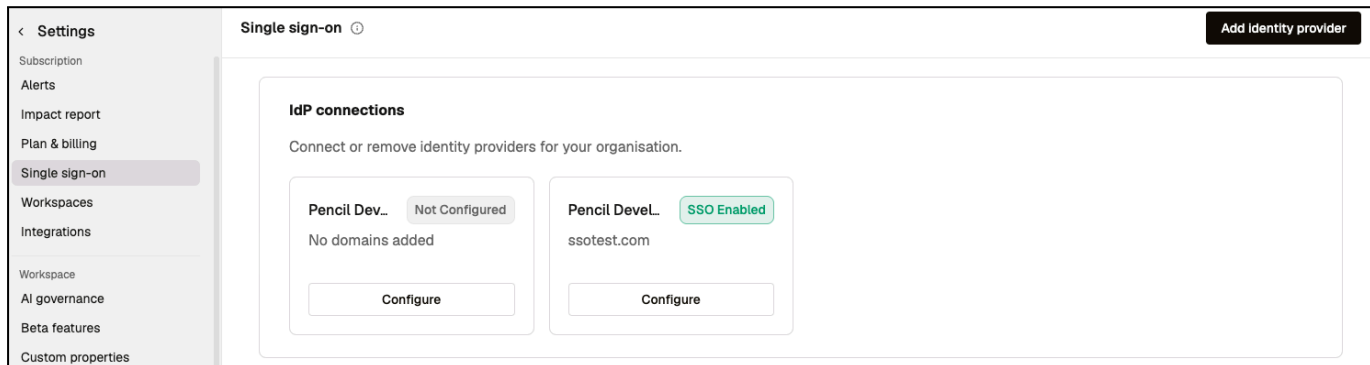


How to configure single sign-on in Pencil

Required role

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

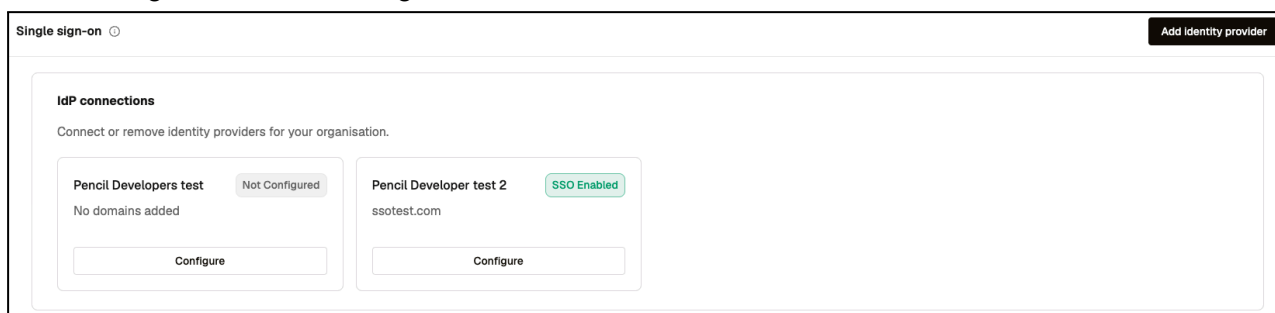


Loom video

<https://www.loom.com/share/3a7cfe54b8f244a7b8f3f28e1f7a6434>

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. **Advanced settings based on specifics of your IdP:** Leave these values with their default setting unless your Identity Provider IT Admin indicates they need to be changed.

Request signing

- ☐ Assertion signed
☐ Response signed
☒ Both

Choose the signature your IdP sends so Pencil can verify each SAML response.

☒ **Enforce audience verification** ⓘ

Verifies that the identity provider explicitly issued the authentication response for this application.

☐ **Disable requested authentication context** ⓘ

Stops requesting strict password authentication from your Identity Provider. Enable this if you use Azure AD / Microsoft Entra ID, AD FS, or require Multi-Factor Authentication (MFA).

5. **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)

6. **Save Changes:** Click "Save Changes" under the "Connect your identity provider" section.
7. *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 8-10. If you also want SSO to control which users have access to which workspaces, do steps 8-10.*
8. **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.

9. **Save Changes:** Click "Save Changes" under the "Set group access" section.
10. **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.**
11. **Enable SSO:** When you're ready to test, click the "Enable SSO" toggle at the top.



12. 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 "Require SSO to sign in", "SCIM" and before you enable "Set group access". It's best to make sure people in your IdP can login to Pencil as expected with SSO before disabling their password logins and having their IdP group memberships add them to and remove them from workspaces automatically.

What is SCIM?

System for Cross-domain Identity Management.

While Single Sign-On (SSO) handles authentication (verifying who you are when you log in), SCIM handles provisioning (automating user accounts).

1. **Automates Onboarding:** Automatically creates user accounts in cloud apps when a new hire is added to an identity provider.

2. Handles Deprovisioning: Automatically disables or deletes user access when an employee leaves the company.
3. Handles group provisioning so the Pencil system has access to a list of IdP group names.

To enable SCIM for automatic IdP group detection and automatic user provisioning and deprovisioning

IdP group provisioning

You can connect your IdP to Pencil over SCIM so your IdP group names flow through automatically and show up in the SSO group-to-workspace mapping screen, ready to select from a dropdown instead of typing them in by hand. This removes the risk of a typo silently breaking a mapping.

You'll just need to send your identity provider IT admin the info in the SCIM section of this page after turning it on:

Then, to switch it on, there are a few steps required in your IdP by the IT admin:

1. In your IdP, open the Pencil application and enter the credentials generated for you.
2. Assign the specific groups you want available in Pencil to that application.
3. **If you just want SCIM for group provisioning and not user provisioning:**
Turn group provisioning on but leave user provisioning turned off for now.
4. Start the sync.

