Manage SSO Connections

ATTENTION!

SSO is available to our business platform customers.
If you are interested in SSO, please contact us for additional information.

Alchemer is introducing a new, streamlined way for customers to manage their Single Sign-On (SSO) configurations. This enhanced experience gives admins full control over SSO setup, testing, activation, and user management without needing to contact support.

If you are still on our legacy SSO feature and need help, please go here. This way of connecting will be deprecated in the future, so we encourage you to migrate with the setup steps below.

What's Changing?

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.

The new setup includes:

- A step-by-step self-service setup assistant
- The ability to test and activate new SAML SSO connections
- A user-friendly interface to manage login exceptions and aliases

Key Features

- Self-Service Setup: Configure your SAML-based SSO with guided steps directly in Alchemer.
- Connection Management: Add, test, activate, or deactivate SSO connections as needed.
- Login Exceptions: Add or remove users to the new SSO easily.
- Unique Aliases: Assign and manage unique SSO Aliases for each connection.
- Automatic Migration: Upon activating your first new connection, all active users on your account are automatically migrated.

Access Requirements

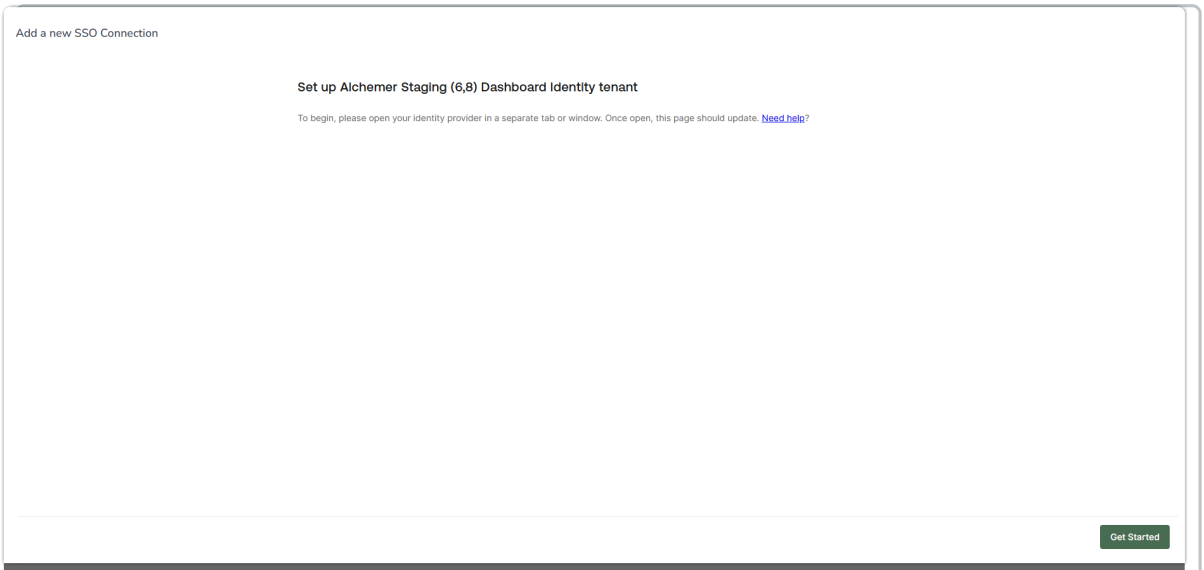
To access the new SSO Connections page, your account must have the appropriate permission. If you don't, please reach out ot your admin or contact Alchemer Support.

