bitwarden | Help Center Article

ADMIN CONSOLE > USER MANAGEMENT >

Sync with Microsoft Entra ID

View in the help center:
https://bitwarden.com/help/microsoft-entra-id/

Sync with Microsoft Entra ID

This article will help you get started using Directory Connector to sync users and groups from your Microsoft Entra ID Directory to your Bitwarden organization.

Microsoft Entra ID Directory setup

Complete the following processes from the Microsoft Azure Portal before configuring Directory Connector. Directory Connector will require information obtained from these processes to function properly.

Create app registration

Complete the following steps to create an app registration for Directory Connector:

1. From your Microsoft Azure portal, navigate to the **Microsoft Entra ID** directory.
2. From the left-hand navigation, select **App registrations** or enter **App registrations** into the search bar.
3. Select the **New registration** button and give your registration a Bitwarden-specific name (such as, `bitwarden-dc`).
4. Select **Register**.

Grant app permissions

Complete the following steps to grant the created app registration the required permissions:

1. On the created Bitwarden app, select **API Permissions** from the left-hand navigation.
2. Select the **Add a permission** button.
3. When prompted to select an API, select **Microsoft Graph**.
4. Set the following **Delegated permissions**:
   - User > User.ReadBasic.All (Read all users' basic profiles)
   - User > User.Read.All (Read all users' full profiles)
   - Group > Group.Read.All (Read all groups)
   - AdministrativeUnit > AdministrativeUnit.Read.All (Only required if you'll be syncing Administrative Units)
5. Set the following **Application Permissions**:
   - User > User.Read.All (Read all users' full profiles)
   - Group > Group.Read.All (Read all groups)
   - AdministrativeUnit > AdministrativeUnit.Read.All (Only required if you'll be syncing Administrative Units)
6. Back on the API Permissions page, select the **Grant admin consent for...** button.

Create app secret key

Complete the following steps to create a secret key to be used by Directory Connector:

1. On the created Bitwarden app, select **Certificates & secrets** from the left-hand navigation.
2. Select the **New client secret** button and add a Bitwarden-specific description (such as, `bitwarden-dc-secret`) and an expiration date. We recommend the longest expiration date period possible, and setting a reminder to update it when required.
3. Select **Save** once you have finished.
4. Copy the secret's **value** to a safe place for later use.

Get app ID

Complete the following steps to obtain the app ID to be used by Directory Connector:

1. On the created Bitwarden app, select **Overview** from the left-hand navigation.
2. Copy the **Application (client) ID** to a safe place for later use.

Get tenant hostname

Complete the following steps to obtain the tenant hostname to be used by Directory Connector:

1. From anywhere in the Azure portal, select the ⚙ icon on the top right navigation bar.
2. Select the **Directory + subscription** filter button from the menu located on the left.
3. Copy the **Current directory:** value to a safe place for later use.

Connect to your directory

Complete the following steps to configure Directory Connector to use Microsoft Entra ID. If you haven't already, take the proper Microsoft Entra ID setup steps before proceeding:

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

   The available fields in this section will change according to your selected type.
4. Enter the collected **tenant**, **application Id**, and **secret key**.

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:

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 checks (in minutes).
Remove disabled users during sync	Check this box to remove users from the Bitwarden organization that have been disabled in your directory.
Overwrite existing organization users based on current sync settings	Check this box to always perform a full sync and remove any users from the Bitwarden organization if they are not in the synced user set.
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.
Sync users	Check this box to sync users to your organization. Checking this box will allow you to specify **User Filters**.
User filter	See Specify sync filters.
Sync groups	Check this box to sync groups to your organization. Checking this box will allow you to specify **Group Filters**.
Group filter	See Specify sync filters.

Specify sync filters

Use comma-separated lists to include or exclude from a sync based on user email, group name, or group membership.

