CLEARSTORY

Configure Okta with Clearstory for SSO

To login with your Okta users via a single sign-on experience, Clearstory's authentication system must be configured based on the application you create in Okta on your end.

Customers can assign their users access to these applications to control access as they see fit. Clearstory simply needs a few pieces of information from these registered applications to be configured.

To get started with Okta, you will need to create an App registration in Okta. To make this easier, Clearstory is in the Okta integration directory (note that due our rebranding, it may still be listed as Clearstory until this listing can be updated) found here:
https://www.okta.com/integrations/clearstory/

Clicking the "+Add Integration" button will install an application with most settings automatically filled in, acting like a template where you first will be given the opportunity to name the application. After clicking "done" you can assign users and adjust the settings like any other application.

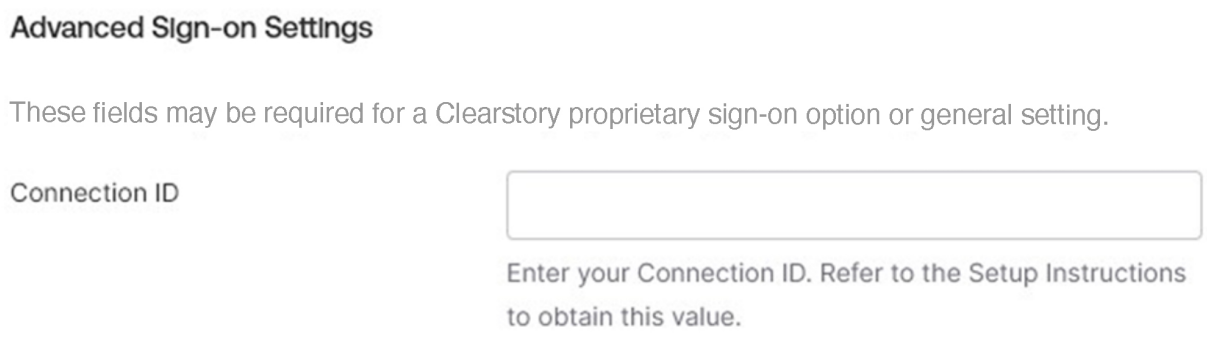
There are just a few areas that will need to be manually configured. The Okta integration also provides some instructions once installed. If you go to the "Sign On" tab, on the right you will see "SAML Setup" with a button that links to instructions specifically with related to your Okta account and application (generic instructions here: https://saml-doc.okta.com/SAML_Docs/How-to-Configure-SAML-2.0-for-clearstory.html)

If you do not wish to use SAML 2.0 or want to configure an application manually for any other reason, please contact Clearstory support for additional instructions.

What you'll need from Clearstory

You will need one primary piece of information here and that is the "Connection ID" as it is ultimately used in the redirect URI between the two systems.

You can technically make up the value here, it only needs to be unique in Clearstory's authentication system. If you contact support first, Clearstory can provide you with a unique value, so you know it doesn't conflict with any other customer's ID value. You'll set that in the settings of your application under the "Sign On" tab.



Note: While you can change the Connection ID in Okta, Clearstory must create and configure a new connection to change on their end. So please do not update this ID once set or if given to you.

What Clearstory will need from you

Clearstory will need the following to configure the connection. This allows our system to verify and work with your Okta application.

