KNOWLEDGE BASE ARTICLE

Password Vault. Solution Overview

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

Introduction 4

Key capabilities 4

How it works 6

- **Where the entries are stored** 6
- **Encryption and the PIN** 6
- **Working on several devices** 7

What Password Vault is designed for 7

Requirements 8

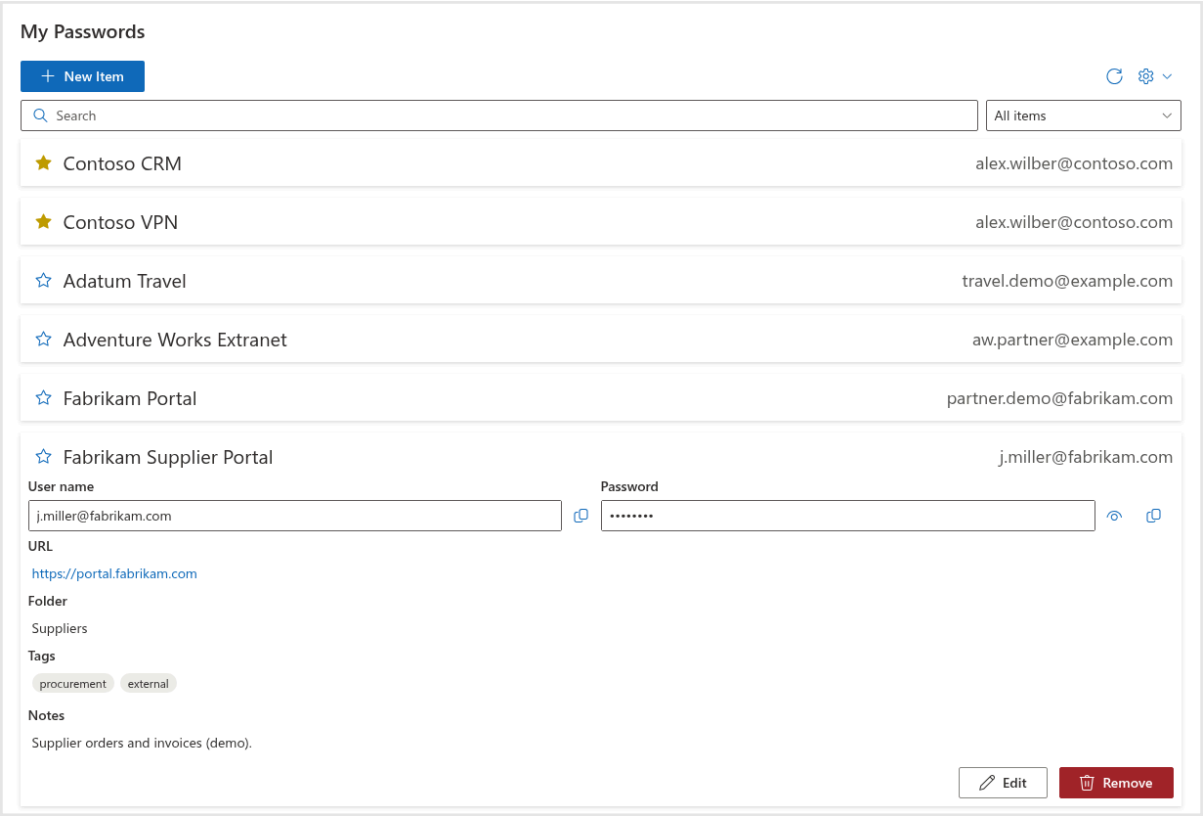
Terms 10

Introduction

Employees collect sign-ins for many systems that are not covered by single sign-on: supplier portals, partner extranets, test environments, conference registrations, hardware consoles. Without a dedicated tool these credentials end up in spreadsheets, sticky notes or e-mail drafts.

Password Vault is a **SharePoint** Framework **web part** that gives every employee a personal password manager inside **Microsoft 365**. Each user keeps their own **list** of entries - name, user name, password, URL, notes, folder and tags - protected by a 4-digit PIN. The entries are stored encrypted in a file in the user's own OneDrive, not in SharePoint lists and not on Vitextra servers. The same web part can be placed on a SharePoint page or in **Microsoft Teams**, and every user always sees their own vault.

