KNOWLEDGE BASE ARTICLE

How to Approve Microsoft Graph API Permissions for Vitextra Solutions in the SharePoint Admin Center

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

What is requested and why 4

Where the requests come from 6

Prerequisites 7

Approving the requests 7

Approving only part of the permissions 9

What users see when a permission is missing 10

Updates and new permissions 10

Reviewing and revoking permissions 10

Security notes for reviewers 11

Terms 12

Overview

Several Vitextra web parts read data that lives outside the **SharePoint site**: user profiles and the manager hierarchy in **Microsoft Entra ID**, presence in **Microsoft Teams**, calendars, tasks in Planner and To Do, files in OneDrive. **SharePoint Framework (SPFx)** solutions reach this data through **Microsoft Graph**, and a **tenant** administrator has to allow it once.

The mechanism is the same for every SPFx solution: the solution package declares the permissions it needs, SharePoint turns the declaration into *permission requests* when the package is deployed to the **App Catalog**, and the requests wait on the **API access** page of the **SharePoint admin center** until an administrator approves or rejects them.

This article explains which Vitextra products request permissions and why, how to approve the requests, how to review and revoke them later, and what you see in the web parts when a permission is missing. It is written for SharePoint and Global Administrators who install Vitextra products, and for security officers who review such requests.

Note

The article covers the API access requests of SPFx solutions only. Installing the package itself is described in KB10035. How to Install a Vitextra Product in SharePoint Online.

What is requested and why

The permissions listed below are **delegated**: the web parts call Microsoft Graph on behalf of the signed-in user. Effective access depends on both the granted scopes and the user's permissions. This does not imply that Graph results match exactly what Outlook or Teams displays. Microsoft Graph

The table lists the permissions declared by the current versions of the products that use Microsoft Graph.

Product	API	Permissions	Used for
Employee Directory	Microsoft Graph	User.Read.All, Directory.Read.All, People.Read, Presence.Read.All, Calendars.Read	Reading user profiles, departments and managers; relevant people; Teams

Product	API	Permissions	Used for
			presence; the free/busy status for the availability indicator
Employee Details	Microsoft Graph	User.Read.All, User.ReadWrite, People.Read.All, Presence.Read.All, Files.Read.All, Sites.Read.All, Calendars.Read.Shared	Reading profiles; letting a user edit his or her own profile fields; relevant people; presence; documents and sites the person recently worked with (Microsoft Graph insights); the free/busy status of colleagues for working hours and availability
Organizational Chart	Microsoft Graph	User.Read.All, Directory.Read.All, Presence.Read.All	Building the reporting hierarchy from the **Manager** attribute; department and job title; Teams presence
Absence & Coverage	Microsoft Graph	User.Read.All	Resolving employees, their managers and direct reports for requests, approvals and substitutions
My Tasks	Microsoft Graph	User.Read, User.ReadBasic.All, Tasks.ReadWrite	Tasks from Planner, To Do and flagged e-mail; names of

Product	API	Permissions	Used for
			task authors
My Tasks	**Azure DevOps**	user_impersonation	The **Azure DevOps** source and the **Azure DevOps Query** web part
Password Vault	Microsoft Graph	Files.ReadWrite.AppFolder	Storing the encrypted vault in the application folder of the user's OneDrive

Products that work only with the current site - Announcements Carousel, **List** Filter Online, **QR Code** Generator, Questions & Answers, Quick Poll, **RSS** Reader, Smart Search and Smart Tiles - request **no** API permissions. Nothing appears for them on the **API access** page.

Note

A permission name such as *Tasks.ReadWrite* or *User.ReadWrite* is the name of the Microsoft Graph scope, which may be broader than what the product does with it. My Tasks only reads tasks; Employee Details writes only the profile fields of the signed-in user. The product-specific articles explain each permission in detail: KB10235. Microsoft Graph Permissions Required by Organizational Chart, KB10303. My Tasks: Required Permissions, Privacy and Security.

