KNOWLEDGE BASE ARTICLE

Password Vault vs. Browser Password Managers and Enterprise Password Managers: Which to Choose

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

Password Vault in short 4

Comparison at a glance 5

When Password Vault is a good fit 6

When a browser password manager is a good fit 7

When an enterprise password manager is a good fit 7

Using the tools side by side 7

Questions to ask before you decide 8

Terms 9

Overview

Organizations that want employees to stop keeping passwords in spreadsheets and notes usually look at three kinds of tools:

- **Browser password managers** - the password storage built into web browsers, which saves credentials as the user signs in to websites.
- **Enterprise password managers** - dedicated products, usually with their own service, client apps and browser extensions, designed for organization-wide credential management.
- **Password Vault** - a Vitextra **SharePoint** Framework **web part** that gives every employee a lightweight personal vault inside **Microsoft 365** (**SharePoint Online** and **Microsoft Teams**).

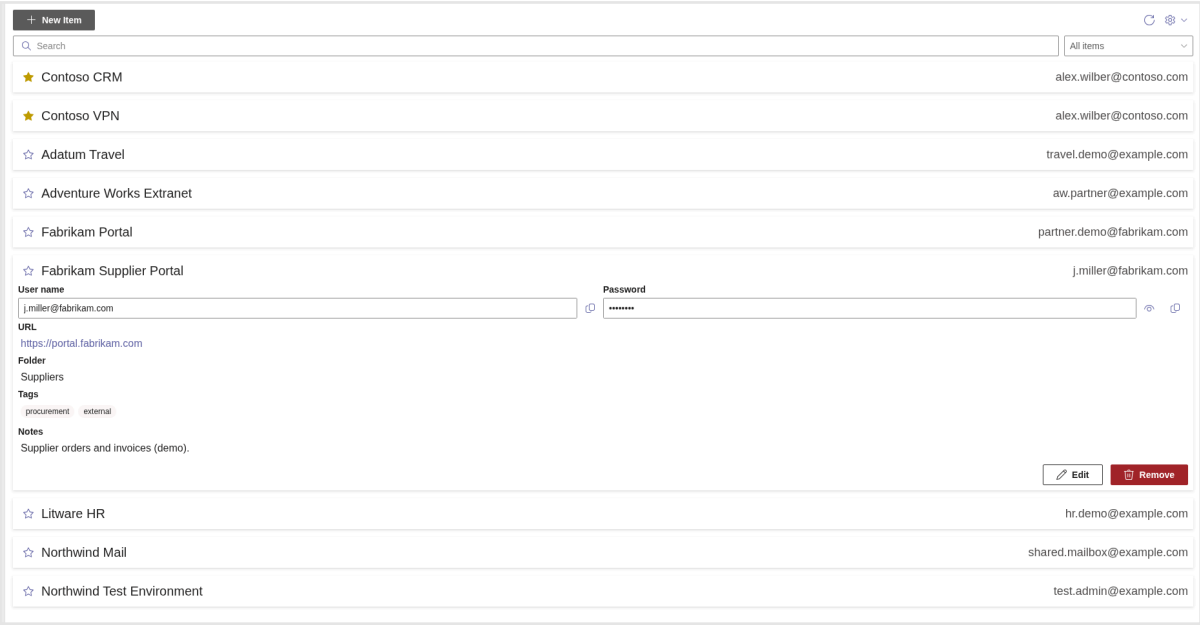
These tools solve different problems. This article describes the general characteristics of each category so that you can decide which one fits a given need. Individual products within a category differ, so check the specifics of any product you consider against your own requirements.

Password Vault in short

Password Vault stores each user's entries encrypted in a file in that user's own OneDrive and shows them in a web part on a SharePoint page or in Teams. Access inside the web part is protected by a 4-digit PIN, from which the encryption key is derived; while the vault is locked, no entries are shown, and it locks automatically after 5 minutes without interaction. Because a PIN has only 4 digits, access control to OneDrive remains the first line of protection for the file. It includes a password generator, a strength meter, folders, tags, favorites and search. For details, see KB10437. Password Vault. Solution Overview.

