

CONSOLE ADMIN > GESTION DES UTILISATEURS >

Synchroniser avec Microsoft Entra ID

Afficher dans le centre d'aide:

<https://bitwarden.com/help/microsoft-entra-id/>

Synchroniser avec Microsoft Entra ID

Cet article vous aidera à commencer à utiliser Directory Connector pour synchroniser les utilisateurs et les groupes de votre répertoire Microsoft Entra ID avec votre organisation Bitwarden.

Configuration de l'annuaire Microsoft Entra ID

Terminez les processus suivants depuis le portail Microsoft Azure avant de configurer le connecteur de répertoire. Le connecteur de répertoire nécessitera des informations obtenues à partir de ces processus pour fonctionner correctement.

Créer une inscription d'application

Suivez les étapes suivantes pour créer une inscription d'application pour le Connecteur de Répertoire :

1. Depuis votre portail Microsoft Azure, naviguez vers le répertoire **Microsoft Entra ID**.
2. Dans la navigation à gauche, sélectionnez **Enregistrements d'application**.
3. Sélectionnez le bouton **Nouvelle inscription** et donnez à votre inscription un nom spécifique à Bitwarden (par exemple, **bitwarden-dc**).
4. Sélectionnez **S'inscrire**.

Accorder des autorisations d'application

Suivez les étapes suivantes pour accorder à l'application créée l'autorisation requise :

1. Sur l'application Bitwarden créée, sélectionnez **Autorisations API** dans la navigation à gauche.
2. Sélectionnez le bouton **Ajouter une autorisation**.
3. Lorsqu'on vous demande de sélectionner une API, sélectionnez **Microsoft Graph**.
4. Définissez les **autorisations déléguées** suivantes :
 - Utilisateur > Utilisateur.LireBasique.Tout (Lire tous les profils basiques des utilisateurs)
 - Utilisateur > Utilisateur.Lire.Tout (Lire tous les profils complets des utilisateurs)
 - Groupe > Groupe.Lire.Tout (Lire tous les groupes)
 - UnitéAdministrative > UnitéAdministrative.Lire.Tout (Uniquement nécessaire si vous allez synchroniser [les Unités Administratives](#))
5. Définissez les **Autorisations d'Application** suivantes :
 - Utilisateur > Utilisateur.Lire.Tout (Lire tous les profils complets des utilisateurs)
 - Groupe > Groupe.Lire.Tout (Lire tous les groupes)
 - UnitéAdministrative > Unité.Administrative.Lire.Tout (Uniquement nécessaire si vous allez synchroniser [les Unités Administratives](#))
6. Retournez à la page des autorisations de l'API, sélectionnez le bouton **Accorder l'autorisation admin pour...**

Créer une clé secrète d'application

Suivez les étapes suivantes pour créer une clé secrète à utiliser par le connecteur de répertoire :

1. Sur l'application Bitwarden créée, sélectionnez **Certificats & secrets** dans la navigation à gauche.
2. Sélectionnez le bouton **Nouveau secret client** et ajoutez une description spécifique à Bitwarden (par exemple, **bitwarden-dc-secret**) et une date d'expiration. Nous recommandons de sélectionner **Jamais**.
3. Sélectionnez **Enregistrer** une fois que vous avez terminé.
4. Copiez la **valeur** du secret dans un endroit sûr pour une utilisation ultérieure.


Obtenez l'ID de l'application

Suivez les étapes suivantes pour obtenir l'ID de l'application à utiliser par le connecteur de répertoire :

1. Sur l'application Bitwarden créée, sélectionnez **Aperçu** dans la navigation à gauche.
2. Copiez l'**ID de l'application (client)** dans un endroit sûr pour une utilisation ultérieure.

Obtenir le nom d'hôte du locataire

Suivez les étapes suivantes pour obtenir le nom d'hôte du locataire à utiliser par le connecteur de répertoire :

1. À partir de n'importe où dans le portail Azure, sélectionnez l'icône  dans la barre de navigation supérieure droite.
2. Sélectionnez le bouton de filtre **Répertoire + abonnement** dans le menu situé à gauche.
3. Copiez la valeur du **Répertoire actuel**: dans un endroit sûr pour une utilisation ultérieure.

