Active Directory または LDAP との同期

Active Directory または LDAP との同期

この記事は、LDAP または Active Directory サービスから Bitwarden 組織にユーザーとグループを同期するための Directory Connector の使用開始に役立ちます。Bitwarden は、以下を含む最も一般的な LDAP ディレクトリサーバー用の組み込みコネクタを提供しています：

- Microsoft Active Directory
- Apache Directory Server (ApacheDS)
- Apple Open Directory
- Fedora Directory Server
- Novell eDirectory
- OpenDS
- OpenLDAP
- Sun Directory Server Enterprise Edition (DSEE)
- 一般的な LDAP ディレクトリサーバー

サーバーへの接続

以下の手順を完了して、LDAP または Active Directory を使用するようDirectory Connector を構成設定します：

1. Directory Connector デスクトップアプリを開きます。
2. **設定 (Settings)** タブに移動します。
3. **タイプ (Type)** のドロップダウンから、**Active Directory / LDAP** を選択します。

   このセクションで利用可能なフィールドは、選択するタイプによって異なります。
4. 次のオプションを構成設定します：

オプション	記述説明	例
サーバーホスト名	ディレクトリサーバーのホスト名。	`ad.example.com`、`ldap.company.org`
サーバーポート	ディレクトリサーバーがリッスンしているポート。	`389` または `10389`
ルートパス	Directory Connector がすべてのクエリを開始するべきルートパス。	`cn=users`、`dc=ad`、`dc=example`、`dc=com`、`dc=ldap`、`dc=company`、`dc=org`
このサーバーはアクティブディレクトリを使用します	サーバーが Active Directory サーバーの場合にこのボックスにチェックマークを入れます。	
このサーバーは検索結果をページングします	サーバーが検索結果をページ分割する場合は、このボックスにチェックを入れます (LDAPのみ) 。	

オプション	記述説明	例
このサーバーは暗号化された接続を使用します	このボックスにチェックマークを入れると、以下のオプションから1つ選択するよう求められます： **SSL を使用（Use SSL）**（LDAPS）LDAPS サーバーが信頼できない証明書を使用している場合、この画面で証明書のオプションを構成設定することができます。 **TSL を使用（Use TSL）**（STARTTLS）LDAP サーバーが STARTTLS 向けの自己署名証明書を使用する場合、この画面で証明書のオプションを構成設定することができます。	
ユーザー名	アプリケーションがディレクトリサーバーに接続する際に使用する、一意の管理ユーザー名。**Active Directory** について、ディレクトリから削除されたユーザーの状態を同期する場合、ユーザーはビルトインの管理者グループのメンバーであることが必要です。	
パスワード	上記のユーザーのパスワード。パスワードは、オペレーティングシステムのネイティブ資格情報マネージャーに安全に保管されています。	

同期オプションの構成設定

> **Tip**
> 構成設定が完了したら、**その他（More）**のタブに移動し、**同期キャッシュをクリア（Clear Sync Cache）**ボタンを選択して以前の同期操作との潜在的な相反が生じないようにします。詳細については、同期キャッシュをクリア（Clear Sync Cache）を確認します。

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

> **Note**
> Active Directory を使用している場合、これらの設定の大半は、あらかじめ決定されていることから表示されません。

1. Directory Connector デスクトップアプリを開きます。
2. **設定（Settings）**タブに移動します。
3. **同期（Sync）**セクションで、必要に応じて以下のオプションを構成設定します：

オプション	記述説明
間隔	自動同期チェックの間隔（分単位）。
同期中に無効なユーザーを削除します	このボックスにチェックマークを入れると、組織で無効化されたユーザーが Bitwarden 組織から削除されます。
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	このボックスにチェックマークを入れると、ディレクトリユーザーセットから不在のユーザーを組織から削除するなど、各同期でユーザーセットが完全に上書きされます。 **何らかの理由でこのオプションが有効な状態で空の同期が実行されると、Directory Connector はすべてのユーザーを削除します。**

