WISSENSDATENBANKARTIKEL

Von Employee Directory benötigte Microsoft-Graph-Berechtigungen

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

Einführung 4

Die Berechtigungen 4

Delegierte Berechtigungen, keine Anwendungsberechtigungen 6

Die Quelle „Benutzerprofile“ und die SharePoint-Suche 7

Was Benutzer sehen, wenn eine Berechtigung fehlt 7

Die Berechtigungen genehmigen 10

Den Status der Berechtigungen prüfen 10

Hinweise für Sicherheitsprüfungen 11

Ausdrücke 12

Einführung

Die Vitextra-Lösung Employee Directory führt keine eigene Mitarbeiterdatenbank. Personen, Profilattribute, Fotos, Vorgesetzte, die Teams-Anwesenheit und Frei/Gebucht-Informationen werden zur Laufzeit über die **Microsoft Graph API** aus Microsoft 365 gelesen. Dafür fordert das Lösungspaket fünf Microsoft-Graph-Berechtigungen an, die ein Mandantenadministrator einmalig genehmigt.

Dieser Artikel listet die Berechtigungen auf, erklärt, wofür jede verwendet wird und welches Webpart sie benötigt, beschreibt genau, was Benutzer sehen, wenn eine Berechtigung nicht genehmigt ist, und zeigt, wie Sie die Berechtigungen genehmigen und ihren Status prüfen. Er richtet sich an SharePoint- und Microsoft 365-Administratoren sowie an Sicherheitsprüfer, die das Produkt vor der Bereitstellung bewerten.

Die Berechtigungen

Das Paket **Vitextra Employee Directory** enthält drei Webparts – **Employee Directory**, **Employee Directory (Entra ID)** und **New Employees** – und fordert für alle zusammen einen gemeinsamen Satz von Berechtigungen an. Alle fünf sind delegierte Berechtigungen für Microsoft Graph:

Berechtigung	Verwendet für	Benötigt von	Wenn nicht genehmigt
`Directory.Read.All`	Lesen der Mitglieder von Microsoft Entra-Verzeichnisrollen für die Bedingung **Nutzerrollen** im Filter-Editor. Zusammen mit `User.Read.All` deckt sie auch das Lesen von Benutzerkonten ab	Employee Directory (Entra ID), New Employees – nur wenn der Filter eine Bedingung **Nutzerrollen** enthält	Die Bedingung verhält sich so, als hätte niemand die ausgewählten Rollen. Es wird kein Fehler angezeigt
`User.Read.All`	Lesen und Durchsuchen von Benutzerkonten und ihren	Alle drei Webparts; im Webpart **Employee Directory** mit der Quelle	Die Personenliste kann nicht geladen werden, und ein Fehler wird

Berechtigung	Verwendet für	Benötigt von	Wenn nicht genehmigt
	Profilattributen, der Vorgesetzte und die direkten Mitarbeiter einer Person, das eigene Team des angemeldeten Benutzers sowie Mitarbeiterfotos	**Benutzerprofile** nur der Detailbereich und die Schnellfilter	angezeigt (siehe **unten**)
`Presence.Read.All`	Die Microsoft Teams-Anwesenheitsanzeige auf Karten, die Spalte **Status** und die Meldung **Abwesend** im Detailbereich	Alle drei Webparts	Personen werden ohne Anwesenheit angezeigt; die Spalte **Status** zeigt **Offline**
`Calendars.Read`	Der heutige Frei/Gebucht-Zeitplan der Person und des angemeldeten Benutzers sowie die Zeitzone und die Arbeitszeiten der Person	Employee Directory, Employee Directory (Entra ID) – Detailbereich	Der Abschnitt **Ortszeit**, **Arbeitszeiten** und **Verfügbarkeit** wird nicht angezeigt
`People.Read`	Die Liste der Personen, mit denen der angemeldete Benutzer am häufigsten zusammenarbeitet	Employee Directory, Employee Directory (Entra ID) – Schnellfilter **Personen, mit denen ich zusammenarbeite**	Die Registerkarte **Personen, mit denen ich zusammenarbeite** wird nicht angezeigt

Hinweis

`Directory.Read.All` und `User.Read.All` überschneiden sich: Für das Lesen von Benutzerkonten akzeptiert Microsoft Graph jede der beiden. Der in der Zeile `User.Read.All` beschriebene Fehler tritt daher auf, wenn keine der beiden genehmigt ist – der normale Zustand direkt nach der Bereitstellung, solange alle fünf Anforderungen noch ausstehen. Genehmigen Sie beide, wie es das Paket anfordert.

