WISSENSDATENBANKARTIKEL

So genehmigen Sie Microsoft-Graph-API-Berechtigungen für Vitextra-Lösungen im SharePoint Admin Center

2026 © Vitextra SIA. Alle Rechte vorbehalten.

Haftungsausschluss

Für die Zwecke dieses Haftungsausschlusses:

- **Das Unternehmen** (in diesem Haftungsausschluss entweder als „das Unternehmen“, „wir“, „uns“ oder „unser“ bezeichnet) bezieht sich auf Vitextra SIA, LV-1009 Riga, Matīsa iela 61 – 25.
- **Dokument** verweist auf den Wissensdatenbank-Artikel.
- **Sie** sind die Person, die auf das Dokument zugreift, bzw. das Unternehmen oder eine andere juristische Person, in deren Namen eine solche Person auf das Dokument zugreift oder es nutzt.
- **Die Website** verweist auf Vitextra, zugänglich über https://vitextra.com

Haftungsausschluss

Die in diesem Dokument enthaltenen Informationen dienen nur der allgemeinen Information.

Das Unternehmen übernimmt keine Verantwortung für Fehler oder Auslassungen im Inhalt des Dokuments.

In keinem Fall haftet das Unternehmen für besondere, direkte, indirekte oder zufällige Schäden oder für Schäden jeglicher Art, die sich aus der Nutzung des Inhalts des Dokuments ergeben, unabhängig davon, ob es sich um eine Klage aufgrund von Vertrag, Fahrlässigkeit oder anderen Delikten handelt. Das Unternehmen behält sich das Recht vor, den Inhalt des Dokuments jederzeit und ohne vorherige Ankündigung zu ergänzen, zu streichen oder zu ändern.

Haftungsausschluss für Fehler und Auslassungen

Die in dem Dokument enthaltenen Informationen dienen lediglich als allgemeine Orientierungshilfe zu Fragen von Interesse. Daher können Fehler auftreten, auch wenn das Unternehmen alle Vorsichtsmaßnahmen ergreift, um sicherzustellen, dass der Inhalt des Dokuments aktuell und korrekt ist. Außerdem kann es angesichts der sich ändernden Gesetze, Regeln und Vorschriften zu Verzögerungen, Auslassungen oder Ungenauigkeiten bei den in diesem Dokument enthaltenen Informationen kommen.

Das Unternehmen haftet nicht für etwaige Fehler oder Auslassungen oder für die Ergebnisse, die sich aus der Verwendung dieser Informationen ergeben.

Haftungsausschluss für faire Nutzung

Das Unternehmen darf urheberrechtlich geschütztes Material verwenden, das der Urheberrechtsinhaber nicht ausdrücklich genehmigt hat. Das Unternehmen stellt dieses Material für Kritik, Kommentare, Berichterstattung, Schulung, Wissenschaft oder Forschung zur Verfügung.

Das Unternehmen ist der Ansicht, dass dies eine „faire Nutzung“ von urheberrechtlich geschütztem Material im Sinne von Abschnitt 107 des US-Urheberrechtsgesetzes darstellt.

Wenn Sie urheberrechtlich geschütztes Material aus dem Dokument für Ihre eigenen Zwecke verwenden möchten, die über eine angemessene Nutzung hinausgehen, müssen Sie die Erlaubnis des Urheberrechtsinhabers einholen.

„Benutzung auf eigene Gefahr“ Haftungsausschluss

Alle Informationen in diesem Dokument werden im Ist-Zustand zur Verfügung gestellt, ohne Garantie auf Vollständigkeit, Genauigkeit, Aktualität oder auf die Ergebnisse, die sich aus der Verwendung dieser Informationen ergeben, und ohne jegliche ausdrückliche oder stillschweigende Garantie, einschließlich, aber nicht beschränkt auf Garantien für Leistung, Marktgängigkeit und Eignung für einen bestimmten Zweck.

Das Unternehmen haftet weder Ihnen noch anderen gegenüber für Entscheidungen oder Handlungen, die im Vertrauen auf die Informationen des Dienstes getroffen wurden, noch für Folgeschäden, besondere oder ähnliche Schäden, selbst wenn auf die Möglichkeit solcher Schäden hingewiesen wurde.

