Google Workspace Single Sign-On

Login to Peerdom with your Google Workspace credentials

A little background

Single sign-on (**SSO**) is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems, such as Peerdom. That is, employees can log in with one single set of credentials to get access to all corporate apps, websites, and data for which they have permission. SSO solves key problems by providing greater security and standardized password compliance. Your team will not have to create yet another account on yet another service – they can use a pre-existing, familiar username and password to log in to Peerdom.

Google Workspace can serve as the service provider to third-party identity providers (Peerdom, in this case). More details can be found here:

https://support.google.com/a/answer/60224?hl=en

What to do

1. Write down your Google Domain

We will need your **Google Domain** to activate SSO authentication. The domain is usually the part after the @ in your email. For example, in: john.doe@myorganisation.org *myorganisation.org* is the domain we are looking for.

If you are unsure, you can check the Google Workspace admin to see what domains are available in your Google Workspace.

2. Enable Domain-wide delegation for the Peerdom service account

- Visit the Google Admin: https://admin.google.com
- Navigate to the *Security* > *API Controls* section and then click *MANAGE DOMAIN WIDE DELEGATION* under *Domain wide delegation*.

- Add a new API client:

Client ID: 100767850732510667368

OAuth Scope:

https://www.googleapis.com/auth/admin.directory.user.readonly

If you would like to restrict access to Peerdom to certain groups, you can also add a second OAuth Scope:

https://www.googleapis.com/auth/admin.directory.group.readonly

3. Prepare admin user email

We will need you to add an admin user email that will be used for impersonation by the service account.

IMPORTANT: Only users with access to the Admin APIs can access the Admin SDK Directory API, therefore your service account needs to impersonate one of those users to access the Admin SDK Directory API. Additionally, the user must have logged in at least once and accepted the Google Workspace Terms of Service.

This account will only be able to perform actions that are defined by the scopes you assigned in Step 2. That is, this account will only be able to read user data and if you supplied the group scope, read groups data.

4. (Optional) Create a group to define peer synchronisation

Your Peerdom directory will stay up to date with the current names and email addresses defined in your Google Workspace. If you wish to restrict access and synchronisation with Peerdom to certain people from the Workspace database, you will need to create a group with the users you'd like to synchronise and write down the Group ID.

5. (Optional) Create a group to restrict logins

By default, Peerdom will accept all log in attempts from your top-level domain. To restrict log in access to a particular group of users, you must create a new group, add the users you'd like to give log in access to Peerdom, and write down the Group ID. This group (GroupID) may be the same you created in step 4 for peer synchronisation, but it can also differ if you'd like to control logging in and synchronisation separately.

peerdom
Redesigning organisations

6. Send us the following information

1. **Google domain**

2. **Admin email address from within the Google Workspace domain**
   the service account would be impersonating this user to retrieve the data (peer names, email addresses, images)

3. **Enable synchronisation: yes/no**
   If yes: #5, #6, #7 are optional
   If no: #5, #6, #7 do not apply

4. (Optional) **Group ID** for SSO log in accounts
   If no group is provided, all users from your domain are able to log into Peerdom.

5. (Optional) **Group ID** for peer synchronisation
   If no group is provided, we will synchronise all users from the domain. It can be same or different as #4

6. (Optional) **Image synchronisation**: **yes/no**
   Yes: synchronise images from Google workspace
   No: images are uploaded and managed in Peerdom

7. (Optional) **Default access rights**
   When you add a new colleague to your Google Workspace, a new peer will be created in Peerdom. We need to know what access rights to give them by default.

   Member: **View** content
   Editor: **Edit** content, invite/add/remove other peers
   Owner: Edit content, invite/add/remove, **administer** access rights

Once we receive this information, we will connect your Google Workspace to Peerdom and confirm the success of this syncing operation.

Peerdom - c/o Nothing AG**,** Kirchstrasse 175**,** 3084 Wabern**,** Schweiz
hello@peerdom.org

How to log in

1. Case 1: You have already entered email addresses in Peerdom

If the email address already exists in Peerdom, you can log in to the standard login form at https://peerdom.org/login

Peerdom detects SSO logins and automatically redirects to the Google Workspace login (SP initiated SSO).

2. Case 2: You have not yet entered email addresses in Peerdom.

If the email address does not yet exist in Peerdom, please log in at https://peerdom.org/login/google.

Following the first log in, Peerdom will mark the email address as a Google Workspace SSO account, and future log in attempts can be made at the standard login form at https://peerdom.org/login

Peerdom - c/o Nothing AG, Kirchstrasse 175, 3084 Wabern, Schweiz
hello@peerdom.org