OKTA SSO Guide

Outline

Prerequisites

Before you start integrating OKTA as your SSO provider with StackIdentity you need the following:

1. Okta Application Administrator Role
2. StackIdentity Organization Administrator Role

Both need to be activated to your account before you can configure OKTA as an IdP for your organization.

Supported Features

Currently, StackIdentity SSO login supports logging in to the StackIdentity platform using your Organization's IdP. The workflow enabled is IdP Initiated Login. We currently do not support runtime provisioning of accounts. So, if an account does not exist on the StackIdentity platform but exists on OKTA it will not be able to login.

For a successful login to work, you need to have an account on Stack Identity for the user that is going to use OKTA to login. Accounts can be created by the Organization Owner and the Organization Administrator Roles on the Stack Identity Platform. The total number of users within an organization are tied to a particular Plan type.

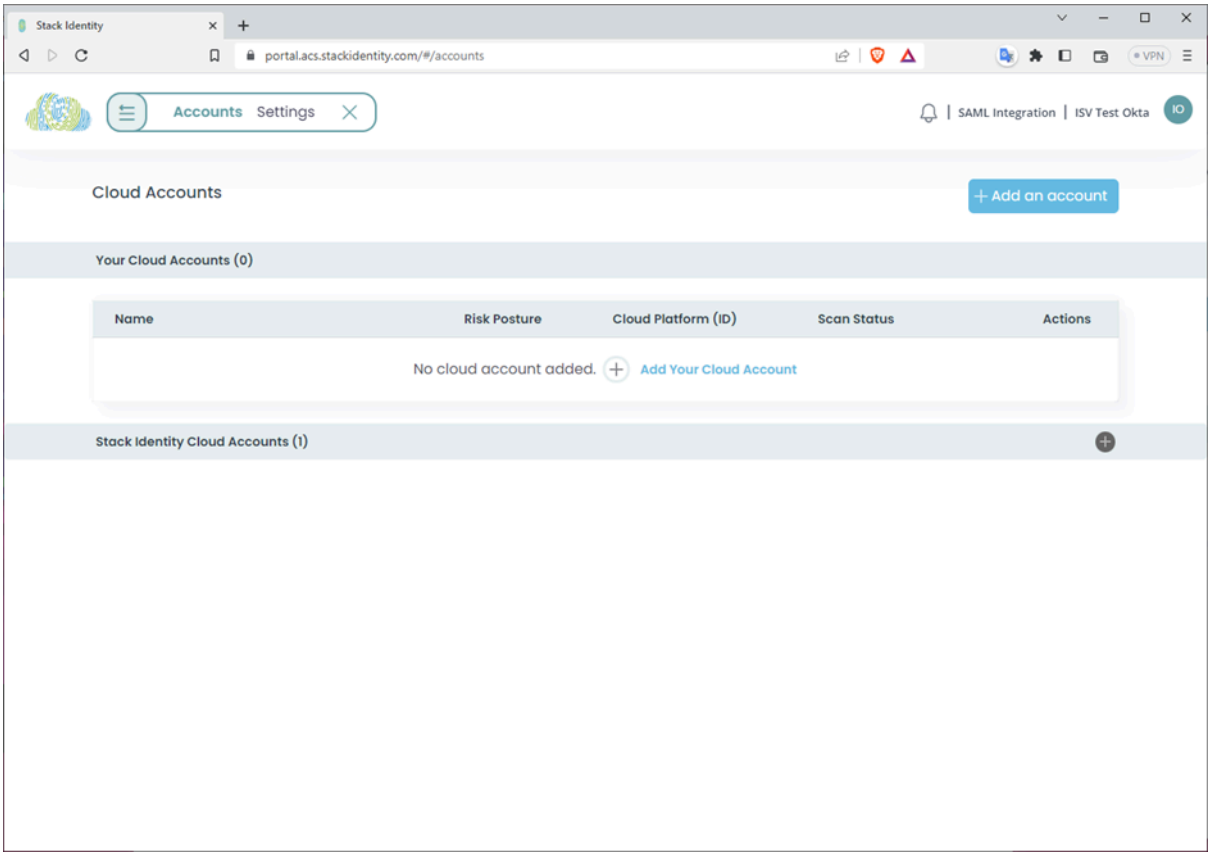
Features

- IdP-initiated SSO

For more information on the listed feature, visit the Okta Glossary.