Kontaktieren Sie uns

Wenn Sie Fragen zu diesem Haftungsausschluss haben, können Sie uns per E-Mail kontaktieren: support@vitextra.com.

Inhaltsverzeichnis

Überblick 4

Was angefordert wird und warum 4

Woher die Anforderungen kommen 7

Voraussetzungen 7

Anforderungen genehmigen 8

Nur einen Teil der Berechtigungen genehmigen 9

Was Benutzer sehen, wenn eine Berechtigung fehlt 9

Updates und neue Berechtigungen 10

Berechtigungen überprüfen und widerrufen 10

Sicherheitshinweise für Prüfer 11

Begriffe 12

Überblick

Mehrere Vitextra-Webparts lesen Daten, die außerhalb der SharePoint-Website liegen: Benutzerprofile und die Vorgesetztenhierarchie in **Microsoft Entra ID**, den Anwesenheitsstatus in **Microsoft Teams**, Kalender, Aufgaben in Planner und To Do, Dateien in OneDrive. Lösungen auf Basis des **SharePoint Framework (SPFx)** greifen über **Microsoft Graph** auf diese Daten zu, und ein Mandantenadministrator muss dies einmalig erlauben.

Der Mechanismus ist für jede SPFx-Lösung derselbe: Das Lösungspaket deklariert die benötigten Berechtigungen, **SharePoint** wandelt die Deklaration in *Berechtigungsanforderungen* um, sobald das Paket im **App-Katalog** bereitgestellt wird, und die Anforderungen warten auf der Seite **API-Zugriff** des SharePoint Admin Centers, bis ein Administrator sie genehmigt oder ablehnt.

Dieser Artikel erläutert, welche Vitextra-Produkte Berechtigungen anfordern und warum, wie Sie die Anforderungen genehmigen, wie Sie sie später überprüfen und widerrufen und was Sie in den Webparts sehen, wenn eine Berechtigung fehlt. Er richtet sich an SharePoint-Administratoren und Globale Administratoren, die Vitextra-Produkte installieren, sowie an Sicherheitsverantwortliche, die solche Anforderungen prüfen.

Hinweis

Der Artikel behandelt nur die API-Zugriffsanforderungen von SPFx-Lösungen. Die Installation des Pakets selbst ist in KB10035. So installieren Sie ein Vitextra-Produkt in SharePoint Online beschrieben.

Was angefordert wird und warum

Die unten aufgeführten Berechtigungen sind **delegiert**: Die Webparts rufen Microsoft Graph im Namen des angemeldeten Benutzers auf. Der effektive Zugriff hängt sowohl von den erteilten Bereichen als auch von den Berechtigungen des Benutzers ab. Daraus folgt nicht, dass Graph-Ergebnisse genau der Anzeige in Outlook oder Teams entsprechen. Microsoft Graph

Die Tabelle führt die Berechtigungen auf, die die aktuellen Versionen der Produkte deklarieren, die Microsoft Graph verwenden.

Produkt	API	Berechtigungen	Verwendet für
Employee Directory	Microsoft Graph	User.Read.All, Directory.Read.All, People.Read, Presence.Read.All, Calendars.Read	Lesen von Benutzerprofilen, Abteilungen und Vorgesetzten; relevante Personen; Teams-Anwesenheitsstatus; Frei/Gebucht-Status für die Verfügbarkeitsanzeige
Employee Details	Microsoft Graph	User.Read.All, User.ReadWrite, People.Read.All, Presence.Read.All, Files.Read.All, Sites.Read.All, Calendars.Read.Shared	Lesen von Profilen; Bearbeiten der eigenen Profilfelder durch den Benutzer; relevante Personen; Anwesenheitsstatus; Dokumente und Websites, mit denen die Person zuletzt gearbeitet hat (Microsoft Graph Insights); Frei/Gebucht-Status von Kollegen für Arbeitszeiten und Verfügbarkeit
Organizational Chart	Microsoft Graph	User.Read.All, Directory.Read.All, Presence.Read.All	Aufbau der Berichtshierarchie aus dem Attribut **Vorgesetzter** (Manager); Abteilung und Position; Teams-