How to Set Up a New SSO Connection

1. Go to **Account > Security > SSO Connections**

2. Click **Add a new connection**

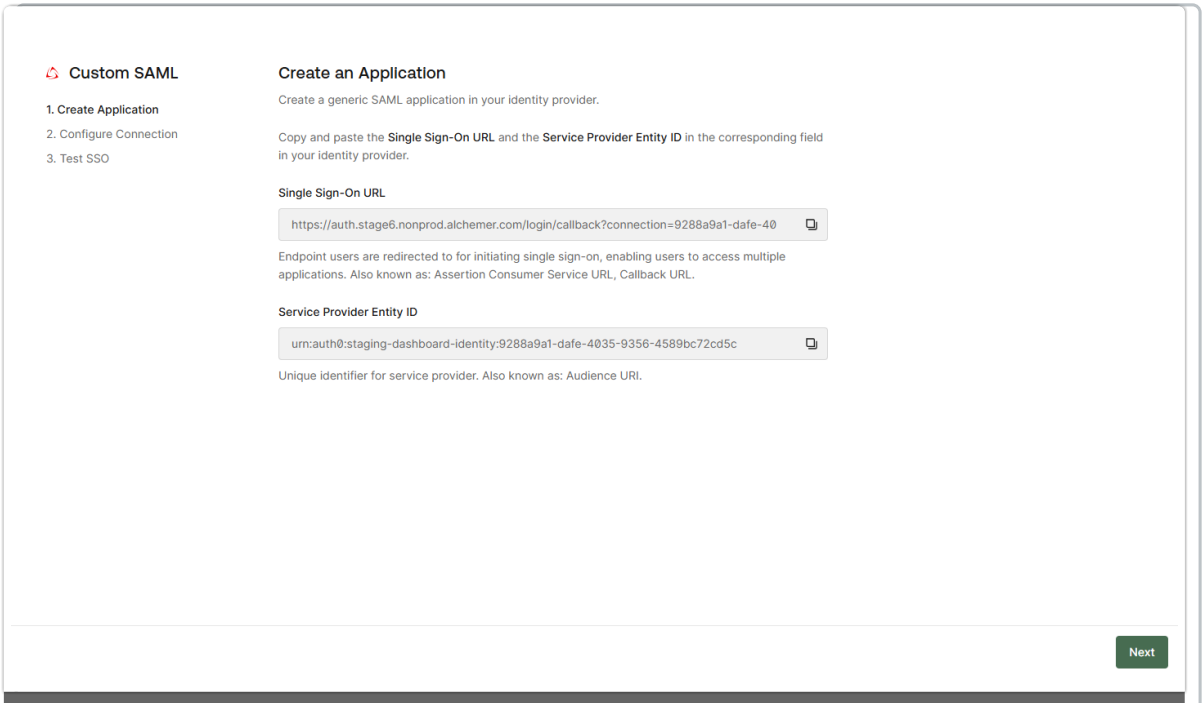
3. Name your connection and choose a unique SSO Alias. Most customers use their organization's name.



Enter a meaningful name for your connection and define a unique SSO Alias.

