KNOWLEDGE BASE ARTICLE

# How Password Vault Protects Your Data: Encryption, PIN and Storage

2026 © Vitextra SIA. All rights reserved.

# Disclaimer

For the purposes of this Disclaimer:

- **Company** (referred to as either "the Company", "We", "Us" or "Our" in this Disclaimer) refers to Vitextra SIA, LV-1009 Riga, Matise iela 61 - 25.
- **Document** refers to the Knowledgebase Article.
- **You** means the individual accessing the Document, or the company, or other legal entity on behalf of which such individual is accessing or using the Document, as applicable.
- **Website** refers to Vitextra, accessible from https://vitextra.com

## Disclaimer

The information contained in the Document is for general information purposes only.

The Company assumes no responsibility for errors or omissions in the contents of the Document.

In no event shall the Company be liable for any special, direct, indirect, consequential, or incidental damages or any damages whatsoever, whether in an action of contract, negligence, or other torts, arising out of or in connection with the use of the contents of the Document. The Company reserves the right to make additions, deletions, or modifications to the contents in the Document at any time without prior notice.

## Errors and Omissions Disclaimer

The information given by the Document is for general guidance on matters of interest only. Therefore, errors can occur even if the Company takes every precaution to ensure that the Document's content is current and accurate. Plus, given the changing nature of laws, rules, and regulations, there may be delays, omissions, or inaccuracies in the information contained in the Document.

The Company is not responsible for any errors or omissions, or for the results obtained from the use of this information.

## Fair Use Disclaimer

The Company may use copyrighted material that the copyright owner has not explicitly authorized. The Company is making such material available for criticism, comment, news reporting, teaching, scholarship, or research.

The Company believes this constitutes a "fair use" of any such copyrighted material as provided for in section 107 of the United States Copyright law.

If You wish to use copyrighted material from the Document for your own purposes that go beyond fair use, You must obtain permission from the copyright owner.

## "Use at Your Own Risk" Disclaimer

All information in the Document is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose.

The Company will not be liable to You or anyone else for any decision made or action taken in reliance on the information given by the Service or for any consequential, special or similar damages, even if advised of the possibility of such damages.

## Contact Us

If you have any questions about this Disclaimer, You can contact Us by email: support@vitextra.com.

# Table of contents


**Overview** 4

**Summary** 4

**Layer 1: Microsoft 365 sign-in and OneDrive access control** 5

**Layer 2: Encryption of the entries in the browser** 5

- **What is and is not encrypted** 6
- **Existing vaults are upgraded automatically** 7

**Layer 3: The PIN and the locked vault** 7

**Automatic lock** 8

**Failed-attempt limit** 9

**No data at Vitextra** 9

**What Password Vault is designed for** 9

**Recommendations** 10

**Terms** 11

# Overview

Password Vault is a personal password manager for **SharePoint Online** pages and **Microsoft Teams**. Each user keeps his or her own credentials in a single encrypted file in his or her own OneDrive. This article explains, layer by layer, how the data is protected, what the PIN does and does not do, which parts of the vault are encrypted, and what kind of credentials Password Vault is designed for. It is intended for end users who want to understand the product and for administrators and security officers who review it.

# Summary

| Question | Answer |
|---|---|
| Where is the vault stored? | In one file, `vitextra-password-vault.json`, in the app folder of the user's own OneDrive |
| Who can open the file? | Whoever has access to the user's OneDrive under **Microsoft 365** permissions - by default only the user |
| Which identity is used? | The signed-in Microsoft 365 user, through **Microsoft Graph** with the delegated permission *Files.ReadWrite.AppFolder* |
| What is encrypted? | The text fields of every entry: name, user name, password, URL, notes, folder and tags (AES, in the browser, with a key derived from the PIN) |
| What does the PIN do? | The encryption key is derived from the 4-digit PIN; until the PIN is entered, the **web part** shows no entries at all |
| When is the PIN asked again? | After 5 minutes without interaction in the web part, and after the page is reloaded |
| What happens after wrong PINs? | After 5 wrong PINs in a row the vault is blocked and can only be reset, which erases all entries |

| Question | Answer |
| --- | --- |
| What is sent to Vitextra? | No vault data; only the technical identifiers of the license check and usage telemetry |

## Layer 1: Microsoft 365 sign-in and OneDrive access control

Password Vault has no accounts, servers or databases of its own. The web part runs in the browser of the signed-in user and reads and writes the vault through Microsoft Graph with that user's identity. The file is stored in the user's own OneDrive, so it is protected by the same mechanisms as any other file there: Microsoft 365 sign-in (including multifactor authentication and **Conditional Access**, if your organization uses them), OneDrive permissions and your organization's Microsoft 365 policies.

