bitwarden | Hilfezentrum Artikel

ADMINISTRATOR KONSOLE > BENUTZERVERWALTUNG >

Synchronisation mit Microsoft Entra ID

Ansicht im Hilfezentrum:
https://bitwarden.com/help/microsoft-entra-id/

Synchronisation mit Microsoft Entra ID

Dieser Artikel wird Ihnen helfen, den Directory Connector zu verwenden, um Benutzer und Gruppen aus Ihrem Microsoft Entra ID-Verzeichnis mit Ihrer Bitwarden Organisation zu synchronisieren.

Microsoft Entra ID Verzeichniseinrichtung

Vervollständigen Sie die folgenden Prozesse aus dem Microsoft Azure Portal, bevor Sie den Directory Connector konfigurieren. Der Directory Connector benötigt Informationen, die aus diesen Prozessen gewonnen wurden, um ordnungsgemäß zu funktionieren.

App-Registrierung erstellen

Führen Sie die folgenden Schritte aus, um eine App-Registrierung für den Directory Connector zu erstellen:

1. Von Ihrem Microsoft Azure-Portal aus navigieren Sie zum **Microsoft Entra ID**-Verzeichnis.
2. Wählen Sie aus der linken Navigation **App-Registrierungen** aus.
3. Wählen Sie die Schaltfläche **Neue Registrierung** und geben Sie Ihrer Registrierung einen Bitwarden-spezifischen Namen (wie zum Beispiel `bitwarden-dc`).
4. Wählen Sie **Registrieren**.

App-Berechtigungen gewähren

Führen Sie die folgenden Schritte aus, um der erstellten App-Registrierung die erforderlichen Berechtigungen zu gewähren:

1. Wählen Sie in der erstellten Bitwarden-App **API-Berechtigungen** aus der linken Navigation aus.
2. Wählen Sie die Schaltfläche **Berechtigung hinzufügen**.
3. Wenn Sie aufgefordert werden, eine API auszuwählen, wählen Sie **Microsoft Graph**.
4. Setzen Sie die folgenden **Delegierten Berechtigungen**:
   - Benutzer > Benutzer.LesenBasis.Alle (Lese alle grundlegenden Benutzerprofile)
   - Benutzer > Benutzer.Lesen.Alle (Lese alle vollständigen Profile der Benutzer)
   - Gruppe > Gruppe.Lesen.Alle (Alle Gruppen lesen)
   - AdministrativeUnit > AdministrativeUnit.Read.All (Nur erforderlich, wenn Sie Administrative Einheiten zur Synchronisation verwenden)
5. Setzen Sie die folgenden **Anwendungsberechtigungen**:
   - Benutzer > Benutzer.Lesen.Alle (Lese alle vollständigen Profile der Benutzer)
   - Gruppe > Gruppe.Lesen.Alle (Alle Gruppen lesen)
   - Verwaltungseinheit > Verwaltungseinheit.Lesen.Alle (Nur erforderlich, wenn Sie eine Synchronisation der Verwaltungseinheiten durchführen werden)
6. Zurück auf der API-Berechtigungsseite, wählen Sie die Schaltfläche **Administrator-Berechtigung erteilen für...**.

App geheimer Schlüssel erstellen

Führen Sie die folgenden Schritte aus, um einen geheimen Schlüssel zu erstellen, der vom Directory Connector verwendet wird:

1. In der erstellten Bitwarden-App wählen Sie **Zertifikate & Geheimnisse** aus der linken Navigation aus.
2. Wählen Sie die Schaltfläche **Neues Client-Geheimnis** und fügen Sie eine Bitwarden-spezifische Beschreibung (wie zum Beispiel `bitwarden-dc-secret`) und ein Ablaufdatum hinzu. Wir empfehlen die Auswahl von **Nie**.
3. Wählen Sie **Speichern**, sobald Sie fertig sind.
4. Kopieren Sie den **Wert** des Geheimnisses zur späteren Verwendung an einen sicheren Ort.

