ARTICLE DE LA BASE DE CONNAISSANCES

Configurer les rôles et les autorisations de Policy Acknowledgement

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

Comprendre les rôles 4

Attribuer des groupes 4

Comprendre les effets de l'application des autorisations 5

Distinguer public, propriété et autorisation 6

Utiliser un test d’accès représentatif 6

Maintenir les accès après des changements organisationnels 7

Vérifier et maintenir les accès 8

Les rôles du produit déterminent les opérations et les vues disponibles dans Policy Acknowledgement. Policy Admin applique également aux listes du hub des autorisations SharePoint fondées sur les rôles. Examinez ces deux niveaux lors de la conception des accès.

Comprendre les rôles

Rôle	Utilisation principale dans les composants WebPart
Administrateur produit	Configuration, paramètres, rôles et administration ; accès à la gestion et aux rapports.
Responsable de la conformité	Politiques, campagnes, rapports et exemptions dans l'ensemble du produit.
Auteur de la politique	Création de politiques et gestion des politiques dont l'auteur est responsable.
Auditeur	Rapports et vérifications sans actions de gestion des politiques.
Employé	Attributions personnelles et contenu des politiques.

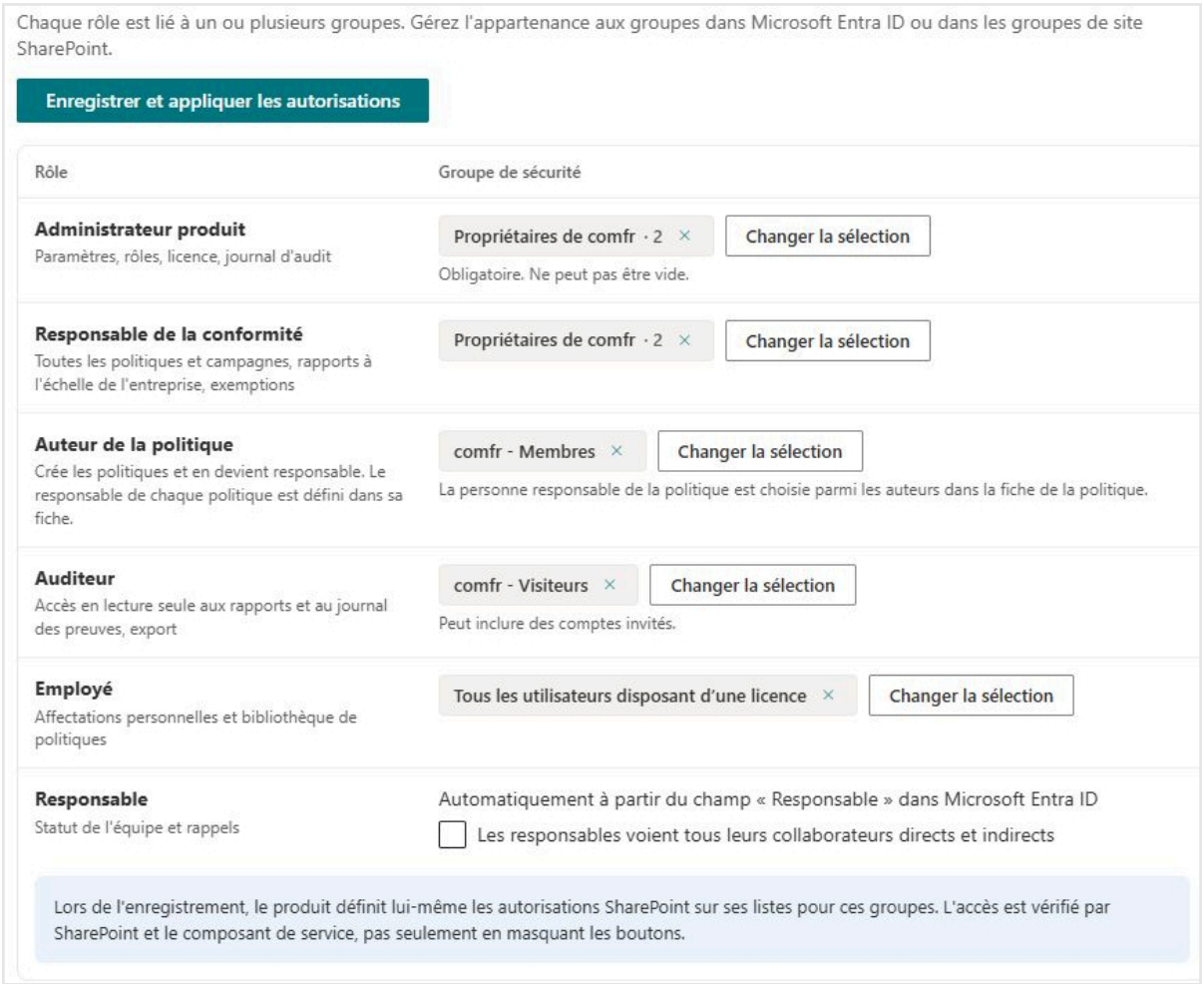
Le périmètre d'un responsable d'équipe découle des relations hiérarchiques, avec un réglage pour les collaborateurs directs ou toute la branche hiérarchique. Il ne s'agit pas d'un sixième rôle attribué dans la liste des rôles. Le responsable est enregistré dans chaque politique ; la vue auteur filtre les politiques selon ce responsable.

Attribuer des groupes

1 Ouvrez Policy Admin en tant qu'administrateur du produit et sélectionnez **Rôles**.
2 Sélectionnez des groupes de sécurité Entra ID ou des groupes SharePoint appartenant au site hub pour les rôles nécessaires.
3 Conservez au moins un groupe pour **Administrateur produit**.
4 Vérifiez la population d'employés et **Les responsables voient tous leurs collaborateurs directs et indirects**.
5 Sélectionnez **Enregistrer et appliquer les autorisations** et attendez la fin de la synchronisation.