4. Click **Save & Continue**, then **Get Started** to launch the setup assistant

5. Follow the prompts to: Select "Custom SAML"

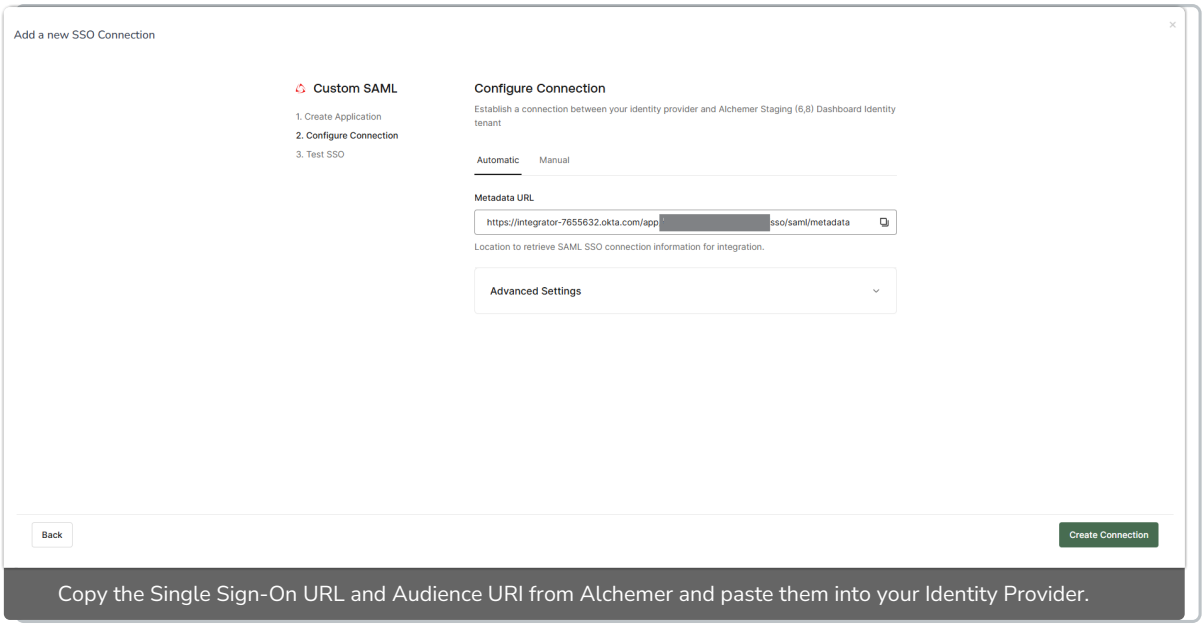


Select your Identity Provider type. Currently, "Custom SAML" is supported.

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

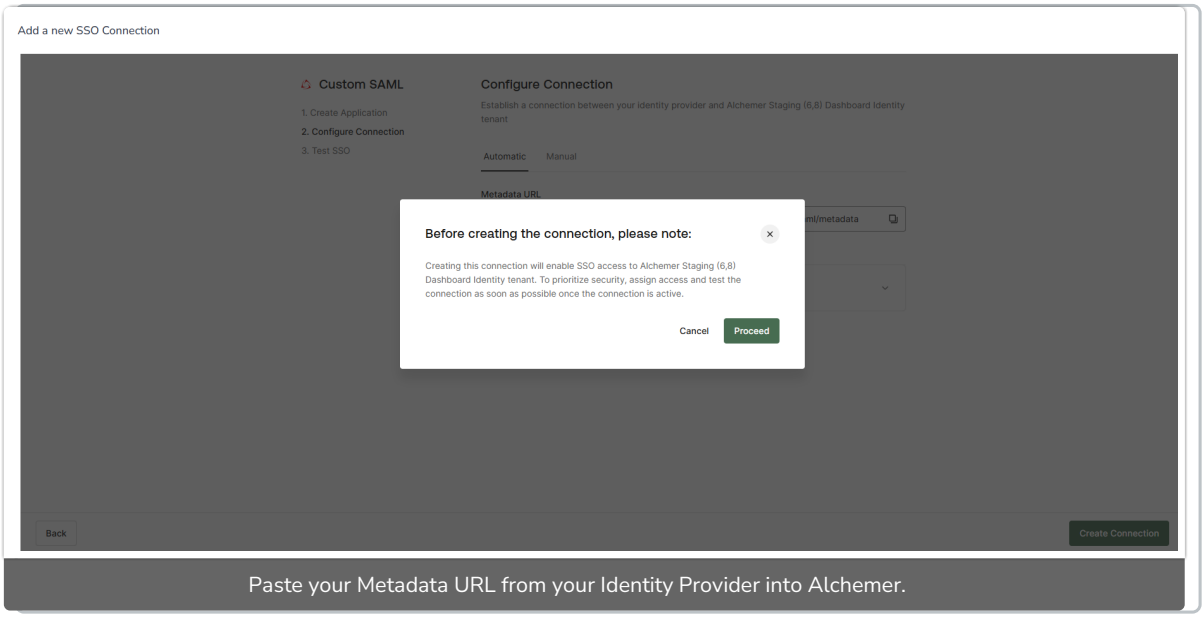
The SSO URL = The Assertion Consumer Service URL
The Identity Provider Entity ID = the Entity ID P

