bitwarden | Help Center Article

ADMIN CONSOLE > USER MANAGEMENT >

Sync with Active Directory or LDAP

View in the help center:
https://bitwarden.com/help/ldap-directory/

Sync with Active Directory or LDAP

This article will help you get started using Directory Connector to sync users and groups from your LDAP or Active Directory service to your Bitwarden organization. Bitwarden provides built-in connectors for the most popular LDAP directory servers, including:

- Microsoft Active Directory
- Apache Directory Server (ApacheDS)
- Apple Open Directory
- Fedora Directory Server
- Novell eDirectory
- OpenDS
- OpenLDAP
- Sun Directory Server Enterprise Edition (DSEE)
- Any generic LDAP directory server

Connect to your server

Complete the following steps to configure Directory Connector to use your LDAP or Active Directory:

1. Open the Directory Connector desktop app.
2. Navigate to the **Settings** tab.
3. From the **Type** dropdown, select **Active Directory / LDAP**.

   The available fields in this section will change according to your selected type.
4. Configure the following options:

Option	Description	Examples
Server Hostname	Hostname of your directory server.	`ad.example.com`, `ldap.company.org`
Server Port	Port on which your directory server is listening.	`389` or `10389`

Option	Description	Examples
Root Path	Root path at which Directory Connector should start all queries.	`cn=users`, `dc=ad`, `dc=example`, `dc=com` or `dc=ldap`, `dc=company`, `dc=org`
This server uses active directory	Check this box if the server is an Active Directory server.	
This server pages search results	Check this box if the server paginates search results (LDAP only).	
This server uses an encrypted connection	Checking this box will prompt you to select one of the following options: **Use SSL** (LDAPS) If your LDAPS server uses an untrusted certificate, you can configure certificate options on this screen. **Use TSL** (STARTTLS) If your LDAP server uses a self-signed certificate for STARTTLS, you can configure certification options on this screen.	
Username	The distinguished name of an administrative user that the application will use when connecting to the directory server. For **Active Directory**, if synchronizing the status of users removed from the directory is desired, the user should be a member of the built-in administrator group.	
Password	The password of the user specified above. The password is safely stored in the operating system's native credential manager.	

Configure sync options

> **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.

Complete the following steps to configure the settings used when syncing using Directory Connector:

> **Note**
> If you are using Active Directory, many of these settings are predetermined for you and are therefore are not shown.

1. Open the Directory Connector desktop app.
2. Navigate to the **Settings** tab.
3. In the **Sync** section, configure the following options as desired:

Option	Description
Interval	Time between automatic sync check (in minutes).
Remove disabled users during sync (**Not available for LDAP**)	Check this box to remove users from the Bitwarden organization that have been disabled in your organization.
More than 2000 users or groups are expected to sync	Check this box if you expect to sync 2000+ users or groups. If you don't check this box, Directory Connector will limit a sync at 2000 users or groups.
Member Attribute	Name of the attribute used by the directory to define a group's membership (for example, `uniqueMember`).
Creation Data Attribute	Name of the attribute used by the directory to specify when an entry was created (for example, `whenCreated`).
Revision Date Attribute	Name of the attribute used by the directory to specify when an entry was last changed (for example, `whenChanged`).
If a user has no email address, combine a username prefix with a suffix value to form an email	Check this box to form valid email options for users that do not have an email address. This option is available after selecting **This server uses Active Directory**. **Users without real or formed email addresses will be skipped by Directory Connector.** Formed Email = **Email Prefix Attribute** + **Email Suffix**

Option	Description
Email Prefix Attribute	Attribute used to create a prefix for formed email addresses.
Email Suffix	A string (`@example.com`) used to create a suffix for formed email addresses.
Sync users	Check this box to sync users to your organization. Checking this box will allow you to specify a **User Filter**, **User Path**, **User Object Class**, and **User Email Attribute**.
User Filter	See Specify sync filters.
User Path	Attribute used with the specified **Root Path** to search for users (for example, `ou=users`). If no value is supplied, the subtree search will start from the root path.
User Object Class	Name of the class used for the LDAP user object (for example, `user`).
User Email Attribute	Attribute to be used to load a user's stored email address.
Sync groups	Check this box to sync groups to your organization. Checking this box will allow you to specify a **Group Filter**, **Group Path**, **Group Object Class**, **Group Name Attribute**.
Group Filter	See Specify sync filters.
Group Path	Attribute used with the specified **Root Path** to search for groups (for example, `ou=groups`). If no value is supplied, the subtree search will start from the root path.

Option	Description
Group Object Class	Name of the class used for the LDAP group object (for example, `groupOfUniqueNames`).
Group Name Attribute	Name of the attribute used by the directory to define the name of a group (for example, `name`).

Specify sync filters

User and group filters can be in the form of any LDAP-compatible search filter.

Active Directory provides some advanced options and limitations for writing search filters, when compared to standard LDAP directions. Learn more about writing Active Directory search filters here.

> **Note**
> Nested groups can sync multiple group objects with a single referent in the Directory Connector. Do this by creating a group whose members are other groups.