Holen Sie sich die App-ID

Führen Sie die folgenden Schritte aus, um die App-ID zu erhalten, die vom Directory Connector verwendet werden soll:

1. In der erstellten Bitwarden-App wählen Sie **Übersicht** aus der linken Navigation aus.
2. Kopieren Sie die **Anwendungs- (Client) ID** an einen sicheren Ort für die spätere Verwendung.

Mieter-Hostname abrufen

Führen Sie die folgenden Schritte aus, um den Mieter-Hostname zu erhalten, der vom Directory Connector verwendet werden soll:

1. Wählen Sie von überall im Azure-Portal das ⚙ Symbol in der oberen rechten Navigationsleiste aus.
2. Wählen Sie im Menü links die Schaltfläche **„Verzeichnis + Abonnementfilter** “ aus.
3. Kopieren Sie den Wert des **Aktuellen Verzeichnisses:** an einen sicheren Ort für die spätere Verwendung.

Verbinden Sie sich mit Ihrem Verzeichnis

Führen Sie die folgenden Schritte aus, um den Directory Connector für die Verwendung von Microsoft Entra ID zu konfigurieren. Wenn Sie es noch nicht getan haben, führen Sie die entsprechenden Schritte zur Einrichtung der Microsoft Entra ID durch, bevor Sie fortfahren:

1. Öffnen Sie die Directory Connector Desktop-App.
2. Navigieren Sie zum **Einstellungen** Tab.
3. Wählen Sie aus dem Dropdown-Menü **Typ** die Option **Azure Active Directory** aus.

   Die verfügbaren Felder in diesem Abschnitt ändern sich je nach Ihrem ausgewählten Typ.
4. Geben Sie den gesammelten Mieter Hostname, Anwendungs-ID, und Geheimer Schlüssel ein.

Konfigurieren Sie die Synchronisationsoptionen

> **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.

Führen Sie die folgenden Schritte aus, um die Einstellungen zu konfigurieren, die verwendet werden, wenn die Synchronisation mit dem Directory Connector durchgeführt wird:

1. Öffnen Sie die Directory Connector Desktop-App.

2. Navigieren Sie zum **Einstellungen** Tab.

3. Im Abschnitt **Synchronisation** konfigurieren Sie die folgenden Optionen nach Wunsch:

Option	Beschreibung
Intervall	Zeit zwischen automatischen Synchronisationsprüfungen (in Minuten).
Entfernen Sie deaktivierte Benutzer während der Synchronisation	Markieren Sie dieses Kästchen, um Benutzer aus der Bitwarden Organisation zu entfernen, die in Ihrem Verzeichnis deaktiviert wurden.
Überschreiben Sie vorhandene Benutzer der Organisation basierend auf den aktuellen Synchronisationseinstellungen	Markieren Sie dieses Kästchen, um immer eine vollständige Synchronisation durchzuführen und alle Benutzer aus der Bitwarden Organisation zu entfernen, wenn sie nicht im synchronisierten Benutzersatz enthalten sind.
Es wird erwartet, dass mehr als 2000 Benutzer oder Gruppen eine Synchronisation durchführen.	Markieren Sie dieses Kästchen, wenn Sie erwarten, 2000+ Benutzer oder Gruppen zu synchronisieren. Wenn Sie dieses Kästchen nicht ankreuzen, wird der Directory Connector eine Synchronisation auf 2000 Benutzer oder Gruppen beschränken.
Benutzer synchronisieren	Markieren Sie dieses Kästchen, um Benutzer mit Ihrer Organisation zu synchronisieren. Wenn Sie dieses Kästchen ankreuzen, können Sie **Benutzerfilter** festlegen.
Benutzerfilter	Siehe Synchronisationsfilter festlegen.
Synchronisationsgruppen	Markieren Sie dieses Kästchen, um Gruppen mit Ihrer Organisation zu synchronisieren. Wenn Sie dieses Kästchen ankreuzen, können Sie **Gruppenfilter** festlegen.
Gruppenfilter	Siehe Synchronisationsfilter festlegen.