Where the requests come from

A permission request is created when the `.sppkg` package is deployed to the tenant App Catalog. The requests belong to the package, not to the individual web parts, so a solution that contains two web parts shows one set of requests, and a permission that is needed only by an optional **feature** (the Azure DevOps source of My Tasks, for example) is requested together with the others.

Two points are important for governance:

- **Approval is tenant-wide.** SharePoint grants the permission to a single Microsoft Entra ID application that it uses for all SPFx solutions - *Web Client Extensibility* (earlier: *SharePoint Online Client Extensibility Web Application Principal*). Once

User.Read.All has been approved for Employee Directory, the same grant is used by Organizational Chart and by any other SPFx solution in the tenant that requests it. This is how the SharePoint Framework works, not a Vitextra design decision.

- **Deployment does not depend on approval.** A Vitextra product can be deployed, added to sites and placed on pages while its requests are still pending or even rejected. Only the features that depend on the missing permission fail.

Prerequisites

- The Vitextra package is uploaded to the tenant App Catalog and deployed (**Enable app**).
- To approve Microsoft Graph and other Microsoft API permissions, sign in as a **Global Administrator**. The **Application Administrator** role is sufficient for third-party APIs registered in the tenant. The SharePoint Administrator role alone does not authorize approval of Microsoft Graph permissions. Microsoft

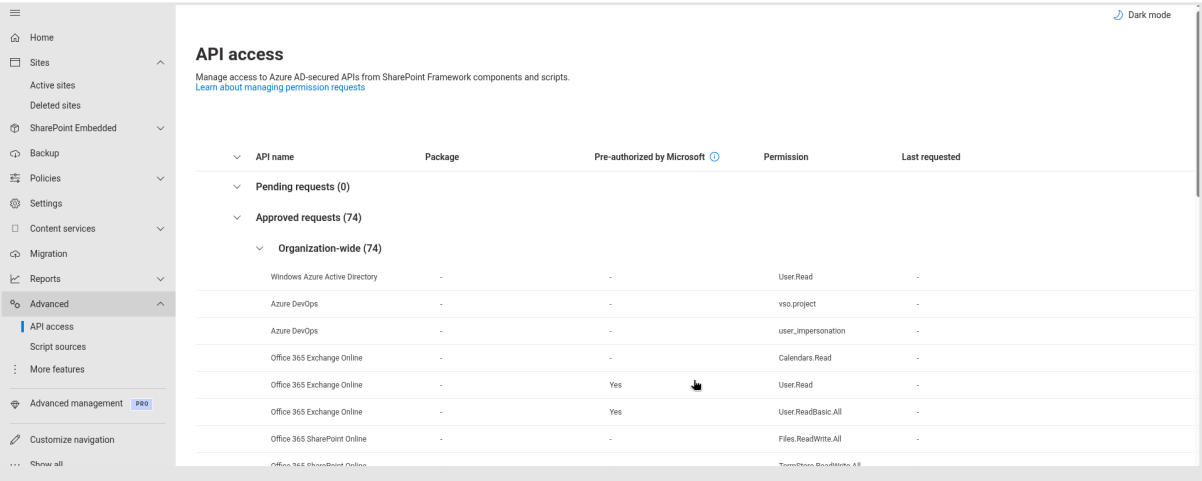
Warning

The **API access** page shows the requests of packages deployed to the **tenant** App Catalog. If you prefer to deploy Vitextra products from a site collection app catalog, deploy the package to the tenant App Catalog first and approve the requests there; the approved permissions are tenant-wide and are then available to the copy in the site collection app catalog as well.

