten, mit dem Schlüssel verschlüsselten Text –, den die Datei zusammen mit dem Salt und der Anzahl der Iterationen speichert. Weder die PIN noch ein Hash der PIN wird gespeichert. Daher genügt die Tresordatei allein nicht, um die Einträge zu lesen: Dazu wird die PIN benötigt.

Warnung

Die PIN hat nur 4 Ziffern, also 10.000 mögliche Kombinationen. PBKDF2 verlangsamt jeden Rateversuch absichtlich, doch wer eine Kopie Ihrer Tresordatei erlangt, könnte trotzdem offline, außerhalb des Webparts, alle PINs ausprobieren: Die Begrenzung auf fünf Versuche gilt nur innerhalb des Webparts. Die Zugriffssteuerung für Ihr OneDrive bleibt daher die erste Schutzlinie. Halten Sie Ihr Microsoft-365-Konto sicher und geben Sie weder die Tresordatei noch den Ordner, der sie enthält, frei.

Was verschlüsselt wird und was nicht

Daten in der Tresordatei	Verschlüsselt
Name des Eintrags	Ja
Benutzername	Ja
Kennwort	Ja
URL	Ja
Hinweise	Ja

Daten in der Tresordatei	Verschlüsselt
Ordner	Ja
Tags	Ja
Favoritenkennzeichen (der Stern)	Nein
Eintragsbezeichner, Erstellungs- und Änderungsdatum	Nein
Salt, Anzahl der Iterationen und Prüfwert (dienen zur Prüfung der PIN)	Salt und Anzahl der Iterationen: Nein; der Prüfwert ist ein bekannter, mit dem Schlüssel verschlüsselter Text. Die PIN, ein Hash davon und der Schlüssel werden nicht gespeichert
Objekt-ID des Benutzers in **Microsoft Entra ID**	Nein
Zähler der PIN-Fehlversuche	Nein

Tresordaten werden weder in SharePoint-Listen noch in Webpart-Eigenschaften oder im dauerhaften Browserspeicher abgelegt. Solange der Tresor entsperrt ist, befinden sich Schlüssel und entschlüsselte Werte im Arbeitsspeicher der geöffneten Seite. Konfigurationseinstellungen und Lizenzcache sind von den Tresordaten getrennt.

Bestehende Tresore werden automatisch umgestellt

Tresore, die mit früheren Versionen von Password Vault erstellt wurden, verwenden das bisherige Dateiformat, in dem der Schlüssel aus einem in der Datei gespeicherten SHA-256-Hash der PIN und der Objekt-ID des Benutzers in Microsoft Entra ID abgeleitet wurde. Wenn Sie in der neuen Version zum ersten Mal die korrekte PIN eingeben, verschlüsselt das Webpart alle Einträge mit einem neuen, mit PBKDF2 abgeleiteten Schlüssel neu und speichert den Tresor im neuen Format. Die Einträge und ihre Änderungsdaten bleiben erhalten, und der Zähler der Fehlversuche wird zurückgesetzt. Sie müssen nichts unternehmen. Nach der Umstellung enthält die Datei den PIN-Hash nicht mehr.

Die Umstellung wird nur abgeschlossen, wenn alle Einträge entschlüsselt und die aktualisierte Datei erfolgreich gespeichert werden können. Schlägt einer dieser Schritte fehl, kann das Webpart die aktuelle Sitzung im bisherigen Format fortsetzen; das Entsperren allein bestätigt keine erfolgreiche Umstellung.

Hinweis

Die Umstellung ändert nur die aktuelle Tresordatei. Frühere Versionen der Datei, die OneDrive in seinem Versionsverlauf oder Papierkorb aufbewahrt, sowie Kopien in Sicherungen bleiben im bisherigen Format, in dem die Einträge aus der Datei selbst, ohne die PIN, entschlüsselt werden konnten. Wer sie öffnen kann, wird durch die OneDrive-Zugriffssteuerung und durch die Aufbewahrungs- und Sicherungseinstellungen Ihrer Organisation bestimmt.

Schicht 3: Die PIN und der gesperrte Tresor

Die PIN ist ein 4-stelliger Code, den der Benutzer beim Anlegen des Tresors festlegt (siehe KB10442. So richten Sie Ihre PIN in Password Vault ein). Sie wird einmal benötigt, um den Tresor zu öffnen: Das Webpart prüft sie, sobald die vierte Ziffer eingegeben ist. Bis dahin ist der Tresor gesperrt, und das Webpart zeigt überhaupt keine Einträge an – nicht einmal ihre Namen. Statt der **Liste** zeigt es die Eingabeaufforderung **PIN eingeben** mit „Geben Sie Ihre PIN ein, um fortzufahren“ und vier Ziffernfeldern, und die Symbolleiste bietet nur die Schaltfläche **Aktualisieren**.