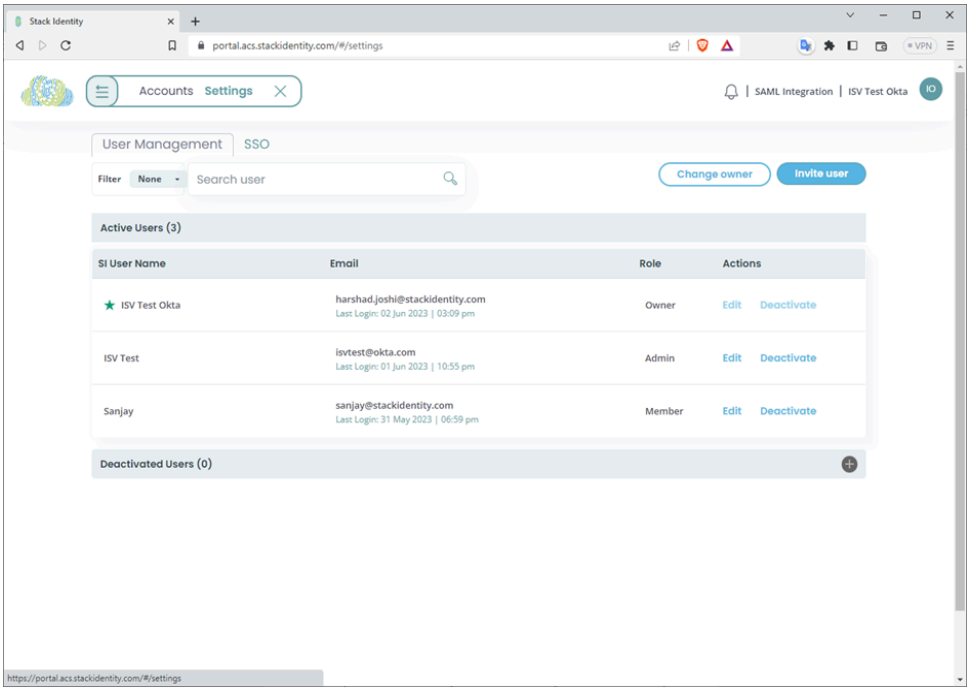
Configuration Steps

1. Login to the StackIdentity Website using your account. This account needs to be Organization Owner or the Organization Administrator.

