KNOWLEDGE BASE ARTICLE

# Microsoft Graph Permission Files.ReadWrite.AppFolder: Why Password Vault Needs It and How to Approve It

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

**Why Password Vault needs the permission** 4

**What the permission allows and what it does not** 4

**How to approve the permission** 5

**What users see until the permission is approved** 6

**Related articles** 6

**Terms** 7

# Overview

Password Vault keeps each user's vault in a file in the app folder of that user's OneDrive. To read and write this file, the solution package requests exactly one **Microsoft Graph** permission: **Files.ReadWrite.AppFolder**. A **tenant** administrator must approve it once after the package is deployed; until then the **web part** cannot open or create any vault. This article explains the permission and the approval.

# Why Password Vault needs the permission

The web part uses Microsoft Graph for three operations, all in the signed-in user's OneDrive app folder:

- finding the vault file `vitextra-password-vault.json`;
- creating it the first time the user opens Password Vault;
- reading it and saving it after every change.

Password Vault requests no other Microsoft Graph permission and needs no **SharePoint list** permissions: any user who can open the page can use his or her own vault.

Users also need a provisioned OneDrive and approved access. The permission-specific error described below assumes that no other existing grant provides the required file access.

# What the permission allows and what it does not

| Aspect | Details |
|---|---|
| Permission type | **Delegated**: it works only on behalf of the signed-in user, not as an independent application identity |
| Allows | Reading and writing files in the app folder of the signed-in user's own OneDrive |
| Does not allow | Reading or changing the user's other OneDrive files, other users' OneDrive, SharePoint sites, mail, calendars or directory data |
| Application (app-only) access | None; Password Vault has no service |

| Aspect | Details |
|---|---|
| | account and no background process |

**Note**

In **SharePoint Online**, API permissions of SPFx solutions are granted to one **Microsoft Entra ID** application shared by all SPFx solutions in the tenant, *SharePoint Online Client Extensibility Web Application Principal*. Once *Files.ReadWrite.AppFolder* is approved, it is available to every SPFx solution deployed in your tenant, and the app folder is the folder of that shared application. This is how the SharePoint Framework works for all vendors. Deploy only SPFx solutions that you trust; see the security notes in KB10360. How to Approve Microsoft Graph API Permissions for Vitextra Solutions in the SharePoint Admin Center.

## How to approve the permission

The permission request is created when the Password Vault package is deployed to the **tenant App Catalog** (see KB10035. How to Install a Vitextra Product in SharePoint Online). You need the **Global Administrator** role; the SharePoint Administrator role alone is insufficient for Microsoft Graph permissions. Microsoft

1. Open the **SharePoint admin center**.

2. Go to **Advanced** > **API access**.

3. On the **Pending requests** tab, select the request of the *Vitextra Password Vault* package for *Microsoft Graph / Files.ReadWrite.AppFolder*.

4. Click **Approve** and confirm.

5. Check that the permission now appears on the **Approved requests** tab.

If *Files.ReadWrite.AppFolder* has already been approved for another SPFx solution, no new request appears: SharePoint reuses the existing grant. Users do not see a consent prompt; after the approval the web part works for everyone in the tenant, usually within a few minutes. If it does not, reload the page.

**Tip**

For screenshots, PowerShell commands, partial approval, revoking permissions and the behaviour during updates, see KB10360. How to Approve Microsoft Graph API Permissions for Vitextra Solutions in the SharePoint Admin Center.

## What users see until the permission is approved

The package can be deployed and the web part can be added to pages while the request is still pending. Without the permission, however, the web part cannot read or create the vault. Instead of the **Set up PIN** screen or the **Enter PIN** prompt, users see the message "Sorry, something went wrong. Please refresh the page and try again." with a **Refresh** button. No vault file is created.

After the approval, users press **Refresh** or reload the page, and the web part opens normally.

The same message appears if an approved permission is later removed on the **Approved requests** tab. Removing the permission does not delete any vault files: they stay in the users' OneDrive and open again once the permission is approved. For other causes of the message, see KB10459. Why Password Vault Does Not Load: "Something Went Wrong" and Permission Errors.

## Related articles

- KB10453. Where Password Vault Stores Your Passwords: The OneDrive App Folder
- KB10452. How Password Vault Protects Your Data: Encryption, PIN and Storage
- KB10363. Where Vitextra Products Store Your Data: Privacy, Data Residency and GDPR

# 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 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.

**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.

# Terms

**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.