WISSENSDATENBANKARTIKEL

Password Vault: Kurzanleitung für Endbenutzer

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

Übersicht 4

Schritt 1: PIN einrichten 4

Der Hauptbildschirm 4

Den Tresor entsperren 5

Einen Eintrag hinzufügen 5

Ein starkes Kennwort erstellen 5

Mit einem Eintrag anmelden 6

Einen Eintrag bearbeiten und löschen 6

Einträge organisieren 6

Einen Eintrag finden 7

Ihre PIN ändern 7

Den Tresor an mehreren Orten verwenden 7

Wenn Sie eine falsche PIN eingeben 7

Bewährte Vorgehensweisen 8

Übersicht

Password Vault ist Ihr persönlicher Kennwortmanager in Microsoft 365. Sie finden ihn auf einer SharePoint-Seite oder in Microsoft Teams – als Kanalregisterkarte oder als persönliche App **Passwords**. Wo auch immer Sie ihn öffnen, Sie sehen Ihren eigenen Tresor: Ihre Einträge werden verschlüsselt in Ihrem eigenen OneDrive gespeichert, und Kollegen, die dieselbe Seite öffnen, sehen nur ihre eigenen Einträge.

Diese Anleitung führt durch die alltäglichen Aufgaben. Jeder Abschnitt verweist auf einen ausführlichen Artikel.

Schritt 1: PIN einrichten

Wenn Sie Password Vault zum ersten Mal öffnen, erscheint der Bildschirm **PIN einrichten**.

1 Geben Sie eine 4-stellige PIN in die vier Felder ein.
2 Klicken Sie auf **Speichern**.

Ihr Tresor ist bereit, und die Liste zeigt *Diese Liste enthält keine Elemente.* an.

Warnung

Wenn Sie Ihren PIN-Code vergessen, können Sie nicht mehr auf die Daten zugreifen. Niemand – weder Ihr Administrator noch Vitextra – kann ihn wiederherstellen oder zurücksetzen. Wählen Sie eine PIN, die Sie sich merken können, und bewahren Sie sie an einem sicheren Ort auf. Details: KB10442. So richten Sie Ihre PIN in Password Vault ein.

Der Hauptbildschirm

- **Neues Element** – fügt einen Eintrag hinzu. Wird nach dem Entsperren des Tresors angezeigt.
- **Aktualisieren** (Kreispfeil) – lädt Ihren Tresor erneut aus OneDrive. Die einzige Schaltfläche, die bei gesperrtem Tresor angezeigt wird.
- **Konfigurieren** (Zahnrad) – öffnet das Menü mit **PIN ändern**. Wird nach dem Entsperren des Tresors angezeigt.
- **Suchen** und die Filter-Dropdownliste – erscheinen, sobald der Tresor mindestens einen Eintrag enthält.
- Die Liste – eine Zeile pro Eintrag mit einem Stern, dem Namen und dem Benutzernamen. Klicken Sie auf eine Zeile, um sie zu erweitern.

Den Tresor entsperren

Wenn Sie die Seite öffnen, ist der Tresor **gesperrt**: Statt Ihrer Einträge zeigt das Webpart die Abfrage **PIN eingeben** mit *Geben Sie Ihre PIN ein, um fortzufahren* und vier Feldern an. Geben Sie die 4 Ziffern ein – sie werden maskiert, und die PIN wird geprüft, sobald Sie die vierte eingeben –, und Ihre Liste erscheint. Bei einer falschen PIN werden *Die PIN ist falsch* und **Verbleibende Versuche** angezeigt.

Sie geben die PIN einmal ein, um den Tresor zu öffnen. Solange er entsperrt ist, können Sie Kennwörter anzeigen und kopieren, Einträge erstellen, bearbeiten und löschen, Favoriten markieren und die PIN ändern, ohne erneut nach der PIN gefragt zu werden.

Der Tresor bleibt entsperrt, solange Sie damit arbeiten, und wird nach **5 Minuten** ohne Klick oder Tastendruck im Webpart oder beim Neuladen der Seite wieder gesperrt. Beim Sperren wird die Liste ausgeblendet, und ein geöffnetes Dialogfeld wird ohne Speichern geschlossen. Siehe KB10451. Automatische Sperre: Wann Password Vault erneut nach der PIN fragt.

