vitextra

ARTICLE DE LA BASE DE CONNAISSANCES

Comment approuver les autorisations d'API Microsoft Graph pour les solutions Vitextra dans le Centre d'administration SharePoint

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

Vue d'ensemble 4

Ce qui est demandé et pourquoi 4

D'où viennent les demandes 7

Prérequis 7

Approuver les demandes 8

Approuver seulement une partie des autorisations 9

Ce que voient les utilisateurs lorsqu'une autorisation manque 9

Mises à jour et nouvelles autorisations 10

Vérifier et révoquer les autorisations 10

Notes de sécurité pour les réviseurs 11

Termes 12

Vue d'ensemble

Plusieurs composants WebPart Vitextra lisent des données qui se trouvent en dehors du **site SharePoint** : les profils utilisateur et la hiérarchie des responsables dans **Microsoft Entra ID**, la présence dans **Microsoft Teams**, les calendriers, les tâches dans Planner et To Do, les fichiers dans OneDrive. Les solutions **SharePoint Framework (SPFx)** accèdent à ces données par l'intermédiaire de **Microsoft Graph**, et un administrateur du locataire doit l'autoriser une seule fois.

Le mécanisme est le même pour toutes les solutions SPFx : le package de la solution déclare les autorisations dont il a besoin, SharePoint transforme cette déclaration en *demandes d'autorisation* lorsque le package est déployé dans le catalogue d'applications, et les demandes attendent sur la page **Accès aux API** (API access) du Centre d'administration SharePoint jusqu'à ce qu'un administrateur les approuve ou les rejette.

Cet article explique quels produits Vitextra demandent des autorisations et pourquoi, comment approuver les demandes, comment les vérifier et les révoquer par la suite, et ce que vous voyez dans les composants WebPart lorsqu'une autorisation manque. Il s'adresse aux administrateurs SharePoint et aux administrateurs généraux qui installent les produits Vitextra, ainsi qu'aux responsables de la sécurité qui examinent ce type de demandes.

Remarque

L'article ne traite que des demandes d'accès aux API des solutions SPFx. L'installation du package lui-même est décrite dans KB10035. Comment installer un produit Vitextra dans SharePoint Online.

Ce qui est demandé et pourquoi

Les autorisations ci-dessous sont **déléguées** : les composants WebPart appellent Microsoft Graph au nom de l'utilisateur connecté. L'accès effectif dépend à la fois des étendues accordées et des autorisations de l'utilisateur. Cela ne signifie pas que les résultats Graph correspondent exactement à ce qu'affichent Outlook ou Teams. Microsoft Graph

Le tableau répertorie les autorisations déclarées par les versions actuelles des produits qui utilisent Microsoft Graph.

Produit	API	Autorisations	Utilisation
Employee Directory	Microsoft Graph	User.Read.All, Directory.Read.All, People.Read, Presence.Read.All, Calendars.Read	Lecture des profils utilisateur, des services et des responsables ; personnes pertinentes ; présence Teams ; état de disponibilité (libre/ occupé) pour l'indicateur de disponibilité
Employee Details	Microsoft Graph	User.Read.All, User.ReadWrite, People.Read.All, Presence.Read.All, Files.Read.All, Sites.Read.All, Calendars.Read.Shared	Lecture des profils ; possibilité pour un utilisateur de modifier les champs de son propre profil ; personnes pertinentes ; présence ; documents et sites sur lesquels la personne a récemment travaillé (insights Microsoft Graph) ; état de disponibilité des collègues pour les heures de travail et la disponibilité
Organizational Chart	Microsoft Graph	User.Read.All, Directory.Read.All, Presence.Read.All	Construction de la hiérarchie à partir de l'attribut **Responsable** ;

