Synchronisation mit Active Directory oder LDAP

Synchronisation mit Active Directory oder LDAP

Dieser Artikel hilft Ihnen bei der Verwendung des Directory Connectors, um Benutzer und Gruppen aus Ihrem LDAP oder Active Directory Dienst mit Ihrer Bitwarden Organisation zu synchronisieren. Bitwarden bietet integrierte Connectors für die beliebtesten LDAP-Verzeichnisserver, einschließlich:

- Microsoft Active Directory
- Apache Directory Server (ApacheDS)
- Apple Open Directory
- Fedora Directory Server
- Novell eDirectory
- OpenDS
- OpenLDAP
- Sun Directory Server Enterprise Edition (DSEE)
- Jeder generische LDAP Directory Server

Verbinden Sie sich mit Ihrem Server

Führen Sie die folgenden Schritte aus, um den Directory Connector für die Verwendung Ihres LDAP oder Active Directory zu konfigurieren:

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

   Die verfügbaren Felder in diesem Abschnitt ändern sich je nach Ihrem ausgewählten Typ.
4. Konfigurieren Sie die folgenden Optionen:

Option	Beschreibung	Beispiele
Server Hostname	Hostname Ihres Verzeichnisservers.	`ad.beispiel.com`, `ldap.firma.org`
Server Port	Port, auf dem Ihr Verzeichnisserver lauscht.	`389` oder `10389`

Option	Beschreibung	Beispiele
Root-Pfad	Stammverzeichnispfad, in dem Directory Connector alle Abfragen starten sollte.	`cn=users`, `dc=ad`, `dc=example`, `dc=com`, `dc=ldap`, `dc=company`, `dc=org`
Dieser Server verwendet Active Directory.	Markieren Sie dieses Kästchen, wenn der Server ein Active Directory Server ist.	
Dieser Server paginiert Suchergebnisse	Markieren Sie dieses Kästchen, wenn der Server Suchergebnisse paginiert (nur LDAP).	
Dieser Server verwendet eine verschlüsselte Verbindung.	Wenn Sie dieses Kästchen ankreuzen, werden Sie aufgefordert, eine der folgenden Optionen auszuwählen: **Verwenden Sie SSL** (LDAPS) Wenn Ihr LDAPS-Server ein nicht vertrauenswürdiges Zertifikat verwendet, können Sie auf diesem Bildschirm Zertifikatsoptionen konfigurieren. **Verwenden Sie TSL** (STARTTLS) Wenn Ihr LDAP-Server ein selbstsigniertes Zertifikat für STARTTLS verwendet, können Sie auf diesem Bildschirm Zertifizierungsoptionen konfigurieren.	
Benutzername	Der Distinguished Name eines administrativen Benutzers, den die Anwendung bei der Verbindung mit dem Verzeichnisserver verwenden wird. Für **Active Directory**, wenn die Synchronisation des Status von Benutzern gewünscht ist, die aus dem Verzeichnis entfernt wurden, sollte der Benutzer ein Mitglied der eingebauten Administratorgruppe sein.	
Passwort	Das Passwort des oben genannten Benutzers. Das Kennwort wird sicher in der systemeigenen Anmeldeinformationsverwaltung des Betriebssystems gespeichert.	

Synchronisationsoptionen konfigurieren

> **Tip**
> Wenn Sie mit der Konfiguration fertig sind, navigieren Sie zum Tab **Mehr** und wählen Sie die Schaltfläche **Synchronisations-Cache löschen**, um mögliche Konflikte mit vorherigen Synchronisationsoperationen zu vermeiden. Für weitere Informationen, siehe Synchronisations-Cache leeren.

Führen Sie die folgenden Schritte aus, um die Einstellungen zu konfigurieren, die bei der Synchronisation mit dem Directory Connector verwendet werden:

> **Note**
> Wenn Sie Active Directory verwenden, sind viele dieser Einstellungen für Sie voreingestellt und werden daher nicht angezeigt.

1. Öffnen Sie die Directory Connector Desktop-App.
2. Navigieren Sie zum Tab **Einstellungen**.
3. Im Abschnitt **Synchronisation** konfigurieren Sie die folgenden Optionen nach Wunsch:

Option	Beschreibung
Intervall	Zeit zwischen automatischer Synchronisationsprüfung (in Minuten).
Deaktivierte Benutzer während der Synchronisation entfernen	Markieren Sie dieses Kästchen, um Benutzer aus der Bitwarden Organisation zu entfernen, die in Ihrer Organisation deaktiviert wurden.
Überschreiben Sie vorhandene Benutzer der Organisation basierend auf den aktuellen Synchronisationseinstellungen	Aktivieren Sie dieses Kontrollkästchen, um den Benutzersatz bei jeder Synchronisierung vollständig zu überschreiben, einschließlich des Entfernens von Benutzern aus Ihrer Organisation, wenn sie nicht mehr im Verzeichnisbenutzersatz enthalten sind. **Wenn aus irgendeinem Grund eine leere Synchronisation durchgeführt wird, während diese Option aktiviert ist, wird der Directory Connector alle Benutzer entfernen.** Führen Sie immer eine Test-Synchronisation durch, bevor Sie nach Aktivierung dieser Option eine Synchronisation durchführen.