Einen Eintrag hinzufügen

1 Klicken Sie auf **Neues Element**.
2 Füllen Sie **Name**, **Benutzername** und **Kennwort** aus – diese drei Felder sind Pflichtfelder.
3 Füllen Sie optional **URL** aus, wählen Sie unter **Ordner** einen Ordner aus oder geben Sie einen ein, fügen Sie unter **Tags** durch Kommas getrennte Tags hinzu und schreiben Sie **Hinweise**.
4 Klicken Sie auf **Speichern**. Die Meldung *Neues Element wurde erstellt.* bestätigt dies.

Details: KB10443. So fügen Sie Einträge in Password Vault hinzu, bearbeiten und löschen sie.

Ein starkes Kennwort erstellen

Klicken Sie im Dialogfeld **Neues Element** oder **Eigenschaften bearbeiten** auf **Kennwort generieren**. Ein zufälliges Kennwort wird sofort in das Feld **Kennwort** eingefügt, und es öffnet sich ein Bereich, in dem Sie die **Länge** festlegen (8 bis 64 Zeichen, standardmäßig 16), **Großbuchstaben (A-Z)**, **Kleinbuchstaben (a-z)**, **Ziffern (0-9)** und **Sonderzeichen (!@#$)** auswählen und **Ähnliche Zeichen ausschließen (I, l, 1, O, 0)** aktivieren können. Jede Änderung erstellt ein neues Kennwort; **Neu generieren** erstellt ein weiteres mit denselben Optionen. Siehe KB10445. So generieren Sie ein starkes Kennwort mit dem Kennwortgenerator von Password Vault.

Unter dem Kennwort zeigt die Anzeige **Stärke** eine Einschätzung von *Sehr schwach* bis *Sehr stark*. Sie dient nur als Orientierung und verhindert nicht, dass ein schwaches Kennwort gespeichert wird. Siehe KB10446. Kennwort-Stärkeanzeige in Password Vault: Was die Stufen bedeuten.

Hinweis

Das Generieren eines Kennworts in Password Vault ändert nicht das Kennwort in dem System, zu dem es gehört. Ändern Sie es zuerst dort (oder gleichzeitig), und speichern Sie dann dasselbe Kennwort im Eintrag.

Mit einem Eintrag anmelden

1 Klicken Sie auf den Eintrag, um ihn zu erweitern.
2 Klicken Sie auf die **URL**, um die Website in einer neuen Registerkarte zu öffnen.
3 Verwenden Sie **In Zwischenablage kopieren** neben **Benutzername** und fügen Sie den Wert in das Anmeldeformular ein.
4 Verwenden Sie **In Zwischenablage kopieren** neben **Kennwort** und fügen Sie es ein. Zur Bestätigung erscheint kurz *Kopiert*.

Um das Kennwort stattdessen auf dem Bildschirm zu sehen, klicken Sie auf die Augen-Schaltfläche daneben. Siehe KB10444. So zeigen Sie ein Kennwort oder einen Benutzernamen in Password Vault an und kopieren sie.

Tipp

Kopieren ist sicherer als Anzeigen: Niemand in Ihrer Nähe kann das Kennwort von Ihrem Bildschirm ablesen.

Einen Eintrag bearbeiten und löschen

- **Bearbeiten** öffnet das Dialogfeld **Eigenschaften bearbeiten**; ändern Sie die Felder und klicken Sie auf **Speichern**. Die Meldung lautet *Der Speichervorgang war erfolgreich*.
- **Entfernen** fragt *Möchten Sie dieses Element wirklich löschen?*; klicken Sie zur Bestätigung auf **Entfernen**. Das Löschen ist endgültig – im Webpart gibt es keinen Papierkorb.

