bitwarden | Article du Centre d'Aide

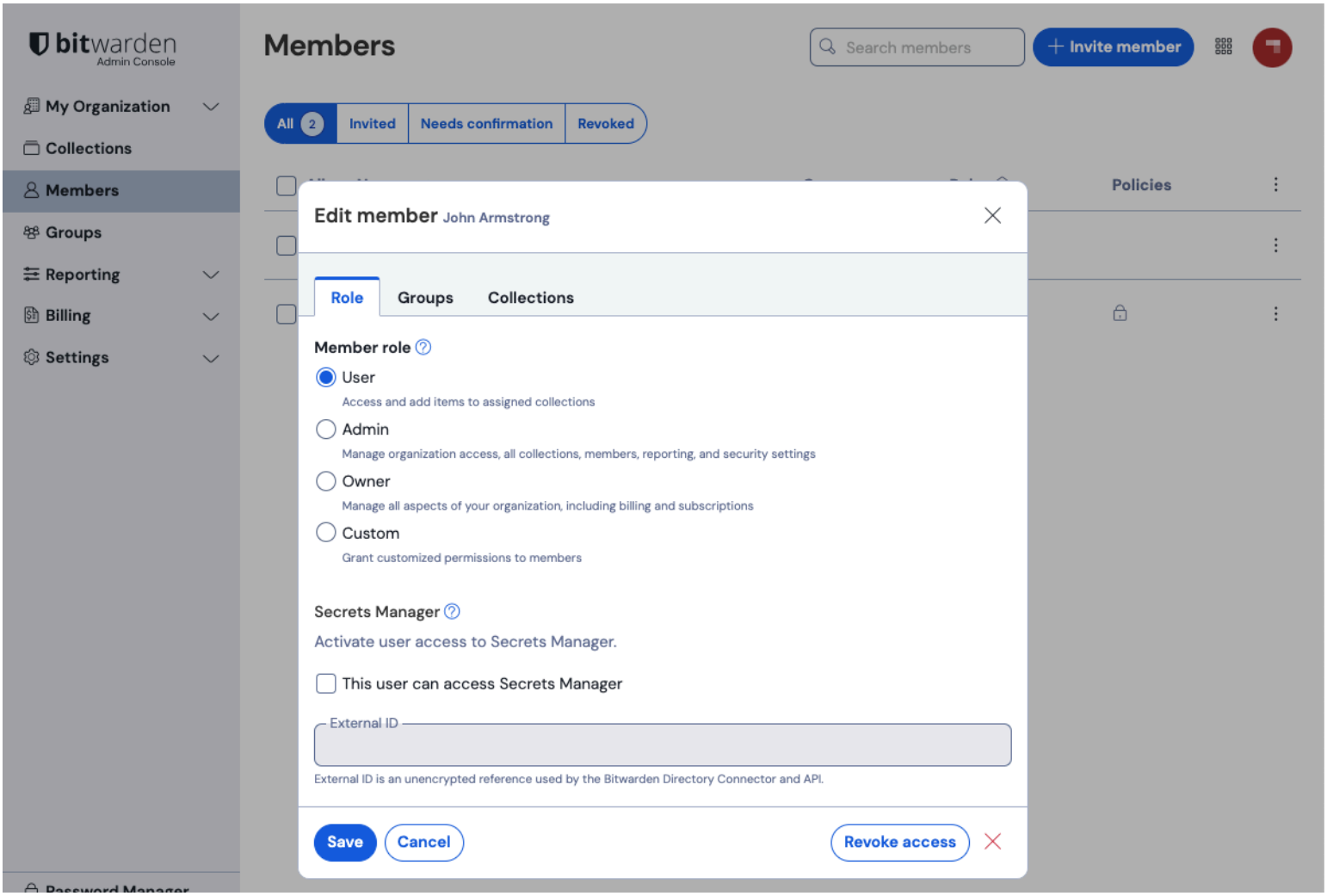
CONSOLE ADMIN > GESTION DES UTILISATEURS

Rôles et Autorisations des Membres

Afficher dans le centre d'aide:
https://bitwarden.com/help/user-types-access-control/

Rôles et Autorisations des Membres

Les membres des organisations Bitwarden peuvent se voir accorder une variété de rôles et de niveaux d'autorisation pour les collections. Vous pouvez définir des rôles et des autorisations de collection lorsque vous invitez des utilisateurs à votre organisation, ou à tout moment depuis l'écran **Membres** de votre organisation en utilisant le menu ⋮ options :



Éditer les rôles des membres

Rôles des membres

Le rôle détermine quelles actions un membre peut prendre dans le contexte des outils disponibles de votre organisation. Les rôles ne déterminent pas à quelles collections ils ont accès.