Produit	API	Autorisations	Utilisation
			service et fonction ; présence Teams
Absence & Coverage	Microsoft Graph	User.Read.All	Résolution des employés, de leurs responsables et de leurs subordonnés directs pour les demandes, les approbations et les remplacements
My Tasks	Microsoft Graph	User.Read, User.ReadBasic.All, Tasks.ReadWrite	Tâches de Planner, de To Do et e-mails marqués d'un indicateur ; noms des auteurs des tâches
My Tasks	**Azure DevOps**	user_impersonation	La source **Azure DevOps** et le composant WebPart **Azure DevOps Query**
Password Vault	Microsoft Graph	Files.ReadWrite.AppFolder	Stockage du coffre chiffré dans le dossier d'application du OneDrive de l'utilisateur

Les produits qui ne travaillent qu'avec le site actuel - Announcements Carousel, List Filter Online, QR Code Generator, Questions & Answers, Quick Poll, **RSS** Reader, Smart Search et Smart Tiles - ne demandent **aucune** autorisation d'API. Rien n'apparaît pour eux sur la page **Accès aux API**.

Remarque

Un nom d'autorisation tel que *Tasks.ReadWrite* ou *User.ReadWrite* est le nom de l'étendue Microsoft Graph, qui peut être plus large que ce que le produit en fait réellement. My Tasks ne fait que lire les tâches ; Employee Details n'écrit que les champs de profil de l'utilisateur connecté. Les articles propres à chaque produit détaillent chaque autorisation : KB10235. Autorisations Microsoft Graph requises par Organizational Chart, KB10303. My Tasks : autorisations requises, confidentialité et sécurité.

D'où viennent les demandes

Une demande d'autorisation est créée lorsque le package `.sppkg` est déployé dans le catalogue d'applications du locataire. Les demandes appartiennent au package, et non aux composants WebPart individuels ; une solution qui contient deux composants WebPart présente donc un seul ensemble de demandes, et une autorisation nécessaire uniquement à une **fonctionnalité** facultative (la source Azure DevOps de My Tasks, par exemple) est demandée avec les autres.

Deux points sont importants pour la gouvernance :

- **L'approbation vaut pour l'ensemble du locataire.** SharePoint accorde l'autorisation à une seule application Microsoft Entra ID qu'il utilise pour toutes les solutions SPFx - *Web Client Extensibility* (anciennement *SharePoint Online Client Extensibility Web Application Principal*). Une fois *User.Read.All* approuvée pour Employee Directory, la même autorisation est utilisée par Organizational Chart et par toute autre solution SPFx du locataire qui la demande. C'est ainsi que fonctionne SharePoint Framework ; il ne s'agit pas d'un choix de conception de Vitextra.
- **Le déploiement ne dépend pas de l'approbation.** Un produit Vitextra peut être déployé, ajouté aux sites et placé sur des pages pendant que ses demandes sont encore en attente, voire rejetées. Seules les fonctionnalités qui dépendent de l'autorisation manquante ne fonctionnent pas.

Prérequis

- Le package Vitextra est chargé dans le catalogue d'applications du locataire et déployé (**Activer l'application**).
- Pour approuver les autorisations Microsoft Graph et des autres API Microsoft, connectez-vous avec le rôle **Administrateur général**. Le rôle **Administrateur d'applications** suffit pour les API tierces enregistrées dans le locataire. Le rôle

> Administrateur SharePoint seul ne permet pas d'approuver les autorisations Microsoft Graph. Microsoft

Avertissement

La page **Accès aux API** affiche les demandes des packages déployés dans le catalogue d'applications du **locataire**. Si vous préférez déployer les produits Vitextra depuis un catalogue d'applications de collection de sites, déployez d'abord le package dans le catalogue d'applications du locataire et approuvez-y les demandes ; les autorisations approuvées valent pour l'ensemble du locataire et sont alors également disponibles pour la copie placée dans le catalogue d'applications de la collection de sites.

Approuver les demandes

1. Ouvrez le Centre d'administration Microsoft 365 et accédez au **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. Chaque ligne indique le nom du package (par exemple *Vitextra Employee Directory*), l'API (*Microsoft Graph* ou *Azure DevOps*) et l'autorisation.