- Connection ID (if not provided to you by Clearstory)
- Metadata URL

Connection ID

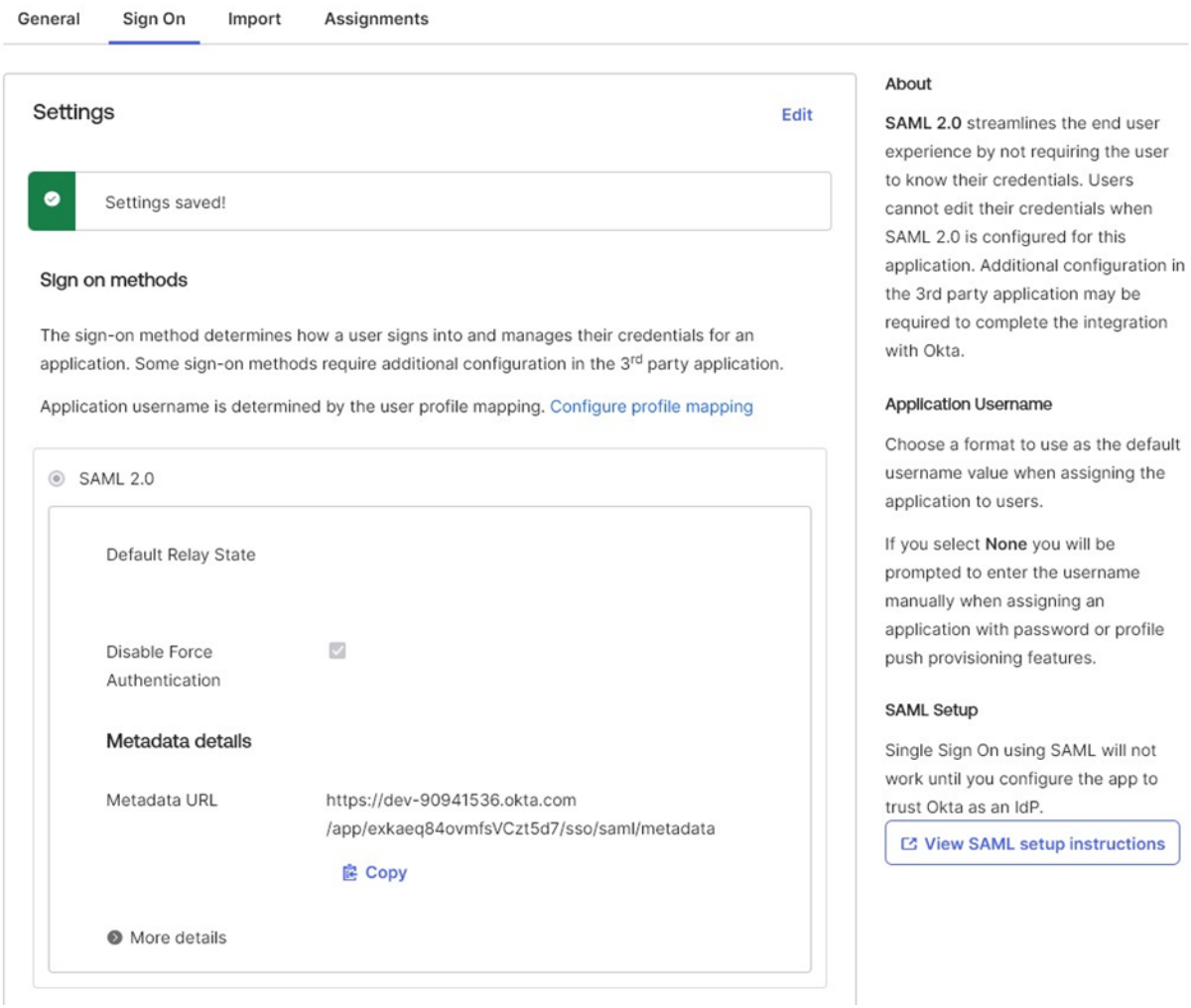
This is how the two systems are able to refer to one another. It's a unique value in Clearstory's authentication system that refers to your Okta application as a connection provider. If you change it, you will effectively disable the SSO connection.

After users login to your Okta portal they will be redirected back to Clearstory with this connection ID in the URL. If it doesn't match a connection configured on Clearstory's side, it will show an error about the connection not being found and prevent login.

You can always review, or update, this value from your application's settings in Okta under the "Sign On" tab. It's under the "Advanced Sign-on Settings" area.

Metadata URL

You can get this link from your application's settings in Okta under the "Sign On" tab.



This URL will contain the rest of the information needed to configure your connection in Clearstory's system. Specifically, Clearstory is configuring the following:

· Sign In URL

This is so users with a matching email domain will be redirected to your Okta login portal's URL

· X509 Signing Certificate

This is for Clearstory to authenticate responses sent from your login portal

- Identity Provider domain(s)

This is to match your user's email addresses to redirect them to your login portal as they attempt to login to Clearstory

The last piece of information, the domain(s), won't come from your metadata URL. Please provide this information though, especially if it isn't obvious based on the email address you're sending from. You may also have multiple email domains you want Clearstory to configure to be redirected when your users login.

Additional Notes

You will need to ensure that you assign your users access to the application you have created in Okta for SSO with Clearstory.

Please note that if you had users previously using Clearstory, you may want to communicate to them that they will no longer be able to login using the email and password they set for Clearstory once SSO is enabled. This may or may not be so obvious to them when they see your Okta login portal. Users will also not be able to go through a reset password flow from Clearstory's application at this point since this is handled by your IdP (Okta).

Clearstory Identifies Users by Email Address

Clearstory will direct to your login portal when there is a matching email domain. Clearstory currently doesn't recommend IdP-Initiated SSO as that flow carries security risks. More information can be found from our authentication service provider auth0 (Okta): https://auth0.com/docs/authenticate/protocols/saml/saml-sso-integrations/identity-provider-initiated-single-sign-on

IdP-Initiated SSO would be one alternative to the domain match and redirect method though. If you have more complex needs, please reach out to Clearstory to coordinate a solution that works for you.

This also means no matter how your users login, so long as the email address matches, they will be treated as the same user in Clearstory. In other words, if you allowed your users to login using Procore SSO as well, this would work in addition to your own SSO *so long as the email address from both providers were the same*.

Each time a user logs into Clearstory, very basic profile information is synced with our authentication system, though users are still asked to set their first and last name when initially onboarding with the Clearstory software. The Clearstory application is not currently syncing information like first/last name, but users can update their name at any time from their profile settings in the Clearstory app.

Changing Email Addresses

Users, of course, will not be able to change their email address from the Clearstory application when using SSO. For help with linking a different email address (or identity) with an existing user in Clearstory, please contact support. Clearstory will be able to make the necessary adjustments to ensure your users continue to have access to their existing Clearstory account.

Multiple Domain Names

If you have multiple domains, we can configure the login experience to redirect anyone providing an email address with those domains. You are not limited to just one for the purposes of SSO and redirecting to your login portal. However, it's important to note that Clearstory's system will suggest users to join companies based on their email domain.

If using multiple email domains, you may need to add users from within Clearstory's application under the "Settings > Manager Users" section. When users are added here, they will already have a user record in Clearstory's database that has your associated company linked as well as the email address. This way, when your user logs in with SSO, they will immediately be linked to the proper user account in Clearstory even despite having a different email domain.