bitwarden | Help Center Article

ADMIN CONSOLE > MANAGE MEMBERS > DIRECTORY CONNECTOR

Google Workspace Directory

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

Google Workspace Directory

This article will help you get started using Directory Connector to sync users and groups from your Google Workspace (formerly "G Suite") Directory to your Bitwarden organization.

Google Workspace setup

To setup directory sync with Google Workspace (formerly "G Suite"), you will need access to the **Google Workspace Admin Console** and **Google Cloud Platform Console**. Directory Connector will require information obtained from these processes to function properly.

Create a cloud project

Complete the following steps to create a Google Cloud project to use to connect Directory Connector to your directory. If you already have a Google Cloud project available, skip to Enable Admin SDK:

1. In the GCP Console, use the left-hand navigation to select **IAM & Admin** → **Manage Resources**.
2. Select the **Create Project** button.
3. On the New Project screen:
   - Enter a Bitwarden-specific name for the project (for example, `bitwarden-dc-project`).
   - Choose an organization to attach it to the project.
   - Choose the parent organization or folder.
   - Select **Create**.

Enable Admin SDK

Complete the following steps to enable the Admin SDK API, to which Directory Connector will make requests:

1. In the GCP Console, open the created or pre-existing project.
2. From the left-hand navigation, select **APIs & Services** → **Library**.
3. In the search box, enter `Admin SDK` and open the **Admin SDK API** service.
4. Select the **Enable** button.

Create service account

Complete the following steps to create a service account to use when making API calls:

1. In the GCP Console, select the created or pre-existing project.
2. From the left-hand navigation, select **APIs & Services** → **Credentials**.
3. Select the **Create Credentials** button, and select **Service account** from the dropdown.

4. Fill in the **Service account details** section, and select the **Create and continue** button.
5. In the **Grant this service account access to project** section, select **Project → Owner** from the **Role** dropdown and select the **Continue** button.
6. Select the **Done** button.

Obtain service account credentials

Complete the following steps to obtain the appropriate permissions for the created service account:

1. In the GCP Console, open the created or pre-existing project.
2. From the left-hand navigation, select **IAM & Admin → Service Accounts**.
3. Select the created or pre-existing service account.
4. From the **Keys** tab, select the **Add Key** button and select **Create new key** from the dropdown.
5. Select the Key type **JSON** and select the **Create** button to download a JSON-formatted key to your local machine.
6. Back on the **Details** tab of the service account, select the **Advanced settings** drop-down.
7. Scroll to the **Google Workspace Marketplace OAuth Client** section and select **Create Google Workspace Marketplace-Compatible OAuth Client**, or, if you see box that reads "An OAuth consent screen must be configured in order to create an OAuth client.", select **Configure**.
8. Select **Get Started** and in the project configuration:
   - Enter the name of the app asking for consent (e.g. `Bitwarden Directory Connector`).
   - Choose a **user support email**.
   - In the **Audience** section, choose **Internal**.
   - Continue through the wizard to create the consent screen.
9. Once created, open the **Data Access** tab and select **Add or remove scopes**.
10. In the **Manually add scopes** section, paste the following:

```
Plain Text

https://www.googleapis.com/auth/admin.directory.user.readonly,https://www.googleapis.com/auth/admin.directory.group.readonly,https://www.googleapis.com/auth/admin.directory.group.member.readonly
```

Select **Add to table** and then **Update**.

11. Click **Save**.

Using service account credentials with the CLI

If you're going to use the Directory Connector CLI, the JSON-formatted key you've downloaded will be used for the command `bwdc config gsuite.key`, however intermediary steps are required to allow the CLI to use the private key found in the key file:

- **On Linux**, run the command `bwdc config gsuite.key "\n$(cat projectid-key.json | jq -r '.private_key')"`, being sure to replace `projectid-key.json` with the name of your `.json` file, which is typically a combination of the Project ID and Key.
- **On other OSs**:
  1. Copy the value of `private_key` into a separate `.crt` file, for example named `google-bwdc-key.crt`.
  2. Run the command `bwdc config gsuite.key "\n$(cat google-bwdc-key.crt)\n"`, being sure to replace the `.crt` file name with the one you've created.