Spezifizieren Sie Synchronisationsfilter

Verwenden Sie durch Kommas getrennte Listen, um auf Basis der Benutzer-E-Mail-Adresse, des Gruppennamens oder der Gruppenmitgliedschaft eine Synchronisation einzuschließen oder auszuschließen.

Benutzerfilter

Die folgenden Filter-Syntaxen sollten im Feld **Benutzerfilter** verwendet werden:

Benutzer per E-Mail-Adresse einbeziehen/ausschließen

Um bestimmte Benutzer auf Basis der E-Mail-Adresse in eine Synchronisation einzubeziehen oder auszuschließen:

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

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

Benutzer nach Gruppenmitgliedschaft

Sie können Benutzer auf Basis ihrer Microsoft Entra ID Gruppenmitgliedschaft in eine Synchronisation einbeziehen oder ausschließen, indem Sie die Schlüsselwörter `includeGroup` und `excludeGroup` verwenden. `includeGroup` und `excludeGroup` verwenden die Gruppenobjekt-ID, die auf der **Übersichts**seite der Gruppe im Azure Portal oder über das Azure AD Powershell verfügbar ist:

```Bash
includeGroup:963b5acd-9540-446c-8e99-29d68fcba8eb,9d05a51c-f173-4087-9741-a7543b0fd3bc
```

```Bash
excludeGroup:963b5acd-9540-446c-8e99-29d68fcba8eb,9d05a51c-f173-4087-9741-a7543b0fd3bc
```

Gruppenfilter

> **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.

Die folgenden Filter-Syntaxen sollten im Feld **Gruppenfilter** verwendet werden:

Gruppen einbeziehen/ausschließen

Um Gruppen basierend auf dem Gruppennamen in eine Synchronisation einzubeziehen oder auszuschließen:

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

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

Gruppieren nach Verwaltungseinheit (AU)

Sie können Gruppen auf Basis ihrer markierten Microsoft Entra ID Verwaltungseinheiten in eine Synchronisation einbeziehen oder ausschließen, indem Sie die Schlüsselwörter `includeadministrativeunit` und `excludeadministrativeunit` verwenden. `includeadministrativeunit` und `excludeadministrativeunit` verwenden die **Objekt ID** der Verwaltungseinheit:

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

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

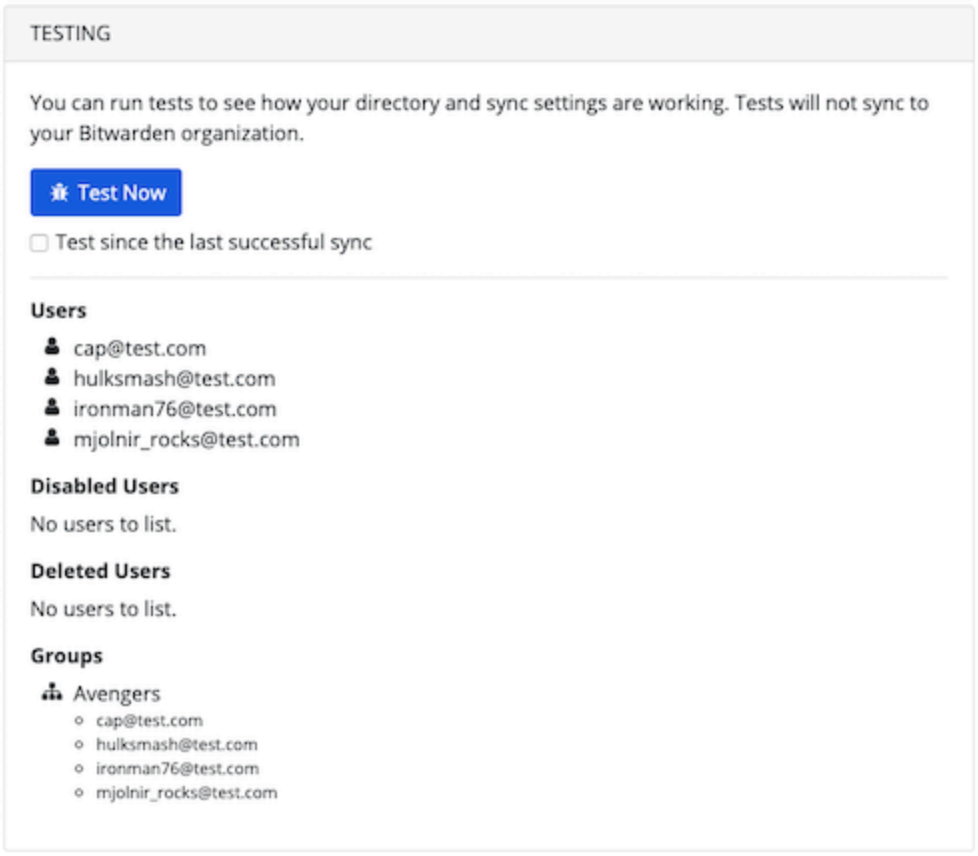
Testen Sie eine Synchronisation

> **Tip**
>
> Bevor Sie eine Synchronisation testen oder ausführen, überprüfen Sie, ob der Directory Connector mit dem richtigen Cloud-Server (z. B. US oder EU) oder selbst gehostetem Server verbunden ist. Erfahren Sie, wie Sie dies mit der Desktop-App oder CLI machen können.

Um zu testen, ob der Directory Connector erfolgreich eine Verbindung zu Ihrem Verzeichnis herstellt und die gewünschten Benutzer und Gruppen zurückgibt, navigieren Sie zum **Dashboard** Tab und wählen Sie die **Jetzt testen** Schaltfläche aus. Wenn erfolgreich, werden Benutzer und Gruppen gemäß den angegebenen Synchronisationsoptionen und Filtern im Directory Connector-Fenster angezeigt.

Es kann bis zu 15 Minuten dauern, bis die Berechtigungen für Ihre Anwendung richtig verbreitet sind. In der Zwischenzeit können Sie möglicherweise `Unzureichende Berechtigungen zur Durchführung der Operation` Fehler erhalten.

> **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.



Testergebnisse der Synchronisation

Starten Sie die automatische Synchronisation

Sobald die Synchronisationsoptionen und Filter konfiguriert und getestet sind, können Sie mit der Synchronisation beginnen. Führen Sie die folgenden Schritte aus, um die automatische Synchronisation mit dem Directory Connector zu starten:

1. Öffnen Sie die Directory Connector Desktop-App.
2. Navigieren Sie zum **Dashboard** Tab.
3. Im Abschnitt **Synchronisation**, wählen Sie die Schaltfläche **Synchronisation starten**.

   Sie können alternativ die Schaltfläche **Jetzt synchronisieren** auswählen, um eine einmalige manuelle Synchronisation auszuführen.

Der Directory Connector beginnt mit dem Abfragen Ihres Verzeichnisses basierend auf den konfigurierten Synchronisationsoptionen und Filtern.

Wenn Sie die Anwendung beenden oder schließen, wird die automatische Synchronisation gestoppt. Um den Directory Connector im Hintergrund laufen zu lassen, minimieren Sie die Anwendung oder verstecken Sie sie im Infobereich.

> **Note**
>
> Wenn Sie den Teams Starter-Tarif haben, sind Sie auf 10 Mitglieder begrenzt. Der Directory Connector zeigt einen Fehler an und stoppt die Synchronisation, wenn Sie versuchen, mehr als 10 Mitglieder zu synchronisieren.