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



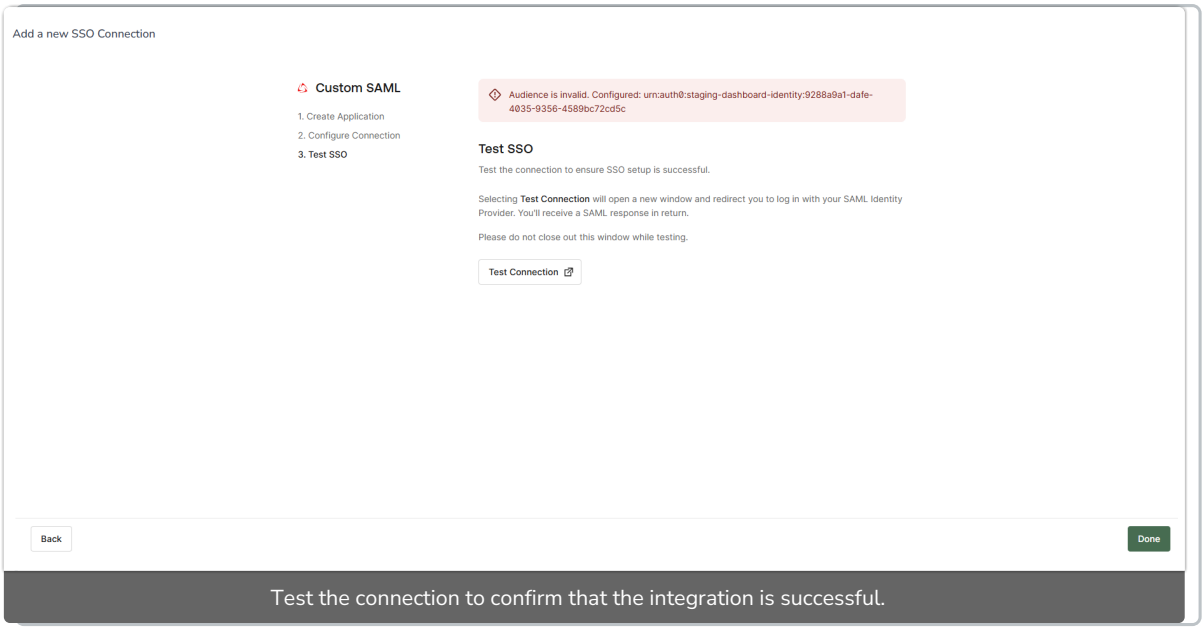
Copy the Single Sign-On URL and Audience URI from Alchemer and paste them into your Identity Provider.

7. Provide your Metadata URL



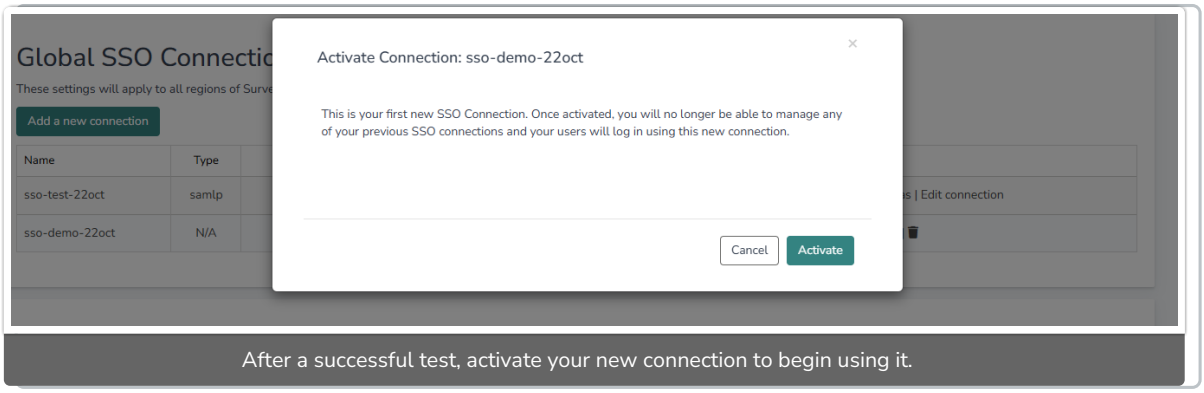
Paste your Metadata URL from your Identity Provider into Alchemer.