Produkt	API	Berechtigungen	Verwendet für
			Anwesenheitsstatus
Absence & Coverage	Microsoft Graph	User.Read.All	Auflösen von Mitarbeitern, ihren Vorgesetzten und direkt unterstellten Mitarbeitern für Anträge, Genehmigungen und Vertretungen
My Tasks	Microsoft Graph	User.Read, User.ReadBasic.All, Tasks.ReadWrite	Aufgaben aus Planner, To Do und gekennzeichneten E-Mails; Namen der Aufgabenersteller
My Tasks	**Azure DevOps**	user_impersonation	Die Quelle **Azure DevOps** und das Webpart **Azure DevOps Query**
Password Vault	Microsoft Graph	Files.ReadWrite.AppFolder	Speichern des verschlüsselten Tresors im Anwendungsordner des OneDrive des Benutzers

Produkte, die nur mit der aktuellen **Website** arbeiten – Announcements Carousel, List Filter Online, QR Code Generator, Questions & Answers, Quick Poll, **RSS** Reader, Smart Search und Smart Tiles – fordern **keine** API-Berechtigungen an. Für sie erscheint nichts auf der Seite **API-Zugriff**.

Hinweis

Ein Berechtigungsname wie *Tasks.ReadWrite* oder *User.ReadWrite* ist der Name des Microsoft-Graph-Bereichs, der weiter gefasst sein kann als das, was das Produkt damit tut. My Tasks liest Aufgaben nur; Employee Details schreibt nur die Profilfelder des angemeldeten Benutzers. Die produktspezifischen Artikel erläutern jede Berechtigung im Detail: KB10235. Von Organizational Chart benötigte Microsoft-Graph-Berechtigungen, KB10303. My Tasks: Erforderliche Berechtigungen, Datenschutz und Sicherheit.

Woher die Anforderungen kommen

Eine Berechtigungsanforderung wird erstellt, wenn das `.sppkg`-Paket im Mandanten-App-Katalog bereitgestellt wird. Die Anforderungen gehören zum Paket, nicht zu den einzelnen Webparts. Eine Lösung mit zwei Webparts zeigt daher einen Satz Anforderungen, und eine Berechtigung, die nur ein optionales **Feature** benötigt (zum Beispiel die Azure-DevOps-Quelle von My Tasks), wird zusammen mit den übrigen angefordert.

Zwei Punkte sind für die Governance wichtig:

- **Die Genehmigung gilt mandantenweit.** SharePoint erteilt die Berechtigung einer einzigen Microsoft-Entra-ID-Anwendung, die es für alle SPFx-Lösungen verwendet – *Web Client Extensibility* (früher: *SharePoint Online Client Extensibility Web Application Principal*). Sobald *User.Read.All* für Employee Directory genehmigt wurde, nutzen Organizational Chart und jede andere SPFx-Lösung im Mandanten, die diese Berechtigung anfordert, dieselbe Erteilung. So funktioniert das SharePoint Framework; es ist keine Designentscheidung von Vitextra.
- **Die Bereitstellung hängt nicht von der Genehmigung ab.** Ein Vitextra-Produkt kann bereitgestellt, Websites hinzugefügt und auf Seiten platziert werden, während seine Anforderungen noch ausstehen oder sogar abgelehnt wurden. Nur die Features, die von der fehlenden Berechtigung abhängen, funktionieren nicht.