Allow read-access to Google Workspace

Complete the following steps to authorize the client to read your directory:

1. Open the Google Admin Console.
2. From the left-hand navigation, select **Security → Access and data control → API controls**.
3. Select the **Manage Domain Wide Delegation** button.
4. Select the **Add new** button.
5. In the Client ID field, paste the created **Unique ID** you can find by opening the GCP Console, navigating to **API & Services → Credentials**, opening your service account and looking for the **Unique ID**.
6. In the OAuth scopes field, paste the following value to grant only read-access:

```
Bash

https://www.googleapis.com/auth/admin.directory.user.readonly,https://www.googleapis.com/auth/admin.directory.group.readonly,https://www.googleapis.com/auth/admin.directory.group.member.readonly
```

7. Select the **Authorize** button.

Connect to your directory

Complete the following steps to configure Directory Connector to use your Google directory:

1. Open the Directory Connector desktop app.

2. Navigate to the **Settings** tab.
3. From the **Type** dropdown, select **G Suite (Google)**.

   The available fields in this section will change according to your selected type.
4. Enter the **Domain** of your Google account.
5. Enter the email address of an **Admin User** with full access to your Google directory.
6. If you have one, enter the **Customer ID** of your directory. Many users will not have or be required to enter a Customer ID.
7. Select the **Choose File** button and select the downloaded JSON key.

Configure sync options

> **Tip**
>
> When you're 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 setting used when syncing using Directory Connector:

1. Open the Directory Connector desktop app.
2. Navigate to the **Settings** tab.
3. In the **Sync** section, confiture 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.

Option	Description
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 a **User Filter**.
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 a **Group Filter**.
Group Filter	See Specify sync filters.

Specify sync filters

User filters

Use a comma-separated lists to specify filters for sync inclusion or exclusion. The Google Workspace Directory API allows you to sync users based on email and sync batches of users based on organizational unit. To sync a sub-set of your directory's users, Bitwarden recommends creating an organizational unit and moving relevant users to it.

Sync a specific organizational unit

To sync the users assigned to a specific organizational unit (OU), for example the OU `EngineeringUsers`, use a pipe (`|`) to declare a query parameter. A query declaration at the start of your **User filter** indicates that only matches on the query should be synced:

```
Plain Text
```

```
|orgUnitPath=/Engineering
```

Your Root Group, under which OUs are nested, is always referred to as a `/` in the `orgUnitPath`. Using the query `|orgUnitPath=/` is equivalent to using no user filter.

Syncs based on OU can be combined with additional filters to determine which specific users in the OU to sync, for example to sync users in an OU with a specific `orgTitle`:

```
Bash

|orgUnitPath=/Engineering orgTitle:Manager
```

More user attributes than `orgTitle` can be combined with OU queries to determine which users to sync, and can be found in the Google Directory API documentation.

Include or exclude users by email

Filters to include or exclude specific users can be combined with OU queries, or used on their own, however any `include:` or `exclude:` filters must be placed before any query declaration (`|`). For example, to exclude a specific user from an OU sync of users with a specific `orgTitle`:

```
Bash

exclude:bill@example.com|orgUnitPath=/Engineering orgTitle:Manager
```

Or, to sync only a selection of users based on their `email`:

```
Bash

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

Notice that, in this last example, no query declaration (`|`) is required because no further query parameters (for example, OU or `orgTitle`) are declared.

Group filters

Use a comma-separated lists to specify filters for sync inclusion or exclusion. The Google Workspace Directory API allows you to sync groups based on their names and a few other group attributes, which can be found in the Google Directory API documentation.

When a **Group filter** is used, any users caught by the **User filter** will have their group membership synced for groups caught by the **Group filter**.

> **ⓘ Note**
>
> Syncing nested groups is not supported by Google Workspace.

Sync groups by name

Individual groups can be included in a sync by specifically filtering on their `name` attribute, for example:

```
Bash

include:Group A,Group B
```

Using a pipe (`|`) to declare a query parameter, a subset of groups can also be synced by matching on any term surrounded by wildcard characters (`*`). A query declaration at the start of your **Group filter** indicates that only matches on the query should be synced, for example to sync only any groups with a name that contains the term `engineering`:

