ARTICLE DE LA BASE DE CONNAISSANCES

Autorisations Microsoft Graph requises par Employee Directory

2026 © Vitextra SIA. Tous droits réservés.

Clause d'exclusion de responsabilité

Aux fins du présent Avis de non-responsabilité :

- La **Société** (désignée par « la Société », « Nous » ou « Notre » dans le présent Avis de non-responsabilité) désigne Vitextra SIA, Matīsa iela 61-25, Rīga, LV-1009, Latvia.
- Le **Document** désigne l'article de la base de connaissances.
- **Vous** désigne la personne physique qui accède au Document, ou la société ou autre entité juridique pour le compte de laquelle cette personne accède au Document ou l'utilise, selon le cas.
- Le **Site web** désigne Vitextra, accessible à l'adresse https://vitextra.com

Avis de non-responsabilité

Les informations contenues dans le Document sont fournies à titre purement informatif et général.

La Société décline toute responsabilité quant aux erreurs ou omissions dans le contenu du Document.

En aucun cas la Société ne pourra être tenue responsable de dommages spéciaux, directs, indirects, consécutifs ou accessoires, ni de quelque dommage que ce soit, que ce soit dans le cadre d'une action contractuelle, d'une action en négligence ou d'une autre action délictuelle, résultant de l'utilisation du contenu du Document ou en lien avec celle-ci. La Société se réserve le droit d'ajouter, de supprimer ou de modifier le contenu du Document à tout moment et sans préavis.

Avis de non-responsabilité relatif aux erreurs et omissions

Les informations fournies dans le Document sont destinées uniquement à une orientation générale sur des sujets d'intérêt. Par conséquent, des erreurs peuvent survenir, même si la Société prend toutes les précautions pour que le contenu du Document soit à jour et exact. En outre, compte tenu de l'évolution des lois, règles et réglementations, les informations contenues dans le Document peuvent comporter des retards, des omissions ou des inexactitudes.

La Société n'est responsable ni des erreurs ou omissions, ni des résultats obtenus par l'utilisation de ces informations.

Avis de non-responsabilité relatif à l'usage équitable

La Société peut utiliser des contenus protégés par le droit d'auteur que le titulaire des droits n'a pas expressément autorisés. La Société met ces contenus à disposition à des fins de critique, de commentaire, de reportage d'actualité, d'enseignement, d'étude ou de recherche.

La Société estime que cela constitue un « usage équitable » (« fair use ») de ces contenus protégés par le droit d'auteur, au sens de la Section 107 de la loi américaine sur le droit d'auteur (United States Copyright Act).

Si Vous souhaitez utiliser des contenus protégés par le droit d'auteur issus du Document pour Vos propres besoins, au-delà de l'usage équitable, Vous devez obtenir l'autorisation du titulaire des droits d'auteur.

Avis de non-responsabilité « Utilisation à Vos propres risques »

Toutes les informations du Document sont fournies « en l'état », sans garantie d'exhaustivité, d'exactitude, d'actualité ni des résultats obtenus par l'utilisation de ces informations, et sans garantie d'aucune sorte, expresse ou implicite, y compris, mais sans s'y limiter, les garanties de performance, de qualité marchande et d'adéquation à un usage particulier.

La Société ne sera responsable ni envers Vous ni envers quiconque de toute décision prise ou de toute action entreprise sur la base des informations fournies dans le Document, ni de tout dommage consécutif, spécial ou similaire, même si elle a été informée de la possibilité de tels dommages.

Nous contacter

Si Vous avez des questions concernant le présent Avis de non-responsabilité, Vous pouvez Nous contacter par e-mail : support@vitextra.com.

Table des matières

Introduction 4

Les autorisations 4

Des autorisations déléguées, pas des autorisations d'application 6

La source Profils utilisateur et la recherche SharePoint 7

Ce que voient les utilisateurs lorsqu'une autorisation manque 7

Approuver les autorisations 10

Vérifier l'état des autorisations 10

Remarques pour les revues de sécurité 11

Conditions 12

Introduction

La solution Vitextra Employee Directory ne gère pas de base de données d'employés qui lui soit propre. Les personnes, les attributs de profil, les photos, les responsables, la présence Teams et les informations de disponibilité sont lus dans Microsoft 365 au moment de l'exécution, par l'intermédiaire de l'**API Microsoft Graph**. Pour cela, le package de la solution demande cinq autorisations Microsoft Graph, qu'un administrateur du locataire approuve une seule fois.

