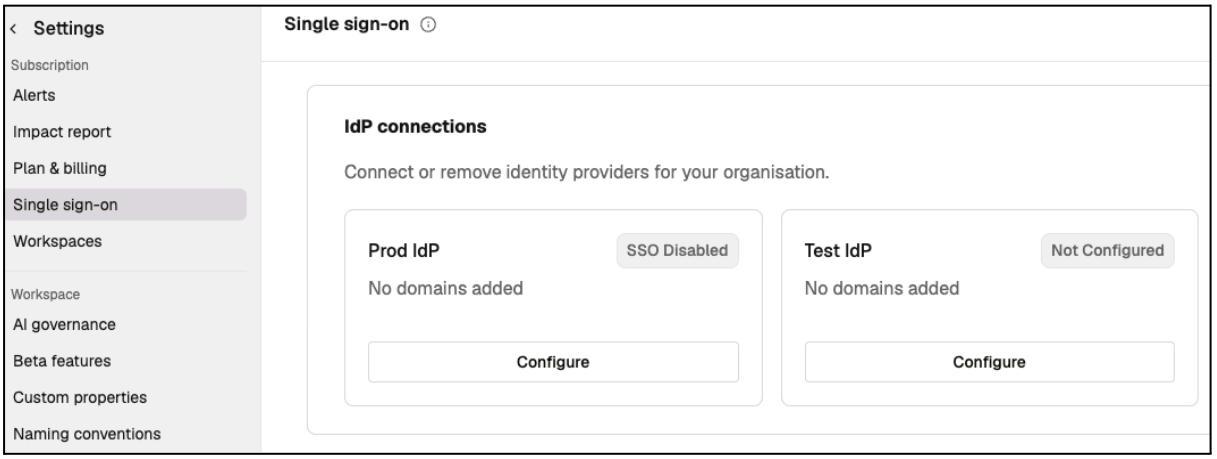
Introducing Self-Serve Single Sign-On (SSO)

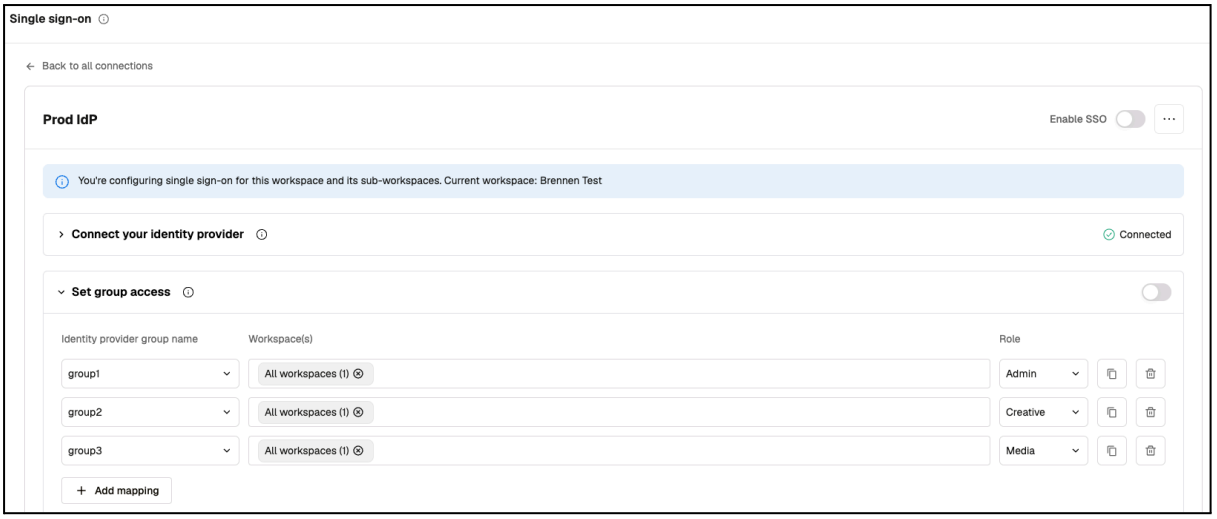
We've introduced self-serve SAML 2.0 single sign-on, so:

1. Enterprise IT admins can connect their identity provider to control who can log in and optionally automate which workspaces and roles each person receives, all from Pencil's settings without Pencil engineering involvement.
2. End users don’t need to have a Pencil specific password as they can log in through their organizations identity provider.

Until now, setting up SSO for a Pencil subscription required custom engineering work from Pencil and, even after a user authenticated, someone had to invite them into each workspace with the right role. At enterprise scale, with dozens of workspaces across different teams, that manual, per-workspace invitation didn't scale.

Self-serve single sign-on turns setup into a configuration task: a subscription admin connects a SAML 2.0 identity provider, sets the email domains allowed to sign in, and can optionally map identity provider groups to workspaces and roles so users are placed in and removed from workspaces automatically on login according to their current identity provider group membership.





What's new

- **Self-serve SAML setup:** From Settings → Single sign-on, a subscription admin adds an identity provider, downloads Pencil's SP metadata, and connects their IdP by metadata URL or by uploading the metadata XML.
- **Email-domain sign-in:** Admins list the email domains used by people in their identity provider, so the right users can sign in with SSO from the Pencil login page.
- **Optional group access mapping:** Map each identity provider group to one or more workspaces and a role, with multiple rows per group allowed when a group needs different roles in different workspaces.
- **Automatic provisioning on login:** With Set group access enabled, users are created on first SSO login and added to the workspaces their groups map to, in the mapped role, with no manual invitations required.
- **Access that stays in sync:** Group membership is re-checked at every login, so people are added to the workspaces they should have and removed from those their groups no longer map to.
- **Login-only or full provisioning:** Use SSO purely for login, or turn on group-based access when you're ready for Pencil to manage workspace membership too. Accounts that were manually created before SSO was enabled aren't duplicated and can still sign in with their existing credentials and sign in with SSO if they’re also present in the identity provider.

Why it matters

- **No need for custom engineering for SSO:** Admins connect their own identity provider and manage access from settings, so SSO becomes a setup task rather than a custom build.
- **Onboarding at scale:** Hundreds of users land in the right workspaces with the right role automatically, instead of being invited one workspace at a time.
- **Access that mirrors your directory:** Because mappings are validated at every login, workspace access stays aligned with your identity provider as teams change.
- **Security-review ready:** Standard SAML 2.0 with domain-scoped sign-in gives IT the controls enterprise security teams expect.

- **Adopt at your own pace:** Start with login-only SSO, then enable group-based provisioning once you're confident in your mappings.

Who it's for

- Enterprise accounts running many workspaces
- Subscription admin role is required to configure
- Enterprise IT and identity admins

What this unlocks

Self-serve single sign-on turns SSO from a per-account engineering project into a configuration any enterprise admin can own, letting teams connect their identity provider once and have the right people land in the right workspaces automatically, while access stays governed by their directory.

Give it a try and let us know what you think! 🚀

A guide for how to set this up can be found here.