オプション	記述説明
	このオプションを有効にした上で同期する前に、必ずテスト同期を実行してください。
2000人を超える数のユーザーまたはグループが同期されることが予想されます。	2000人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は、 このボックスにチェックマークを入れてください。 このボックスにチェックマークが入っていないと、Directory Connector は同期を2000人のユーザーまたはグループに制限します。
メンバー属性	グループのメンバー資格を定義するためにディレクトリによって使用される属性の名称（例：`uniqueMember`）。
作成データ属性	エントリが作成された時点を指定するためにディレクトリによって使用される属性の名称（例：`whenCreated`）。
改訂日属性	エントリが最後に変更された時点を指定するためにディレクトリによって使用される属性の名称（例：`whenChanged`）。
ユーザーがEメールアドレスを持っていない場合、 ユーザー名の接頭辞と接尾辞の値を組み合わせてEメールアドレスを作成します。	このボックスにチェックマークを入れ、 Eメールアドレスを持っていないユーザー用に有効なEメールアドレスのオプションを作成します。 **実際の、または作成済みのEメールアドレスを持たないユーザーは Directory Connector によってスキップされます。** 作成済みのEメールアドレス = **Eメールの接頭辞属性** + **Eメールの接尾辞**
Eメール接頭辞属性	作成済みのEメールの接尾辞を作成するために使用される属性。
Eメールの接尾辞	作成済みEメールアドレス用の接尾辞を作成するために使用される文字列（`@example.com`）。
ユーザーの同期	このボックスにチェックマークを入れ、ユーザーを組織と同期させます。 このボックスにチェックマークを入れると、**ユーザーフィルター（User Filter）**、**ユーザーパス（User Path）**、**ユーザーオブジェクトクラス（User Object Class）**、そして**ユーザーEメール属性（User Email Attribute）**を指定することができます。
ユーザーフィルター	同期フィルターを指定（Specify sync filters）を確認します。
ユーザーパス	ユーザーを検索するための、指定された**ルートパス（Root Path）**と一緒に使用される属性（例：`ou=users`）。値が提供されない場合、サブツリーの検索はルートパスから開始されます。
ユーザーオブジェクトクラス	LDAP ユーザーオブジェクトに使用されるクラスの名称（例：`ユーザー`）。
ユーザーのEメール属性	ユーザーの保存されたEメールアドレスを読み込むために使用される属性。
グループの同期	このボックスにチェックマークを入れて、グループを組織と同期します。 このボックスにチェックマークを入れると、**グループフィルター（Group Filter）**、**グループパス**

オプション	記述説明
	（Group Path）、**グループオブジェクトクラス（Group Object Class）**、**グループ名属性（Group Name Attribute）**を指定することができます。
グループフィルター	同期フィルターを指定（Specify sync filters）を確認します。
グループパス	グループを検索するための、指定された**ルートパス**と一緒に使用される属性（例：`ou=groups`）。値が提供されない場合、サブツリーの検索はルートパスから開始されます。
グループオブジェクトクラス	LDAP グループオブジェクトに使用されるクラスの名称（例：`groupOfUniqueNames`）。
グループ名属性	グループの名前を定義するためにディレクトによって使用される属性の名称（例：`名称`）。

同期フィルターの指定

ユーザーとグループのフィルターは、任意の LDAP 互換検索フィルターの形式の場合があります。

Active Directory は、標準的な LDAP の指示や指令と異なり、検索フィルターを書き込むためのいくつかの高度なオプションと制限を用意します。Active Directory の検索フィルターの書き込みについては、こちら。

> **Note**
> ネストされたグループは、Directory Connector 内の単一の参照先で複数のグループオブジェクトを同期することができます。これを行うには、メンバーが他のグループであるグループを作成します。

サンプル

`objectClass=user`、および `cn`（一般名）（`マーケティング（Marketing）`を含む）を備えたすべてのエントリについて同期をフィルタリングするには：

```
Bash

(&(objectClass=user)(cn=*Marketing*))
```

（**LDAP のみ**）`ou`（組織単位）のコンポーネントが `dn`（識別名）（`マイアミ（Miami）`または`オーランド（Orlando）のいずれか）`を備えたすべてのエントリについて同期をフィルタリングするには：

```
Bash

(|(ou:dn:=Miami)(ou:dn:=Orlando))
```