```
Bash

|name:*engineering*
```

Wildcards are supported on both or either side of the term, and matches are not case sensitive.

Sync groups by member key

The memberKey attribute can use used to sync all groups for which a user, as identified by the key, has membership. For example, to sync only the groups of which `user@company` is a member:

```
Bash

|memberKey=user@company.com
```

Note again that a query declaration at the start of your **Group filter** indicates that only matches on the query should be synced, and that wildcards can also be used in this context.

Filters to include or exclude specific groups can be combined with larger queries, however any `include:` or `exclude:` filters must be placed before any query declaration (`|`). For example, to sync the groups of which `user@company` is a member except `Group A`:

```
Bash

exclude:Group A|memberKey:user@company
```

Sync groups by group email

These **Group filter** principles can also be used to sync based on a group's email address, for example:

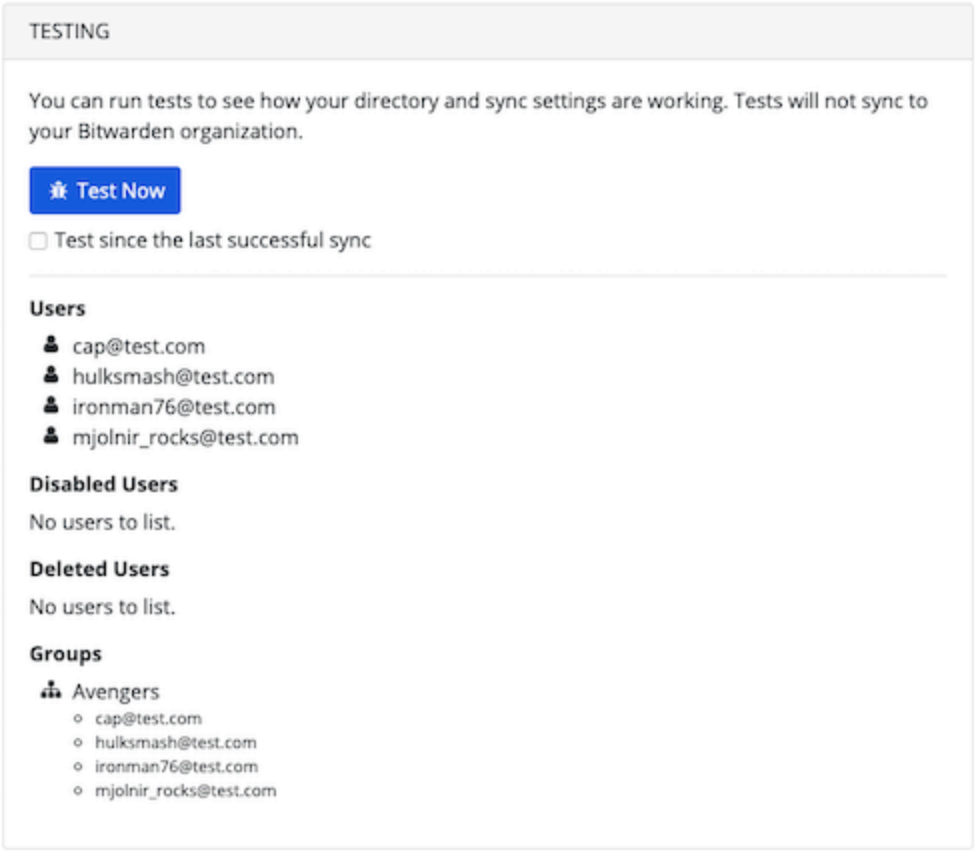
```
Bash

exclude:Group B|email:admin*
```

Test a sync

> **Tip**
>
> Before testing or executing a sync, check that Directory Connector is connected to the right cloud server (e.g. US or EU) or self-hosted server. Learn how to do so with the desktop app or 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 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 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**
>
> If you're on the Teams Starter plan, you are limited to 10 members. Directory Connector will display an error and stop syncing if you try to sync more than 10 members.
>
> **This plan is no longer available for purchase**. This error does not apply to Teams plans.