Equally important is what it does **not** do:

- no automatic filling of sign-in forms and no browser extension - credentials are copied with **Copy to Clipboard**;
- no sharing of entries and no team vaults;
- no administration console and no recovery of a forgotten PIN - after 5 incorrect PINs the only option is to reset the vault, which erases all entries;
- no export or import.



Password Vault as a personal app in Microsoft Teams

Comparison at a glance

The Password Vault column describes the product; the other two columns describe what is typical for the category.

Aspect	Password Vault	Browser password managers (typical)	Enterprise password managers (typical)
Purpose	Personal credentials of an employee, inside Microsoft 365	Personal convenience while browsing	Organization-wide credential management
Where the data is kept	Encrypted file in the user's own OneDrive	In the browser profile, often synchronized through the browser vendor's account	In the product's own service or an infrastructure the organization operates
Access	SharePoint page or Microsoft Teams, with the work account and a 4-digit PIN	The browser where the profile is signed in	Client apps, browser extensions and web access of the product

Aspect	Password Vault	Browser password managers (typical)	Enterprise password managers (typical)
Autofill of sign-in forms	No	Yes	Usually yes
Sharing with colleagues	No	Limited or none in a work context	Usually yes, with shared folders or vaults
Administration, policies, audit	No; deployment and the Graph permission only	Depends on the browser's management options	Usually extensive
Recovery of lost access	None; reset erases the vault	Depends on the browser account	Usually offers recovery options for administrators or users
Deployment	One SPFx package and one Graph permission; no extra client software	Already present in the browser	A separate product to roll out, configure and license per user
Typical cost model	Per **tenant** license	Included with the browser	Usually per user subscription

When Password Vault is a good fit

- Employees need a place for **their own** work-related credentials - supplier portals, partner extranets, test systems, device consoles - and the organization wants that place to be inside Microsoft 365 rather than in personal tools or files.
- The organization prefers that the data stay in **its own tenant** (each user's OneDrive) and not with an additional third-party service.
- A simple tool that works on a SharePoint page and in Teams without installing extensions or client software is more important than autofill.
- The credentials are not shared and losing them, if a PIN is forgotten, is acceptable because they can be restored from their source (for example, through the service's own "forgot password" process).

When a browser password manager is a good fit

- The main need is convenience: saving and automatically filling passwords for websites while browsing.
- Users work mainly in one browser and the organization's policy allows storing work credentials in it.

Keep in mind that a browser password manager stores credentials in the browser profile, so what is available depends on the browser and the account the user is signed in with, and on how the organization manages browsers.

When an enterprise password manager is a good fit

- Credentials must be **shared** within teams, for example service accounts or shared partner-portal accounts.
- The organization needs central **policies, audit trails, access reviews and recovery** procedures.
- **Highly privileged** administrative accounts must be managed - often in combination with privileged access management.
- Autofill across browsers, desktop and mobile apps is required.

These capabilities come with a separate product to deploy, configure, train users on and license, usually per user.

Warning

Password Vault is designed for personal credentials. It is not a replacement for a solution that manages shared or highly privileged accounts. For such accounts, follow your organization's security policy.

Using the tools side by side

The categories are not mutually exclusive. An organization may run an enterprise password manager for IT and shared accounts and offer Password Vault to all employees as an easy personal place for the remaining work credentials - or allow browser storage for low-risk websites. What matters is a clear policy that says which kind of credential belongs where.

Note

Password Vault has no import or export, so moving entries into or out of it means adding them one by one. Plan the choice before employees start building up their vaults.

Questions to ask before you decide

1 Do credentials have to be shared, or are they strictly personal?
2 Is automatic filling of sign-in forms required?
3 Where may the encrypted data be stored - in your Microsoft 365 tenant, in a browser vendor's account or in a third-party service?
4 Do you need administrative recovery, policies and audit?
5 What can you deploy: an SPFx web part, or client software and extensions on every device?
6 What happens to the credentials if a user loses access - can they be restored from the source system?

Tip

To see how Password Vault protects data and who can access it, read KB10452. How Password Vault Protects Your Data: Encryption, PIN and Storage and KB10456. Who Can See Your Passwords in Password Vault. To try it, see KB10438. How to Add the Password Vault Web Part to a Page and Create Your Vault.

Learn more about the product: *https://vitextra.com/en/products/password-vault*

Terms

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

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.

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.

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.