Voraussetzungen

- Das Vitextra-Paket ist in den Mandanten-App-Katalog hochgeladen und bereitgestellt (**App aktivieren**).
- Melden Sie sich zum Genehmigen von Microsoft-Graph- und anderen Microsoft-API-Berechtigungen als **Globaler Administrator** an. Für im Mandanten registrierte Drittanbieter-APIs genügt die Rolle **Anwendungsadministrator**. Die Rolle SharePoint-

Administrator allein berechtigt nicht zur Genehmigung von Microsoft-Graph-Berechtigungen. Microsoft

Warnung

Die Seite **API-Zugriff** zeigt die Anforderungen von Paketen, die im **Mandanten**-App-Katalog bereitgestellt sind. Wenn Sie Vitextra-Produkte lieber aus einem Websitesammlungs-App-Katalog bereitstellen, stellen Sie das Paket zuerst im Mandanten-App-Katalog bereit und genehmigen Sie die Anforderungen dort; die genehmigten Berechtigungen gelten mandantenweit und stehen dann auch der Kopie im Websitesammlungs-App-Katalog zur Verfügung.

Anforderungen genehmigen

1. Öffnen Sie das Microsoft 365 Admin Center und wechseln Sie zum **SharePoint Admin Center**.

2. Erweitern Sie in der linken Navigation **Erweitert** und wählen Sie **API-Zugriff**.

3. Suchen Sie auf der Registerkarte **Ausstehende Anforderungen** die Anforderungen des Vitextra-Pakets. Jede Zeile zeigt den Paketnamen (zum Beispiel *Vitextra Employee Directory*), die API (*Microsoft Graph* oder *Azure DevOps*) und die Berechtigung.

4. Wählen Sie eine Anforderung aus und klicken Sie auf **Genehmigen**. Lesen Sie die Beschreibung im Bereich und bestätigen Sie mit **Genehmigen**.

5. Wiederholen Sie dies für jede Anforderung des Pakets. Eine Berechtigung, die bereits für eine andere Lösung genehmigt wurde, erscheint nicht erneut: SharePoint verwendet die vorhandene Erteilung weiter.

6. Wechseln Sie zur Registerkarte **Genehmigte Anforderungen** und prüfen Sie, ob alle Berechtigungen des Pakets aufgeführt sind.

Benutzer sehen keine Zustimmungsaufforderung: Nach der Genehmigung funktionieren die Webparts für alle im Mandanten. Die Erteilung wird in der Regel innerhalb weniger Minuten wirksam; meldet ein Webpart weiterhin eine fehlende Berechtigung, laden Sie die Seite neu oder melden Sie sich ab und wieder an, um ein neues Token zu erhalten.

Tipp

Sie können die Anforderungen in einem Durchgang mit der SharePoint Online-Verwaltungsshell genehmigen: `Get-SPOTenantServicePrincipalPermissionRequests` listet die ausstehenden Anforderungen auf, und `Approve-SPOTenantServicePrincipalPermissionRequest -RequestId <id>` genehmigt eine davon. Das ist praktisch, wenn Sie mehrere Vitextra-Produkte gleichzeitig einführen.

Nur einen Teil der Berechtigungen genehmigen

Sie können einige Anforderungen genehmigen und andere ablehnen. Das Webpart funktioniert weiter, nur das abhängige Feature ist betroffen:

- *Presence.Read.All* abgelehnt – Employee Directory, Employee Details und Organizational Chart zeigen Personen ohne den Teams-Anwesenheitsindikator.
- *Calendars.Read* / *Calendars.Read.Shared* abgelehnt – die Informationen zu Verfügbarkeit und Arbeitszeiten werden nicht angezeigt.
- *Files.Read.All* / *Sites.Read.All* abgelehnt – Employee Details zeigt keine zuletzt verwendeten Dateien und Websites.
- *user_impersonation* (Azure DevOps) abgelehnt – die Azure-DevOps-Quelle von My Tasks und das Webpart Azure DevOps Query können sich nicht bei Azure DevOps anmelden.

Wird die Kernberechtigung eines Produkts abgelehnt (*User.Read.All* für die personenbezogenen Produkte, *Tasks.ReadWrite* für My Tasks, *Files.ReadWrite.AppFolder* für Password Vault), bleibt das Webpart ohne Daten.

