KNOWLEDGE BASE ARTICLE

Microsoft Graph Permissions Required by Employee Directory

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

The permissions 4

Delegated, not application permissions 6

The User Profiles source and SharePoint search 6

What users see when a permission is missing 7

Approving the permissions 9

Checking the status of the permissions 9

Notes for security reviews 10

Terms 11

Introduction

The Vitextra Employee Directory solution does not keep an employee database of its own. People, profile attributes, photos, managers, Teams presence and free/busy information are read at run time from Microsoft 365 through the **Microsoft Graph API**. For that, the solution package requests five Microsoft Graph permissions, which a tenant administrator approves once.

This article lists the permissions, explains what each of them is used for and which web part needs it, describes exactly what users see when a permission is not approved, and shows how to approve the permissions and check their status. It is intended for SharePoint and Microsoft 365 administrators and for security reviewers who assess the product before deployment.

The permissions

The **Vitextra Employee Directory** package contains three web parts — **Employee Directory**, **Employee Directory (Entra ID)** and **New Employees** — and requests one set of permissions for all of them. All five are delegated permissions for Microsoft Graph:

Permission	Used for	Needed by	If not approved
`Directory.Read.All`	Reading the members of Microsoft Entra directory roles for the **User Roles** condition of the filter editor. It also covers reading user accounts, together with `User.Read.All`	Employee Directory (Entra ID), New Employees — only when the filter uses a **User Roles** condition	The condition behaves as if nobody held the selected roles. No error is shown
`User.Read.All`	Reading and searching user accounts and their profile attributes, the manager and direct reports of a person, the signed-in user's own team,	All three web parts; in the **Employee Directory** web part with the **User profiles** source — only the details pane and the quick filters	The list of people cannot be loaded and an error is shown (see **below**)

Permission	Used for	Needed by	If not approved
	and employee photos		
`Presence.Read.All`	The Microsoft Teams presence indicator on cards, the **Status** column and the **Out of Office** message in the details pane	All three web parts	People are shown without presence; the **Status** column shows **Offline**
`Calendars.Read`	Today's free/busy schedule of the person and of the signed-in user, together with the person's time zone and working hours	Employee Directory, Employee Directory (Entra ID) — details pane	The **Local time**, **Working hours** and **Availability** section is not shown
`People.Read`	The list of people the signed-in user works with most	Employee Directory, Employee Directory (Entra ID) — **People I work with** quick filter	The **People I work with** tab is not shown

Note

`Directory.Read.All` and `User.Read.All` overlap: Microsoft Graph accepts either of them for reading user accounts. The error described in the `User.Read.All` row therefore appears when neither of them is approved — which is the normal state right after deployment, when all five requests are still pending. Approve both, as the package requests.

Employee Directory only **reads** data. It does not create, change or delete anything in Microsoft Entra ID, Exchange Online, Teams or SharePoint, and it requests no permission with *Write* in its name.

Delegated, not application permissions

All five permissions are **delegated**: every call to Microsoft Graph is made from the browser of the signed-in user, with a token issued for that user. The web parts have no application (app-only) permissions, no service account and no back-end of their own that reads your directory.

For the reader of the page this means one simple rule: **a user never sees more in Employee Directory than this user could see in Microsoft 365 anyway**. Microsoft Graph applies the user's own rights on top of the delegated scope, so the web part only presents the directory, presence and free/busy information in a more convenient form. In addition, the web parts exclude guest accounts from their lists.

Note

The permissions are not granted to the Employee Directory package itself. SharePoint grants them to a single Microsoft Entra ID application that it uses for all SPFx solutions in the tenant — *SharePoint Online Web Client Extensibility* (earlier: *SharePoint Online Client Extensibility Web Application Principal*). If a permission has already been approved for another solution, for example the Vitextra Organizational Chart, the same grant is reused and the request does not appear as pending again. The same approval also covers the web parts when they run in Microsoft Teams.

The User Profiles source and SharePoint search

The **Employee Directory** web part can read people from two sources, selected in its settings:

- **Entra ID (Azure AD)** — the list, search and paging go through Microsoft Graph and depend on the permissions above.
- **User profiles** — the list, search, refiners and sorting come from **SharePoint search** (the People results of the SharePoint search service), not from Microsoft Graph. They work under the user's own SharePoint search rights with the usual security trimming and need none of the Microsoft Graph permissions. The **Recent Documents** section of the details pane also uses SharePoint search.

Even with the **User profiles** source, some parts of the web part still call Microsoft Graph: photos, presence and the **Out of Office** message, the **Manager** and **Direct Reports** sections and the **Local time**, **Working hours** and **Availability** section in the details pane, as well as the **My team** and **People I work with** quick filters. They depend on the same permissions as in the **Entra ID (Azure AD)** mode.

The **Employee Directory (Entra ID)** and **New Employees** web parts always use Microsoft Graph.

Tip

For the differences between the two directory web parts and their sources, see KB10310. Employee Directory vs. Employee Directory (Entra ID): Which Web Part to Choose.