4. Sélectionnez une demande et cliquez sur **Approuver**. Lisez la description dans le volet et confirmez avec **Approuver**.

5. Répétez l'opération pour chaque demande du package. Une autorisation déjà approuvée pour une autre solution n'apparaît pas une seconde fois : SharePoint réutilise l'autorisation existante.

6. Passez à l'onglet **Demandes approuvées** et vérifiez que toutes les autorisations du package y figurent.

Les utilisateurs ne voient aucune invite de consentement : après l'approbation, les composants WebPart fonctionnent pour tout le monde dans le locataire. L'autorisation prend généralement effet en quelques minutes ; si un composant WebPart signale toujours une autorisation manquante, rechargez la page ou déconnectez-vous puis reconnectez-vous pour obtenir un nouveau jeton.

Conseil

Vous pouvez approuver les demandes en une seule fois avec SharePoint Online Management Shell : `Get-SPOTenantServicePrincipalPermissionRequests` répertorie les demandes en attente, et `Approve-SPOTenantServicePrincipalPermissionRequest -RequestId <id>` en approuve une. C'est pratique lorsque vous déployez plusieurs produits Vitextra en même temps.

Approuver seulement une partie des autorisations

Vous pouvez approuver certaines demandes et en rejeter d'autres. Le composant WebPart continue de fonctionner, et seule la fonctionnalité dépendante est concernée :

- *Presence.Read.All* rejetée - Employee Directory, Employee Details et Organizational Chart affichent les personnes sans l'indicateur de présence Teams.
- *Calendars.Read* / *Calendars.Read.Shared* rejetées - les informations de disponibilité et d'heures de travail ne sont pas affichées.
- *Files.Read.All* / *Sites.Read.All* rejetées - Employee Details n'affiche pas les fichiers et les sites récents.
- *user_impersonation* (Azure DevOps) rejetée - la source Azure DevOps de My Tasks et le composant WebPart Azure DevOps Query ne peuvent pas se connecter à Azure DevOps.

Le rejet de l'autorisation principale d'un produit (*User.Read.All* pour les produits centrés sur les personnes, *Tasks.ReadWrite* pour My Tasks, *Files.ReadWrite.AppFolder* pour Password Vault) laisse le composant WebPart sans données.

Ce que voient les utilisateurs lorsqu'une autorisation manque

Symptôme	Cause probable
Le composant WebPart affiche une erreur indiquant un accès refusé, des privilèges insuffisants ou un consentement manquant	L'autorisation principale est en attente ou rejetée
Les employés sont affichés, mais le point	*Presence.Read.All* n'est pas approuvée

Symptôme	Cause probable
de présence coloré manque	
L'organigramme est vide ou n'affiche que l'utilisateur actuel	*User.Read.All* ou *Directory.Read.All* n'est pas approuvée
My Tasks n'affiche rien pour Planner, To Do et Outlook, alors que la source SharePoint fonctionne	*Tasks.ReadWrite* n'est pas approuvée
Tout fonctionnait, et après une mise à jour une fonctionnalité a cessé de fonctionner	La nouvelle version demande une autorisation supplémentaire qui est encore en attente

Ouvrez la page **Accès aux API** et comparez les onglets **Demandes en attente** et **Demandes approuvées** avec le tableau figurant au début de cet article.

Mises à jour et nouvelles autorisations

Lorsque vous chargez une nouvelle version d'un package (voir KB10050. Comment mettre à jour une solution Vitextra SPFx dans SharePoint Online), les autorisations approuvées précédemment restent approuvées. Si la nouvelle version déclare une autorisation que la version précédente ne déclarait pas, la nouvelle demande apparaît dans l'onglet **Demandes en attente** et doit être approuvée de la même manière. Vitextra indique ces changements dans les notes de publication du produit.