This article explains what the web part does and how it works. To place it on a page, see KB10438. How to Add the Password Vault Web Part to a Page and Create Your Vault.



Password Vault on a SharePoint page

Key capabilities

A personal vault for every user. The web part shows the vault of the person who opens the page. Placing it on a shared page or in a team channel does not share any

passwords: each visitor sees only their own entries.

PIN protection. On first use, the user sets a 4-digit PIN. While the vault is locked, the web part shows no entries at all, only a prompt for the PIN; once the PIN is entered, all entries and actions are available. See KB10442. How to Set Up Your PIN in Password Vault.

Automatic lock. After the PIN is entered, the vault stays unlocked while the user works with it and locks again after 5 minutes without interaction: the list is hidden and open dialogs are closed. Reloading the page also locks it. See KB10451. Automatic Lock: When Password Vault Asks for the PIN Again.

Entries with all the details. Each entry has a **Name**, **User name**, **Password**, an optional **URL** that opens in a new tab, a **Folder**, **Tags** and **Notes**. See KB10443. How to Add, Edit and Delete Entries in Password Vault.

One-click copy. The user name and the password are copied to the clipboard with the **Copy to Clipboard** buttons, so passwords do not need to be shown on the screen. See KB10444. How to View and Copy a Password or User Name in Password Vault.

Password generator. The built-in generator creates random passwords of 8 to 64 characters from the character sets the user selects, using the browser's cryptographic random number generator. See KB10445. How to Generate a Strong Password with the Password Vault Generator.

Strength meter. While a password is typed, a five-step bar shows its estimated strength, from *Very weak* to *Very strong*. See KB10446. Password Strength Meter in Password Vault: What the Levels Mean.

Folders, tags and favorites. Entries can be grouped in folders, labeled with tags and marked as favorites, which are always listed at the top. See KB10447. Organizing Entries with Folders and Tags in Password Vault and KB10448. Favorites in Password Vault: Keeping Frequently Used Entries at the Top.

Search and filter. The **Search** box finds entries by name, user name, URL, folder, notes and tags; the filter drop-down narrows the list to favorites, a folder or a tag. See KB10449. Searching and Filtering Entries in Password Vault.

SharePoint and Microsoft Teams. The web part works on modern **SharePoint Online** pages, as a Teams channel tab and as the Teams personal app **Passwords**. It is the same vault everywhere.

Theme and language. The web part follows the **site** theme, including section backgrounds, and the site font. Its interface is translated into the SharePoint

languages and follows the language of SharePoint or Teams. In a narrow column (less than 500 pixels wide) the list switches to a compact layout.

How it works

Where the entries are stored

Each user's vault is a single file, `vitextra-password-vault.json`, in the app folder of that user's own OneDrive. The web part reads and writes the file through **Microsoft Graph** on behalf of the signed-in user. Nothing is stored in SharePoint lists, in the web part properties or on Vitextra servers.

Because the vault lives in the user's OneDrive and not on the page, the same vault appears on every page, site and **Teams tab** where the web part is placed. If the web part finds no vault file for the user, it creates an empty one and asks the user to set up a PIN. Details: KB10453. Where Password Vault Stores Your Passwords: The OneDrive App Folder.

Encryption and the PIN

The name, user name, password, URL, notes, folder and tags of every entry are encrypted with AES in the user's browser before the file is saved. The encryption key is derived from the PIN with PBKDF2-SHA256 (a random salt per vault, 600,000 iterations); it is not stored anywhere and exists only in the memory of the open page while the vault is unlocked, so the vault file alone is not enough to read the entries. The file travels only between the browser and the user's OneDrive, and access to it is governed by Microsoft 365 and OneDrive permissions, like any other file in the user's OneDrive.