Was Benutzer sehen, wenn eine Berechtigung fehlt

Symptom	Wahrscheinliche Ursache
Das Webpart zeigt einen Fehler zu verweigertem Zugriff, unzureichenden Berechtigungen oder fehlender Zustimmung	Die Kernberechtigung steht aus oder wurde abgelehnt
Mitarbeiter werden aufgelistet, aber der farbige Anwesenheitspunkt fehlt	*Presence.Read.All* ist nicht genehmigt

Symptom	Wahrscheinliche Ursache
Das Organigramm ist leer oder zeigt nur den aktuellen Benutzer	*User.Read.All* oder *Directory.Read.All* ist nicht genehmigt
My Tasks zeigt nichts für Planner, To Do und Outlook, während die SharePoint-Quelle funktioniert	*Tasks.ReadWrite* ist nicht genehmigt
Alles funktionierte, und nach einem Update fiel ein Feature aus	Die neue Version fordert eine zusätzliche Berechtigung an, die noch aussteht

Öffnen Sie die Seite **API-Zugriff** und vergleichen Sie die Registerkarten **Ausstehende Anforderungen** und **Genehmigte Anforderungen** mit der Tabelle am Anfang dieses Artikels.

Updates und neue Berechtigungen

Wenn Sie eine neue Version eines Pakets hochladen (siehe KB10050. So aktualisieren Sie eine Vitextra-SPFx-Lösung in SharePoint Online), bleiben die zuvor genehmigten Berechtigungen genehmigt. Deklariert die neue Version eine Berechtigung, die die vorherige nicht hatte, erscheint die neue Anforderung auf der Registerkarte **Ausstehende Anforderungen** und muss auf dieselbe Weise genehmigt werden. Vitextra führt solche Änderungen in den Versionshinweisen des Produkts auf.

Berechtigungen überprüfen und widerrufen

Da die Erteilungen von allen SPFx-Lösungen gemeinsam genutzt werden, widerruft das Entfernen eines Vitextra-Produkts die von ihm angeforderten Berechtigungen **nicht**. So widerrufen Sie eine Berechtigung:

1 Öffnen Sie **API-Zugriff** und wechseln Sie zur Registerkarte **Genehmigte Anforderungen**.
2 Wählen Sie die Berechtigung aus und klicken Sie auf **Zugriff entfernen** (Remove access).
3 Bestätigen Sie.

Warnung

Prüfen Sie vor dem Entfernen einer Berechtigung, ob eine andere Lösung im Mandanten davon abhängt – Ihre eigenen SPFx-Webparts, Produkte anderer Anbieter und die von Microsoft vorab autorisierten Berechtigungen erscheinen auf derselben Registerkarte. Das Entfernen einer Berechtigung, die eine andere Lösung verwendet, bringt diese Lösung sofort zum Ausfall.

Eine abgelehnte Anforderung wird von der Seite API-Zugriff entfernt und bleibt nicht unter **Ausstehende Anforderungen** stehen. Um die Berechtigung erneut anzufordern, muss der Entwickler eine neue Anforderung für dieselbe Ressource und denselben Bereich stellen. Microsoft

Sicherheitshinweise für Prüfer

- Jeder Aufruf von Microsoft Graph erfolgt aus dem Browser des angemeldeten Benutzers mit einem für diesen Benutzer ausgestellten Token. Vitextra-Webparts haben keine **Anwendungsberechtigungen** (App-only) und kein Dienstkonto.
- Microsoft Graph prüft die erteilten delegierten Bereiche und die Berechtigungen des Benutzers. Adressbuchsichtbarkeit und anwendungsspezifische Filter sind getrennte Mechanismen; ein in Outlook ausgeblendeter Benutzer ist nicht zwangsläufig in Graph-Abfragen ausgeblendet.
- Produktspezifische Datenflüsse, Lizenzanfragen, Telemetrie und Speicherung werden hier beschrieben: KB10363. Wo Vitextra-Produkte Ihre Daten speichern: Datenschutz, Datenresidenz und DSGVO.

Begriffe

Anwendungsberechtigungen
Anwendungsberechtigungen ermöglichen es einer Anwendung, ohne angemeldeten Benutzer ausgeführt zu werden, z. B. als Hintergrunddienst oder Daemon. Sie erfordern immer die Zustimmung eines Administrators, und die Anwendung hat Zugriff auf alle von der Berechtigung abgedeckten Daten.