Option	Beschreibung
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.
Mitglieds-Attribut	Name des Attributs, das vom Verzeichnis verwendet wird, um die Mitgliedschaft einer Gruppe zu definieren (zum Beispiel `uniqueMember`).
Erstellungsdatums-Attribut	Name des Attributs, das vom Verzeichnis verwendet wird, um anzugeben, wann ein Eintrag erstellt wurde (zum Beispiel `whenCreated`).
Revisionsdatums-Attribut	Name des Attributs, das vom Verzeichnis verwendet wird, um anzugeben, wann ein Eintrag zuletzt geändert wurde (zum Beispiel `whenChanged`).
Wenn ein Benutzer keine E-Mail-Adresse hat, kombinieren Sie ein Benutzernamen-Präfix mit einem Suffix-Wert, um eine E-Mail-Adresse zu bilden.	Markieren Sie dieses Kästchen, um gültige E-Mail-Optionen für Benutzer zu erstellen, die keine E-Mail-Adresse haben. **Benutzer ohne echte oder gebildete E-Mail-Adressen werden vom Directory Connector übersprungen.** Gebildete E-Mail-Adresse = **E-Mail-Präfix-Attribut**+ **E-Mail-Suffix**
E-Mail-Präfix-Attribut	Attribut, das verwendet wird, um ein Präfix für gebildete E-Mail-Adressen zu erstellen.
E-Mail-Suffix	Ein String (`@example.com`), der verwendet wird, um ein Suffix für gebildete E-Mail-Adressen zu erstellen.

Option	Beschreibung
Benutzer synchronisieren	Markieren Sie dieses Kästchen, um Benutzer mit Ihrer Organisation zu synchronisieren. Wenn Sie dieses Kästchen ankreuzen, können Sie einen **Benutzerfilter**, einen **Benutzerpfad**, eine **Benutzerobjektklasse** und ein **Benutzer-E-Mail-Attribut** festlegen.
Benutzerfilter	Siehe Synchronisationsfilter festlegen.
Benutzerpfad	Attribut, das mit dem angegebenen **Root-Pfad** verwendet wird, um nach Benutzern zu suchen (zum Beispiel `ou=Benutzer`). Wenn kein Wert angegeben wird, beginnt die Suche im Subtree vom Root-Pfad aus.
Benutzerobjektklasse	Name der Klasse, die für das LDAP-Benutzerobjekt verwendet wird (zum Beispiel `Benutzer`).
Benutzer E-Mail-Attribut	Attribut, das verwendet wird, um die gespeicherte E-Mail-Adresse eines Benutzers zu laden.
Gruppen-Synchronisation	Markieren Sie dieses Kästchen, um Gruppen mit Ihrer Organisation zu synchronisieren. Durch Ankreuzen dieses Kästchens können Sie einen **Gruppenfilter**, **Gruppenpfad**, **Gruppenobjektklasse**, **Gruppennamenattribut** festlegen.
Gruppenfilter	Siehe Synchronisationsfilter festlegen.
Gruppenpfad	Attribut, das mit dem angegebenen **Root-Pfad** verwendet wird, um nach Gruppen zu suchen (zum Beispiel `ou=Gruppen`). Wenn kein Wert angegeben wird, beginnt die Suche im Subtree vom Root-Pfad aus.

Option	Beschreibung
Gruppenobjektklasse	Name der Klasse, die für das LDAP-Gruppenobjekt verwendet wird (zum Beispiel `groupOfUniqueNames`).
Gruppennamenattribut	Name des Attributs, das vom Verzeichnis zur Definition des Namens einer Gruppe verwendet wird (zum Beispiel `Name`).

Synchronisationsfilter festlegen

Benutzer- und Gruppenfilter können in Form eines beliebigen LDAP-kompatiblen Suchfilters vorliegen.

Active Directory bietet einige erweiterte Optionen und Einschränkungen beim Schreiben von Suchfiltern im Vergleich zu standardmäßigen LDAP-Richtlinien. Hier Erfahren Sie mehr über das Schreiben von Active Directory-Suchfiltern.

> **ⓘ Note**
>
> Verschachtelte Gruppen können mehrere Gruppenobjekte mit einem einzigen Referenten im Directory Connector durch Synchronisation abgleichen. Erstellen Sie dazu eine Gruppe, deren Mitglieder andere Gruppen sind.