What users see when a permission is missing

The web parts are designed so that a missing optional permission removes only the dependent feature. The exact behavior, as implemented in the current version:

Web part / mode	Missing permission	What users see
Employee Directory (Entra ID)	`User.Read.All` (and `Directory.Read.All`)	Instead of the list, an error icon with the error text returned by Microsoft Graph; if there is no text, the message *Sorry, something went wrong. Please refresh the page and try again.*
Employee Directory, **Entra ID (Azure AD)** source	`User.Read.All` (and `Directory.Read.All`)	The same error instead of the search results
Employee Directory, **User profiles** source	`User.Read.All` (and `Directory.Read.All`)	The list, search and refiners keep working. In the details pane, the **Manager** and **Direct Reports** sections are not shown, and photos are taken from SharePoint instead of Microsoft Graph
New Employees	`User.Read.All` (and `Directory.Read.All`)	An error icon with *Sorry, something went wrong. Please refresh the page and try again.* followed by the

Web part / mode	Missing permission	What users see
		error text returned by Microsoft Graph
Employee Directory (Entra ID), New Employees	`Directory.Read.All`	A **User Roles** condition with **Contains** matches nobody, and one with **Does not contain** matches everyone. No error is shown
All web parts	`Presence.Read.All`	Cards show no presence indicator, the **Status** column shows **Offline** for everybody, and the details pane shows no **Out of Office** message
Employee Directory, Employee Directory (Entra ID)	`Calendars.Read`	The **Local time**, **Working hours** and **Availability** section of the details pane is not shown. No error is shown
Employee Directory, Employee Directory (Entra ID)	`People.Read`	The **People I work with** tab is hidden from the quick-filter bar. The other tabs keep working

Warning

The **Employee Directory (Entra ID)** web part keeps a copy of the loaded list in the browser and shows it on the next visit. If a permission is revoked after users have opened the web part, their browsers keep showing the cached list until the copy is older than 24 hours or the user clicks **Refresh**; then the error appears. When you test a permission change, clear the browser data of the site or use a private window.

Note

Presence and free/busy information need more than the permission: the person must use Microsoft Teams to have a presence status, and must have an Exchange Online mailbox to have a free/busy schedule. For details on the availability section, see KB10317. Employee Directory: Local Time, Working Hours and Availability; for the quick filters, see KB10214. Employee Directory Quick Filters: My Department, My Team, People I Work With, Favorites.

Approving the permissions

The permission requests are created automatically when the Employee Directory package is deployed to the tenant App Catalog. A **SharePoint Administrator** or **Global Administrator** approves them:

1 Open the **SharePoint admin center**.
2 In the left navigation, expand **Advanced** and select **API access**.
3 On the **Pending requests** tab, find the requests of the **Vitextra Employee Directory** package for **Microsoft Graph** — `Directory.Read.All`, `User.Read.All`, `Presence.Read.All`, `Calendars.Read` and `People.Read`.
4 Select each request, click **Approve** and confirm.

Users get no consent prompt: after the approval the web parts work for everybody in the tenant. If a web part still shows an error a few minutes after the approval, reload the page.

Tip

The full procedure, including approving with PowerShell, partial approval and revoking permissions, is described in KB10360. How to Approve Microsoft Graph API Permissions for Vitextra Solutions in the SharePoint Admin Center.

Checking the status of the permissions

To check which permissions are in place, open **Advanced** › **API access** in the SharePoint admin center:

- The **Approved requests** tab must list all five Microsoft Graph permissions. Because the grants are tenant-wide, a permission may be listed there under another package that requested it first — that is enough.
- Any permission still listed on the **Pending requests** tab is not yet in effect; the

features that depend on it behave as described in **What users see when a permission is missing**.

When you update Employee Directory, the permissions approved earlier stay approved. If a new version requests an additional permission, it appears on the **Pending requests** tab and must be approved in the same way.

Notes for security reviews

For a security review, these points are usually relevant:

- All five permissions are delegated and read-only. Employee Directory never writes to Microsoft 365.
- Directory data, photos, presence and calendar information are requested by the user's browser directly from Microsoft Graph and SharePoint and are not sent to Vitextra or to any third party.
- The **User profiles** source reads people through SharePoint search under the user's own rights and needs no Microsoft Graph permission for the list itself.
- Favorites, the cached employee list and the default configuration of the Teams personal app are stored outside Microsoft Graph; where exactly, and what data the web parts read, is described in KB10469. Employee Directory: What Data It Reads and Where Favorites and Settings Are Stored.
- The only requests to Vitextra services are the license check and usage telemetry with technical identifiers; see KB10363. Where Vitextra Products Store Your Data: Privacy, Data Residency and GDPR.

Tip

To install the solution, see KB10035. How to Install a Vitextra Product in SharePoint Online. To add the web part to a page, see KB10309. How to Add and Configure the Employee Directory Web Part.

Terms

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.