

BEHEERCONSOLE > GEBRUIKERSBEHEER >

Synchroniseren met Actieve Directory (AD) of LDAP

Synchroniseren met Actieve Directory (AD) of LDAP

Dit artikel helpt u op weg met Directory Connector voor het synchroniseren van gebruikers en groepen vanuit uw LDAP- of Actieve Directory (AD)-service naar uw Bitwarden-organisatie. Bitwarden biedt ingebouwde connectoren voor de populairste LDAP-directoryservers, waaronder:

- Microsoft Actieve Directory
- Apache Directory Server (ApacheDS)
- Apple open directory
- Fedora Directory Server
- Novell eDirectory
- OpenDS
- OpenLDAP
- Sun Directory Server Enterprise Editie (DSEE)
- Elke algemene LDAP-directoryserver

Maak verbinding met uw server

Voer de volgende stappen uit om Directory Connector te configureren om uw LDAP of Actieve Directory (AD) te gebruiken:

1. Open de Directory Connector [desktop app](#).
2. Navigeer naar het tabblad **Instellingen**.
3. In de dropdownlijst **Type** selecteert u **Actieve Directory / LDAP**.

De beschikbare velden in dit gedeelte veranderen afhankelijk van het geselecteerde type.

4. Configureer de volgende opties:

Optie	Beschrijving	Voorbeelden
Server hostnaam	Hostnaam van uw mapserver.	<code>ad.example.com</code> , <code>ldap.company.org</code>
Serverpoort	Poort waarop u directory server luistert.	<code>389</code> of <code>10389</code>
Root Path	Root path waarop Directory Connector alle query's moet starten.	<code>cn=users, dc=ad, dc=example, dc=com, dc=ld</code>

Optie	Beschrijving	Voorbeelden
Deze server gebruikt Actieve Directory (AD)	Vink dit vakje aan als de server een Actieve Directory (AD)-server is.	ap, dc=company, dc=org
Deze server geeft zoekresultaten weer	Vink dit vakje aan als de server zoekresultaten pagineert (alleen LDAP).	
Deze server gebruikt een versleutelde verbinding	Als u dit vakje aanvinkt, wordt u gevraagd een van de volgende opties te selecteren: SSL gebruiken (LDAPS) Als uw LDAPS-server een niet-vertrouwd certificaat gebruikt, kunt u op dit scherm certificaatopties configureren. TSL gebruiken (STARTTLS) Als u LDAP-server een zelfondertekend certificaat voor STARTTLS gebruikt, kunt u op dit scherm certificeringsopties configureren.	
Gebruikersnaam	De gedistingeerde naam van een administratieve gebruiker die de toepassing zal gebruiken bij het verbinden met de directoryserver. Voor Actieve Directory (AD) , als het synchroniseren van de status van gebruikers die verwijderd zijn uit de directory gewenst is, moet de gebruiker lid zijn van de ingebouwde beheerdersgroep.	
Wachtwoord	Het wachtwoord van de gebruiker die hierboven is opgegeven. Het wachtwoord wordt veilig opgeslagen in de wachtwoordmanager van het eigen besturingssysteem.	

Synchronisatie-opties configureren



Als u klaar bent met configureren, navigeer dan naar het tabblad **Meer** en selecteer de knop **Synchronisatiecache wissen** om mogelijke conflicten met eerdere synchronisatiebewerkingen te voorkomen. Zie [Synchronisatiecache wissen](#) voor meer informatie.

Voer de volgende stappen uit om de instellingen te configureren die worden gebruikt bij het synchroniseren met Directory Connector:

Note

Als u Actieve Directory (AD) gebruikt, zijn veel van deze instellingen vooraf voor ubepaald en worden daarom niet weergegeven.