Einträge organisieren

- **Ordner** – weisen Sie einem Eintrag unter **Ordner** einen Ordner zu, indem Sie einen vorhandenen auswählen oder einen neuen Namen eingeben. Jeder Eintrag befindet

sich in höchstens einem Ordner. Bei Ordnernamen wird die Groß-/Kleinschreibung nicht beachtet: *Finance* und *finance* sind derselbe Ordner. Siehe KB10447. Einträge mit Ordnern und Tags in Password Vault organisieren.
- **Tags** – fügen Sie beliebig viele Tags hinzu, getrennt durch Kommas; sie erscheinen als Chips am Eintrag.
- **Favoriten** – klicken Sie auf den Stern eines Eintrags, damit er oben in der Liste bleibt. Siehe KB10448. Favoriten in Password Vault: Häufig verwendete Einträge oben halten.

Einen Eintrag finden

Geben Sie Text in das Feld **Suchen** ein, um Einträge nach Name, Benutzername, URL, Ordner, Hinweisen oder Tags zu finden (Kennwörter werden nicht durchsucht). Verwenden Sie die Filter-Dropdownliste, um **Alle Elemente**, **Favoriten**, einen Ordner (oder **Kein Ordner**) oder ein Tag anzuzeigen. Suche und Filter wirken zusammen; wenn nichts passt, zeigt die Liste *Nichts gefunden.* an. Siehe KB10449. Einträge in Password Vault suchen und filtern.

Ihre PIN ändern

Klicken Sie auf das Zahnrad **Konfigurieren**, wählen Sie **PIN ändern**, geben Sie die neue 4-stellige PIN ein und klicken Sie auf **PIN ändern**. Die Meldung *Die PIN wurde geändert.* bestätigt dies. Siehe KB10450. So ändern Sie Ihre PIN in Password Vault.

Den Tresor an mehreren Orten verwenden

Ihr Tresor ist auf jeder Seite und in Teams derselbe. Wenn Sie ihn in einer anderen Browserregisterkarte oder auf einem anderen Gerät geändert haben, klicken Sie auf **Aktualisieren**, um die Änderungen zu sehen; sie erscheinen auch nach Ihrem nächsten Speichern oder wenn Sie den Tresor entsperren. Ihr Speichern überschreibt keine an anderer Stelle vorgenommenen Änderungen. Wenn Sie Ihre PIN auf einem anderen Gerät geändert haben, sperrt sich der Tresor selbst und fragt nach der neuen PIN.

Wenn Sie eine falsche PIN eingeben

Bei einer falschen PIN wird *Die PIN ist falsch* und die Anzahl der verbleibenden Versuche angezeigt. Die Zählung läuft geräte- und sitzungsübergreifend weiter, bis Sie die richtige PIN eingeben. Nach **5** falschen PINs in Folge wird der Tresor mit *Sie haben zu oft eine falsche PIN eingegeben.* blockiert, und die einzige Option ist **Zurücksetzen**. Nachdem Sie die Frage *Möchten Sie Ihren Tresor wirklich zurücksetzen? Diese Aktion löscht alle Ihre im Tresor gespeicherten Kennwörter.* bestätigt haben, werden alle Einträge gelöscht, und Sie beginnen mit einer neuen PIN neu. Siehe KB10461. Warum

Password Vault gesperrt ist: „Sie haben zu oft eine falsche PIN eingegeben“ und KB10460. PIN für Password Vault vergessen: Welche Möglichkeiten habe ich?.

Bewährte Vorgehensweisen

- Wählen Sie eine schwer zu erratende PIN (nicht *1234* oder eine Jahreszahl), denn eine PIN hat nur 4 Ziffern; der Schutz Ihres Geschäftskontos und Ihres OneDrive ist ebenso wichtig.
- Sperren Sie Ihren Computer, wenn Sie ihn verlassen, auch nur kurz.
- Speichern Sie wichtige Anmeldedaten zusätzlich an einem anderen von Ihrer Organisation genehmigten Ort, falls Sie Ihre PIN vergessen.
- Verwenden Sie Password Vault für Ihre persönlichen Anmeldedaten; für gemeinsam genutzte oder hochprivilegierte Konten befolgen Sie die Richtlinie Ihrer Organisation.

Tipp

Weitere Antworten finden Sie in KB10439. Password Vault: Häufig gestellte Fragen. Wie Ihre Daten geschützt sind, erfahren Sie in KB10452. Wie Password Vault Ihre Daten schützt: Verschlüsselung, PIN und Speicherung.