App-Katalog
Der App-Katalog ist eine spezielle SharePoint-Website, in der Apps für SharePoint, Teams und andere Microsoft 365-Dienste gespeichert werden. Globale oder SharePoint-Administratoren können Anwendungen aus dem AppSource-Marktplatz, benutzerdefiniert entwickelte Apps oder Apps von Drittanbietern für die interne Verwendung in der Organisation hochladen und verwalten. In einem Mandanten kann es nur einen App-Katalog auf Mandantenebene geben; für einzelne Websitesammlungen können zusätzliche App-Kataloge für Websitesammlungen hinzugefügt werden.

Azure DevOps
Azure DevOps Services (früher Visual Studio Team Services) ist ein cloudbasiertes Produkt, das Versionskontrolle, Anforderungsverwaltung, automatisierte Pipelines für Builds und Releases sowie Testfunktionen bietet.

Feature
Ein Feature ist ein Satz von SharePoint-Elementen (Artefakten), z. B. Websitespalten, Inhaltstypen, Webparts, Anwendungsseiten, benutzerdefinierte Aktionen, Listenvorlagen, Listeninstanzen und weitere.

Microsoft Entra ID
Microsoft Entra ID (früher Azure Active Directory) ist ein cloudbasierter Identitäts- und Zugriffsverwaltungsdienst von Microsoft. Organisationen können damit die Identitäten ihrer Benutzer und deren Zugriff auf eine Vielzahl interner und externer Ressourcen effizient verwalten und schützen. Zu diesen Ressourcen gehören Microsoft 365, die Azure-Plattform und Tausende weitere SaaS-Anwendungen (Software as a Service).

Microsoft Graph
Microsoft Graph ist eine REST-API, die mit Microsoft Entra ID (früher Azure Active

Directory) und OAuth 2.0 gesichert ist. Sie stellt einen einzigen Endpunkt für den Zugriff auf Daten und Dienste in Microsoft 365 bereit, z. B. SharePoint, Outlook, OneDrive, Teams und weitere.

Microsoft Teams
Microsoft Teams ist eine chatbasierte Zusammenarbeitsplattform für die Unternehmenskommunikation mit Funktionen für Onlinebesprechungen, Liveereignisse und die gemeinsame Nutzung von Dokumenten.

RSS
RSS (Really Simple Syndication) ist ein weit verbreitetes Web-Feed-Format, das verwendet wird, um Updates von Websites in einem standardisierten, maschinenlesbaren Format an Benutzer und Anwendungen zu liefern. Dieses Format wird häufig zur Verteilung von Nachrichtenartikeln, Blogbeiträgen und anderen häufig aktualisierten Inhalten verwendet.

SharePoint
SharePoint ist eine webbasierte Zusammenarbeitsplattform, die Inhaltsverwaltung, Dokumentverwaltung, Workflowanwendungen, Suche und weitere Tools bietet, mit denen Mitarbeiter und Teams gemeinsam arbeiten können. SharePoint ist außerdem ein sicherer Ort zum Speichern, Organisieren und Abrufen freigegebener Informationen.

SharePoint Framework (SPFx)
SharePoint Framework (SPFx) ist ein Modell zum Erstellen clientseitiger Webparts, Komponenten und Erweiterungen für SharePoint Online, SharePoint Server (lokal) und Microsoft Teams. SPFx-Anpassungen basieren auf JavaScript und unterstützen die moderne Benutzeroberfläche nativ.

Website
Eine SharePoint-Website ist ein Container für Informationen innerhalb der SharePoint-Plattform. Websites bieten in der Regel Funktionen wie Dokumentbibliotheken, Listen, Kalender, Diskussionsforen und Workflows und erleichtern so die Zusammenarbeit, Kommunikation und Dokumentverwaltung innerhalb von Teams oder abteilungsübergreifend. Websites können angepasst und konfiguriert werden, um die spezifischen Anforderungen und Workflows einer Organisation zu erfüllen.

Begriffe