ARTICLE DE LA BASE DE CONNAISSANCES

Autorisations Microsoft Graph requises par Organizational Chart

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

Approuver les autorisations 5

Que se passe-t-il lorsqu'une autorisation manque 6

Qui peut voir l'organigramme 7

Traitement des données 7

Conditions 9

Introduction

Le composant WebPart Organizational Chart de Vitextra ne stocke aucune donnée d'employé qui lui soit propre. Tout ce qu'il affiche — noms, intitulés de poste, liens hiérarchiques, photos et présence — est lu en temps réel dans **Microsoft Entra ID** via l'**API Microsoft Graph**. Pour que cela fonctionne, le composant WebPart a besoin d'un petit ensemble d'autorisations d'API qu'un administrateur du locataire approuve une seule fois.

Cet article énumère ces autorisations, explique à quoi sert chacune d'elles, montre comment les approuver et décrit l'aspect de l'organigramme lorsqu'une autorisation manque. Il s'adresse aux administrateurs SharePoint et Microsoft 365, ainsi qu'aux responsables de la sécurité qui doivent évaluer le produit avant son déploiement.

Les autorisations

Organizational Chart demande trois autorisations déléguées pour Microsoft Graph :

Autorisation	Utilisation	En cas d'absence
`Directory.Read.All`	Lecture de la liste des utilisateurs et de la relation de **responsable** (manager) de chaque compte — les données à partir desquelles la hiérarchie est construite	L'organigramme ne peut charger aucun employé et affiche une erreur
`User.Read.All`	Lecture des attributs de profil affichés sur les cartes (intitulé de poste, service, localisation du bureau, numéros de téléphone, adresse, etc.) et des photos des employés	L'organigramme ne peut pas charger les profils des employés et affiche une erreur
`Presence.Read.All`	Affichage de l'indicateur de présence Microsoft Teams en direct (Disponible, Occupé, Absent, Ne pas déranger, Hors ligne) sur chaque carte	L'organigramme fonctionne, mais aucun indicateur de présence n'est affiché

Les trois sont des autorisations **déléguées** : le composant WebPart appelle toujours Microsoft Graph au nom de l'utilisateur connecté, jamais avec une identité d'application qui lui serait propre. L'organigramme ne montre donc à un visiteur rien

que celui-ci ne pourrait voir en parcourant lui-même l'annuaire dans Microsoft 365 — il se contente de le présenter sous une forme plus pratique.

Remarque

Les autorisations sont demandées au niveau du principal d'application SharePoint Online Client Extensibility, que partagent toutes les solutions SPFx du locataire. Si un autre produit Vitextra — par exemple Employee Directory — a déjà été approuvé pour la même étendue, la demande d'Organizational Chart est accordée automatiquement et n'apparaît pas comme en attente.

Approuver les autorisations

Les demandes d'autorisation sont enregistrées automatiquement lors du déploiement du package Organizational Chart dans le catalogue d'applications (App Catalog) du locataire. Pour les approuver :

1 Connectez-vous au **centre d'administration SharePoint** (SharePoint admin center) avec un compte disposant du rôle **Global Administrator** ou **SharePoint Administrator**.
2 Dans la navigation de gauche, développez **Advanced** et sélectionnez **API access**.
3 Sous **Pending requests**, repérez les demandes du package **Organizational Chart** pour la ressource **Microsoft Graph** — `Directory.Read.All`, `User.Read.All` et `Presence.Read.All`.
4 Sélectionnez chaque demande et cliquez sur **Approve**. Confirmez l'approbation dans le volet qui s'ouvre.

Les autorisations approuvées passent dans la liste **Approved requests**, où elles peuvent être consultées ou révoquées à tout moment.

Avertissement

L'approbation prend effet immédiatement, mais les utilisateurs qui ont déjà la page ouverte doivent la recharger. Les navigateurs conservent en outre pendant un court instant le résultat de l'autorisation précédente : si l'organigramme affiche encore une erreur quelques minutes après l'approbation, patientez un peu et actualisez la page avant d'approfondir l'investigation.

