

管理者コンソール > ユーザー管理 > ディレクトリ-コネクタ

Microsoft Entra IDと同期

Microsoft Entra IDと同期

この記事は、Directory Connectorを使用して、Microsoft Entra ID DirectoryからのユーザーとグループをBitwarden組織に同期する方法を開始するのに役立ちます。

Microsoft Entra IDディレクトリ設定

Microsoft Azure PortalからDirectory Connectorを設定する前に以下のプロセスを完了してください。ディレクトリコネクタは、これらのプロセスから得られる情報を適切に機能するために必要とします。

アプリ登録を作成する

次の手順を完了して、ディレクトリコネクターのアプリ登録を作成します：

1. あなたのMicrosoft Azureポータルから、**Microsoft Entra ID**ディレクトリに移動してください。
2. 左側のナビゲーションから、**アプリ登録**を選択してください。
3. **新規登録**ボタンを選択し、登録にBitwarden固有の名前（例えば、`bitwarden-dc`）を付けてください。
4. **登録**を選択してください。

アプリの権限を付与する

作成したアプリ登録に必要な権限を付与するための次の手順を完了してください：

1. 作成したBitwardenアプリで、左側のナビゲーションから**API 権限**を選択してください。
2. **権限を追加**ボタンを選択してください。
3. APIを選択するように求められたときは、**Microsoft Graph**を選択してください。
4. 次の**委任された権限**を設定します：
 - ユーザー > User.ReadBasic.All (すべてのユーザーの基本プロフィールを読む)
 - ユーザー > User.Read.All (全ユーザーの完全なプロフィールを読む)
 - グループ > グループ.全て読む (全てのグループを読む)
 - AdministrativeUnit > AdministrativeUnit.Read.All (あなたが**管理ユニット**を同期する場合のみ必要です)
5. 次の**アプリケーションの権限**を設定します：
 - ユーザー > User.Read.All (全ユーザーのフルプロファイルを読む)
 - グループ > グループ.全て読む (全てのグループを読む)
 - AdministrativeUnit > Administrative.Unit.Read.All (**管理ユニット**を同期する場合のみ必要です)
6. API権限ページに戻り、**管理者の同意を求める...**ボタンを選択します。

アプリの秘密鍵を作成する

次の手順を完了して、Directory Connectorで使用する秘密鍵を作成します：

1. 作成されたBitwardenアプリで、左側のナビゲーションから**証明書とシークレット**を選択します。

2. 新しいクライアントシークレットボタンを選択し、Bitwarden特有の説明（例えば、`bitwarden-dc-secret`）と有効期限を追加します。
私たちは決してを選択することをお勧めします。
3. 終了したら、**保存**を選択してください。
4. 秘密の値を後で使用するために安全な場所にコピーしてください。

アプリIDを取得する

次の手順を完了して、ディレクトリコネクタで使用するアプリIDを取得します：

1. 作成されたBitwardenアプリで、左側のナビゲーションから**概要**を選択します。
2. **アプリケーション（クライアント）ID**を安全な場所にコピーして、後で使用するために保存してください。

テナントのホスト名を取得する

次の手順を完了して、ディレクトリコネクタが使用するテナントホスト名を取得します：

1. Azureポータルのどこからでも、右上のナビゲーションバーにある⚙️アイコンを選択してください。
2. メニューの左側にある**ディレクトリ + サブスクリプション**フィルターボタンを選択してください。
3. **現在のディレクトリ:** の値を後で使用するために安全な場所にコピーしてください。

あなたのディレクトリに接続してください

次の手順を完了して、ディレクトリコネクタをMicrosoft Entra IDを使用するように設定します。まだ行っていない場合は、進む前に適切な[Microsoft Entra ID設定](#)の手順を踏んでください：

1. ディレクトリコネクタ**デスクトップアプリ**を開きます。
2. **設定**タブに移動してください。
3. **タイプ**のドロップダウンから、**Azure Active Directory**を選択してください。
このセクションで利用可能なフィールドは、選択したタイプによって変わります。
4. 収集された**テナント ホスト名**、**アプリケーションId**、そして**秘密鍵**を入力してください。

同期オプションを設定する

💡 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](#).