Aktion	**Verfügbar, solange der Tresor gesperrt ist**
Die Liste mit Name, Benutzername, URL, Ordner, Tags und Hinweisen der Einträge anzeigen	Nein – die Liste ist ausgeblendet
Ein Kennwort anzeigen (Augen-Schaltfläche) oder **In Zwischenablage kopieren** für ein Kennwort oder einen Benutzernamen	Nein
Neues Element, **Bearbeiten**, **Entfernen**	Nein
PIN ändern (das Zahnrad **Konfigurieren**)	Nein
Zu Favoriten hinzufügen / **Aus Favoriten entfernen**	Nein
Suchen und Filter	Nein
Aktualisieren	Ja

Nach der korrekten PIN ist der Tresor entsperrt, und alle diese Aktionen funktionieren direkt, ohne erneute Abfrage der PIN, bis der Tresor gesperrt wird.



Die Eingabeaufforderung „PIN eingeben“ eines gesperrten Tresors

Warnung

Solange der Tresor entsperrt ist, kann jeder, der Ihren Computer benutzt, alles darin – einschließlich der Kennwörter – anzeigen und kopieren, bis der Tresor wieder gesperrt wird. Sperren Sie Ihren Computer, wann immer Sie ihn verlassen.

In der Eingabeaufforderung **PIN eingeben** werden die Ziffern während der Eingabe maskiert. Auf den Bildschirmen **PIN einrichten** und **PIN ändern** sind sie sichtbar; legen Sie Ihre PIN daher dort fest oder ändern Sie sie dort, wo niemand Ihren Bildschirm sehen kann.

Automatische Sperre

Nach dem Laden der Seite ist der Tresor gesperrt: Es werden keine Einträge angezeigt, nur die Eingabeaufforderung **PIN eingeben**. Nach einer korrekten PIN wird der Tresor geöffnet und bleibt entsperrt, während Sie arbeiten. Wenn **5 Minuten** lang kein Klick und kein Tastendruck innerhalb des Webparts erfolgt ist (Aktivität auf dem Bildschirm **PIN ändern** zählt ebenfalls), wird der Tresor wieder gesperrt: Die Liste verschwindet, angezeigte Kennwörter werden ausgeblendet, der Schlüssel wird aus dem Arbeitsspeicher entfernt, und jedes geöffnete Dialogfeld (**Neues Element**, **Eigenschaften bearbeiten**, die Bestätigung des Entfernens) wird ohne Speichern geschlossen. Auch das Neuladen der Seite sperrt den Tresor, weil der entsperrte Zustand nur in der geöffneten Seite existiert. Siehe KB10451. Automatische Sperre: Wann Password Vault erneut nach der PIN fragt.

Begrenzung der Fehlversuche

Der Zähler wird nicht mit der Zeit zurückgesetzt. Das Webpart zeigt *Die PIN ist falsch* und die Anzahl der verbleibenden Versuche an. Wenn das Speichern erfolgreich ist, wird der Zähler in der Tresordatei gespeichert und erfasst Versuche auf verschiedenen Geräten und in verschiedenen Sitzungen. Eine richtige PIN oder eine PIN-Änderung setzt den Zähler zurück; auch dieses Ergebnis muss erfolgreich in der Datei gespeichert werden. Wenn die Datei nicht gelesen oder der Zähler nicht gespeichert werden kann, verwendet die Seite möglicherweise zuvor geladene Daten und zählt einen Fehlversuch nur lokal. Stellen Sie die Verbindung wieder her und aktualisieren Sie die Daten, bevor Sie fortfahren. Nach 5 falschen PINs in Folge wird der Tresor mit der Meldung *Sie haben zu oft eine falsche PIN eingegeben.* blockiert, und nur **Zurücksetzen** ist verfügbar. Siehe KB10455. Falsche PIN-Eingaben in Password Vault: Was nach fünf Fehlversuchen passiert.

Warnung

Ist der Tresor noch entsperrt, können Sie die PIN ändern, ohne die alte PIN einzugeben. Schließen Sie die Änderung ab und speichern Sie sie, bevor der Tresor gesperrt wird; bei erfolgreichem Speichern bleiben die Einträge erhalten. Sind alle Sitzungen gesperrt und haben Sie die PIN vergessen, bietet Password Vault weder Ihnen noch Ihrem Administrator oder Vitextra eine Wiederherstellungsfunktion. Das Zurücksetzen eines blockierten Tresors löscht alle Einträge. Bewahren Sie wichtige Zugangsdaten zusätzlich an einem anderen von Ihrer Organisation genehmigten Ort auf. KB10460. PIN für Password Vault vergessen: Welche Möglichkeiten habe ich?