Password Vault requests the delegated permission *Files.ReadWrite.AppFolder* to work with the signed-in user's app folder. This permission does not grant access to the rest of that user's files or to another user's OneDrive. SPFx solutions use a shared application identity, so administrators must also consider other permissions granted to that identity. KB10454. Microsoft Graph Permission Files.ReadWrite.AppFolder: Why Password Vault Needs It and How to Approve It

Because the vault is kept in the user's OneDrive and not on the page, every user who opens a page or **Teams tab** with the web part sees only his or her own vault. Placing the web part on a shared page does not share any passwords.

## Layer 2: Encryption of the entries in the browser

Before the vault is saved, Password Vault encrypts the text fields of every entry with AES. Encryption and decryption take place in the user's browser; the file travels only between the browser and the user's OneDrive through Microsoft Graph. As a result, the values are never stored or transferred as plain text: a person who opens the file sees encrypted strings instead of names, user names and passwords.

The encryption key is derived from the PIN in the browser with PBKDF2-SHA256 (Web Crypto), using a random 16-byte salt and 600,000 iterations; a new salt is created whenever a PIN is set or changed. The key is not stored anywhere - not in the vault file, not in the browser storage and not at Vitextra. It exists only in the memory of the open page while the vault is unlocked. To verify a PIN, the web part derives the key from it and decrypts a check value - a known text encrypted with the key - that the file stores together with the salt and the iteration count. Neither the PIN nor a hash of the

PIN is stored. As a result, the vault file alone is not enough to read the entries: the PIN is needed.

**Warning**

The PIN has only 4 digits, that is 10,000 possible combinations. PBKDF2 makes every guess deliberately slow, but someone who obtains a copy of your vault file could still try all PINs offline, outside the web part: the limit of five attempts applies only inside the web part. Access control to your OneDrive therefore remains the first line of protection. Keep your Microsoft 365 account secure and do not share the vault file or the folder that contains it.

## What is and is not encrypted

| Data in the vault file | Encrypted |
|---|---|
| **Name** of the entry | Yes |
| **User name** | Yes |
| **Password** | Yes |
| **URL** | Yes |
| **Notes** | Yes |
| **Folder** | Yes |
| **Tags** | Yes |
| Favorite flag (the star) | No |
| Entry identifiers, creation and modification dates | No |
| Salt, iteration count and check value (used to verify the PIN) | Salt and iteration count: no; the check value is a known text encrypted with the key. The PIN, a hash of it and the key are not stored |
| **Microsoft Entra ID** object ID of the user | No |
| Failed PIN attempt counter | No |

Vault data is not written to SharePoint lists, web part properties or persistent browser storage. While the vault is unlocked, its key and decrypted values are held in the open page's memory. Configuration settings and licensing caches are separate from vault data.

### Existing vaults are upgraded automatically

Vaults created with earlier versions of Password Vault use the previous file format, in which the key was derived from a SHA-256 hash of the PIN stored in the file and the user's Microsoft Entra ID object ID. The first time you enter the correct PIN in the new version, the web part re-encrypts all entries with a new key derived with PBKDF2 and saves the vault in the new format. The entries and their modification dates are kept, and the failed-attempt counter is reset. You do not need to do anything. After the upgrade, the file no longer contains the PIN hash.

The upgrade completes only if every entry can be decrypted and the updated file is saved successfully. If either step fails, the web part can keep the current session on the previous format; unlocking alone does not confirm a successful upgrade.

**Note**

The upgrade changes only the current vault file. Earlier versions of the file that OneDrive keeps in its version history or recycle bin, and copies in backups, remain in the previous format, in which the entries could be decrypted from the file itself, without the PIN. Who can open them is governed by OneDrive access control and by your organization's retention and backup settings.