次の手順を完了して、Directory Connectorを使用して同期する際に使用する設定を構成します：

1. ディレクトリコネクタ**デスクトップアプリ**を開きます。

2. **設定**タブに移動してください。

3. **同期**セクションで、必要に応じて以下のオプションを設定します:

オプション	説明
間隔	自動同期チェック間の時間（分単位）。
同期中に無効なユーザーを削除します	あなたのディレクトリで無効にされたユーザーをBitwarden組織から削除するためには、このボックスをチェックしてください。
現在の同期設定に基づいて既存の組織ユーザーを上書きします	このボックスをチェックすると、常にフル同期を実行し、同期されたユーザーセットにいない場合はBitwarden組織からユーザーを削除します。
2000人以上のユーザーまたはグループが同期する予定です。	このボックスをチェックしてください、もし2000以上のユーザーまたはグループを同期する予定がある場合。このボックスをチェックしないと、ディレクトリコネクタは同期を2000ユーザーまたはグループに制限します。
ユーザーを同期する	このボックスをチェックして、ユーザーをあなたの組織と同期させてください。 このボックスをチェックすると、 ユーザーフィルタ を指定することができます。
ユーザーフィルタ	同期フィルタ を指定してください。
グループを同期する	このボックスをチェックして、グループをあなたの組織に同期します。 このボックスをチェックすると、 グループフィルタ を指定できます。
グループフィルタ	同期フィルタ を指定してください。

同期フィルタを指定してください

ユーザーのメールアドレス、グループ名、またはグループのメンバーシップに基づいて、カンマ区切りのリストを使用して同期から含めるか除外します。

ユーザーフィルタ

次のフィルタリング構文は、**ユーザーフィルタ**フィールドで使用する必要があります:

メールアドレスによるユーザーの含める/除く

メールアドレスに基づいて特定のユーザーを同期に含めるか除外するには:

Bash

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

Bash

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

ユーザーはグループメンバーシップによる

`includeGroup` および `excludeGroup` キーワードを使用して、Microsoft Entra IDグループメンバーシップに基づいてユーザーを同期に含めたり除外したりすることができます。 `includeGroup` と `excludeGroup` は、グループの概要ページから利用可能なGroup Object IDを使用します。これは[Azure Portal](#)または[Azure AD Powershell](#)を通じて利用できます。

Bash

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

Bash

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

グループフィルター

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.

次のフィルタリング構文は、**グループフィルタ**フィールドで使用する必要があります：

グループを含む/除外する

グループ名に基づいて、グループを同期に含めるか除外する方法：

Bash

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

Bash

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

管理単位 (AU) ごとにグループ化

タグ付けされた [Microsoft Entra ID 管理ユニット](#) に基づいて、

`includeadministrativeunit` および `excludeadministrativeunit` キーワードを使用して、グループを同期に含めるか除外することができます。
`includeadministrativeunit` および `excludeadministrativeunit` は、管理ユニットの **オブジェクトID** を使用します。

Bash

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

Bash

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

同期をテストする

💡 Tip

同期をテストまたは実行する前に、Directory Connector が正しいクラウドサーバー（例：US または EU）、あるいは自己ホスト型サーバーに接続されていることを確認します。 [デスクトップアプリ](#) または [CLI](#) を使用して、方法を確認します。

Directory Connector があなたのディレクトリに成功裏に接続し、希望のユーザーとグループを返すかどうかをテストするには、**ダッシュボード** タブに移動し、**今すぐテストボタン** を選択します。成功した場合、ユーザーとグループは、指定された [同期オプション](#) と [フィルター](#) に従って、ディレクトリコネクタウィンドウに表示されます。

あなたのアプリケーションの権限が適切に伝播するまでに最大15分かかるかもしれません。その間、あなたは `操作を完了するための権限が不足している` というエラーを受け取るかもしれません。

📌 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

同期のテスト 結果

自動同期を開始します

一度[同期オプション](#)と[フィルター](#)が設定され、テストされたら、同期を開始できます。次の手順を完了して、ディレクトリコネクターとの自動同期を開始します:

1. ディレクトリコネクタ[デスクトップアプリ](#)を開きます。
2. [ダッシュボード](#)タブに移動してください。
3. [同期](#)セクションで、[同期開始](#)ボタンを選択します。

あるいは、一度だけ手動で同期を実行するために、[今すぐ同期](#)ボタンを選択することもできます。

Directory Connectorは、設定された[同期オプション](#)と[フィルター](#)に基づいて、あなたのディレクトリのポーリングを開始します。

アプリケーションを終了または閉じると、自動同期は停止します。ディレクトリコネクタをバックグラウンドで実行し続けるには、アプリケーションを最小化するか、システムトレイに隠してください。

① Note

[Teams Starter](#) プランの場合、メンバーは10人に制限されます。10人以上のメンバーを同期しようすると、Directory Connector はエラーを表示して同期を停止します。

© 2025 Bitwarden Inc | Page 7 of 7