Employee Directory **liest** Daten nur. Es erstellt, ändert oder löscht nichts in Microsoft Entra ID, Exchange Online, Teams oder SharePoint und fordert keine Berechtigung an, deren Name *Write* enthält.

Delegierte Berechtigungen, keine Anwendungsberechtigungen

Alle fünf Berechtigungen sind **delegiert**: Jeder Aufruf von Microsoft Graph erfolgt aus dem Browser des angemeldeten Benutzers mit einem Token, das für diesen Benutzer ausgestellt wurde. Die Webparts haben keine Anwendungsberechtigungen (App-only), kein Dienstkonto und kein eigenes Back-End, das Ihr Verzeichnis liest.

Für den Leser der Seite gilt daher eine einfache Regel: **Ein Benutzer sieht in Employee Directory nie mehr, als er in Microsoft 365 ohnehin sehen könnte.** Microsoft Graph wendet zusätzlich zum delegierten Bereich die eigenen Rechte des Benutzers an, sodass das Webpart Verzeichnis, Anwesenheit und Frei/Gebucht-Informationen lediglich übersichtlicher darstellt. Außerdem schließen die Webparts Gastkonten aus ihren Listen aus.

Hinweis

Die Berechtigungen werden nicht dem Employee Directory-Paket selbst erteilt. SharePoint erteilt sie einer einzigen Microsoft-Entra-ID-Anwendung, die es für alle SPFx-Lösungen im Mandanten verwendet – *SharePoint Online Web Client Extensibility* (früher: *SharePoint Online Client Extensibility Web Application Principal*). Wurde eine Berechtigung bereits für eine andere Lösung genehmigt, zum Beispiel für Vitextra Organizational Chart, wird dieselbe Erteilung wiederverwendet, und die Anforderung erscheint nicht erneut als ausstehend. Dieselbe Genehmigung gilt auch, wenn die Webparts in Microsoft Teams ausgeführt werden.

Die Quelle „Benutzerprofile“ und die SharePoint-Suche

Das Webpart **Employee Directory** kann Personen aus zwei Quellen lesen, die in seinen Einstellungen ausgewählt werden:

- **Entra ID (Azure AD)** – Liste, Suche und Seitenaufteilung laufen über Microsoft Graph und hängen von den oben genannten Berechtigungen ab.
- **Benutzerprofile** – Liste, Suche, Verfeinerungen und Sortierung stammen aus der **SharePoint-Suche** (den Personenergebnissen des SharePoint-Suchdiensts), nicht aus Microsoft Graph. Sie arbeiten mit den eigenen SharePoint-Suchrechten des Benutzers und der üblichen Sicherheitskürzung und benötigen keine der Microsoft-Graph-Berechtigungen. Auch der Abschnitt **Zuletzt verwendete Dokumente** im Detailbereich verwendet die SharePoint-Suche.

Auch mit der Quelle **Benutzerprofile** rufen einige Teile des Webparts weiterhin Microsoft Graph auf: Fotos, die Anwesenheit und die Meldung **Abwesend**, die Abschnitte **Manager** und **Untergeordnete** sowie der Abschnitt **Ortszeit**, **Arbeitszeiten** und **Verfügbarkeit** im Detailbereich und die Schnellfilter **Mein Team** und **Personen, mit denen ich zusammenarbeite**. Sie hängen von denselben Berechtigungen ab wie im Modus **Entra ID (Azure AD)**.

Die Webparts **Employee Directory (Entra ID)** und **New Employees** verwenden immer Microsoft Graph.