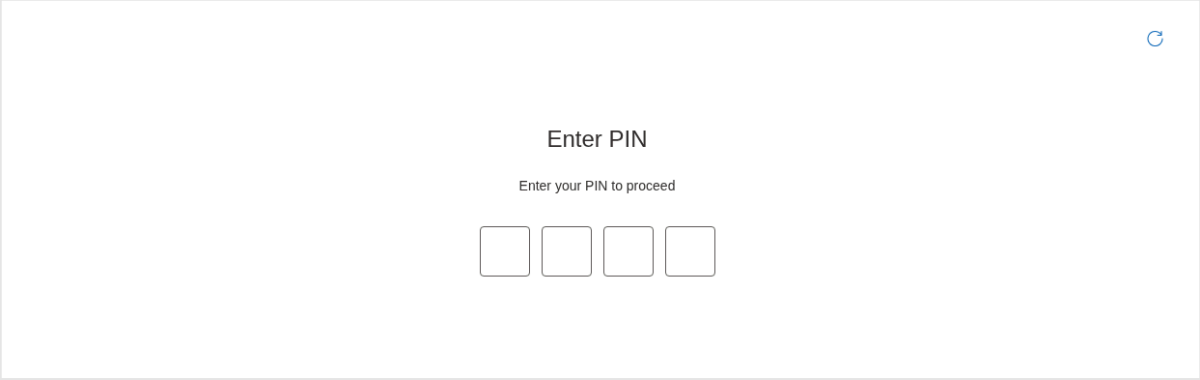
## Layer 3: The PIN and the locked vault

The PIN is a 4-digit code that the user sets when the vault is created (see KB10442. How to Set Up Your PIN in Password Vault). It is needed once, to open the vault: the web part checks it as soon as the fourth digit is typed. Until then the vault is locked, and the web part shows no entries at all - not even their names. Instead of the **list**, it shows the **Enter PIN** prompt with "Enter your PIN to proceed" and four digit boxes, and the toolbar offers only the **Refresh** button.

| Action | Available while the vault is locked |
|---|---|
| View the list with the name, user name, URL, folder, tags and notes of the entries | No - the list is hidden |
| Show a password (eye button) or **Copy to** | No |

| Action | Available while the vault is locked |
|---|---|
| **Clipboard** for a password or a user name | |
| **New Item**, **Edit**, **Remove** | No |
| **Change PIN** (the **Configure** gear) | No |
| **Add to favorites** / **Remove from favorites** | No |
| **Search** and filter | No |
| **Refresh** | Yes |

After the correct PIN, the vault is unlocked and all these actions work directly, without asking for the PIN again, until the vault locks.




*The Enter PIN prompt of a locked vault*

**Warning**

While the vault is unlocked, everything in it - including passwords - can be shown and copied by anyone who uses your computer, until the vault locks again. Lock your computer whenever you leave it.

On the **Enter PIN** prompt, the digits are masked while you type them. On the **Set up PIN** and **Change PIN** screens they are visible, so set or change your PIN where nobody can watch your screen.

## Automatic lock

After the page loads, the vault is locked: no entries are shown, only the **Enter PIN** prompt. After a correct PIN the vault opens and stays unlocked while you work. When there has been no click or key press inside the web part for **5 minutes** (activity on the

**Change PIN** screen counts too), the vault locks again: the list disappears, shown passwords are hidden, the key is removed from memory, and every open dialog (**New Item**, **Edit Properties**, the removal confirmation) is closed without saving. Reloading the page also locks the vault, because the unlocked state exists only in the open page. See KB10451. Automatic Lock: When Password Vault Asks for the PIN Again.

## Failed-attempt limit

The counter does not reset with time. The web part shows *The PIN is incorrect* and the number of attempts left. When the save succeeds, the counter is stored in the vault file, so attempts count across devices and sessions. A correct PIN or a PIN change resets the counter; saving that reset to the file also requires a successful write. If the file cannot be read or the counter cannot be saved, the page may use cached data and a failed attempt may be counted only locally; restore the connection and refresh before continuing. After 5 incorrect PINs in a row, the vault is blocked with the message *You've entered an incorrect PIN too many times.* and only **Reset** is available. See KB10455. Incorrect PIN Attempts in Password Vault: What Happens After Five Failed Tries.

