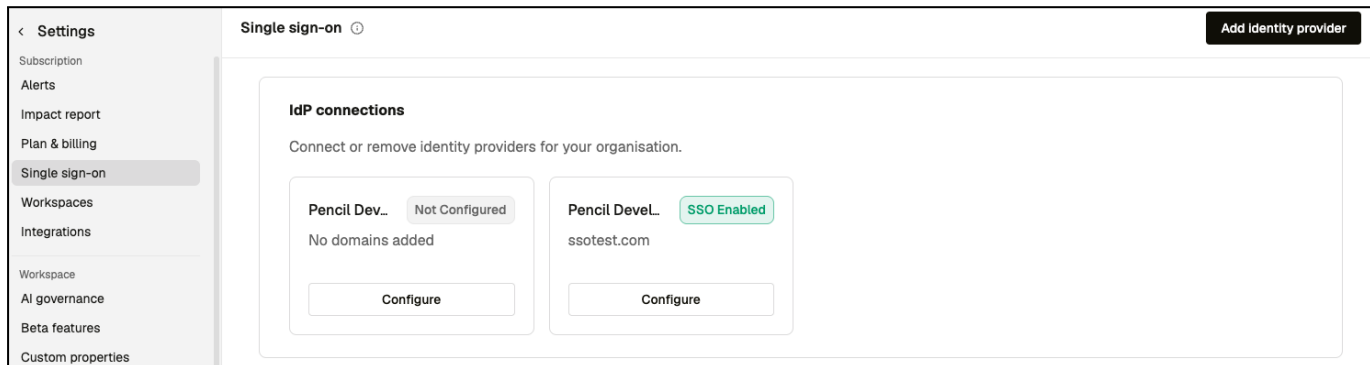


How to configure single sign-on in Pencil

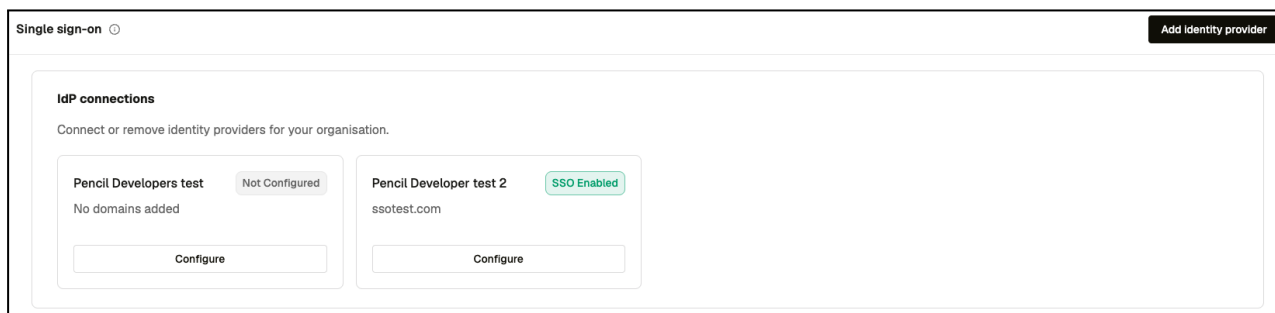
Required role

You need to be a subscription admin to reach this "Single sign-on" page in Settings.



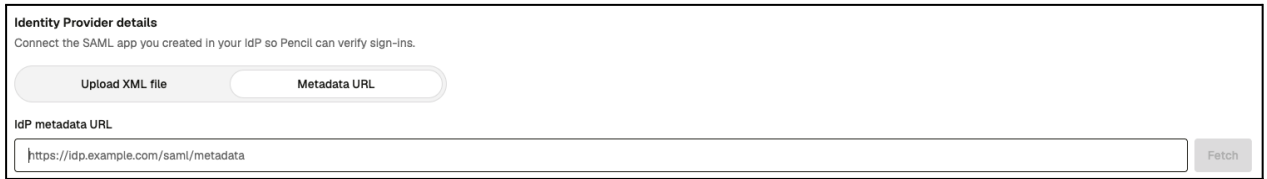
From the Single sign-on page, follow these steps to enable SSO

1. **Add identity provider (IdP):** If there are no IdP connections yet, click "Add identity provider". If there is one already and you're not looking to configure multiple IdPs, click "Configure" on the existing one.



2. **Download SP metadata:** Click "Download metadata" to see Pencil's Service Provider (SP) Metadata. Your Identity Provider (IdP), will need to provide information using the exact same field names as specified in this SP metadata for SSO to work.
3. **Provide IdP metadata:** Click "Metadata URL", add the URL to your IdP metadata XML file and click Fetch or use "Upload XML file" if you don't have such a URL but

have the XML file.



Identity Provider details

Connect the SAML app you created in your IdP so Pencil can verify sign-ins.

Upload XML file Metadata URL

IdP metadata URL

Fetch

4. **Enter email domains:** Under Email domains, enter any email domains used by people in your IdP who will log in to Pencil with SSO.

Email domains ⓘ

Add email domains (e.g. trypencil.com)

5. **Save Changes:** Click “Save Changes” under the “Connect your identity provider” section.
6. *If you just want to use SSO for login only and not have it automatically control which users have access to which workspaces, skip steps 7-9. If you also want SSO to control which users have access to which workspaces, do steps 7-9.*
7. **Set group access settings:** Under "Set group access", for each IdP group you have that indicates what workspaces a user should belong to in Pencil.:
 - a. Click "Add mapping".
 - b. "Add new group".
 - c. Enter the exact IdP group name.
 - d. "Add group".
 - e. Select the Workspace(s) people in that IdP group should have access to and the Role they should get access with. Note: you can have multiple rows for the same IdP group if they need different roles in different workspaces.



Set group access ⓘ

You can set up group access now. Your identity provider needs to be configured before you can turn it on.

Identity provider group name	Workspace(s)	Role
test	Pencil Developers test ⓘ Sub-workspace-1 ⓘ	Creative ⓘ ⓘ

+ Add mapping

8. **Save Changes:** Click "Save Changes" under the “Set group access” section.
9. **Enable Set group access:** Before clicking the toggle for “Set group access”, please note that users will be created when they log in through your IdP and they’ll also be added to workspaces that their IdP groups are mapped to in this user interface. **Additionally, if the user logs in and they belong to any workspaces that their IdP groups are not mapped to here, they’ll be removed from those workspaces, even if they were manually added to them. So please proceed with caution when enabling set group access, as it can take away people's access to workspaces which can be problematic if the mappings are not correct.**

10. **Enable SSO:** When you're ready to test, click the "Enable SSO" toggle at the top.



11. Then people in your IdP will be able to "Sign in with SSO" from this page: <https://pro.trypencil.com/login>. If you've enabled "Set group access", they'll be automatically added to the workspaces that correspond to the IdP groups they belong to in the corresponding role and automatically removed from workspaces that don't correspond to their IdP groups.

General advice for testing

Generally, we recommend testing SSO just for login first BEFORE you enable Set group access. It's best to make sure people in your IdP can login to Pencil as expected before having their IdP group memberships add them to and remove them from workspaces automatically.

FAQ

1. If I created team members manually and they have username and passwords to login and then I enable SSO later, what happens to the users who have usernames and passwords already? Will they be duplicated?
 - a. **Answer: No, the team members will not be duplicated if their email address in your identity provider matches the email address that was used when they were manually created. There will just be one team member for that individual, and they'll be able to log in both with SSO and with their username and password.**