Approving the requests

1. Open the Microsoft 365 admin center and go to the **SharePoint admin center**.

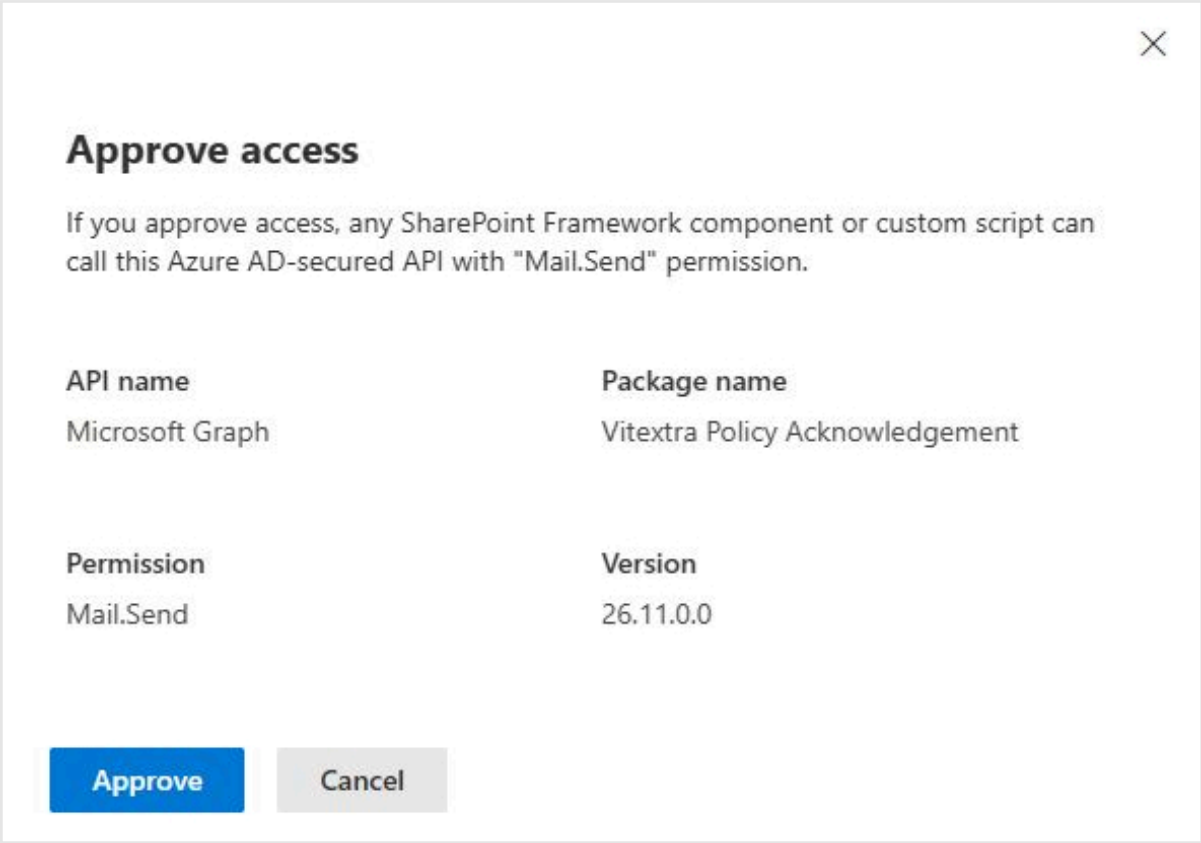
2. In the left navigation, expand **Advanced** and select **API access**.



API access requests

3. On the **Pending requests** tab, find the requests of the Vitextra package. Each row shows the package name (for example *Vitextra Employee Directory*), the API (*Microsoft Graph* or *Azure DevOps*) and the permission.

4. Select a request and click **Approve**. Read the description in the panel and confirm with **Approve**.



Approving an API access request

5. Repeat for every request of the package. A permission that has already been approved for another solution does not appear again: SharePoint reuses the existing grant.