1. Open de Directory Connector [desktop app](#).
2. Navigeer naar het tabblad **Instellingen**.
3. Configureer de volgende opties naar wens in het gedeelte **Sync**:

Optie	Beschrijving
Interval	Tijd tussen automatische synchronisatiecontrole (in minuten).
Verwijder uitgeschakelde gebruikers tijdens synchronisatie	Vink dit vakje aan om gebruikers uit de Bitwarden-organisatie te verwijderen die in uw organisatie zijn uitgeschakeld.
Bestaande organisatiegebruikers overschrijven op basis van huidige synchronisatie-instellingen	<p>Vink dit vakje aan om de gebruikersset volledig te overschrijven bij elke synchronisatie, inclusief het verwijderen van gebruikers uit uw organisatie als ze afwezig zijn in de gebruikersset van de directory.</p> <p>Als er om wat voor reden dan ook een lege synchronisatie wordt uitgevoerd wanneer deze optie is ingeschakeld, zal Directory Connector alle gebruikers verwijderen.</p> <p>Voer altijd een testsynchronisatie uit voordat u synchroniseert nadat u deze optie hebt ingeschakeld.</p>
Naar verwachting zullen er meer dan 2000 gebruikers of groepen gesynchroniseerd worden	Vink dit vakje aan als u verwacht 2000+ gebruikers of groepen te synchroniseren. Als u dit vakje niet aanvinkt, zal Directory Connector een synchronisatie beperken tot 2000 gebruikers of groepen.
Lid Attribuut	Naam van het attribuut dat door de directory wordt gebruikt om het groepslidmaatschap te definiëren (bijvoorbeeld uniqueMember).
Aanmaakgegevens Attribuut	Naam van het attribuut dat door de map wordt gebruikt om aan te geven wanneer een record werd aangemaakt (bijvoorbeeld whenCreated).

Optie	Beschrijving
Herzieningsdatum Attribuut Als een gebruiker geen e-mailadres heeft, combineer dan een voorvoegsel voor de gebruikersnaam met een achtervoegsel om een e-mailadres te vormen.	Naam van het attribuut dat door de map wordt gebruikt om aan te geven wanneer een record voor het laatst is gewijzigd (bijvoorbeeld wh enChanged). Vink dit vakje aan om geldige e-mailopties te vormen voor gebruikers die geen e-mailadres hebben. Gebruikers zonder echte of aangemaakte e-mailadressen worden overgeslagen door Directory Connector. Aangemaakte e-mail = attribuut voorvoegsel e-mail + achtervoegsel e-mail
E-mail Voorvoegsel Attribuut	Attribuut dat wordt gebruikt om een voorvoegsel aan te maken voor aangemaakte e-mailadressen.
achtervoegsel e-mail	Een tekenreeks (@voorbeeld.com) die wordt gebruikt om een achtervoegsel te maken voor aangemaakte e-mailadressen.
Gebruikers synchroniseren	Vink dit vakje aan om gebruikers te synchroniseren met uw organisatie. Als u dit vakje aanvinkt, kunt u een gebruikersfilter , gebruikerspad , gebruikersobjectklasse en gebruikerse-mailkenmerk opgeven.
Gebruikersfilter	Zie Sync-filters opgeven.
Gebruikerspad	Attribuut dat wordt gebruikt met het opgegeven root path om te zoeken naar gebruikers (bijvoorbeeld ou=users). Als er geen waarde wordt opgegeven, start het zoeken naar subtrees vanaf het root path
Klasse Gebruikersobject	Naam van de klasse die wordt gebruikt voor het LDAP-gebruikersobject (bijvoorbeeld gebruiker).

Optie	Beschrijving
Email attribuut gebruiker	Attribuut dat moet worden gebruikt om het opgeslagen e-mailadres van een gebruiker te laden.
Groepen synchroniseren	Vink dit vakje aan om groepen te synchroniseren met uw organisatie. Als u dit vakje aanvinkt, kunt u een groepsfilter , groepsfad , groepsobjectklasse en groepsnaamattribuut opgeven.
Groepsfilter	Zie Sync-filters opgeven .
Groepsfad	Attribuut dat wordt gebruikt met het opgegeven root path om groepen te zoeken (bijvoorbeeld ou=groups). Als er geen waarde wordt opgegeven, start het zoeken naar subtrees vanaf het root path
Klasse groepsobject	Naam van de klasse die wordt gebruikt voor het LDAP-groepsobject (bijvoorbeeld groupOfUniqueNames).
Attribuut Groepsnaam	Naam van het attribuut dat door de map wordt gebruikt om de naam van een groep te definiëren (bijvoorbeeld naam).