Tipp

Die Unterschiede zwischen den beiden Verzeichnis-Webparts und ihren Quellen beschreibt der Artikel KB10310. Employee Directory oder Employee Directory (Entra ID): Welches Webpart sollten Sie wählen?.

Was Benutzer sehen, wenn eine Berechtigung fehlt

Die Webparts sind so gestaltet, dass eine fehlende optionale Berechtigung nur die davon abhängige Funktion entfernt. Das genaue Verhalten der aktuellen Version:

Webpart / Modus	Fehlende Berechtigung	Was Benutzer sehen
Employee Directory (Entra ID)	`User.Read.All` (und `Directory.Read.All`)	Statt der Liste ein Fehlersymbol mit dem von Microsoft Graph zurückgegebenen Fehlertext; gibt es keinen

Webpart / Modus	Fehlende Berechtigung	Was Benutzer sehen
		Text, die Meldung *Leider ist ein Fehler aufgetreten. Aktualisieren Sie die Seite, und versuchen Sie es erneut.*
Employee Directory, Quelle **Entra ID (Azure AD)**	`User.Read.All` (und `Directory.Read.All`)	Derselbe Fehler statt der Suchergebnisse
Employee Directory, Quelle **Benutzerprofile**	`User.Read.All` (und `Directory.Read.All`)	Liste, Suche und Verfeinerungen funktionieren weiter. Im Detailbereich werden die Abschnitte **Manager** und **Untergeordnete** nicht angezeigt, und Fotos werden aus SharePoint statt aus Microsoft Graph geladen
New Employees	`User.Read.All` (und `Directory.Read.All`)	Ein Fehlersymbol mit *Leider ist ein Fehler aufgetreten. Aktualisieren Sie die Seite, und versuchen Sie es erneut.*, gefolgt von dem von Microsoft Graph zurückgegebenen Fehlertext
Employee Directory (Entra ID), New Employees	`Directory.Read.All`	Eine Bedingung **Nutzerrollen** mit **Enthält** trifft auf niemanden zu, eine mit **Enthält nicht** auf alle. Es wird kein Fehler angezeigt
Alle Webparts	`Presence.Read.All`	Karten zeigen keine Anwesenheitsanzeige, die Spalte **Status** zeigt für alle **Offline**, und der

Webpart / Modus	Fehlende Berechtigung	Was Benutzer sehen
		Detailbereich zeigt keine Meldung **Abwesend**
Employee Directory, Employee Directory (Entra ID)	`Calendars.Read`	Der Abschnitt **Ortszeit**, **Arbeitszeiten** und **Verfügbarkeit** im Detailbereich wird nicht angezeigt. Es wird kein Fehler angezeigt
Employee Directory, Employee Directory (Entra ID)	`People.Read`	Die Registerkarte **Personen, mit denen ich zusammenarbeite** ist in der Schnellfilterleiste ausgeblendet. Die übrigen Registerkarten funktionieren weiter

Warnung

Das Webpart **Employee Directory (Entra ID)** speichert eine Kopie der geladenen Liste im Browser und zeigt sie beim nächsten Besuch an. Wird eine Berechtigung entzogen, nachdem Benutzer das Webpart bereits geöffnet haben, zeigen deren Browser weiterhin die zwischengespeicherte Liste an, bis die Kopie älter als 24 Stunden ist oder der Benutzer auf **Aktualisieren** klickt; danach erscheint der Fehler. Wenn Sie eine Berechtigungsänderung testen, löschen Sie die Browserdaten der Website oder verwenden Sie ein privates Fenster.

Hinweis

Für Anwesenheit und Frei/Gebucht-Informationen reicht die Berechtigung allein nicht aus: Die Person muss Microsoft Teams verwenden, um einen Anwesenheitsstatus zu haben, und ein Exchange Online-Postfach besitzen, um einen Frei/Gebucht-Zeitplan zu haben. Einzelheiten zum Verfügbarkeitsabschnitt finden Sie in KB10317. Employee Directory: Ortszeit, Arbeitszeiten und Verfügbarkeit, zu den Schnellfiltern in KB10214. Schnellfilter im Employee Directory: Meine Abteilung, Mein Team, Personen, mit denen ich zusammenarbeite, Favoriten.

