

SELF-HOSTING

# Self-hosting SCIM

View in the help center:  
<https://bitwarden.com/help/self-hosting-scim/>

## Self-hosting SCIM

### Note

The steps described in this article are for Docker standard deployments, in Helm deployments you will instead need to set `scim: true` in the `values.yaml` file to enable SCIM.

In order to use SCIM to automatically provision and de-provision members and groups in your self-hosted Bitwarden organization, you will need to enable a flag in your `config.yaml` file. To enable SCIM for your Bitwarden server:

1. Save a backup of, at a minimum, `.bwdata/mssql`. Once SCIM is in use, it's recommended that you have access to a backup image in case of an issue.

### Note

If you are using an external MSSQL database, take a backup of your database in whatever way fits your implementation.

2. Update your self-hosted Bitwarden installation in order to retrieve the latest changes:

*Bash*

```
./bitwarden.sh update
```

3. Edit the `.bwdata/config.yaml` file and enable SCIM by toggling `enable_scim` to `true`.

*Bash*

```
nano bwdata/config.yaml
```

4. Rebuild your self-hosted Bitwarden installation:

*Bash*

```
./bitwarden.sh rebuild
```

5. Update your self-hosted Bitwarden installation again in order to apply the changes:

*Bash*

```
./bitwarden.sh update
```

Now that your server has SCIM enabled, use one of our SCIM integration guides to integrate your Bitwarden organization with:

- [Microsoft Entra ID](#)
- [Okta](#)

- [OneLogin](#)
- [JumpCloud](#)