ARTICLE DE LA BASE DE CONNAISSANCES

Policy Acknowledgement : prérequis et autorisations

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

Accès pour le déploiement et la configuration 4

Autorisations Microsoft Graph 4

Autorisations du hub et du contenu 5

Vérifier indépendamment chaque niveau d’accès 5

Préparer la transmission du déploiement 6

Service et mode d'enregistrement 7

Préparez les autorisations de déploiement, l'accès au contenu source et les rôles du produit avant de lancer une campagne de politique. L'approbation des autorisations Microsoft Graph et l'attribution des rôles du produit sont deux tâches distinctes.

Accès pour le déploiement et la configuration

La solution est un package SPFx pour SharePoint Online. Suivez KB10035. Comment installer un produit Vitextra dans SharePoint Online pour installer le package. La personne qui effectue la configuration initiale doit pouvoir administrer le site de stockage sélectionné et créer les listes nécessaires. La création d'un nouveau site nécessite également l'autorisation correspondante dans le locataire.

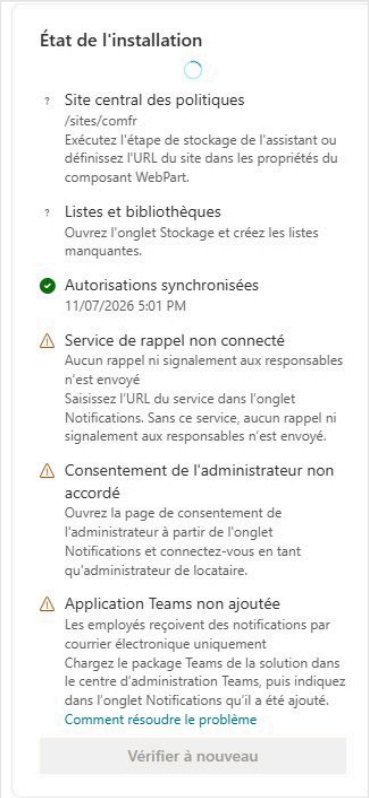
Avant la configuration d'un groupe d'administrateurs, Policy Admin s'appuie par défaut sur les propriétaires du site. Une fois ce groupe attribué, son appartenance détermine l'administration du produit. Les rôles du produit n'accordent pas automatiquement l'autorisation de modifier les pages SharePoint ou de déployer des applications du locataire.

Autorisations Microsoft Graph

Le package de la solution demande les étendues Microsoft Graph suivantes :

Étendue	Utilisation par le produit
`User.Read.All`	Profils des employés et informations organisationnelles.
`GroupMember.Read.All`	Appartenance aux groupes utilisée par les audiences et les rôles.
`Directory.Read.All`	Données d'annuaire utilisées pour rechercher les employés et les groupes.
`Mail.Send`	E-mails de rappel manuels envoyés depuis la boîte aux lettres de l'utilisateur actuel.

Demandez à l'administrateur du locataire d'approuver les demandes du package selon le processus d'administration de l'accès aux API SharePoint de votre organisation. Si les sélecteurs d'employés ou de groupes ne chargent pas les données, vérifiez ces approbations avant de modifier les règles d'audience.



Contrôles d'installation dans Policy Admin

Autorisations du hub et du contenu

Attribuez les groupes de rôles et appliquez les autorisations dans Policy Admin. Tous les composants WebPart doivent se connecter au même hub prévu. Les employés doivent également pouvoir accéder au contenu d'origine : définir une URL dans une fiche de politique n'accorde aucune autorisation sur le fichier, la page ou le site externe référencé.

Pour contrôler l'accès, utilisez des groupes Entra ID ou des groupes SharePoint du site hub explicitement sélectionnés. Ne considérez pas l'option **Tous les utilisateurs disposant d'une licence** comme une validation de licence par utilisateur : sa logique actuelle de résolution des rôles ne vérifie pas la licence de chaque utilisateur.