Connectez-vous à votre répertoire

Suivez les étapes suivantes pour configurer le connecteur de répertoire à utiliser Microsoft Entra ID. Si vous ne l'avez pas déjà fait, suivez les étapes appropriées pour la configuration de [Microsoft Entra ID](#) avant de continuer :

1. Ouvrez l'application de bureau [Directory Connector](#).
2. Naviguez vers l'**onglet Paramètres**.
3. Dans le menu déroulant **Saisir**, sélectionnez **Azure Active Directory**.

Les champs disponibles dans cette section changeront en fonction du type que vous avez choisi de saisir.

4. Entrez le **locataire nom d'hôte** collecté, l'**Id de l'application**, et la **clé secrète**.

Configurer les options de synchronisation

Tip

When you are finished configuring, navigate to the **More** tab and select the **Clear Sync Cache** button to prevent potential conflicts with prior sync operations. For more information, see [Clear Sync Cache](#).

Suivez les étapes suivantes pour configurer les paramètres utilisés lors de la synchronisation à l'aide de Directory Connector:

1. Ouvrez l'application de bureau [Directory Connector](#).

2. Naviguez vers l'**onglet Paramètres**.

3. Dans la section **Synchroniser**, configurez les options suivantes comme vous le souhaitez :

Option	Description
Intervalle	Temps entre les vérifications de synchronisation automatique (en minutes).
Supprimer les utilisateurs désactivés lors de la synchronisation	Cochez cette case pour supprimer les utilisateurs de l'organisation Bitwarden qui ont été désactivés dans votre répertoire.
Écraser les utilisateurs existants de l'organisation en fonction des paramètres de synchronisation actuels	Cochez cette case pour toujours effectuer une synchronisation complète et supprimer tous les utilisateurs de l'organisation Bitwarden s'ils ne sont pas dans l'ensemble des utilisateurs synchronisés.
Plus de 2000 utilisateurs ou groupes sont censés se synchroniser.	Cochez cette case si vous prévoyez de synchroniser 2000+ utilisateurs ou groupes. Si vous ne cochez pas cette case, Directory Connector limitera une synchronisation à 2000 utilisateurs ou groupes.
Synchroniser les utilisateurs	Cochez cette case pour synchroniser les utilisateurs avec votre organisation. Cocher cette case vous permettra de spécifier les Filtres Utilisateur .
Filtre utilisateur	Voir Spécifier les filtres de synchronisation .
Synchroniser les groupes	Cochez cette case pour synchroniser les groupes à votre organisation. Cocher cette case vous permettra de spécifier les Filtres de Groupe .
Filtre de groupe	Voir Spécifier les filtres de synchronisation .

Spécifiez les filtres de synchronisation

Utilisez des listes séparées par des virgules pour inclure ou exclure d'une synchronisation en fonction du courriel de l'utilisateur, du nom du groupe ou de l'adhésion au groupe.

Filtres d'utilisateur

Les syntaxes de filtrage suivantes doivent être utilisées dans le champ **Filtre Utilisateur** :

Inclure/Exclure des utilisateurs par courriel

Pour inclure ou exclure des utilisateurs spécifiques d'une synchronisation basée sur l'adresse de courriel :

Bash

```
include:joe@example.com,bill@example.com,tom@example.com
```

Bash

```
exclude:jow@example.com,bill@example.com,tom@example.com
```

Utilisateur par adhésion de groupe

Vous pouvez inclure ou exclure des utilisateurs d'une synchronisation en fonction de leur adhésion au groupe Microsoft Entra ID en utilisant les mots-clés **includeGroup** et **excludeGroup**. **includeGroup** et **excludeGroup** utilisent l'ID de l'objet Groupe, disponible sur la page **Overview** du groupe dans le [Azure Portal](#) ou via le [Azure AD Powershell](#) :

Bash

```
includeGroup:963b5acd-9540-446c-8e99-29d68fcb8eb,9d05a51c-f173-4087-9741-a7543b0fd3bc
```

Bash

```
excludeGroup:963b5acd-9540-446c-8e99-29d68fcb8eb,9d05a51c-f173-4087-9741-a7543b0fd3bc
```

Filtres de groupe

Note

Nested groups can sync multiple group objects with a single referent in the Directory Connector. Do this by creating an administrative unit with all of your groups listed.