Samples

To filter a sync for all entries that have `objectClass=user` and `cn` (common name) that contains `Marketing`:

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

(**LDAP-only**) To filter a sync for all entries with an `ou` (organization unit) component of their `dn` (distinguished name) that is either `Miami` or `Orlando`:

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

(**LDAP-only**) To exclude entities that match an expression, for example all `ou=Chicago` entries except those that also match a `ou=Wrigleyville` attribute:

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

(**AD Only**) To filter a sync for users in the `Heroes` group:

```
Bash

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

(**AD Only**) To filter a sync for users that are members of the `Heroes` group, either directly or via nesting:

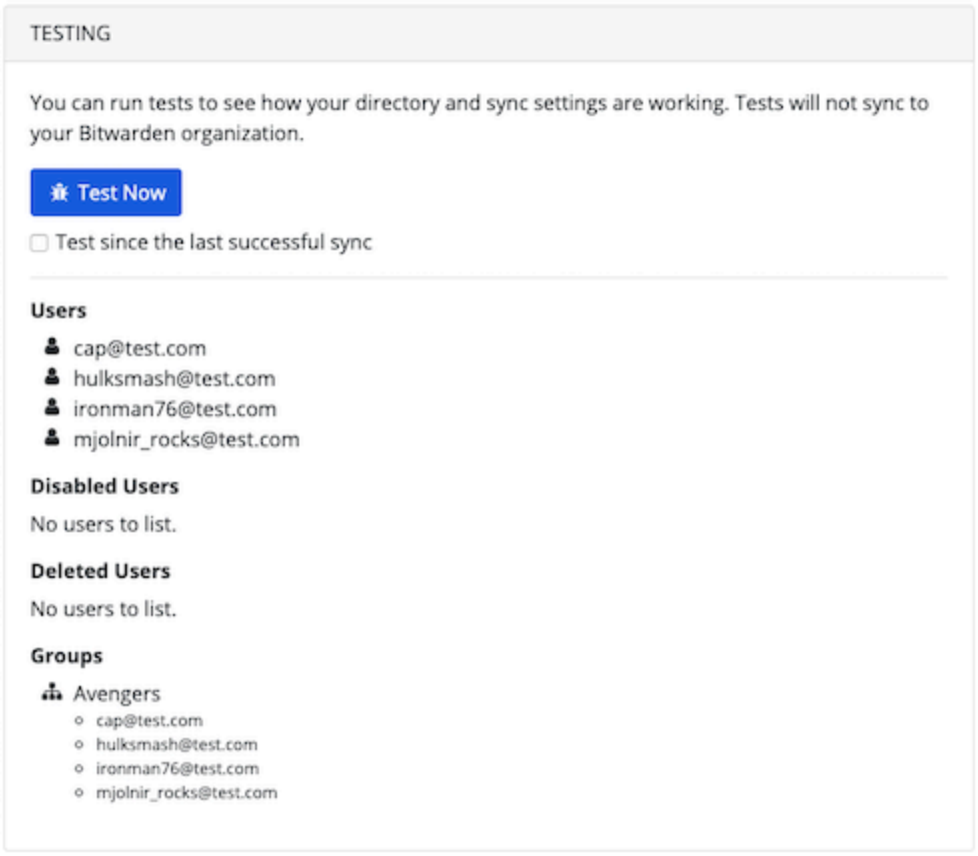
```
Bash

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

Test a sync

> **Tip**
>
> Innan du testar eller kör en synkronisering, kontrollera att Directory Connector är ansluten till rätt molnserver (t.ex. USA eller EU) eller egenhostad server. Lär dig hur du gör det med skrivbordsappen eller CLI.

To test whether Directory Connector will successfully connect to your directory and return the desired users and groups, navigate to the **Dashboard** tab and select the **Test Now** button. If successful, users and groups will be printed to the Directory Connector window according the specified sync options and filters:



Test sync results

Start automatic sync

Once sync options and filters are configured and tested, you can begin syncing. Complete the following steps to start automatic syncing with Directory Connector:

1. Open the Directory Connector desktop application.
2. Navigate to the **Dashboard** tab.
3. In the **Sync** section, select the **Start Sync** button.

   You may alternatively select the **Sync Now** button to execute a one-time manual sync.

Directory Connector will begin polling your directory based on the configured sync options and filters.

If you exit or close the application, automatic sync will stop. To keep Directory Connector running in the background, minimize the application or hide it to the system tray.

> **Note**
>
> Om du har Teams Starter-plan är du begränsad till 10 medlemmar. Directory Connector visar ett felmeddelande och slutar synkronisera om du försöker synkronisera fler än 10 medlemmar.
>
> Den **här planen går inte längre att köpa**. Det här felet gäller inte för Teams planer.

Sync with Active Directory troubleshooting

Value limit reached when synchronizing from an Active Directory instance:

The Active Directory `MaxValRange` has a default setting of 1500. If an attribute, such as `members` on a Group has more than 1500 values, Active Directory will return both a blank `members` attribute, as well as a truncated list of `members` on separate attributes, up to the value of `MaxValRange`.

- You can adjust the `MaxValRange` policy to a value higher than the number of members of your largest group in Active Directory. See the Microsoft documentation for setting Active Directory LDAP policies by using the ntdsutil.exe utility.