Utilisez des groupes d'employés explicitement sélectionnés lorsqu'une limite d'accès

précise est nécessaire. Bien que l'interface propose **Tous les utilisateurs disposant d'une licence**, la résolution actuelle des rôles considère cette option comme correspondant à l'utilisateur actuel sans vérifier sa licence. Elle ne doit pas servir de preuve que l'accès est réservé aux comptes sous licence.



Rôles du produit et groupes attribués

Comprendre les effets de l'application des autorisations

La synchronisation accorde aux groupes de rôles un accès en lecture au site, rompt l'héritage des autorisations sur les listes du produit et applique la matrice d'autorisations des listes. Le compte qui effectue la synchronisation conserve le contrôle total sur ces listes. Évaluez l'impact avant de l'appliquer à un site partagé existant.

En mode Direct, les employés reçoivent des droits de contribution sur les attributions et les enregistrements de confirmation. En mode Service, les entrées des employés dans cette matrice sont en lecture seule pour ces deux listes. Les employés conservent les droits de contribution sur les questions. Un utilisateur ayant plusieurs rôles peut recevoir les autorisations combinées de ses groupes.

Avertissement

Le filtrage par responsable de politique et celui des attributions personnelles sont implémentés dans les composants WebPart. La matrice d'autorisations s'applique au niveau des listes et n'isole pas les données par politique ou par employé. Ne présentez pas ces filtres comme la garantie que les utilisateurs ne peuvent pas accéder à d'autres enregistrements par SharePoint. Une synchronisation réussie ne prouve pas non plus que tous les droits préexistants ou élevés ont été révoqués.

Distinguer public, propriété et autorisation

Ces concepts répondent à des questions différentes. Le public d'une campagne détermine qui doit recevoir une tâche. Le propriétaire de politique détermine la responsabilité et la vue de gestion filtrée pour l'auteur. Un rôle permet des actions du produit, tandis que les autorisations SharePoint régissent l'accès aux enregistrements stockés. Modifier l'un ne réalise pas automatiquement les autres.

Par exemple, attribuer une politique au service financier ne rend pas ses enregistrements de liste sous-jacents privés pour ce service. Transférer une fiche à un autre propriétaire change l'auteur responsable, mais ne transfère pas les autorisations élément par élément. Masquer une page de gestion dans la navigation du portail ne révoque pas non plus l'accès existant d'un utilisateur aux listes.

Concevez les groupes de rôles selon les responsabilités, puis examinez leurs accès effectifs aux données. Si une personne appartient à plusieurs groupes, testez cette combinaison. Un utilisateur ayant un rôle auteur et un groupe administratif peut voir ou modifier bien plus qu'un compte de test uniquement auteur. Supprimer une appartenance peut laisser un accès via un autre groupe ou une autorisation de site élevée.

Utiliser un test d'accès représentatif

Compte de test	Contrôle dans l'application	Contrôle d'accès complémentaire
Administrateur	Ouvrir Policy Admin et examiner les rôles configurés.	Confirmer que l'administration attendue reste disponible après synchronisation.
Auteur	Ouvrir les politiques	Examiner les autorisations

Compte de test	Contrôle dans l'application	Contrôle d'accès complémentaire
	possédées et vérifier les actions de gestion prévues.	réelles des listes plutôt que déduire l'isolation de la vue filtrée.
Auditeur	Ouvrir le rapport concerné et télécharger un export autorisé.	Vérifier si les actions enregistrant un résultat ou un événement d'audit requièrent une écriture supplémentaire.
Employé	Ouvrir une politique attribuée et soumettre une confirmation pilote.	Vérifier l'accès source et le parcours configuré d'écriture des preuves.
Responsable	Charger l'équipe hiérarchique attendue.	Vérifier indépendamment l'accès effectif aux données et le comportement du périmètre.

Certaines actions apparemment orientées lecture écrivent aussi des données. Par exemple, un contrôle d'intégrité enregistre son résultat et un export de rapport écrit un événement d'audit après génération du fichier. Un compte en lecture seule peut donc obtenir un résultat utile puis rencontrer une erreur d'écriture. Examinez l'opération précise en échec avant d'élargir son rôle.

Maintenir les accès après des changements organisationnels

Lorsqu'un auteur change de poste, examinez son appartenance aux groupes et la propriété des politiques qu'il maintenait. Lorsque les responsables changent, examinez les relations d'annuaire et les champs de responsable stockés sur les attributions ; recharger une page ne réécrit pas les attributions historiques. Lorsque le mode d'enregistrement change, examinez le service et réappliquez la matrice d'autorisations correspondante.

Conservez une courte trace de la personne ayant appliqué les autorisations, des groupes prévus et des tests représentatifs réussis. Le compte de synchronisation

conserve le contrôle total : évaluez-le explicitement plutôt que de supposer que le mode Service rend tous les comptes humains en lecture seule. Le paramètre de toute la branche n'est pas non plus appliqué par le sélecteur actuel de Team Compliance ; consultez KB10530. Team Compliance : suivre votre équipe et effectuer les relances pour la limite de rapport qui en résulte.

Vérifier et maintenir les accès

Testez avec des comptes distincts d'administrateur, d'auteur, de consultation des rapports et d'employé. Vérifiez les pages prévues et les autorisations des listes sous-jacentes. Après un changement de mode d'enregistrement des confirmations, exécutez de nouveau **Enregistrer et appliquer les autorisations** et examinez les droits effectifs. Consultez KB10509. Stockage des données Policy Acknowledgement : modes Direct et Service pour les modes d'enregistrement et leurs limites.