（**LDAP のみ**）たとえば、すべての `ou=Chicago` エントリ（ou=Wrigleyville 属性にも一致するもの`を除く）`などの式に一致するエンティティを除外するには：

```
Bash

(&(ou:dn:=Chicago)(!(ou:dn:=Wrigleyville)))
```

（**AD のみ**）`ヒーロー（Heroes）`グループのユーザー向けに同期をフィルタリングするには：

```
Bash

(&(objectCategory=Person)(sAMAccountName=*)(memberOf=cn=Heroes,ou=users,dc=company,dc=com))
```

（**AD のみ**）ディレクトリまたはネストのいずれか経由で、`ヒーロー（Heroes）`グループのメンバーであるユーザー向けに同期をフィルタリングするには：

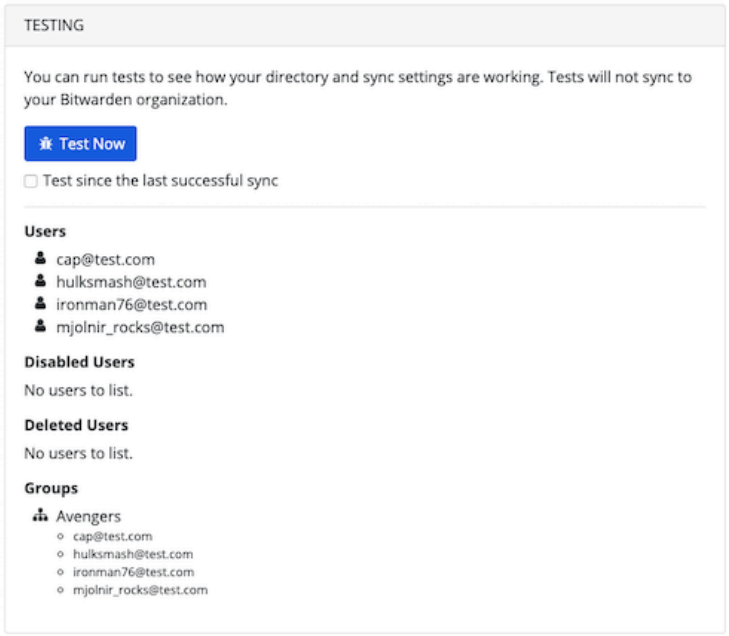
```
Bash

(&(objectCategory=Person)(sAMAccountName=*)(memberOf:1.2.840.113556.1.4.1941:=cn=Heroes,ou=users,dc=company,dc=com))
```

同期のテスト

> **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 がディレクトリに正常に接続し、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（Dashoboard）**タブに移動して**今すぐテスト（Test Now）**ボタンを選択します。上手く行った場合、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、Directory Connector ウィンドウにプリントされます：



同期のテスト 結果

自動同期の開始

いったん同期オプションとフィルターが構成設定されてテストされたら、同期を開始できます。以下の手順を完了して、Directory Connector との自動同期を開始します：

1. Directory Connector デスクトップアプリケーションを開きます。
2. **ダッシュボード（Dashboard）**タブに移動します。
3. **同期（Sync）**セクションで、**同期開始（Start Sync）**ボタンを選択します。

   または、1回のみの手動同期を実行するために、**今すぐ同期（Sync Now）**ボタンを選択しても構いません。

Directory Connector は、構成設定された同期オプションとフィルターに基づいて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したり閉じると、自動同期が停止します。Directory Connector 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ます。

> **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とすると、Directory Connector はエラーを表示して同期を停止します。

Active Directory との同期 トラブルシューティング

Active Directory インスタンスから同期する際に値の上限に達しました：

Active Directory の `MaxValRange` は、デフォルトでの設定が1500です。グループの `メンバー` などの属性に1500を超える値がある場合、Active Directory は空の `メンバー` 属性、および `MaxValRange` の値を上限とする、別の属性上の切り捨てられた `メンバー` のリストの両方を返します。

- Active Directory の最大グループのメンバー数よりも高い値に `MaxValRange` ポリシーを調節することができます。ntdsutil.exe ユーティリティを使用して Active Directory LDAP ポリシーの設定にあたっての Microsoft ドキュメンテーションを参照してください。