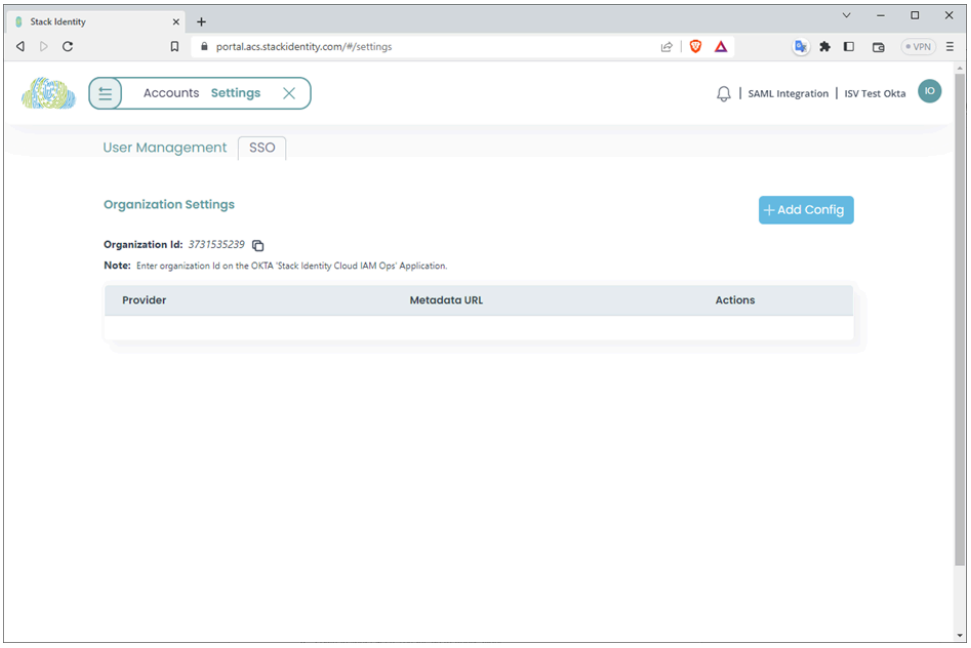


2. In the Dashboard view, go to the Settings Page by clicking on the Settings link in the top Navigation Links. It is located right next to the Accounts link.

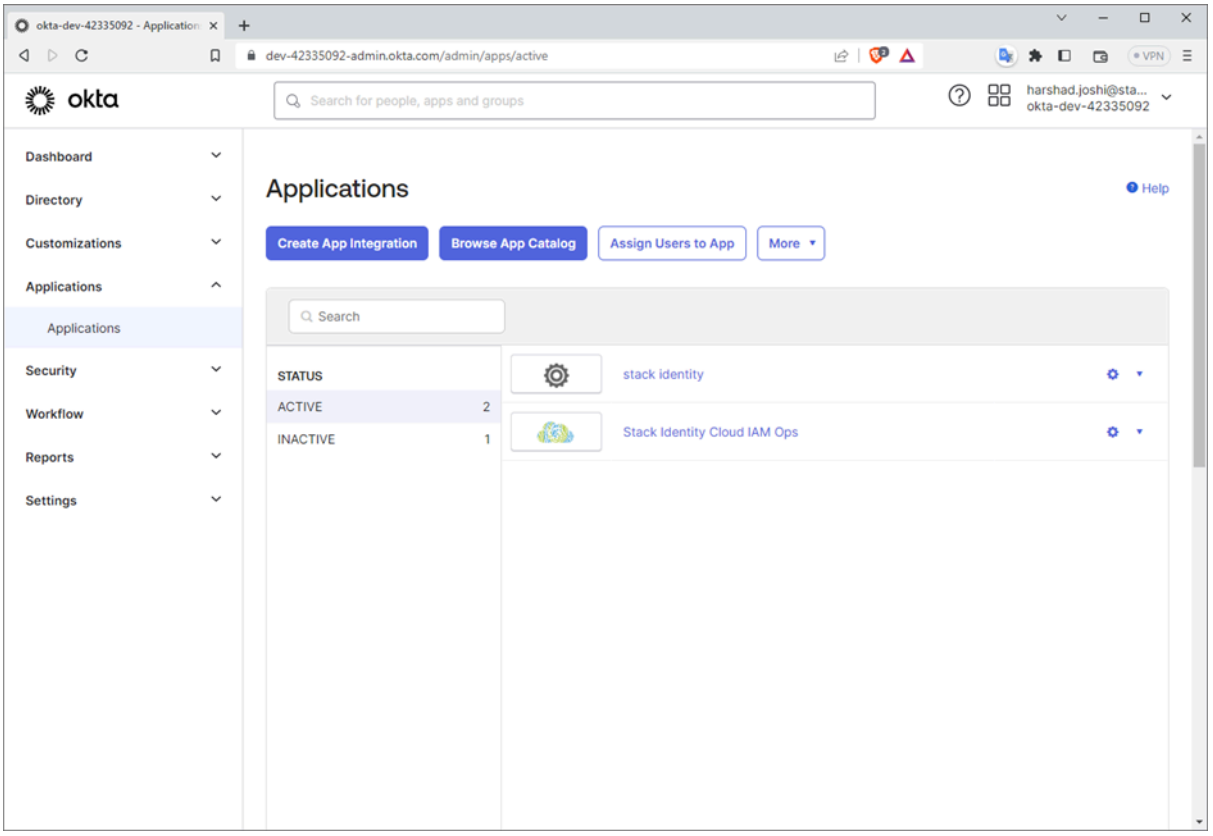
3. Once at the Settings Page click on the SSO Tab.