Cet article répertorie ces autorisations, explique à quoi sert chacune d'elles et quel composant WebPart en a besoin, décrit précisément ce que voient les utilisateurs lorsqu'une autorisation n'est pas approuvée, et montre comment approuver les autorisations et vérifier leur état. Il s'adresse aux administrateurs SharePoint et Microsoft 365 ainsi qu'aux responsables de la sécurité qui évaluent le produit avant son déploiement.

Les autorisations

Le package **Vitextra Employee Directory** contient trois composants WebPart — **Employee Directory**, **Employee Directory (Entra ID)** et **New Employees** — et demande un seul ensemble d'autorisations commun aux trois. Les cinq sont des autorisations déléguées pour Microsoft Graph :

Autorisation	Utilisée pour	Requise par	Si elle n'est pas approuvée
`Directory.Read.All`	Lire les membres des rôles d'annuaire Microsoft Entra pour la condition **Rôles des utilisateurs** de l'éditeur de filtres. Avec `User.Read.All`, elle permet également de lire les comptes d'utilisateurs	Employee Directory (Entra ID), New Employees — uniquement lorsque le filtre utilise une condition **Rôles des utilisateurs**	La condition se comporte comme si personne ne détenait les rôles sélectionnés. Aucune erreur n'est affichée
`User.Read.All`	Lire et rechercher	Les trois	La liste des

Autorisation	Utilisée pour	Requise par	Si elle n'est pas approuvée
	les comptes d'utilisateurs et leurs attributs de profil, le responsable et les subordonnés directs d'une personne, l'équipe de l'utilisateur connecté, ainsi que les photos des employés	composants WebPart ; dans le composant WebPart **Employee Directory** avec la source **Profils utilisateur**, uniquement le volet de détails et les filtres rapides	personnes ne peut pas être chargée et une erreur s'affiche (voir **ci-dessous**)
`Presence.Read.All`	L'indicateur de présence Microsoft Teams sur les cartes, la colonne **État** et le message **Absent du bureau** dans le volet de détails	Les trois composants WebPart	Les personnes s'affichent sans présence ; la colonne **État** indique **Hors connexion**
`Calendars.Read`	Le planning de disponibilité du jour de la personne et de l'utilisateur connecté, avec le fuseau horaire et les heures de travail de la personne	Employee Directory, Employee Directory (Entra ID) — volet de détails	La section **Heure locale**, **Heures de travail** et **Disponibilité** n'est pas affichée
`People.Read`	La liste des personnes avec lesquelles l'utilisateur connecté travaille le plus	Employee Directory, Employee Directory (Entra ID) — filtre rapide **Personnes avec qui je travaille**	L'onglet **Personnes avec qui je travaille** n'est pas affiché

Remarque

`Directory.Read.All` et `User.Read.All` se recoupent : pour lire les comptes d'utilisateurs, Microsoft Graph accepte l'une ou l'autre. L'erreur décrite dans la ligne `User.Read.All` apparaît donc lorsqu'aucune des deux n'est approuvée — ce qui est l'état normal juste après le déploiement, tant que les cinq demandes sont encore en attente. Approuvez les deux, comme le demande le package.

Employee Directory se contente de **lire** les données. Il ne crée, ne modifie et ne supprime rien dans Microsoft Entra ID, Exchange Online, Teams ou SharePoint, et ne demande aucune autorisation dont le nom contient *Write*.

Des autorisations déléguées, pas des autorisations d'application

Les cinq autorisations sont **déléguées** : chaque appel à Microsoft Graph est effectué depuis le navigateur de l'utilisateur connecté, avec un jeton émis pour cet utilisateur. Les composants WebPart n'ont aucune autorisation d'application (app-only), aucun compte de service et aucun back-end propre qui lirait votre annuaire.

Pour le lecteur de la page, cela se traduit par une règle simple : **un utilisateur ne voit jamais dans Employee Directory plus que ce qu'il pourrait voir de toute façon dans Microsoft 365**. Microsoft Graph applique les droits propres de l'utilisateur en plus de l'étendue déléguée ; le composant WebPart ne fait donc que présenter l'annuaire, la présence et les informations de disponibilité sous une forme plus pratique. En outre, les composants WebPart excluent les comptes invités de leurs listes.

Remarque

Les autorisations ne sont pas accordées au package Employee Directory lui-même. SharePoint les accorde à une seule application Microsoft Entra ID qu'il utilise pour toutes les solutions SPFx du locataire — *SharePoint Online Web Client Extensibility* (anciennement *SharePoint Online Client Extensibility Web Application Principal*). Si une autorisation a déjà été approuvée pour une autre solution, par exemple Vitextra Organizational Chart, la même autorisation est réutilisée et la demande n'apparaît plus comme en attente. La même approbation s'applique également lorsque les composants WebPart s'exécutent dans Microsoft Teams.