Vérifier et révoquer les autorisations

Comme les autorisations sont partagées par toutes les solutions SPFx, la suppression d'un produit Vitextra ne révoque **pas** les autorisations qu'il a demandées. Pour révoquer une autorisation :

1 Ouvrez **Accès aux API** et passez à l'onglet **Demandes approuvées**.
2 Sélectionnez l'autorisation et cliquez sur **Supprimer l'accès** (Remove access).
3 Confirmez.

Avertissement

Avant de supprimer une autorisation, vérifiez si une autre solution du locataire en dépend - vos propres composants WebPart SPFx, les produits d'autres éditeurs et les autorisations préautorisées de Microsoft apparaissent dans le même onglet. La suppression d'une autorisation utilisée par une autre solution interrompt immédiatement cette solution.

Une demande rejetée est supprimée de la page Accès aux API et ne reste pas dans **Demandes en attente**. Pour demander à nouveau l'autorisation, le développeur doit soumettre une nouvelle demande pour la même ressource et la même étendue. Microsoft

Notes de sécurité pour les réviseurs

- Chaque appel à Microsoft Graph est effectué depuis le navigateur de l'utilisateur connecté avec un jeton émis pour cet utilisateur. Les composants WebPart Vitextra n'ont aucune autorisation d'application (app-only) et aucun compte de service.
- Microsoft Graph vérifie les étendues déléguées accordées et les autorisations de l'utilisateur. La visibilité dans le carnet d'adresses et les filtres propres aux applications sont des mécanismes distincts ; masquer une personne dans Outlook ne signifie pas qu'elle sera masquée dans les requêtes Graph.
- Pour les flux de données, les demandes de licence, la télémétrie et le stockage propres à chaque produit, voir KB10363. Où les produits Vitextra stockent vos données : confidentialité, résidence des données et RGPD.

Termes

Azure DevOps
Azure DevOps Services (anciennement Visual Studio Team Services) est un produit basé sur le cloud qui fournit le contrôle de version, la gestion des exigences, des pipelines automatisés pour les builds et les mises en production, ainsi que des fonctionnalités de test.

Fonctionnalité
Une fonctionnalité est un ensemble d'éléments SharePoint (artefacts), tels que des colonnes de site, des types de contenu, des composants WebPart, des pages d'application, des actions personnalisées, des modèles de liste, des instances de liste, etc.

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.

Microsoft Teams
Microsoft Teams est une plateforme de collaboration basée sur le chat, destinée à la communication en entreprise, qui offre des fonctionnalités pour les réunions en ligne, les événements en direct et le partage de documents.

RSS
RSS (Really Simple Syndication) est un format de flux web très répandu, utilisé pour diffuser les mises à jour de sites web vers des utilisateurs et des applications dans un format standardisé et lisible par machine. Ce format est couramment utilisé pour distribuer des articles d'actualité, des billets de blog et d'autres contenus

fréquemment mis à jour.

SharePoint
SharePoint est une plateforme de collaboration web qui fournit des outils de gestion de contenu, de gestion de documents, d'applications de flux de travail, de recherche et d'autres outils permettant aux employés et aux équipes de travailler ensemble. SharePoint est également un espace sécurisé pour stocker, organiser et consulter des informations partagées.

SharePoint Framework (SPFx)
SharePoint Framework (SPFx) est un modèle permettant de créer des composants WebPart côté client, des composants et des extensions pour SharePoint Online, SharePoint Server (local) et Microsoft Teams. Les personnalisations SPFx reposent sur JavaScript et prennent en charge l'interface utilisateur moderne de manière native.

Site
Un site SharePoint est un conteneur d'informations au sein de la plateforme SharePoint. Les sites offrent généralement des fonctionnalités telles que des bibliothèques de documents, des listes, des calendriers, des forums de discussion et des flux de travail, qui facilitent la collaboration, la communication et la gestion des documents au sein des équipes ou entre les services. Les sites peuvent être personnalisés et configurés pour répondre aux besoins et aux flux de travail spécifiques d'une organisation.