4. On the SSO Tab Page, at the top you see ‘Organization Id‘ copy this value and keep it handy.

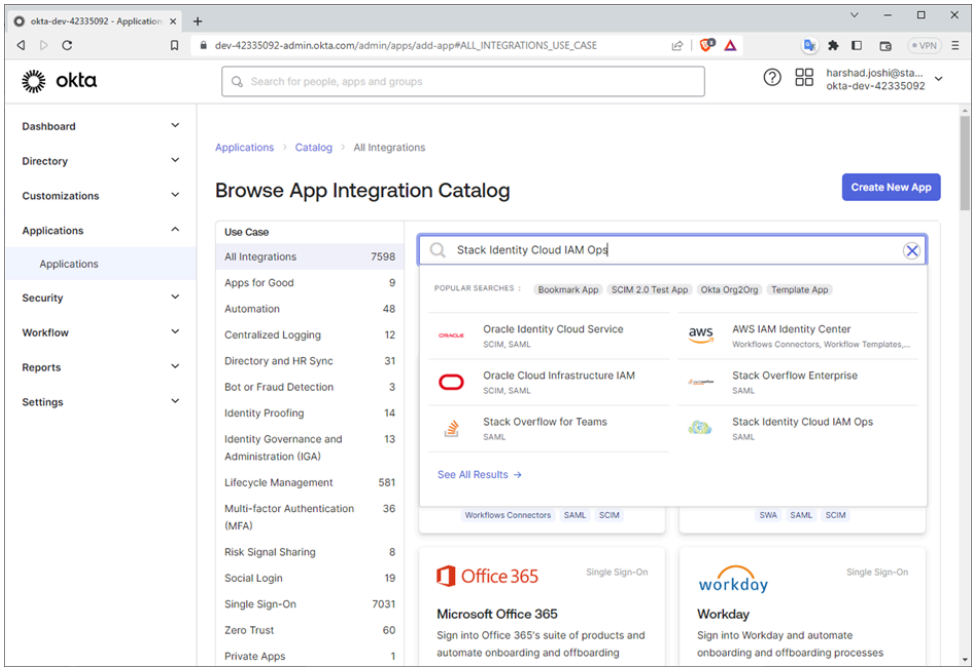


5. Login to your OKTA Tenant, go to Applications

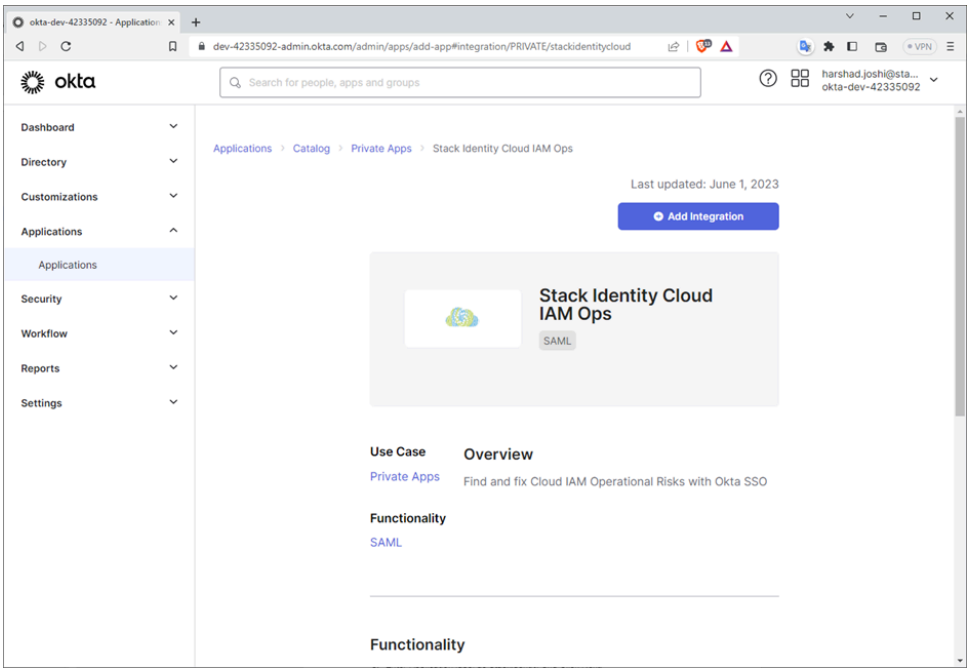