Les syntaxes de filtrage suivantes doivent être utilisées dans le champ **Filtre de Groupe** :

Inclure/Exclure des groupes

Pour inclure ou exclure des groupes d'une synchronisation basée sur le nom du groupe :

Bash

```
include:Group A,Group B
```

Bash

```
exclude:Group A,Group B
```

Groupe par unité administrative (AU)

Vous pouvez inclure ou exclure des groupes d'une synchronisation en fonction de leurs [Unités Administratives Microsoft Entra ID](#) marquées en utilisant les mots-clés `includeadministrativeunit` et `excludeadministrativeunit`. `includeadministrativeunit` et `excludeadministrativeunit` utilisent l'**ID d'Objet** de l'Unité Administrative :

Bash

```
includeadministrativeunit:7ckcq6e5-d733-4b96-be17-5bad81fe679d
```

Bash

```
excludeadministrativeunit:7ckcq6e5-d733-4b96-be17-5bad81fe679d
```

Testez une synchronisation

💡 Tip

Avant de tester ou d'exécuter une synchronisation, vérifiez que Directory Connector est connecté au bon serveur cloud (par exemple, US ou EU) ou au serveur auto-hébergé. Apprenez comment faire avec [l'application de bureau](#) ou le [CLI](#).

Pour vérifier si le connecteur de répertoire se connectera avec succès à votre répertoire et renverra les utilisateurs et les groupes souhaités, naviguez vers l'onglet **Tableau de bord** et sélectionnez le bouton **Tester maintenant**. Si réussi, les utilisateurs et les groupes seront imprimés dans la fenêtre du Connecteur de Répertoire selon les [options de synchronisation](#) et les [filtres](#) spécifiés.

Il peut falloir jusqu'à 15 minutes pour que les autorisations de votre application se propagent correctement. Entre-temps, vous pouvez recevoir des erreurs **Privilèges insuffisants pour terminer l'opération**.

📘 Note

If you get the error message **Resource <user id> does not exist or one of its queried reference-property objects are not present**, you'll need to permanently delete or restore the user(s) with <user id>. **Please note**, this was fixed in a recent version of Directory Connector. Update your application if you're still experiencing this error.

TESTING

You can run tests to see how your directory and sync settings are working. Tests will not sync to your Bitwarden organization.

[🚩 Test Now](#)

Test since the last successful sync

Users

- cap@test.com
- hulksmash@test.com
- ironman76@test.com
- mjolnir_rocks@test.com

Disabled Users

No users to list.

Deleted Users

No users to list.

Groups

- Avengers
 - cap@test.com
 - hulksmash@test.com
 - ironman76@test.com
 - mjolnir_rocks@test.com

Résultats du test de synchronisation

Démarrer la synchronisation automatique

Une fois que les [options de synchronisation](#) et les [filtres](#) sont configurés et testés, vous pouvez commencer à synchroniser. Suivez les étapes suivantes pour commencer la synchronisation automatique avec Directory Connector:

1. Ouvrez l'application de bureau [Directory Connector](#).
2. Naviguez vers l'onglet **Tableau de bord**.
3. Dans la section **Synchroniser**, sélectionnez le bouton **Démarrer la synchronisation**.

Vous pouvez également sélectionner le bouton **Synchroniser maintenant** pour exécuter une synchronisation manuelle unique.

Le connecteur de répertoire commencera à interroger votre répertoire en fonction des [options de synchronisation](#) et des [filtres](#) configurés.

Si vous quittez ou fermez l'application, la synchronisation automatique s'arrêtera. Pour garder Directory Connector en fonctionnement en arrière-plan, minimisez l'application ou cachez-la dans la barre des tâches.

Note

Si vous êtes sur le plan [Teams Starter](#), vous êtes limité à 10 membres. Directory Connector affichera une erreur et arrêtera de synchroniser si vous essayez de synchroniser plus de 10 membres.