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



Test the connection to confirm that the integration is successful.

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



After a successful test, activate your new connection to begin using it.

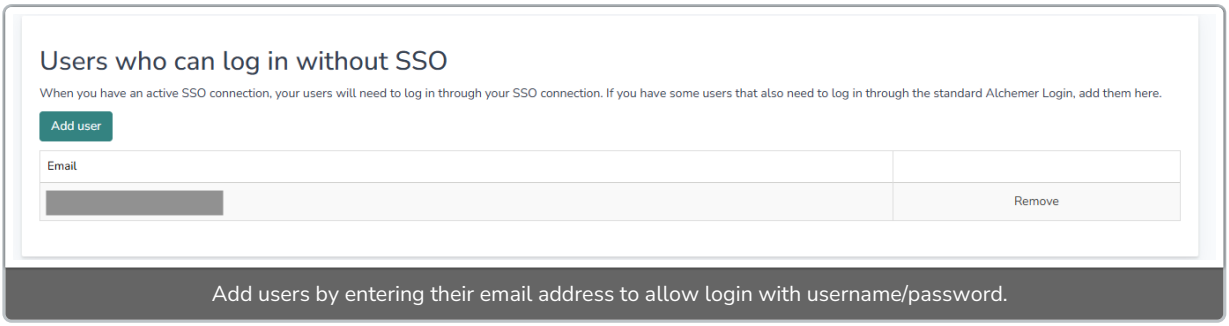
> **Note:** You can create and test a new SSO connection while your existing SSO connection remains active.

Managing Login Exceptions

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

1. Navigate to **SSO Connections**

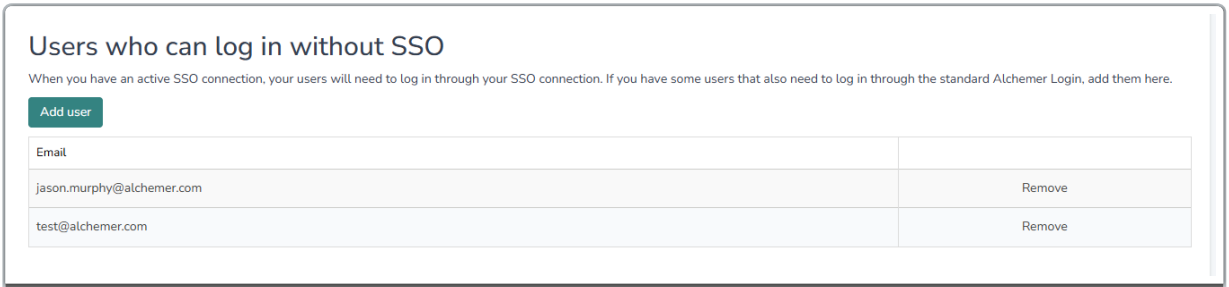
2. Under "Users who can log in without SSO," click **Add User**



Add users by entering their email address to allow login with username/password.

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

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



Successfully added users appear in the list of login exceptions.