6. On the Applications Page, click on the 'Browse App Catalog' button.

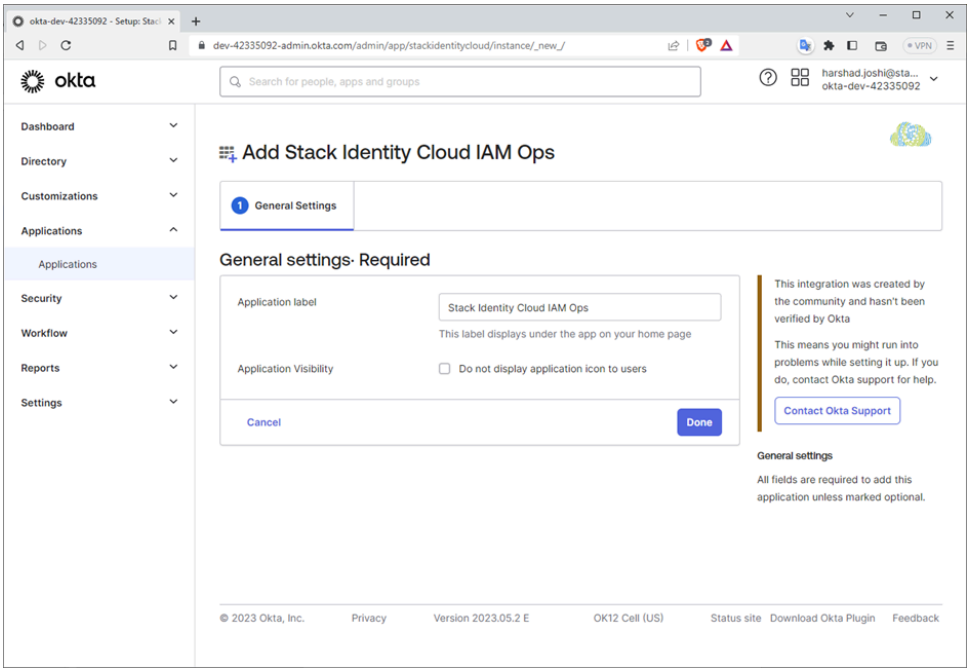
7. In the Browse App Integration Catalog screen search for 'Stack Identity Cloud IAM Ops'.



