KNOWLEDGE BASE ARTICLE

Who Can See Your Passwords in Password Vault

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

Can colleagues who open the same page see my passwords? 4

Can members of a Teams channel see my passwords? 4

Can page owners or site administrators see my passwords? 5

Can Microsoft 365 or OneDrive administrators see my passwords? 5

Can other apps in my organization access the vault file? 5

Can Vitextra see my passwords? 6

What can someone at my unlocked computer see? 6

Can I share an entry with a colleague on purpose? 7

Related articles 7

Terms 8

Overview

Password Vault stores each user's entries in one encrypted file, *json*, in the app folder of that user's own OneDrive. Who can see your entries therefore depends on who can access your OneDrive and who can use your signed-in computer - not on who can open the page. The answers below go through the typical cases.

Who	Can see your entries?
Colleagues who open the same page	No - they see their own vaults
Members of a Teams channel with a Password Vault tab	No - each member sees his or her own vault
Page owners and **site** administrators	No - nothing is stored on the page or the site
Microsoft 365 / OneDrive administrators	They can access the file like any other file in your OneDrive, but cannot read the entries without the PIN; with a copy of the file, they could try all 10,000 PINs offline
Vitextra	No - Vitextra receives no vault data
Someone at your unlocked computer	While the vault is locked, nothing - not even the names of the entries; everything while the vault is unlocked

Can colleagues who open the same page see my passwords?

No. The **web part** always opens the vault of the person who is signed in. If ten colleagues open the same **SharePoint** page, each of them sees only his or her own entries, read from his or her own OneDrive. Placing Password Vault on a shared page does not share any passwords.

Can members of a Teams channel see my passwords?

No. A Password Vault tab in a Teams channel works like the web part on a page: every channel member who opens the tab sees his or her own vault. It is the same vault that the member sees on SharePoint pages and in the personal app.

Can page owners or site administrators see my passwords?

No. Password Vault stores nothing in SharePoint lists, libraries or the web part properties; the page holds only the web part and its title. Owning a page or a site, or being a **site collection** administrator, gives no access to the vault files of the people who use it.

Can Microsoft 365 or OneDrive administrators see my passwords?

Password Vault has no administration console: administrators cannot **view**, manage, unlock or recover vaults through the product.

The vault file itself is an ordinary file in your OneDrive and is protected by Microsoft 365 and OneDrive access control. Like any other file in your OneDrive, it can be accessed by administrators who have, or give themselves, access to your OneDrive under your organization's policies - for example during an investigation, through compliance tools or when the OneDrive of a departed employee is handed over. Its entry fields are encrypted with a key that is derived from your PIN and is not stored in the file, so access to the file alone does not let an administrator read your entries. However, the PIN has only 4 digits: someone with access to the file could copy it and try all 10,000 PINs offline. PBKDF2 slows down every guess, and the limit of five attempts applies only inside the web part.

Warning

Against someone who tries all PINs on a copy of the file, a 4-digit PIN offers only limited protection, so OneDrive access control remains the first line of protection. Password Vault is intended for personal, everyday credentials. For administrator accounts, service accounts and other highly privileged or shared credentials, follow your organization's policy. See KB10452. How Password Vault Protects Your Data: Encryption, PIN and Storage.

Can other apps in my organization access the vault file?

The vault is saved through the **Microsoft Graph** permission *Files.ReadWrite.AppFolder*. In **SharePoint Online**, this permission is granted to one application shared by all SharePoint Framework solutions in the **tenant**, so other SPFx solutions deployed in your organization that use the same permission work with the same app folder on behalf of the signed-in user. Such a solution could read or change the vault file; the

entries in it are encrypted with a key derived from your PIN, with the limitation described in the previous section. Administrators should deploy only SPFx solutions they trust. See KB10454. Microsoft Graph Permission Files.ReadWrite.AppFolder: Why Password Vault Needs It and How to Approve It.

Can Vitextra see my passwords?