Once the first sync finishes, those group names will show up in the dropdown on Pencil's group-to-workspace mapping screen, ready to select. The sync runs on your IdP's schedule rather than instantly, so allow a little time after you start it (most IdPs also have a "provision on demand" option if you want to push a group straight away). Until you push groups this way you can still type group names in manually, so nothing is blocked in the meantime.

IdP user provisioning/deprovisioning via SCIM

With SCIM, you can also have your identity provider (IdP) create users in Pencil and add or remove them from workspaces automatically as changes happen in your IdP, instead of

waiting for each person's next SSO login for IdP changes to apply. With SCIM, when someone is offboarded in your IdP, their Pencil access will be removed automatically.

You'll just need to send your identity provider IT admin the info in the SCIM section of this page after turning it on:

▼ User provisioning (SCIM) ⓘ

Configure your identity provider to provision and deprovision members with SCIM.

OAuth endpoint ⓘ
Token URL your identity provider calls to exchange the client credentials.

SCIM endpoint ⓘ
Base URL your identity provider sends provisioning requests to.

Client ID ⓘ
Identifies this connection when your identity provider requests a token.

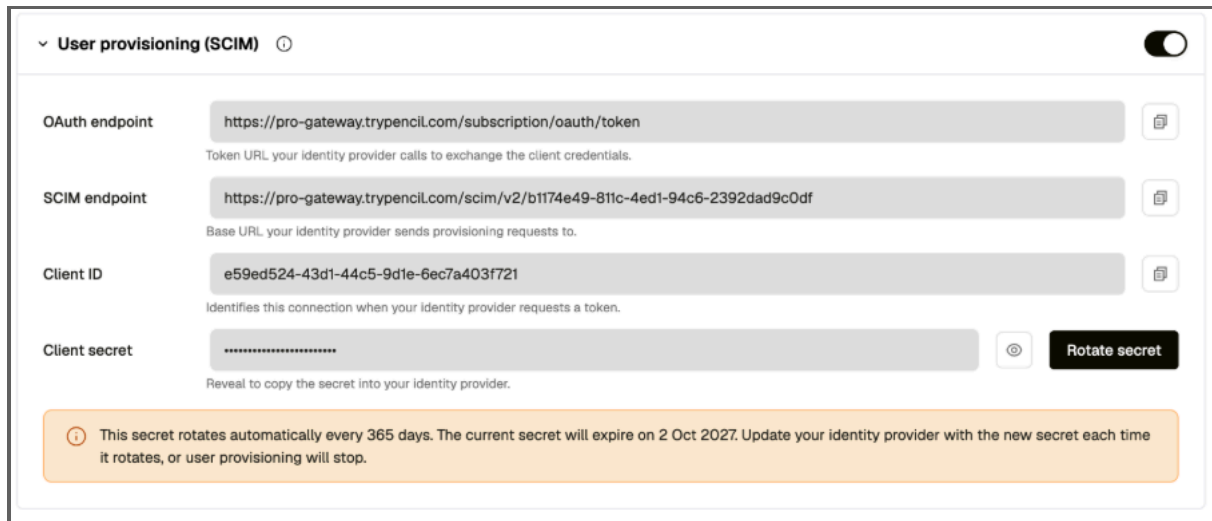
Client secret
Reveal to copy the secret into your identity provider.

Then, to switch it on, there are a few steps required in your IdP by the IT admin:

1. Enter the SCIM credentials from the SCIM section of the Single sign-on page in Pencil, if that isn't done yet.
2. Assign the users and groups you want in Pencil to the application.
3. Turn user provisioning on alongside group provisioning.
4. Start the sync.

SCIM Secret Rotation

Every 365 days, the client secret for SCIM will expire. The UI on the Settings > Single Sign-on page shows the date that the current secret will expire. At some point before that date, please click the "**Rotate secret**" button to get a new secret.



▼ User provisioning (SCIM) ⓘ

OAuth endpoint ⓘ
Token URL your identity provider calls to exchange the client credentials.

SCIM endpoint ⓘ
Base URL your identity provider sends provisioning requests to.

Client ID ⓘ
Identifies this connection when your identity provider requests a token.

Client secret ⓘ **Rotate secret**
Reveal to copy the secret into your identity provider.

ⓘ This secret rotates automatically every 365 days. The current secret will expire on 2 Oct 2027. Update your identity provider with the new secret each time it rotates, or user provisioning will stop.

Once you get a new secret, you have 1 hour to update your IdP with that new secret, as there's a 1-hour overlap where the old secret continues to work.

Rotate client secret?



A new secret will be generated. The current one keeps working for 1 hour after, so update your identity provider before then.

Cancel

Rotate secret

How to amend role priority order for tiebreaking

You can choose which role a user gets when they belong to more than one identity provider group mapped to the same workspace with different roles. Pencil gives them whichever of those roles is highest in your role priority list.

To set the order, go to the Settings > Single sign-on page and click "Amend Role Priority" in the "Set group access" section, drag the roles into the order you want and click Save.

Pencil's standard roles already come in a sensible default order, so this only matters for organisations using custom roles and with Set group access on where a user can belong to multiple IdP groups that map to the same workspace with different roles.

Loom video showing the functionality:

<https://www.loom.com/share/9676e4ff24e14ab49bb927f09fbeccb4>

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 (or only with SSO if you enable the "Require SSO to sign in" toggle and their email domain matches an email domain you've entered).**