La source Profils utilisateur et la recherche SharePoint

Le composant WebPart **Employee Directory** peut lire les personnes à partir de deux sources, sélectionnées dans ses paramètres :

- **Entra ID (Azure AD)** — la liste, la recherche et la pagination passent par Microsoft Graph et dépendent des autorisations ci-dessus.
- **Profils utilisateur** — la liste, la recherche, les affinements et le tri proviennent de la **recherche SharePoint** (les résultats de personnes du service de recherche SharePoint), et non de Microsoft Graph. Ils fonctionnent avec les droits de recherche SharePoint de l'utilisateur, avec le filtrage de sécurité habituel, et ne nécessitent aucune des autorisations Microsoft Graph. La section **Documents récents** du volet de détails utilise elle aussi la recherche SharePoint.

Même avec la source **Profils utilisateur**, certaines parties du composant WebPart appellent toujours Microsoft Graph : les photos, la présence et le message **Absent du bureau**, les sections **Responsable** et **Subordonnés**, la section **Heure locale**, **Heures de travail** et **Disponibilité** du volet de détails, ainsi que les filtres rapides **Mon équipe** et **Personnes avec qui je travaille**. Elles dépendent des mêmes autorisations qu'en mode **Entra ID (Azure AD)**.

Les composants WebPart **Employee Directory (Entra ID)** et **New Employees** utilisent toujours Microsoft Graph.

Conseil

Pour les différences entre les deux composants WebPart d'annuaire et leurs sources, consultez l'article KB10310. Employee Directory ou Employee Directory (Entra ID) : quel composant WebPart choisir.

Ce que voient les utilisateurs lorsqu'une autorisation manque

Les composants WebPart sont conçus de sorte qu'une autorisation facultative manquante ne supprime que la fonctionnalité qui en dépend. Le comportement exact de la version actuelle :

Composant WebPart / mode	Autorisation manquante	Ce que voient les utilisateurs
Employee Directory (Entra ID)	`User.Read.All` (et `Directory.Read.All`)	À la place de la liste, une icône d'erreur avec le

Composant WebPart / mode	Autorisation manquante	Ce que voient les utilisateurs
		texte d'erreur renvoyé par Microsoft Graph ; en l'absence de texte, le message *Désolé, nous avons rencontré un problème. Veuillez actualiser la page, puis réessayer.*
Employee Directory, source **Entra ID (Azure AD)**	`User.Read.All` (et `Directory.Read.All`)	La même erreur à la place des résultats de recherche
Employee Directory, source **Profils utilisateur**	`User.Read.All` (et `Directory.Read.All`)	La liste, la recherche et les affinements continuent de fonctionner. Dans le volet de détails, les sections **Responsable** et **Subordonnés** ne sont pas affichées, et les photos proviennent de SharePoint au lieu de Microsoft Graph
New Employees	`User.Read.All` (et `Directory.Read.All`)	Une icône d'erreur avec *Désolé, nous avons rencontré un problème. Veuillez actualiser la page, puis réessayer.*, suivie du texte d'erreur renvoyé par Microsoft Graph
Employee Directory (Entra ID), New Employees	`Directory.Read.All`	Une condition **Rôles des utilisateurs** avec **Contient** ne correspond à personne, et une condition avec **Ne contient pas** correspond à tout le monde. Aucune erreur n'est affichée
Tous les composants	`Presence.Read.All`	Les cartes n'affichent

Composant WebPart / mode	Autorisation manquante	Ce que voient les utilisateurs
WebPart		aucun indicateur de présence, la colonne **État** indique **Hors connexion** pour tout le monde, et le volet de détails n'affiche aucun message **Absent du bureau**
Employee Directory, Employee Directory (Entra ID)	`Calendars.Read`	La section **Heure locale**, **Heures de travail** et **Disponibilité** du volet de détails n'est pas affichée. Aucune erreur n'est affichée
Employee Directory, Employee Directory (Entra ID)	`People.Read`	L'onglet **Personnes avec qui je travaille** est masqué dans la barre des filtres rapides. Les autres onglets continuent de fonctionner

Avertissement

Le composant WebPart **Employee Directory (Entra ID)** conserve une copie de la liste chargée dans le navigateur et l'affiche lors de la visite suivante. Si une autorisation est révoquée alors que des utilisateurs ont déjà ouvert le composant WebPart, leurs navigateurs continuent d'afficher la liste mise en cache jusqu'à ce que la copie ait plus de 24 heures ou que l'utilisateur clique sur **Actualiser** ; l'erreur apparaît alors. Lorsque vous testez une modification d'autorisation, effacez les données du site dans le navigateur ou utilisez une fenêtre de navigation privée.