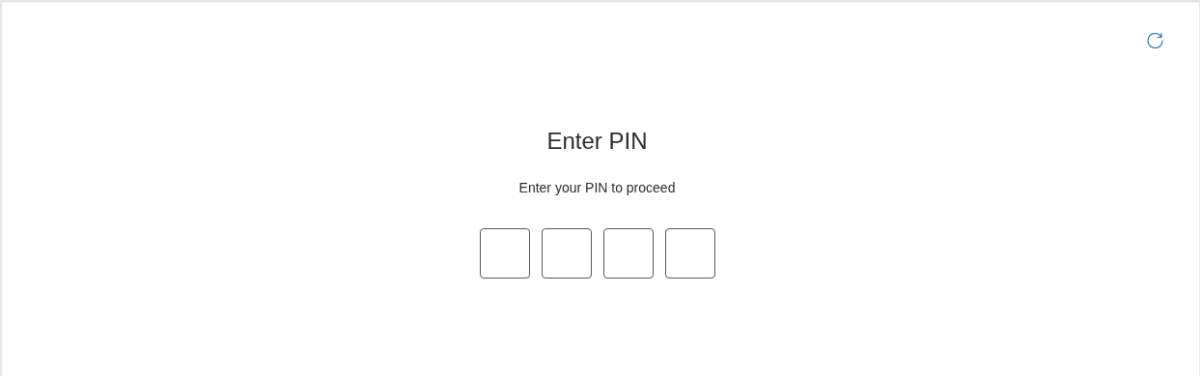
No. Encryption and decryption happen in your browser, and the vault file is transferred only between your browser and your OneDrive. Vitextra does not receive, store or back up vault data, your PIN or the key derived from it. The web part sends Vitextra only the technical identifiers of the license check and usage telemetry; see KB10363. Where Vitextra Products Store Your Data: Privacy, Data Residency and GDPR.

What can someone at my unlocked computer see?

Anyone who can use your browser while you are signed in to Microsoft 365 can open a page with Password Vault. **While the vault is locked and without the PIN**, that person sees no entries at all - not even their names:

- instead of the **list**, the web part shows only the **Enter PIN** prompt, and the toolbar offers only the **Refresh** button;
- passwords, user names, URLs, folders, tags and notes are not shown, and **New Item**, **Change PIN**, **Search**, the filter and the favorites are not available;
- the person can type PINs, and every wrong PIN counts toward the limit of five (see below).

Once the correct PIN has been entered, every action - showing and copying passwords, **New Item**, **Edit**, **Remove** and **Change PIN** - works without asking for the PIN again.



What is visible while the vault is locked

After you have entered the PIN, the vault stays unlocked while the page is open and in use: anyone at the computer can show and copy passwords and change entries until the automatic lock applies after **5 minutes** without interaction (see KB10451.

Automatic Lock: When Password Vault Asks for the PIN Again). A password that you copied also stays on the clipboard until something else is copied. Activity means interaction inside the web part; activity elsewhere on the page does not restart its timer.

Someone who does not know the PIN can also enter wrong PINs. Five wrong PINs in a row block the vault, and the only way out is a reset that erases all entries (see KB10455. Incorrect PIN Attempts in Password Vault: What Happens After Five Failed Tries).

The fifth wrong PIN blocks access; it does not erase entries automatically. Deletion requires confirming **Reset** and successfully saving the empty vault. Failed attempts are shared across pages and devices only after the counter is saved to OneDrive; if saving fails, the increase is local to the open session.

Tip

Lock your computer every time you leave it, and set or change your PIN where nobody can watch the screen: on the **Set up PIN** and **Change PIN** screens the digits are visible while you type them (on the **Enter PIN** prompt they are masked).

Can I share an entry with a colleague on purpose?

No. Password Vault is a personal vault: there are no shared entries, shared folders or team vaults. For credentials that a team must share, follow your organization's policy.

Related articles

- KB10453. Where Password Vault Stores Your Passwords: The OneDrive App Folder
- KB10452. How Password Vault Protects Your Data: Encryption, PIN and Storage
- KB10439. Password Vault: Frequently Asked Questions

Terms

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 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.

SharePoint
SharePoint is a web-based collaboration platform that provides content management, document management, workflow applications, search, and other tools that empower employees and teams to work together. SharePoint is also a secure place to store, organize, and access shared information.

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.

Site
A SharePoint site is a container for information within the SharePoint platform. Sites typically offer features such as document libraries, lists, calendars, discussion boards, and workflows, facilitating collaboration, communication, and document management within teams or across departments. Sites can be customized and configured to suit the specific needs and workflows of an organization.

Site Collection

Terms

A site collection is a group of one or more SharePoint sites, subsites, and related content. A site collection typically shares common settings, permissions, and configuration, providing a cohesive environment for users to work together on projects, departments, or specific areas of focus. Site collections are often used to separate content and control access rights based on organizational structure, security requirements, or project needs.

Tenant
A Microsoft 365 tenant is a dedicated instance of Microsoft 365 services. The tenant holds the organization's information, such as users and domains (Microsoft Entra ID), configurations, subscriptions, and services. An organization receives a tenant by signing up for Microsoft 365 services.

View
A view is a saved configuration that determines which items of a list or library are displayed and how, including the columns, sorting, filtering, grouping, and layout. Views can be personal or public.

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.