Vérifier indépendamment chaque niveau d'accès

Un déploiement fonctionnel nécessite plusieurs formes d'accès indépendantes. La personne qui déploie le package n'est pas nécessairement celle qui gère les politiques, et un employé n'a pas besoin de privilèges de déploiement pour lire une attribution. Séparer ces responsabilités facilite le diagnostic sans accorder de larges droits administratifs comme solution de contournement.

Niveau d'accès	Contrôle d'acceptation utile	Conséquence typique d'un échec
Package et page	L'utilisateur prévu peut charger la page publiée et le composant WebPart.	L'application est inaccessible ou ne s'affiche pas.
Annuaire	L'opérateur autorisé peut résoudre les employés et groupes prévus.	Les sélecteurs, le choix du public ou la résolution des rôles peuvent échouer.
Données du hub	Le compte peut lire les enregistrements requis par son rôle.	Une page s'ouvre mais échoue au chargement des politiques ou attributions.
Contenu source	L'employé peut ouvrir directement le document ou le site.	Une fiche visible peut avoir un contenu illisible.
Écriture des preuves	Un employé pilote peut terminer le parcours d'enregistrement configuré.	La lecture réussit mais la confirmation échoue.
Hiérarchie de rapport	L'annuaire contient les relations de responsable attendues.	L'équipe d'un responsable peut être incomplète ou différente des attentes.

Effectuez les contrôles avec des comptes représentatifs. Un administrateur également propriétaire du site peut réussir grâce à des droits SharePoint élevés alors qu'un employé ordinaire échouerait. De même, un propriétaire de politique membre de plusieurs groupes de rôles ne remplace pas fiablement un compte auteur restreint.

Préparer la transmission du déploiement

Consignez l'URL du hub choisie, la page d'entrée des employés, la page du lecteur, les groupes de rôles et les emplacements source. Identifiez qui peut maintenir chacun de ces éléments. Un propriétaire de politique doit savoir qui contacter lorsqu'un fichier source est déplacé ; un administrateur de support doit pouvoir distinguer un problème de navigation d'un problème d'écriture du service sans reconstituer tout le déploiement.

Vérifiez l'identité d'annuaire et le responsable de l'employé représentatif avant le pilote. Les campagnes stockent les informations d'employé et de responsable sur les attributions. Des changements ultérieurs d'annuaire ne signifient pas que tous les anciens champs d'attribution ont été réécrits. Une réorganisation justifie donc de vérifier les rapports d'équipe, pas seulement la connexion de l'employé.

Pour les rappels manuels par e-mail, testez l'opérateur qui les enverra réellement. L'application utilise sa boîte aux lettres, tandis que les notifications automatiques dépendent de la configuration du service distinct. Approuver une demande d'API liée au courrier ne vérifie pas à lui seul une boîte aux lettres, la livraison à un destinataire précis ou le service d'arrière-plan.

Conservez les résultats de ces contrôles avec les détails du déploiement. Lorsqu'un échec est signalé, incluez le compte, le hub et la page concernés, l'opération et l'heure de l'erreur. Ces informations sont plus exploitables qu'une déclaration générale selon laquelle les autorisations ont été approuvées, car chaque niveau peut réussir ou échouer indépendamment.

Service et mode d'enregistrement

Le mode Service nécessite une URL de service accessible et une vérification réussie du consentement administrateur. Le consentement du service est distinct de l'approbation des autorisations Graph du package SPFx. Les rappels automatiques, les escalades et le traitement continu de l'audience nécessitent le composant de service séparé ; saisir des paramètres ne suffit pas à exécuter ces tâches.

Avertissement

Le mode Direct accorde aux employés des droits de contribution sur les listes d'attributions et de confirmations. Consultez KB10500. Configurer les rôles et les autorisations de Policy Acknowledgement et KB10509. Stockage des données Policy Acknowledgement : modes Direct et Service avant d'utiliser des données réelles d'employés. Les filtres des composants WebPart et le ciblage d'audience ne remplacent pas les autorisations sur les données.