Samples

Um eine Synchronisation für alle Einträge zu filtern, die `objectClass=user` und `cn` (common name) haben, die `Marketing` enthält:

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

(**Nur-LDAP**) Um eine Synchronisation für alle Einträge zu filtern, bei denen eine `ou` (Organisationseinheit) Komponente ihres `dn` (distinguished name) entweder `Miami` oder `Orlando` ist:

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

(**Nur-LDAP**) Um Entitäten auszuschließen, die einem Ausdruck entsprechen, zum Beispiel alle `ou=Chicago` Einträge *außer* denen, die auch einem `ou=Wrigleyville` Attribut entsprechen:

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

(**Nur AD**) Um eine Synchronisation für Benutzer in der `Heroes` Gruppe zu filtern:

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

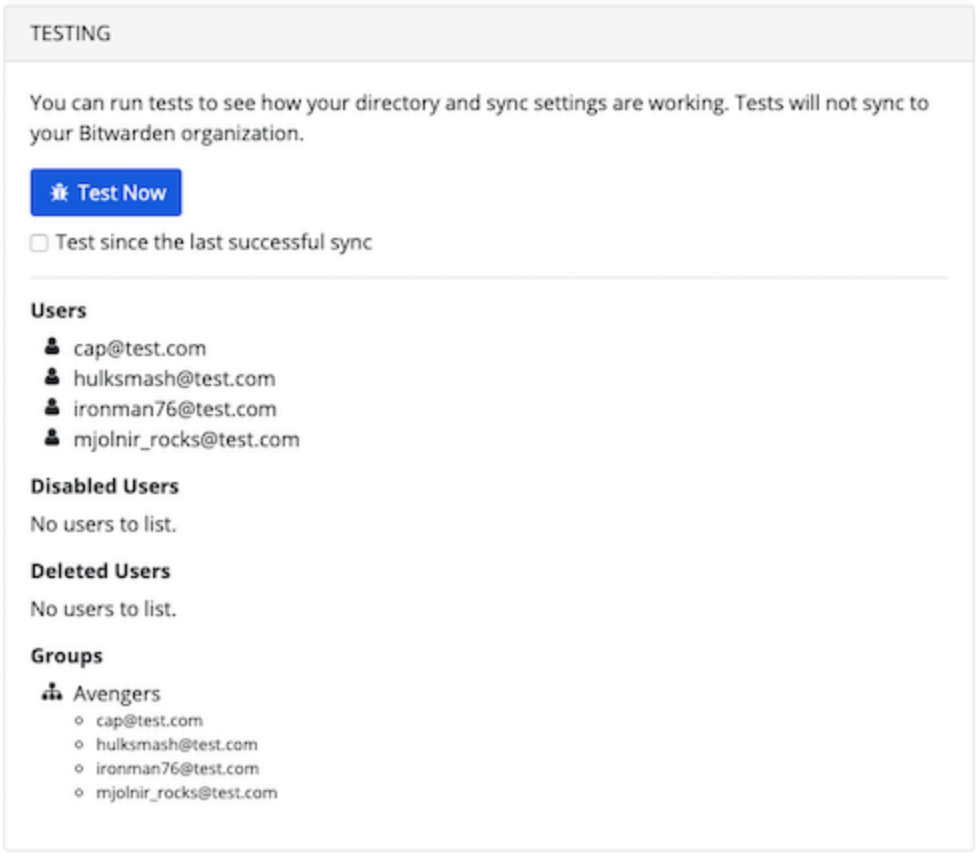
(**Nur AD**) Um eine Synchronisation für Benutzer zu filtern, die Mitglieder der `Heroes` Gruppe sind, entweder über das Verzeichnis oder durch Nesting:

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

Eine Synchronisation testen

> **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 ausgibt, navigieren Sie zum **Dashboard**-Tab und wählen Sie die Schaltfläche **Jetzt testen** aus. Wenn erfolgreich, werden Benutzer und Gruppen gemäß den angegebenen Synchronisationsoptionen und Filtern im Directory Connector-Fenster angezeigt:



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. Wählen Sie im Abschnitt **Synchronisation** 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 Directory Connector im Hintergrund laufen zu lassen, minimieren Sie die Anwendung oder verbergen Sie sie in der Taskleiste.

> **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.

Synchronisation mit Active Directory: Fehlerbehebung

Wertgrenze bei der Synchronisierung aus einer Active Directory-Instanz erreicht:

Der Active Directory `MaxValRange` hat eine Standardeinstellung von 1500. Wenn ein Attribut, z. B. `Mitglieder` in einer Gruppe, mehr als 1500 Werte hat, gibt Active Directory sowohl ein leeres Mitgliederattribut als auch eine abgeschnittene Liste von `Mitgliedern` in separaten Attributen bis zum Wert von MaxValRange `zurück`.

- Sie können die `MaxValRange` Richtlinie auf einen Wert einstellen, der höher ist als die Nummer der Mitglieder Ihrer größten Gruppe im Active Directory. Lesen Sie in der Microsoft-Dokumentation nach, wie Sie Active Directory-LDAP-Richtlinien mithilfe des Dienstprogramms ntdsutll.exe festlegen.