Die Berechtigungen genehmigen

Die Berechtigungsanforderungen werden automatisch erstellt, wenn das Employee Directory-Paket im Mandanten-App-Katalog bereitgestellt wird. Ein **SharePoint-Administrator** oder **Globaler Administrator** genehmigt sie:

1 Öffnen Sie das **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 Pakets **Vitextra Employee Directory** für **Microsoft Graph** – `Directory.Read.All`, `User.Read.All`, `Presence.Read.All`, `Calendars.Read` und `People.Read`.
4 Wählen Sie jede Anforderung aus, klicken Sie auf **Genehmigen** und bestätigen Sie.

Benutzer erhalten keine Zustimmungsaufforderung: Nach der Genehmigung funktionieren die Webparts für alle im Mandanten. Zeigt ein Webpart einige Minuten nach der Genehmigung noch einen Fehler an, laden Sie die Seite neu.

Tipp

Das vollständige Verfahren, einschließlich der Genehmigung mit PowerShell, der teilweisen Genehmigung und des Entziehens von Berechtigungen, beschreibt der Artikel KB10360. So genehmigen Sie Microsoft-Graph-API-Berechtigungen für Vitextra-Lösungen im SharePoint Admin Center.

Den Status der Berechtigungen prüfen

Um zu prüfen, welche Berechtigungen bestehen, öffnen Sie im SharePoint Admin Center **Erweitert** › **API-Zugriff**:

- Die Registerkarte **Genehmigte Anforderungen** muss alle fünf Microsoft-Graph-Berechtigungen auflisten. Da die Erteilungen mandantenweit gelten, kann eine Berechtigung dort unter einem anderen Paket aufgeführt sein, das sie zuerst angefordert hat – das genügt.
- Jede Berechtigung, die noch auf der Registerkarte **Ausstehende Anforderungen** steht, ist noch nicht wirksam; die davon abhängigen Funktionen verhalten sich wie unter **Was Benutzer sehen, wenn eine Berechtigung fehlt** beschrieben.

Wenn Sie Employee Directory aktualisieren, bleiben die zuvor genehmigten Berechtigungen genehmigt. Fordert eine neue Version eine zusätzliche Berechtigung an, erscheint sie auf der Registerkarte **Ausstehende Anforderungen** und muss auf dieselbe Weise genehmigt werden.

Hinweise für Sicherheitsprüfungen

Für eine Sicherheitsprüfung sind in der Regel folgende Punkte relevant:

- Alle fünf Berechtigungen sind delegiert und reine Leseberechtigungen. Employee Directory schreibt nie in Microsoft 365.
- Verzeichnisdaten, Fotos, Anwesenheit und Kalenderinformationen werden vom Browser des Benutzers direkt bei Microsoft Graph und SharePoint abgerufen und weder an Vitextra noch an Dritte gesendet.
- Die Quelle **Benutzerprofile** liest Personen über die SharePoint-Suche mit den eigenen Rechten des Benutzers und benötigt für die Liste selbst keine Microsoft-Graph-Berechtigung.
- Favoriten, die zwischengespeicherte Mitarbeiterliste und die Standardkonfiguration der persönlichen Teams-App werden außerhalb von Microsoft Graph gespeichert; wo genau und welche Daten die Webparts lesen, beschreibt der Artikel KB10469. Employee Directory: Welche Daten gelesen werden und wo Favoriten und Einstellungen gespeichert sind.
- Die einzigen Anfragen an Vitextra-Dienste sind die Lizenzprüfung und Nutzungstelemetrie mit technischen Kennungen; siehe KB10363. Wo Vitextra-Produkte Ihre Daten speichern: Datenschutz, Datenresidenz und DSGVO.

Tipp

Wie Sie die Lösung installieren, beschreibt KB10035. So installieren Sie ein Vitextra-Produkt in SharePoint Online. Wie Sie das Webpart einer Seite hinzufügen, beschreibt KB10309. So fügen Sie das Employee Directory Webpart hinzu und konfigurieren es.

Ausdrücke

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.