

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 to 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.

Add a new SSO Connection

Set up Alchemer Staging (6,8) Dashboard Identity tenant

To begin, please open your identity provider in a separate tab or window. Once open, this page should update. [Need help?](#)

Get Started

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"

Custom SAML

1. Create Application

2. Configure Connection

3. Test SSO

Create an Application

Create a generic SAML application in your identity provider.

Copy and paste the **Single Sign-On URL** and the **Service Provider Entity ID** in the corresponding field in your identity provider.

Single Sign-On URL

https://auth.stage6.nonprod.alchemer.com/login/callback?connection=9288a9a1-dafe-40

Endpoint users are redirected to for initiating single sign-on, enabling users to access multiple applications. Also known as: Assertion Consumer Service URL, Callback URL.

Service Provider Entity ID

urn:auth0:staging-dashboar-identity:9288a9a1-dafe-4035-9356-4589bc72cd5c

Unique identifier for service provider. Also known as: Audience URI.

Next

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)

Add a new SSO Connection

Custom SAML

1. Create Application

2. Configure Connection

3. Test SSO

Configure Connection

Establish a connection between your identity provider and Alchemer Staging (6,8) Dashboard Identity tenant

Automatic

Manual

Metadata URL

https://integrator-7655632.okta.com/app/ sso/saml/metadata

Location to retrieve SAML SSO connection information for integration.

Advanced Settings

Back

Create Connection

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

7. Provide your Metadata URL

Add a new SSO Connection

Custom SAML

1. Create Application

2. Configure Connection

3. Test SSO

Configure Connection

Establish a connection between your identity provider and Alchemer Staging (6,8) Dashboard Identity tenant

Automatic

Manual

Metadata URL

https://integrator-7655632.okta.com/app/ sso/saml/metadata

Location to retrieve SAML SSO connection information for integration.

Advanced Settings

Back

Create Connection

Before creating the connection, please note:

Creating this connection will enable SSO access to Alchemer Staging (6,8) Dashboard Identity tenant. To prioritize security, assign access and test the connection as soon as possible once the connection is active.


Cancel

Proceed


Paste your Metadata URL from your Identity Provider into Alchemer.

8. Click Create Connection and proceed through the test flow

Add a new SSO Connection

 **Custom SAML**

1. Create Application
2. Configure Connection
3. Test SSO

 Audience is invalid. Configured: urn:auth@staging-dashboar-identity:9288a9a1-dafe-4835-9356-4589bc72cd5c

Test SSO

Test the connection to ensure SSO setup is successful.

Selecting **Test Connection** will open a new window and redirect you to log in with your SAML Identity Provider. You'll receive a SAML response in return.

Please do not close out this window while testing.

[Test Connection](#)

[Back](#) [Done](#)

Test the connection to confirm that the integration is successful.

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

Global SSO Connections

These settings will apply to all regions of SurveyMonkey

[Add a new connection](#)

Name	Type	
sso-test-22oct	samlp	
sso-demo-22oct	N/A	

Activate Connection: sso-demo-22oct

This is your first new SSO Connection. Once activated, you will no longer be able to manage any of your previous SSO connections and your users will log in using this new connection.

[Cancel](#) [Activate](#)

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**

Users who can log in without SSO

When you have an active SSO connection, your users will need to log in through your SSO connection. If you have some users that also need to log in through the standard Alchemer Login, add them here.

Add user

Email	
	Remove

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

Users who can log in without SSO

When you have an active SSO connection, your users will need to log in through your SSO connection. If you have some users that also need to log in through the standard Alchemer Login, add them here.