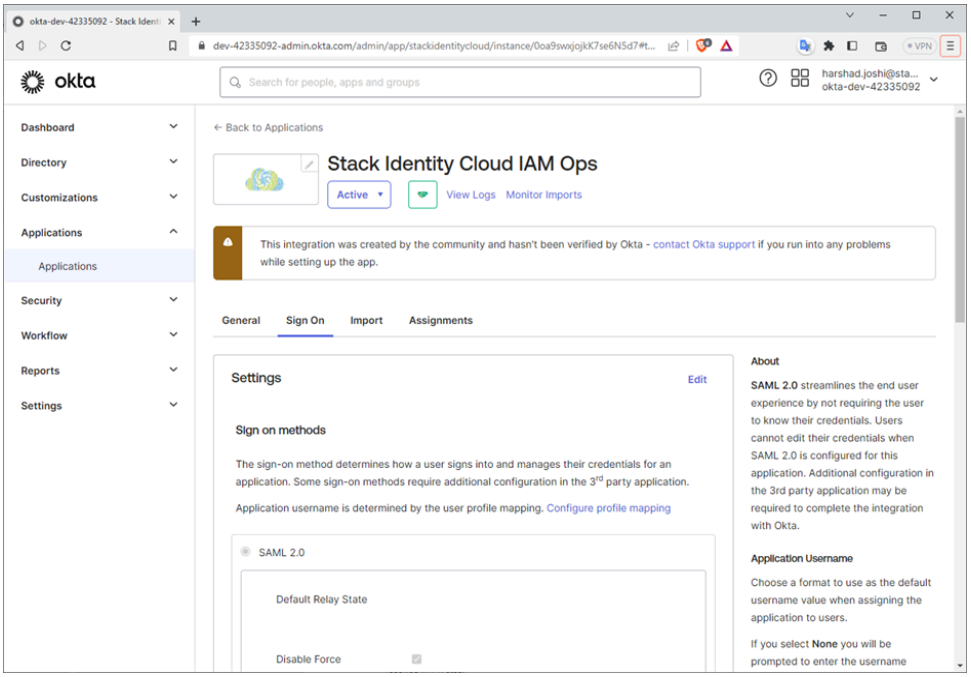
8. Click on the Stack Identity Logo and you are shown the Stack Identity Integration Page. Click on the ‘Add Integration’ button to continue.



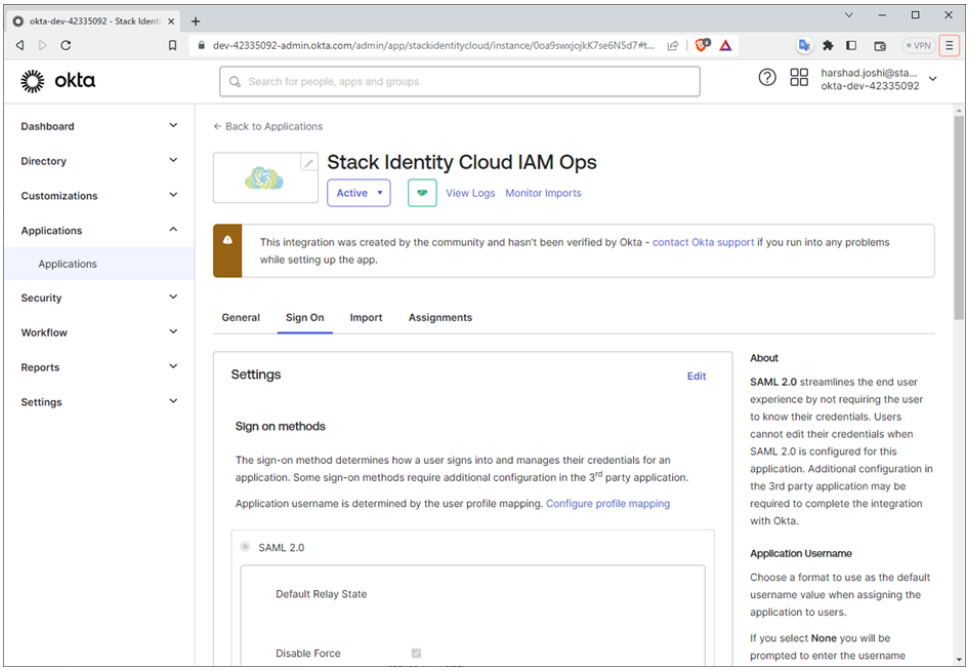
9. You can change the Application label if you want or Continue with the default and Click Done.