6. Switch to the **Approved requests** tab and check that all permissions of the package are listed.

Microsoft Graph	-	Yes	Presence.Read.All	-
Microsoft Graph	-	Yes	TeamsAppInstallation.ReadWriteSel...	-
Microsoft Graph	-	Yes	User.Read	-
Microsoft Graph	-	Yes	User.ReadBasic.All	-
Microsoft Graph	-	Yes	Tasks.ReadWrite	-
Microsoft Graph	-	Yes	Group-Conversation.ReadWrite.All	-
Microsoft Graph	-	Yes	Team.ReadBasic.All	-
Microsoft Graph	-	Yes	Channel.Create	-
Microsoft Graph	-	Yes	Sites.Read.All	-
Microsoft Graph	-	-	Presence.Read	-
Microsoft Graph	-	-	User.Read.All	-
Microsoft Graph	-	Yes	Calendars.Read	-
Microsoft Graph	-	-	Directory.Read.All	-

Approved requests

Users do not see a consent prompt: after the approval the web parts work for everybody in the tenant. The grant usually takes effect within a few minutes; if a web part still reports a missing permission, reload the page or sign out and in again to get a new token.

Tip

You can approve the requests in one go with the SharePoint Online Management Shell: `Get-SPOTenantServicePrincipalPermissionRequests` lists the pending requests, and `Approve-SPOTenantServicePrincipalPermissionRequest -RequestId <id>` approves one of them. This is convenient when you roll out several Vitextra products at once.

Approving only part of the permissions

You may approve some requests and reject others. The web part keeps working, and only the dependent feature is affected:

- *Presence.Read.All* rejected - Employee Directory, Employee Details and Organizational Chart show people without the Teams presence indicator.
- *Calendars.Read* / *Calendars.Read.Shared* rejected - the availability and working-hours information is not shown.
- *Files.Read.All* / *Sites.Read.All* rejected - Employee Details does not show recent files and sites.
- *user_impersonation* (Azure DevOps) rejected - the Azure DevOps source of My Tasks and the Azure DevOps Query web part cannot sign in to Azure DevOps.

Rejecting the core permission of a product (*User.Read.All* for the people-centric products, *Tasks.ReadWrite* for My Tasks, *Files.ReadWrite.AppFolder* for Password Vault) leaves the web part without data.

What users see when a permission is missing

Symptom	Likely cause
The web part shows an error about access being denied, insufficient privileges or a missing consent	The core permission is pending or rejected
Employees are listed, but the colored presence dot is missing	*Presence.Read.All* is not approved
The organizational chart is empty or shows only the current user	*User.Read.All* or *Directory.Read.All* is not approved
My Tasks shows nothing for Planner, To Do and Outlook, while the SharePoint source works	*Tasks.ReadWrite* is not approved
Everything worked, and after an update one feature stopped	The new version requests an additional permission that is still pending

Open the **API access** page and compare the **Pending requests** and **Approved requests** tabs with the table at the beginning of this article.