Add user

Email	
jason.murphy@alchemer.com	Remove
test@alchemer.com	Remove

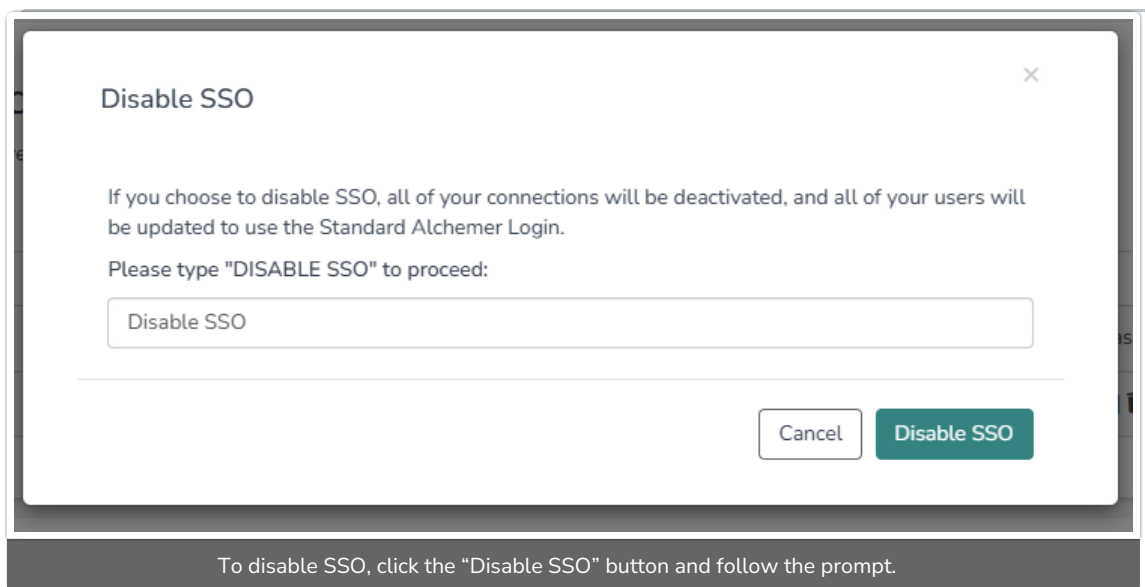
Successfully added users appear in the list of login exceptions.

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

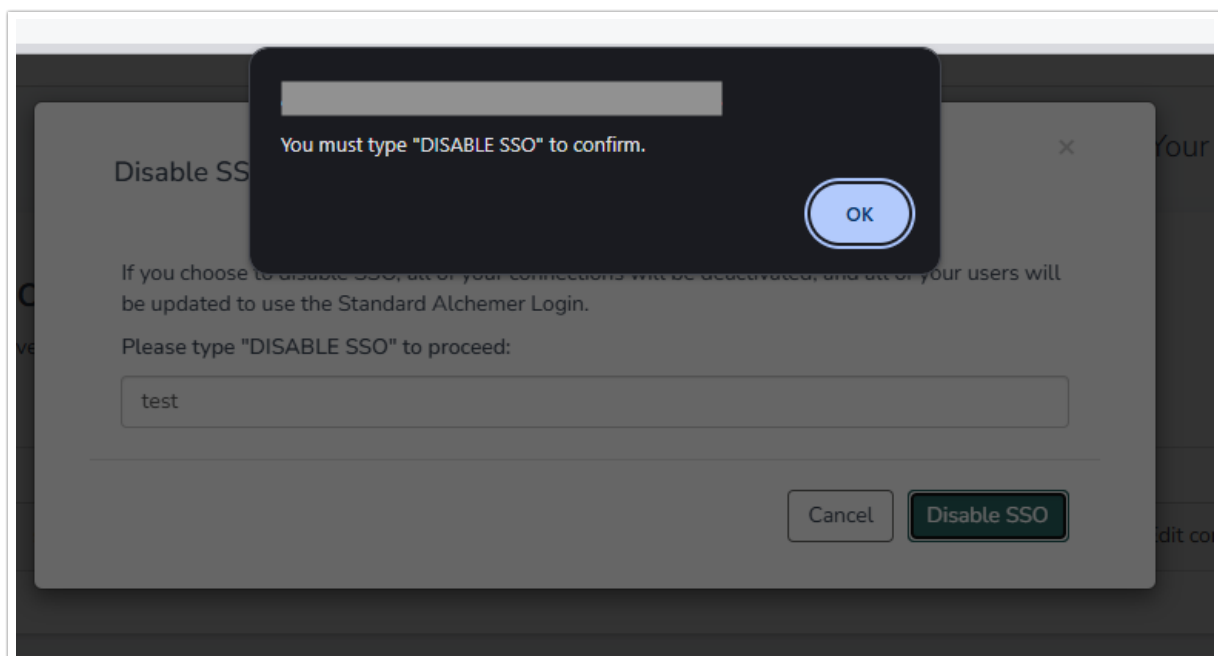
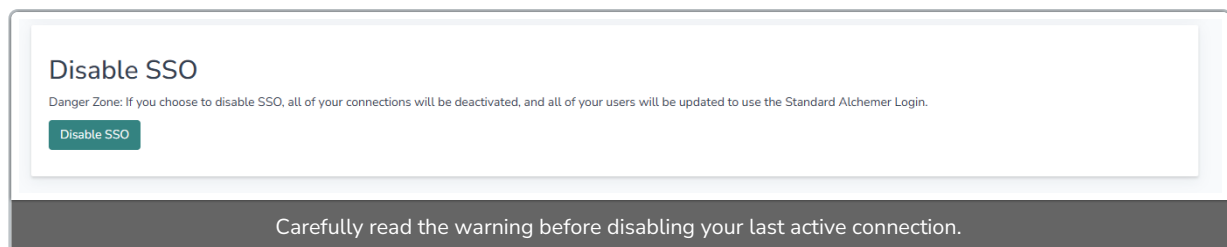
Deactivating a Connection