Note

À partir du 03/07/24, les organisations qui n'ont pas activé la gestion de collection commenceront à être migrées par lots vers une structure d'autorisations mise à jour. Si elle n'a pas encore été migrée, votre organisation le sera dans les prochaines semaines ou si vous activez manuellement la gestion de la collection.

Pendant la migration, tous les gestionnaires sont migrés en membres avec le rôle d'utilisateur et se voient automatiquement attribuer une nouvelle autorisation **Peut gérer** sur les collections assignées. Ils conserveront la capacité de gérer pleinement ces collections, y compris la capacité d'attribuer l'accès à de nouveaux membres ou groupes. Cela aussi :

- Migrer les membres avec un rôle personnalisé qui comprend **Éditer les collections assignées** vers le rôle d'Utilisateur avec **Peut gérer** l'autorisation sur ces collections.
- Migrer les membres avec un rôle personnalisé avec seulement **Supprimer les collections assignées** vers le rôle d'utilisateur sans aucune autorisation sur ces collections.
- Dépréciez l'**Accéder à toutes les collections existantes et futures** autorisation et accordez à tous les utilisateurs qui avaient cette autorisation **Peut gérer** l'autorisation pour toutes les collections existantes.

Les options comprennent :

Rôle du membre	Permissions
Utilisateur	Accédez aux éléments partagés dans les collections assignées. Peut ajouter, éditer ou supprimer des éléments des collections assignées, à moins que l'autorisation **Peut afficher** ne soit attribuée. Peut créer, gérer et supprimer des collections si autorisé par l'organisation.
Administrateur	Tout ce qui précède, + Attribuez des utilisateurs à des groupes d'utilisateurs + Créer ou supprimer des groupes d'utilisateurs + Inviter et confirmer les nouveaux utilisateurs + Gérer les politiques de sécurité de l'Entreprise + Afficher les journaux d'événements + Exporter les données du coffre de l'organisation + Gérer la récupération de compte + Afficher les rapports de santé du coffre + Gérer la vérification du domaine + Gérer la configuration SSO + Gérer les approbations d'appareil + Gérer la configuration SCIM **Les utilisateurs admin ont automatiquement accès à toutes les collections.**

Rôle du membre	Permissions
Propriétaire	Tout ce qui précède, + Gérer les paramètres de gestion de collection + Gérer la facturation, y compris l'abonnement, la méthode de paiement et l'historique de facturation + Gérer la clé API + Gérer l'identifiant à deux étapes de l'organisation + Gérer les informations de l'organisation, par exemple le nom **Les utilisateurs propriétaires ont automatiquement accès à toutes les collections.**
Personnalisé (uniquement pour l'Entreprise)	Permet un contrôle granulaire des autorisations des utilisateurs sur une base utilisateur par utilisateur, voir Rôle personnalisé.

> **Note**
> **Only an owner** can create a new owner or assign the owner type to an existing user. For failover purposes, Bitwarden recommends creating multiple owner users.

Rôle personnalisé

Les rôles personnalisés sont actuellement disponibles pour les organisations Entreprise. La sélection du rôle **Personnalisé** pour un utilisateur permet un contrôle granulaire des autorisations sur une base utilisateur par utilisateur. Un utilisateur avec un rôle personnalisé peut avoir une sélection configurable de capacités de gérer et d'admin, y compris :