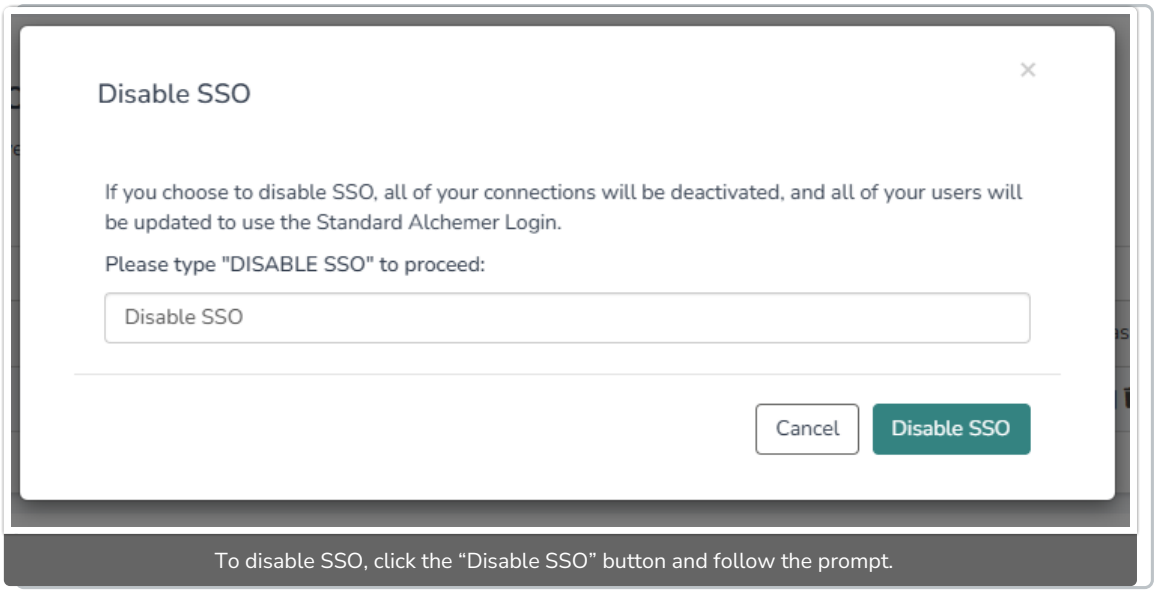
> By default, all users with an Admin role are automatically added to the exception list.

Deactivating a Connection

To deactivate an SSO connection:

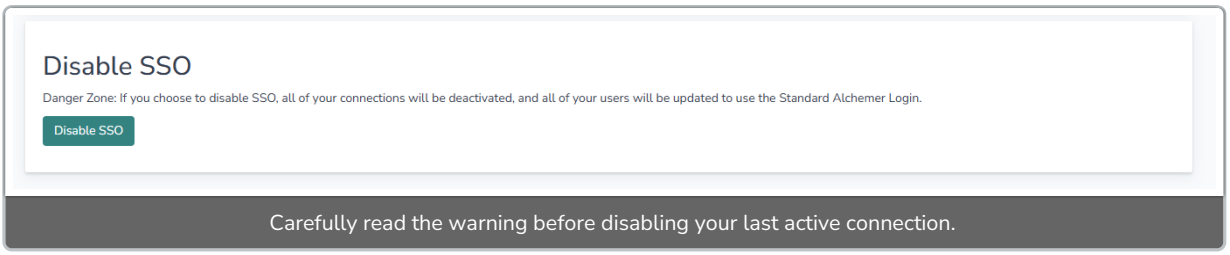
1. Go to **SSO Connections**

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

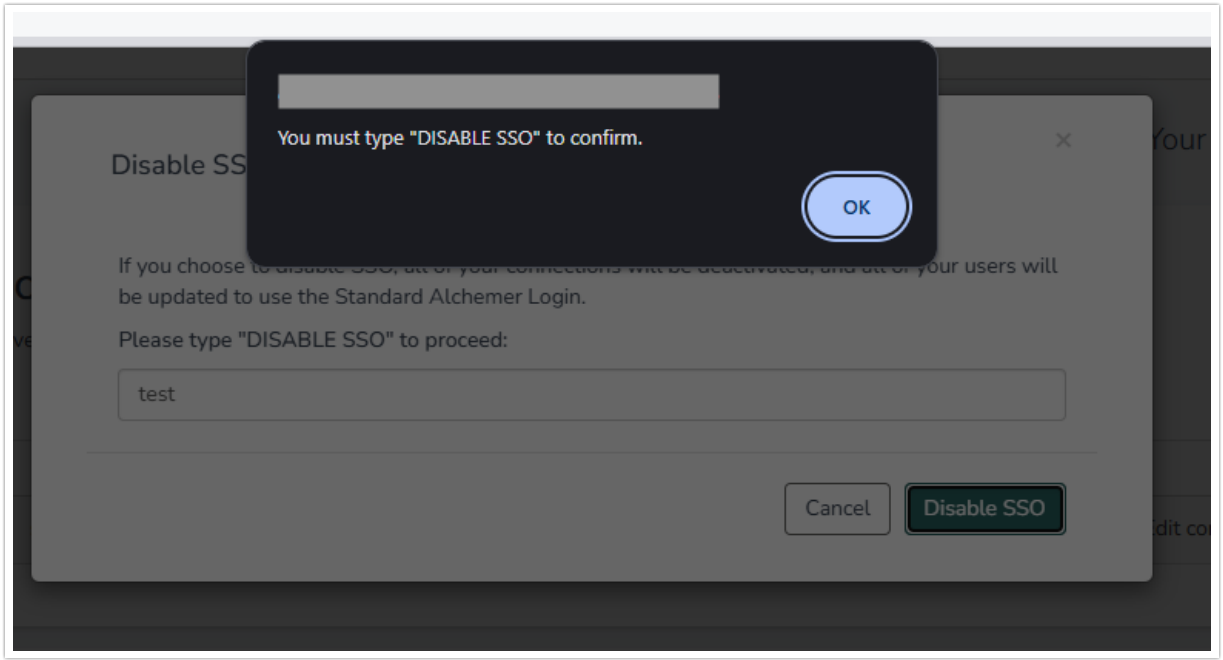


To disable SSO, click the “Disable SSO” button and follow the prompt.

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



Carefully read the warning before disabling your last active connection.



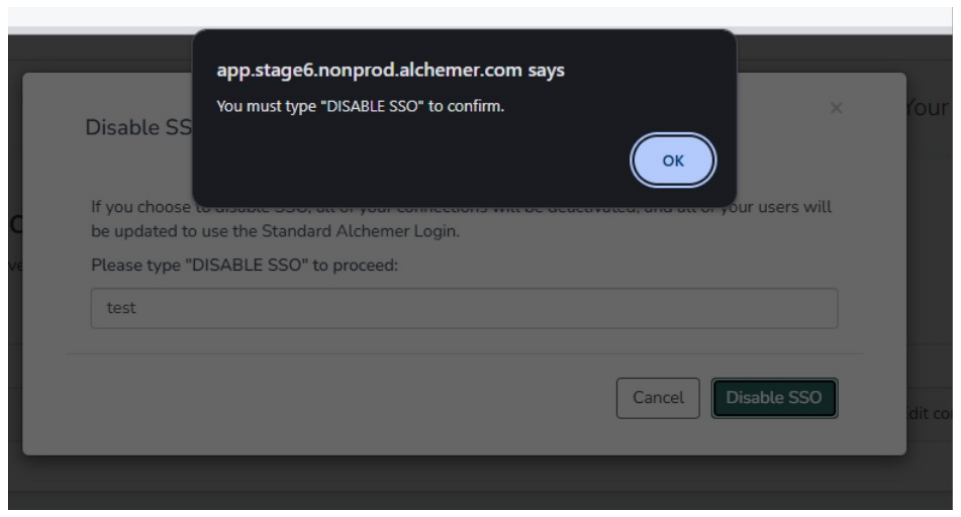
If the last connection is disabled, users will receive an autogenerated username/password login, and a password reset email will be sent.

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.

For additional configuration guidance, see User Single Sign-On | Alchemer Help.

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



Related Articles