Remarque

Pour la présence et les informations de disponibilité, l'autorisation ne suffit pas : la personne doit utiliser Microsoft Teams pour avoir un statut de présence et disposer d'une boîte aux lettres Exchange Online pour avoir un planning de disponibilité. Pour plus de détails sur la section de disponibilité, consultez l'article KB10317. Employee Directory : heure locale, heures de travail et disponibilité ; pour les filtres rapides, consultez l'article KB10214. Filtres rapides d'Employee Directory : Mon service, Mon équipe, Personnes avec qui je travaille, Favoris.

Approuver les autorisations

Les demandes d'autorisation sont créées automatiquement lorsque le package Employee Directory est déployé dans le catalogue d'applications du locataire. Un **Administrateur SharePoint** ou un **Administrateur général** les approuve :

1 Ouvrez le **Centre d'administration SharePoint**.
2 Dans le volet de navigation de gauche, développez **Avancé** et sélectionnez **Accès aux API**.
3 Dans l'onglet **Demandes en attente**, recherchez les demandes du package **Vitextra Employee Directory** pour **Microsoft Graph** — `Directory.Read.All`, `User.Read.All`, `Presence.Read.All`, `Calendars.Read` et `People.Read`.
4 Sélectionnez chaque demande, cliquez sur **Approuver** et confirmez.

Les utilisateurs ne voient aucune demande de consentement : après l'approbation, les composants WebPart fonctionnent pour tout le monde dans le locataire. Si un composant WebPart affiche encore une erreur quelques minutes après l'approbation, actualisez la page.

Conseil

La procédure complète, y compris l'approbation avec PowerShell, l'approbation partielle et la révocation des autorisations, est décrite dans l'article KB10360. Comment approuver les autorisations d'API Microsoft Graph pour les solutions Vitextra dans le Centre d'administration SharePoint.

Vérifier l'état des autorisations

Pour vérifier quelles autorisations sont en place, ouvrez **Avancé** › **Accès aux API** dans le Centre d'administration SharePoint :

- L'onglet **Demandes approuvées** doit répertorier les cinq autorisations Microsoft Graph. Comme les autorisations s'appliquent à l'ensemble du locataire, une autorisation peut y figurer sous un autre package qui l'a demandée en premier — cela suffit.
- Toute autorisation encore répertoriée dans l'onglet **Demandes en attente** n'est pas encore en vigueur ; les fonctionnalités qui en dépendent se comportent comme décrit dans **Ce que voient les utilisateurs lorsqu'une autorisation manque**.

Lorsque vous mettez à jour Employee Directory, les autorisations approuvées précédemment restent approuvées. Si une nouvelle version demande une autorisation supplémentaire, celle-ci apparaît dans l'onglet **Demandes en attente** et doit être approuvée de la même manière.

Remarques pour les revues de sécurité

Pour une revue de sécurité, les points suivants sont généralement pertinents :

- Les cinq autorisations sont déléguées et en lecture seule. Employee Directory n'écrit jamais dans Microsoft 365.
- Les données d'annuaire, les photos, la présence et les informations de calendrier sont demandées par le navigateur de l'utilisateur directement à Microsoft Graph et à SharePoint, et ne sont envoyées ni à Vitextra ni à aucun tiers.
- La source **Profils utilisateur** lit les personnes au moyen de la recherche SharePoint avec les droits de l'utilisateur et n'a besoin d'aucune autorisation Microsoft Graph pour la liste elle-même.
- Les favoris, la liste d'employés mise en cache et la configuration par défaut de l'application personnelle Teams sont stockés en dehors de Microsoft Graph ; l'emplacement exact et les données lues par les composants WebPart sont décrits dans l'article KB10469. Employee Directory : quelles données sont lues et où sont stockés les favoris et les paramètres.
- Les seules requêtes adressées aux services Vitextra sont la vérification de la licence et la télémétrie d'utilisation, avec des identifiants techniques ; voir l'article KB10363. Où les produits Vitextra stockent vos données : confidentialité, résidence des données et RGPD.

Conseil

Pour installer la solution, consultez l'article KB10035. Comment installer un produit Vitextra dans SharePoint Online. Pour ajouter le composant WebPart à une page, consultez l'article KB10309. Comment ajouter et configurer le composant WebPart Employee Directory.

Conditions

Microsoft Graph
Microsoft Graph est une API REST sécurisée par Microsoft Entra ID (anciennement Azure Active Directory) et OAuth 2.0. Elle fournit un point de terminaison unique pour accéder aux données et aux services de Microsoft 365, tels que SharePoint, Outlook, OneDrive, Teams, etc.