User filters

The following filtering syntaxes should be used in the **User Filter** field:

Include/Exclude users by email

To include or exclude specific users from a sync based on email address:

```
Bash

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

```
Bash

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

User by group membership

You can include or exclude users from a sync based on their Microsoft Entra ID group membership using the `includeGroup` and `excludeGroup` keywords. `includeGroup` and `excludeGroup` use Group Object ID, available from the **Overview** page of the group in the Azure Portal or through the Azure AD PowerShell:

```
Bash

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

```
Bash

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

Group filters

> **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.

The following filtering syntaxes should be used in the **Group Filter** field:

Include/Exclude groups

To include or exclude groups from a sync based on group name:

```
Bash

include:Group A,Group B
```

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

Group by administrative unit (AU)

You can include or exclude groups from a sync based on their tagged Microsoft Entra ID Administrative Units by using the `includeadministrativeunit` and `excludeadministrativeunit` keywords. `includeadministrativeunit` and `excludeadministrativeunit` use the **Object ID** of the Administrative Unit:

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

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

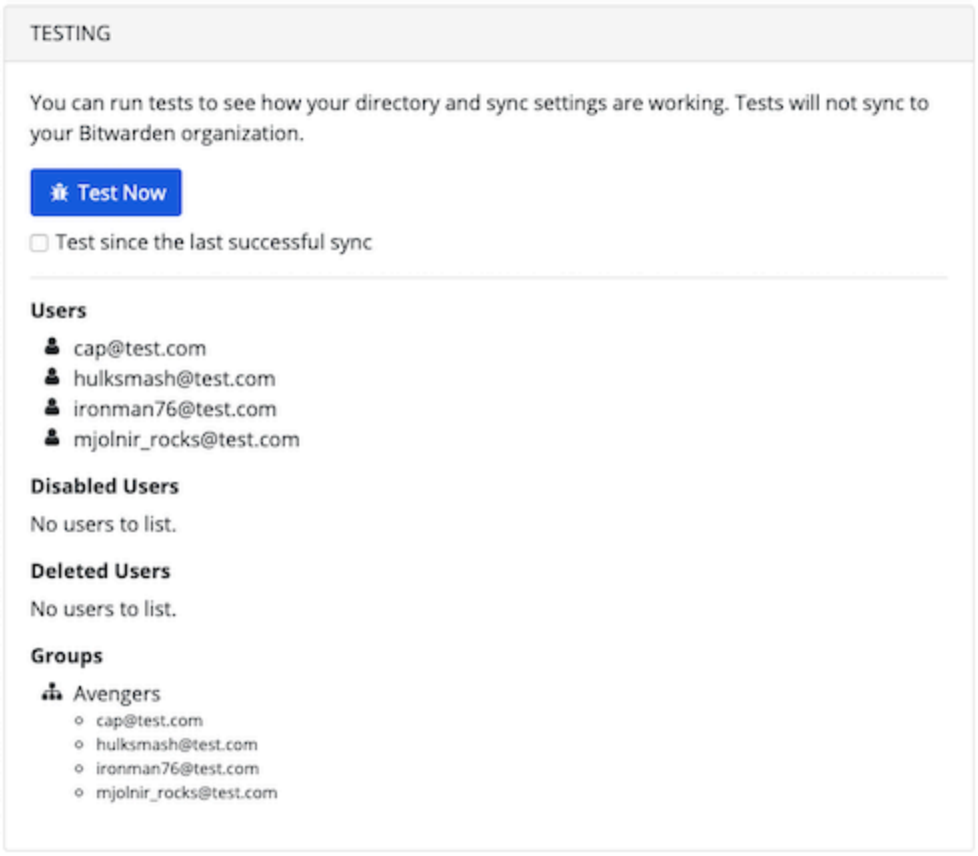
Test a sync

> **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 to specified sync options and filters.

It may take up to 15 minutes for permissions for your application to properly propagate. In the meantime, you may receive `Insufficient privileges to complete the operation` errors.

> **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.



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 app.
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.