To deactivate an SSO connection:

1. Go to **SSO Connections**
2. Click **Disable SSO** next to the relevant connection



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.

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.

Attribute Statements (optional) [LEARN MORE](#)

Name	Name format (optional)	Value
name	Unspecified ▼	user.email ▼
email	Unspecified ▼	user.email ▼

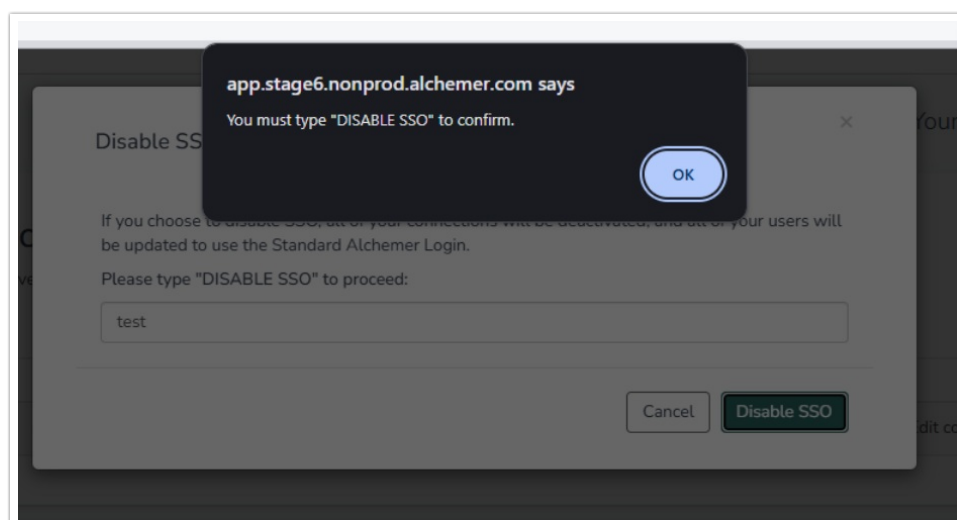
Add Another

Example from Okta SSO Setup

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