**Warning**

If the vault is still unlocked, you can change the PIN without entering the old one. Complete and save the change before the vault locks; the entries are preserved when the save succeeds. If all sessions are locked and you have forgotten the PIN, Password Vault provides no recovery function for you, your administrator or Vitextra. Resetting a blocked vault deletes all entries. Keep important credentials in another location approved by your organization as well. KB10460. I Forgot My PIN in Password Vault: What Are My Options?

## No data at Vitextra

Vitextra does not receive, store or back up vault data. The only requests from the web part to Vitextra services are the license check and usage telemetry with technical identifiers. For the full list, see KB10363. Where Vitextra Products Store Your Data: Privacy, Data Residency and GDPR.

## What Password Vault is designed for

Password Vault is designed as a convenient, personal place for everyday credentials - sign-ins to web portals, partner systems, test accounts and similar entries that a user

would otherwise keep in a notebook or a text file. Its protection combines Microsoft 365 access control with encryption of the stored values under a key derived from a 4-digit PIN.

It is not a privileged access management system: it has no sharing between users, no administrator recovery, no audit log of its own and no master password of high strength. For administrator accounts, service accounts, shared team credentials and other highly privileged secrets, follow your organization's policy and use the tools it prescribes. For a comparison with other approaches, see KB10440. Password Vault vs. Browser Password Managers and Enterprise Password Managers: Which to Choose.

## Recommendations

- Protect your Microsoft 365 account: the vault is only as safe as the account that owns the OneDrive.
- Choose a PIN that is not easy to guess (avoid *0000*, *1234* or your birth year) and keep it in a safe place.
- Do not share or copy the vault file: someone with a copy could try all 10,000 PINs offline.
- Lock your computer when you leave it, even for a short time.
- A copied password stays on the clipboard until you copy something else; clear the clipboard after use on shared computers.
- If you use the vault on several devices or tabs, changes are applied to the latest file automatically; concurrent edits of the same entry use the last saved version of that entry. Press **Refresh** to see changes made elsewhere (see KB10453. Where Password Vault Stores Your Passwords: The OneDrive App Folder).
- Store only credentials that your organization allows you to keep in a personal password manager.

**Tip**

To find out exactly who can and cannot see your entries, see KB10456. Who Can See Your Passwords in Password Vault.

# Terms

**Conditional Access**
Conditional Access is a Microsoft Entra ID capability that evaluates signals such as user, location, device, and risk, and then applies policies that grant, block, or limit access to resources, for example by requiring multifactor authentication.

**List**
A list is a storage unit in SharePoint. A list can contain columns of different types, content types, and views. A document library is a special type of list and therefore inherits the functionality of a list.

**Microsoft 365**
Microsoft 365 is a cloud-based subscription service that combines productivity apps such as Word, Excel, PowerPoint, and Outlook with cloud services such as SharePoint, OneDrive, Teams, and Exchange Online, together with advanced security and device management.

**Microsoft Entra ID**
Microsoft Entra ID (formerly Azure Active Directory) is a cloud-based identity and access management service offered by Microsoft. It allows organizations to efficiently manage and secure their users' identities and access to a variety of resources, both internal and external. These resources include Microsoft 365, the Azure platform, and thousands of other software-as-a-service (SaaS) applications.

**Microsoft Graph**
Microsoft Graph is a REST API secured with Microsoft Entra ID (formerly Azure Active Directory) and OAuth 2.0. It provides a single endpoint for accessing data and services in Microsoft 365, such as SharePoint, Outlook, OneDrive, Teams, and others.

**Microsoft Teams**
Microsoft Teams is a chat-based collaboration platform for business communications with features for online meetings, live events, and document sharing.

**SharePoint Online**
The cloud version of SharePoint, a web-based collaboration platform within Microsoft 365 that provides an extensive range of capabilities to store, share, and manage the

digital information, content, and knowledge of an organization.

**Teams Tab**
A tab in Microsoft Teams is a page that is embedded in a channel, chat, or meeting and displays web content or an app, such as a SharePoint page or a custom application, at the top of the conversation.

**Web Part**
A web part is a primary building block of functionality or content placed on a SharePoint page. Some web parts support customization, such as configuring the web part or changing its appearance.