The PIN opens the vault. While the vault is locked, the web part shows no entries - not even their names - but only the **Enter PIN** prompt with four masked digit boxes. Keep in mind that a PIN has only 4 digits (10,000 combinations): PBKDF2 makes every guess deliberately slow, but someone who obtains a copy of the file could still try all PINs offline, because the limit of 5 attempts applies only inside the web part. Access control to OneDrive therefore remains the first line of protection. For the full description, see KB10452. How Password Vault Protects Your Data: Encryption, PIN and Storage and KB10456. Who Can See Your Passwords in Password Vault.

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. KB10455. Incorrect PIN Attempts in Password Vault: What Happens After Five Failed Tries · KB10460. I Forgot My PIN in Password Vault: What Are My Options?

Note

Vaults created with an earlier version of the web part are migrated to the new encryption automatically the first time the user enters the correct PIN; the entries and their modification dates are kept. Older versions of the web part cannot open a migrated vault, so administrators should update Password Vault in every **app catalog** of the **tenant**. See KB10050. How to Update a Vitextra SPFx Solution in SharePoint Online and KB10361. Tenant App Catalog vs. Site Collection App Catalog: Where to Deploy Vitextra Apps.

Working on several devices

Each save is checked against the version of the vault file it was built from. If the vault was saved elsewhere in the meantime - on another device or in another browser tab - the web part loads the latest file and applies the change to it, so changes to other entries made elsewhere are preserved. If two sessions edit the same entry, the later successfully saved draft replaces that entry; individual fields are not merged. A change saved on one device appears on another after **Refresh**, after the next save or after unlocking there. If the PIN was changed on another device, the open page locks itself as soon as it next loads the latest vault file (on Refresh, unlock or save) and asks for the new PIN.

What Password Vault is designed for

Password Vault is a lightweight **personal** vault. It deliberately keeps a narrow scope:

- Entries cannot be shared with colleagues; there are no team or shared vaults.
- There is no browser extension and no automatic filling of sign-in forms; credentials are copied from the web part.

- Administrators have no console to manage, **view** or recover users' vaults.
- There is no export or import of entries.

For a comparison with other kinds of password managers, see KB10440. Password Vault vs. Browser Password Managers and Enterprise Password Managers: Which to Choose.

Note

Password Vault is intended for personal credentials. For highly privileged administrative accounts and credentials that a team must share, follow your organization's security policy.

Requirements

- Microsoft 365 with SharePoint Online; modern pages. The web part is not available for SharePoint Server.
- Every user must have a OneDrive in the tenant, because the vault is stored there.
- The package is deployed from the App Catalog like any Vitextra product; tenant-wide deployment is supported. See KB10035. How to Install a Vitextra Product in SharePoint Online.
- An administrator must approve the Microsoft Graph delegated permission `Files.ReadWrite.AppFolder`, which lets the web part read and write only in its own app folder of the user's OneDrive. See KB10454. Microsoft Graph Permission Files.ReadWrite.AppFolder: Why Password Vault Needs It and How to Approve It and KB10360. How to Approve Microsoft Graph API Permissions for Vitextra Solutions in the SharePoint Admin Center.
- No SharePoint list permissions are needed: any user who can open the page can use their own vault.
- Licensing is per tenant. When the license expires, the web part shows *We hope you enjoyed your free trial. Buy it now to keep it working.* instead of the vault until the license is renewed; the vault files in OneDrive are not changed. See KB10206. Vitextra Licensing and Account: How to Buy and Activate a License and KB10364. What Happens When Your Vitextra Trial or Subscription Expires.

Tip

New users can start with KB10441. Password Vault: A Quick Guide for End Users. Answers to common questions are collected in KB10439. Password Vault: Frequently Asked Questions.

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

Terms

App Catalog
The App Catalog is a special SharePoint site that stores apps for SharePoint, Teams, and other Microsoft 365 services. Global or SharePoint administrators can upload and manage applications from the AppSource marketplace, custom-developed apps, or third-party apps for the organization's internal use. There can be only one tenant-level App Catalog in a tenant; site collection app catalogs can be added for individual site collections.

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.

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

Terms

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.

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.

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.