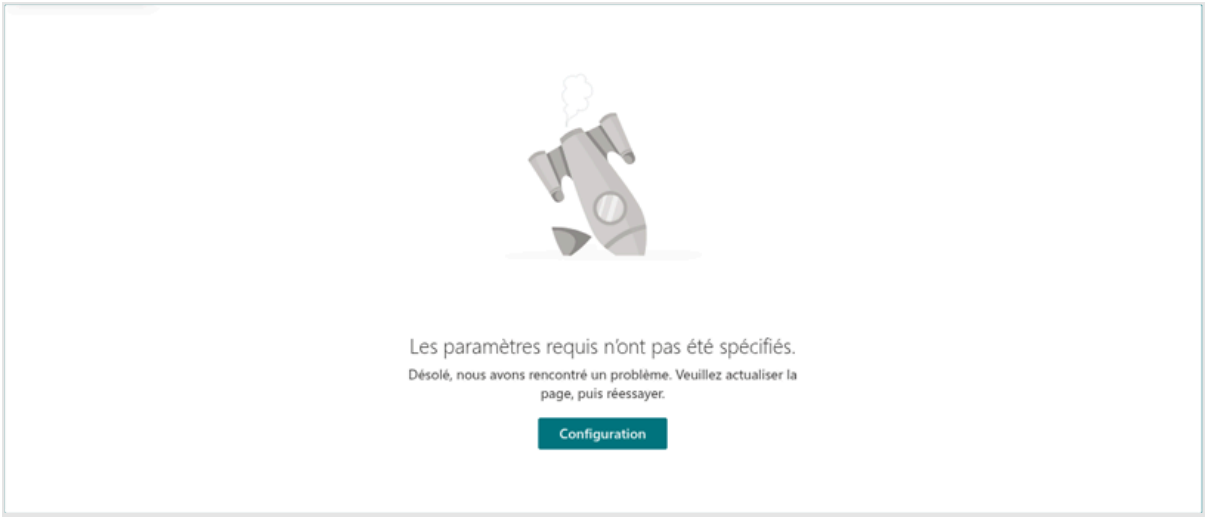
Conseil

La procédure de déploiement complète — chargement du package dans l'App Catalog, activation pour tous les sites et approbation des autorisations — est décrite dans KB10035. Installer un produit cloud.

Que se passe-t-il lorsqu'une autorisation manque

Les trois autorisations ne provoquent pas les mêmes défaillances, ce qui aide à diagnostiquer le problème :

- **non approuvée.** L'organigramme ne peut pas charger l'annuaire. À la place de l'arborescence, le composant WebPart affiche le message *Sorry, something went wrong. Please refresh the page and try again.* avec un bouton **Configure** destiné aux éditeurs de la page. Approuvez les demandes en attente et rechargez la page.
- **non approuvée.** L'organigramme se charge et toutes les cartes s'affichent, mais le point de présence sur les photos est absent pour tout le monde. C'est l'état partiel le plus courant : les deux autorisations d'annuaire ont été approuvées, tandis que la demande de présence a été oubliée.
- **Une autorisation a été révoquée après le déploiement.** Les symptômes sont les mêmes que ci-dessus. Les autorisations révoquées réapparaissent sous **Pending requests** et peuvent être approuvées à nouveau.



L'erreur affichée lorsque l'annuaire ne peut pas être chargé

Remarque

La présence exige davantage que l'autorisation : la personne doit disposer d'une licence Microsoft Teams et être connectée à Teams. Un utilisateur sans Teams apparaît toujours sans indicateur de présence, même lorsque `Presence.Read.All` est approuvée.

Qui peut voir l'organigramme

Le composant WebPart utilisant des autorisations déléguées, l'accès à l'organigramme dépend de deux éléments :

- **L'accès à la page.** Un visiteur doit pouvoir ouvrir la page SharePoint ou l'onglet Teams qui héberge le composant WebPart — les autorisations SharePoint et Teams habituelles s'appliquent.
- **L'accès à l'annuaire.** Par défaut, tous les membres de l'organisation peuvent lire les informations de base de l'annuaire dans Microsoft 365 ; tout visiteur ayant accès à la page voit donc le même organigramme. Les utilisateurs invités, en revanche, ne sont pas chargés dans l'organigramme et ne peuvent généralement pas non plus lire l'intégralité de l'annuaire.

Organizational Chart n'ajoute aucune couche d'autorisation qui lui soit propre : il ne masque pas certains employés à certains visiteurs et ne donne à personne accès à des données qu'il ne pourrait pas lire ailleurs dans Microsoft 365. Pour exclure totalement certains comptes de l'organigramme — comptes de service, boîtes aux lettres partagées, utilisateurs de test —, utilisez les options de filtrage et d'exclusion du composant WebPart, décrites dans KB10233. Comment ajouter et configurer le composant WebPart Organizational Chart.

Traitement des données

Dans le cadre d'une revue de sécurité, les points suivants sont généralement pertinents :

- Les données des employés sont lues dans Microsoft Graph directement par le navigateur de l'utilisateur et ne sont envoyées ni à Vitextra ni à un service tiers.
- Un instantané de l'annuaire chargé est conservé dans le stockage local du navigateur pendant 12 heures maximum afin d'accélérer les visites répétées ; il est stocké par utilisateur et par navigateur et ne quitte jamais l'appareil.
- Les photos et la présence ne sont demandées que pour les cartes visibles à l'écran et ne sont pas mises en cache au-delà de la session de la page.
- Le composant WebPart ne contacte les serveurs de Vitextra que pour vérifier l'état

de la licence du locataire, charger des ressources statiques telles que les icônes et collecter une télémétrie anonyme sur l'utilisation du produit. Aucune donnée d'annuaire n'est incluse dans ces requêtes.

Conseil

Pour une présentation du produit, consultez KB10232. Organizational Chart : présentation de la solution. Si des employés sont absents de l'organigramme alors que toutes les autorisations sont approuvées, consultez KB10236. Pourquoi une personne est-elle absente de l'organigramme ?.

Conditions

Microsoft Entra ID

Microsoft Entra ID (anciennement Azure Active Directory) est un service de gestion des identités et des accès basé sur le cloud, proposé par Microsoft. Il permet aux organisations de gérer et de sécuriser efficacement les identités de leurs utilisateurs et leur accès à diverses ressources, internes et externes. Ces ressources comprennent Microsoft 365, la plateforme Azure et des milliers d'autres applications SaaS (software as a service).

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.