Manage SSO Connections

Update July 2026: Migrate to the New SSO Experience

Alchemer has introduced a new single sign-on (SSO) experience that simplifies how your team signs in and how you manage access. **Complete your migration from the legacy SSO connection to the new SSO experience before October 31, 2026 to keep your team logging in without interruption and to continue to access new features and platform developments.**

> **Not sure if you're on the new or legacy SSO?**
> Go to **Account** > **Security** > **SSO connections**. If no active connection appears there, your organization is still on legacy SSO and should migrate before the **October 31, 2026** cutoff using the steps below. (Legacy connections are managed under **Integrations** > **Data Connections** > **SSO Users.)**

Why Migrate Now?

The legacy SSO connection is currently planned to be deprecated after October 31, 2026. Complete your migration before the deadline to keep your team logging in without interruption.

In addition, new features are being built using the new SSO connection, so those features stay switched off until you migrate. Once you migrate, you get:

- Ongoing user login access. Legacy SSO is currently planned to be deprecated after October 31, 2026. Migrating before then keeps your whole team logging in without interruption.
- Self-service management. You can set up, test, and manage SSO yourself through a simple self-service interface.
- New features as they're released. New capabilities are built using the new SSO connection, so migrating keeps your account current with the newest features.
- Alchemer Dashboard. If eligible, Dashboard lets you view and analyze your feedback across surveys and feedback sources in one place. It only works on the new SSO connection, so migrating is the step that switches it on.

> **Don't wait - Legacy SSO ends October 31, 2026**
> If your organization hasn't migrated by October 31, 2026, your team may lose the ability to sign in through your current SSO connection. Migrating now keeps your access uninterrupted. If you have questions or concerns about the migration deadline, please contact your Customer Success Manager.

How the New SSO Experience Works

Previously, SSO configurations were managed under **Integrations** > **Data Connections** > **SSO Users**. With this update, SSO will be managed in a dedicated section under **Account** > **Security** > **SSO Connections**.

From the new page, you can:

- **Set up new SSO connections yourself** using a step-by-step assistant, on your timeframe.
- **Test before you activate**, then turn a connection on or off whenever you need to.
- **Set login exceptions** for people who need a username and password instead of SSO, like a billing contact or an outside vendor.
- **Assign a unique alias** so users reach the right login screen when you run more than one connection.
- **Migrate everyone at once** when you activate your first new connection, instead of switching users over one by one.

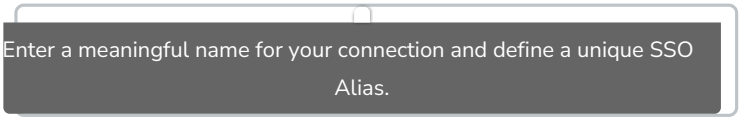
Access Requirements

To access the new SSO Connections page, your account must have the appropriate permission. If you don't, please reach out to your admin or contact Alchemer Support.

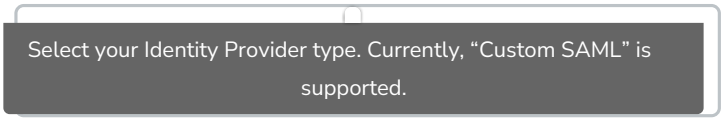
How to Set Up a New SSO Connection

> **Before you start: You'll need Admin permission, access to your Identity Provider (IdP), and about 20 minutes.** You can build and test a new SSO connection while your existing SSO connection remains active, so there's no downtime.

1. Go to **Account> Security > SSO Connections**
2. Click **Add a new connection**
3. Name your connection and choose a unique SSO Alias. Most customers use their organization's name.



4. Click **Save & Continue**, then **Get Started** to launch the setup assistant
5. Follow the prompts to: Select "Custom SAML"

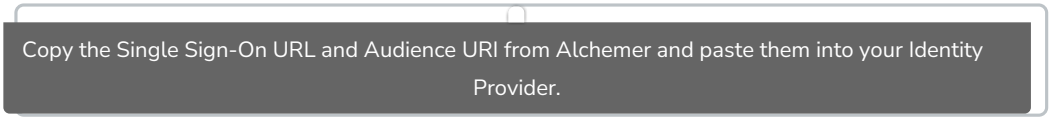


You will need to take the links from Alchemer and paste them into your IDP.

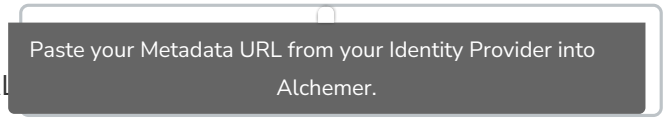
The SSO URL = The Assertion Consumer Service URL
The Identity Provider Entity ID = the Entity ID

> **Note on Attribute Statements**
> In the metadata file, pay particularly close attention to the 'name' and 'email' attribute statements. You must provide these attribute statement names when completing SSO setup with your Identity Provider.
>
> These attribute statements are required for setting up SSO for Alchemer Digital, even if they are listed as optional by some Identity Providers.
>
> 
>

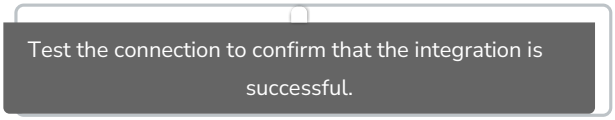
6. Copy and paste values between Alchemer and your IdP (Identity Provider)



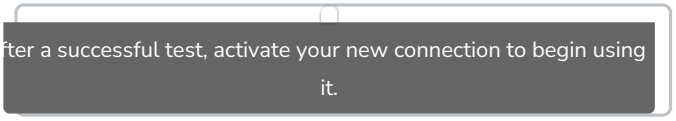
7. Provide your Metadata URL



8. Click **Create Connection** and proceed through the test flow



9. Once testing is complete, click **Activate** to enable the connection



> Once you activate the new connection, any logged in users, including the admin, may be logged out and prompted to login with the new method.

Managing Connections After Setup

Login Exceptions

Admins can define which users are allowed to log in using their Alchemer username and password:

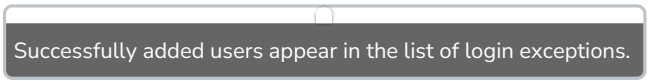
1. Navigate to **SSO Connections**

2. Under "Users who can log in without SSO," click **Add User**



3. Enter the user's email address and click **Add**

4. To remove a user, click **Remove User** next to their name



> By default, all users with an Admin role are automatically added to the exception list.

Deactivating a Connection

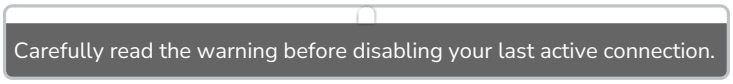
To deactivate an SSO connection:

1. Go to **SSO Connections**

2. Click **Disable SSO** next to the relevant connection



3. If it’s the only active connection, you’ll be prompted to confirm by typing "Disable SSO."



If the last connection is disabled, users will receive an autogenerated username/password login, and a password reset email will be sent.

Important Notes

- Access to the legacy SSO section will remain accessible until you activate your new connection. Future product enhancements will require you to migrate first.

- SSO for survey respondents is unaffected by this change.
- Just-In-Time (JIT) provisioning is not supported for all users yet.

If you have questions or need help, reach out to Alchemer Support.

Related Articles