Sync-filters opgeven

Gebruikers- en groepsfilters kunnen de vorm hebben van elk LDAP-compatibel zoekfilter.

Actieve Directory (AD) biedt een aantal geavanceerde opties en beperkingen voor het schrijven van zoekfilters, vergeleken met standaard LDAP-richtingen. Lees [hier](#) meer over het schrijven van Actieve Directory (AD) zoekfilters.

Note

Geneste groepen kunnen meerdere groepsobjecten synchroniseren met een enkele referentie in de Directory Connector. Doe dit door een groep aan te maken waarvan de leden andere groepen zijn.

Monsters

Om een synchronisatie te filteren op alle items met **objectClass=user** en **cn** (algemene naam) die **Marketing** bevat:

Bash

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

(alleen LDAP) Om een synchronisatie te filteren op alle items met een **ou** (organization unit) component van hun **dn** (distinguished name) die **Miami** of **Orlando** is:

Bash

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

(Alleen LDAP) Om entiteiten uit te sluiten die overeenkomen met een uitdrukking, bijvoorbeeld alle **ou=Chicago** vermeldingen behalve diegene die ook overeenkomen met een **ou=Wrigleyville** kenmerk:

Bash

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

(Alleen AD) Om een synchronisatie te filteren voor gebruikers in de groep **Hellden**:

Bash

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

(Alleen AD) Om een synchronisatie te filteren op gebruikers die lid zijn van de **Hellden** groep, in de directory of via nesting:

Bash

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

Een synchronisatie testen

 **Tip**

Voordat u een synchronisatie test of uitvoert, moet u controleren of Directory Connector is verbonden met de juiste cloudserver (bijv. VS of EU) of zelf gehoste server. Leer hoe u dat doet met de [desktop app](#) of [CLI](#)

Om te testen of Directory Connector succesvol verbinding maakt met uw directory en de gewenste gebruikers en groepen retourneert, navigeert u naar het tabblad **Dashboard** en selecteert u de knop **Nu testen**. Als dit lukt, worden gebruikers en groepen getoond in het Directory Connector-venster volgens de opgegeven [synchronisatieopties](#) en [filters](#):





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

Resultaten testsynchronisatie

Automatische synchronisatie starten

Zodra de [synchronisatieopties](#) en [filters](#) geconfigureerd en getest zijn, kunt u beginnen met synchroniseren. Voer de volgende stappen uit om de automatische synchronisatie met Directory Connector te starten:

1. Open de [bureaubladtoepassing](#) Directory Connector.
2. Navigeer naar het tabblad **Dashboard**.
3. Selecteer in het gedeelte **Synchronisatie** de knop **Synchronisatie starten**.

U kunt ook de knop **Nu synchroniseren** selecteren om een eenmalige handmatige synchronisatie uit te voeren.

Directory Connector begint uw directory te controleren op basis van de geconfigureerde [synchronisatieopties](#) en [filters](#).

Als u de toepassing verlaat of afsluit, stopt de automatische synchronisatie. Als u Directory Connector op de achtergrond wilt laten draaien, minimaliseert u de toepassing of verbergt u deze in het systeemvak.

Note

Als u het [Teams Starter-plan](#) gebruikt, bent u beperkt tot 10 licenties. Directory Connector geeft een fout weer en stopt met synchroniseren als u meer dan 10 licenties probeert te synchroniseren.

Problemen met synchroniseren met Actieve Directory (AD) oplossen

Waardelimiet bereikt bij synchroniseren vanuit een Actieve Directory (AD) instantie:

De Actieve Directory (AD) `MaxValRange` heeft een standaardinstelling van 1.500. Als een attribuut, zoals `leden` van een groep, meer dan 1.500 waarden heeft, retourneert Actieve Directory (AD) zowel een leeg `ledenattribuut` als een ingekorte lijst van `leden` op afzonderlijke attributen, tot de waarde `MaxValRange`.

- U kunt het beleid `MaxValRange` instellen op een waarde die hoger is dan het aantal leden van uw grootste groep in Actieve Directory (AD). Raadpleeg de Microsoft-documentatie voor het instellen van Actieve Directory (AD) LDAP-beleidsregels met het hulpprogramma [ntdsutil.exe](#).