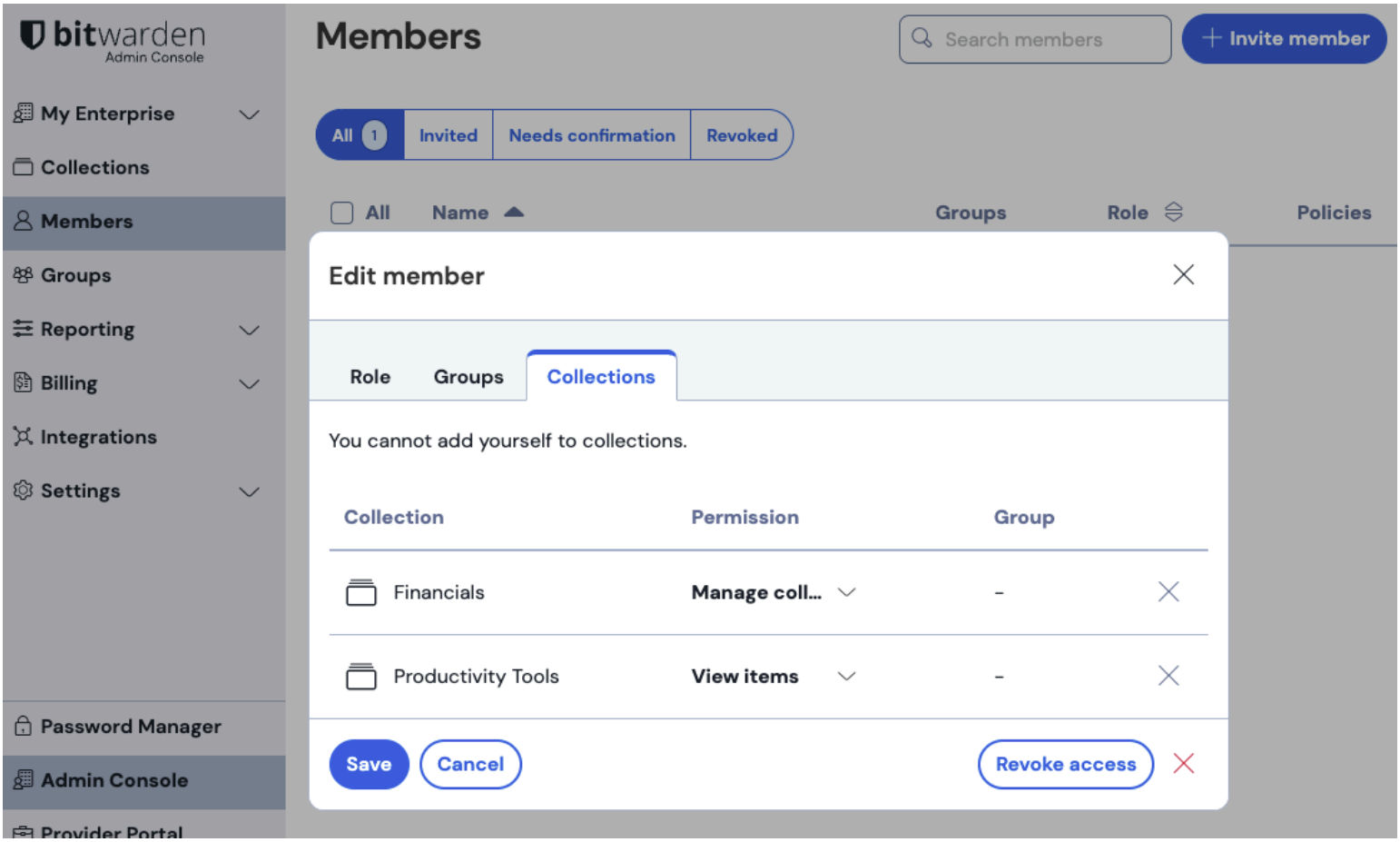
- Accéder aux journaux d'événements
- Accéder aux options d'import et d'export
- Accéder aux rapports
- Gérer toutes les collections (fournit les trois options suivantes)
  - Créer de nouvelles collections
  - Modifier n'importe quelle collection
  - Supprimer n'importe quelle collection
- Gérer les groupes
- Gérer le SSO
- Gérer les politiques de sécurité
- Gérer les utilisateurs

> **Tip**
> Custom users with the **Manage users** permission can manage other custom users, however they can only assign other custom users the permissions that they themselves have.

- Gérer la récupération de compte

Permissions

Les autorisations déterminent quelles actions un utilisateur peut effectuer avec les éléments d'une collection particulière. Bien que le rôle ne puisse être défini qu'au niveau d'un membre individuel, les autorisations peuvent soit être définies pour un membre individuel, soit pour un groupe dans son ensemble :



Options d'autorisation

Permission	Description
Peut voir	L'utilisateur ou le groupe peut afficher tous les éléments de la collection, y compris les champs cachés comme les mots de passe.

Permission	Description
Peut voir, sauf les mots de passe	L'utilisateur ou le groupe peut afficher tous les éléments de la collection sauf les champs cachés comme les mots de passe. Les utilisateurs peuvent toujours utiliser des mots de passe via la saisie automatique. Cacher les mots de passe empêche une copie et un collage faciles, cependant, cela n'empêche pas complètement l'accès de l'utilisateur à cette information. Traitez les mots de passe cachés comme vous le feriez pour toute autre information d'identification partagée.
Peut modifier	L'utilisateur ou le groupe peut ajouter de nouveaux éléments, supprimer des éléments existants et éditer des éléments existants dans la collection, y compris des champs cachés comme les mots de passe.
Peut modifier, sauf les mots de passe	L'utilisateur ou le groupe peut ajouter de nouveaux éléments, supprimer des éléments existants et éditer des éléments existants dans la collection, à l'exception des champs cachés comme les mots de passe. Les utilisateurs peuvent toujours utiliser des mots de passe via la saisie automatique. Cacher les mots de passe empêche la copie et le collage facile, cependant, cela n'empêche pas complètement l'accès de l'utilisateur à cette information. Traitez les mots de passe cachés comme vous le feriez pour toute autre information d'identification partagée.
Peut gérer	L'utilisateur ou le groupe peut attribuer à de nouveaux membres ou groupes l'accès à la collection, y compris l'ajout d'autres membres avec l'autorisation de gérer, et supprimer la collection s'ils le souhaitent.