Updates and new permissions

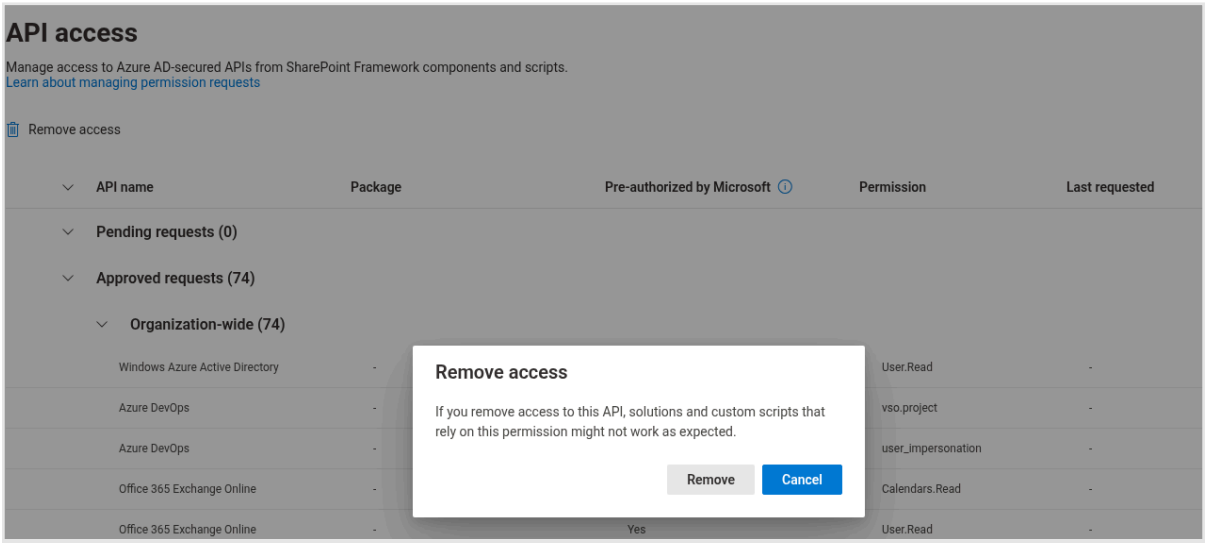
When you upload a new version of a package (see KB10050. How to Update a Vitextra SPFx Solution in SharePoint Online), the permissions that were approved earlier stay approved. If the new version declares a permission that the previous one did not, the new request appears on the **Pending requests** tab and has to be approved in the same way. Vitextra lists such changes in the release notes of the product.

Reviewing and revoking permissions

Because the grants are shared by all SPFx solutions, removing a Vitextra product does **not** revoke the permissions it requested. To revoke a permission:

1 Open **API access** and switch to the **Approved requests** tab.
2 Select the permission and click **Remove access**.

3 Confirm.



Removing an approved permission

Warning

Before you remove a permission, check whether another solution in the tenant depends on it - your own SPFx web parts, products of other vendors and Microsoft's own pre-authorized permissions appear on the same tab. Removing a permission that another solution uses breaks that solution immediately.

Rejecting a request removes it from the API access page; it does not remain under **Pending requests**. To request the permission again, the developer must submit a new request for the same resource and scope. Microsoft

Security notes for reviewers

- Every call to Microsoft Graph is made from the browser of the signed-in user with a token issued for that user. Vitextra web parts have no application (app-only) permissions and no service account.
- Microsoft Graph checks the granted delegated scopes and the user's permissions. Address-book visibility and application-specific filters are separate concerns; do not assume that hiding someone in Outlook also hides them from Graph queries.
- For product-specific data flows, license requests, telemetry and storage, see 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.

Azure DevOps
Azure DevOps Services (formerly Visual Studio Team Services) is a cloud-based product that provides version control, requirements management, automated pipelines for builds and releases, and testing capabilities.

Feature
A feature is a set of SharePoint elements (artifacts), such as site columns, content types, web parts, application pages, custom actions, list templates, list instances, and others.

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.

Microsoft Teams

Terms

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

QR Code
A Quick Response (QR) code is a two-dimensional barcode that stores information. It can be scanned using a QR code reader or a mobile device's camera, providing quick access to the encoded data.

RSS
RSS (Really Simple Syndication) is a popular web feed format used to deliver updates from websites to users and applications in a standardized, machine-readable format. This format is commonly used for distributing news articles, blog posts, and other frequently updated content.

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 Admin Center
The SharePoint admin center is the web portal where SharePoint administrators manage sites, sharing and access settings, the App Catalog, storage, and other SharePoint Online settings for the tenant.

SharePoint Framework (SPFx)
SharePoint Framework (SPFx) is a model for building client-side web parts, components, and extensions for SharePoint Online, SharePoint Server (on-premises), and Microsoft Teams. SPFx customizations are based on JavaScript and support the modern user interface natively.

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.

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.