Keine Daten bei Vitextra

Vitextra empfängt, speichert und sichert keine Tresordaten. Die einzigen Anforderungen des Webparts an Vitextra-Dienste sind die Lizenzprüfung und die Nutzungstelemetrie mit technischen Bezeichnern. Die vollständige Liste finden Sie unter KB10363. Wo Vitextra-Produkte Ihre Daten speichern: Datenschutz, Datenresidenz und DSGVO.

Wofür Password Vault gedacht ist

Password Vault ist als bequemer, persönlicher Ort für alltägliche Anmeldeinformationen gedacht – Anmeldungen bei Webportalen, Partnersystemen, Testkonten und ähnliche Einträge, die ein Benutzer sonst in einem Notizbuch oder einer Textdatei aufbewahren würde. Sein Schutz kombiniert die Zugriffssteuerung von **Microsoft 365** mit der Verschlüsselung der gespeicherten Werte mit einem Schlüssel,

der aus einer 4-stelligen PIN abgeleitet wird.

Es ist kein System für die Verwaltung privilegierter Zugriffe: Es gibt keine Freigabe zwischen Benutzern, keine Wiederherstellung durch Administratoren, kein eigenes Überwachungsprotokoll und kein Hauptkennwort hoher Stärke. Für Administratorkonten, Dienstkonten, gemeinsam genutzte Team-Anmeldeinformationen und andere hochprivilegierte Geheimnisse befolgen Sie die Richtlinie Ihrer Organisation und verwenden Sie die von ihr vorgeschriebenen Werkzeuge. Einen Vergleich mit anderen Ansätzen finden Sie unter KB10440. Password Vault im Vergleich zu Browser-Kennwortmanagern und Enterprise-Kennwortmanagern: Was ist die richtige Wahl?.

Empfehlungen

- Schützen Sie Ihr Microsoft-365-Konto: Der Tresor ist nur so sicher wie das Konto, dem das OneDrive gehört.
- Wählen Sie eine PIN, die nicht leicht zu erraten ist (vermeiden Sie *0000*, *1234* oder Ihr Geburtsjahr), und bewahren Sie sie an einem sicheren Ort auf.
- Geben Sie die Tresordatei nicht frei und kopieren Sie sie nicht: Wer eine Kopie besitzt, könnte offline alle 10.000 PINs ausprobieren.
- Sperren Sie Ihren Computer, wenn Sie ihn verlassen, auch nur für kurze Zeit.
- Ein kopiertes Kennwort bleibt in der Zwischenablage, bis Sie etwas anderes kopieren; leeren Sie auf gemeinsam genutzten Computern die Zwischenablage nach der Verwendung.
- Wenn Sie den Tresor auf mehreren Geräten oder in mehreren Registerkarten verwenden, werden Änderungen automatisch zusammengeführt; klicken Sie auf **Aktualisieren**, um an anderer Stelle vorgenommene Änderungen zu sehen (siehe KB10453. Wo Password Vault Ihre Kennwörter speichert: Der App-Ordner in OneDrive). Wird derselbe Eintrag gleichzeitig bearbeitet, gelten die zuletzt gespeicherten Werte seiner bearbeitbaren Felder.
- Speichern Sie nur Anmeldeinformationen, die Sie laut Ihrer Organisation in einem persönlichen Kennwortmanager aufbewahren dürfen.

Tipp

Wer Ihre Einträge genau sehen kann und wer nicht, erfahren Sie unter KB10456. Wer Ihre Kennwörter in Password Vault sehen kann.

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.

Microsoft Entra ID
Microsoft Entra ID (früher Azure Active Directory) ist ein cloudbasierter Identitäts- und Zugriffsverwaltungsdienst von Microsoft. Organisationen können damit die Identitäten ihrer Benutzer und deren Zugriff auf eine Vielzahl interner und externer Ressourcen effizient verwalten und schützen. Zu diesen Ressourcen gehören Microsoft 365, die Azure-Plattform und Tausende weitere SaaS-Anwendungen (Software as a Service).

Microsoft Graph
Microsoft Graph ist eine REST-API, die mit Microsoft Entra ID (früher Azure Active Directory) und OAuth 2.0 gesichert ist. Sie stellt einen einzigen Endpunkt für den Zugriff auf Daten und Dienste in Microsoft 365 bereit, z. B. SharePoint, Outlook, OneDrive, Teams und weitere.

Microsoft Teams
Microsoft Teams ist eine chatbasierte Zusammenarbeitsplattform für die Unternehmenskommunikation mit Funktionen für Onlinebesprechungen, Liveereignisse und die gemeinsame Nutzung von Dokumenten.

Teams-Registerkarte
Eine Registerkarte in Microsoft Teams ist eine Seite, die in einen Kanal, einen Chat oder eine Besprechung eingebettet ist und Webinhalte oder eine App anzeigt, z. B. eine SharePoint-Seite oder eine benutzerdefinierte Anwendung, am oberen Rand der Unterhaltung.

Begriffe

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.