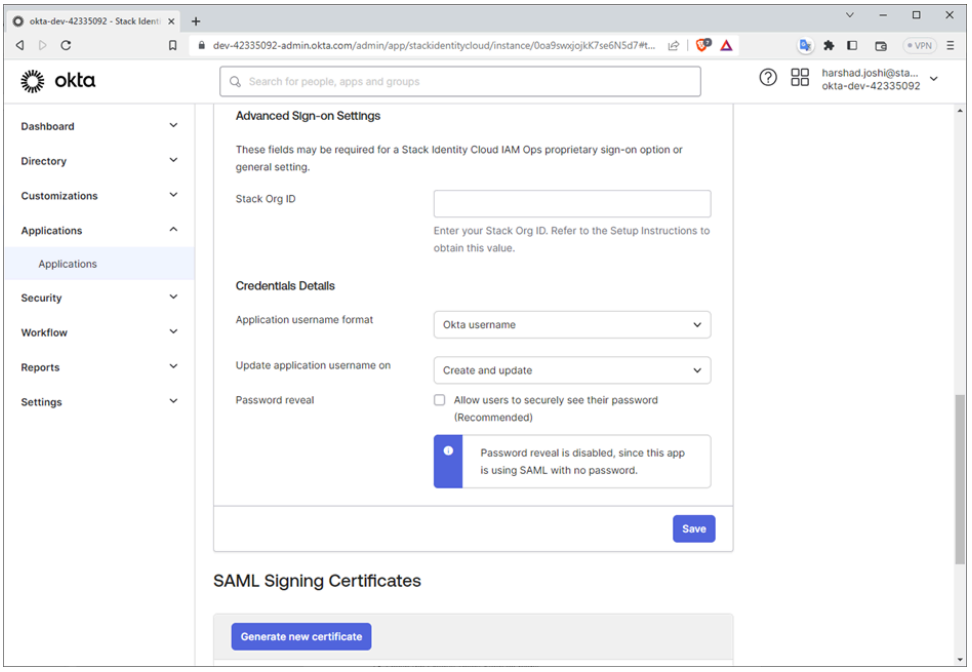
10. Click on the ‘Sign On’ tab



11. Click ‘Edit’ against ‘Settings’.



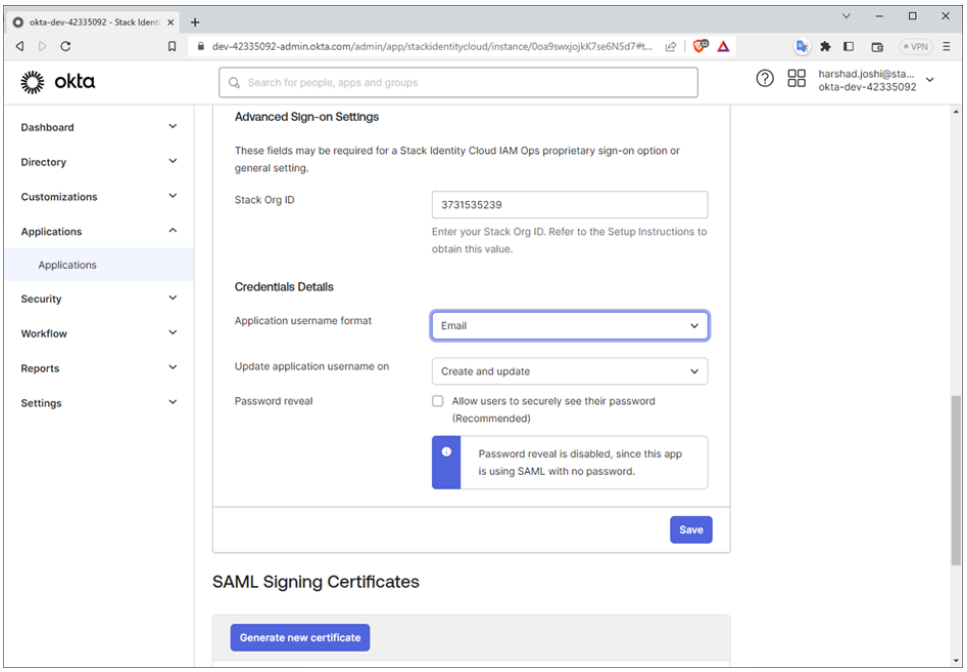
12. Scroll down to the ‘Advanced Sign-on Settings’ section.



13. Enter the following Values:

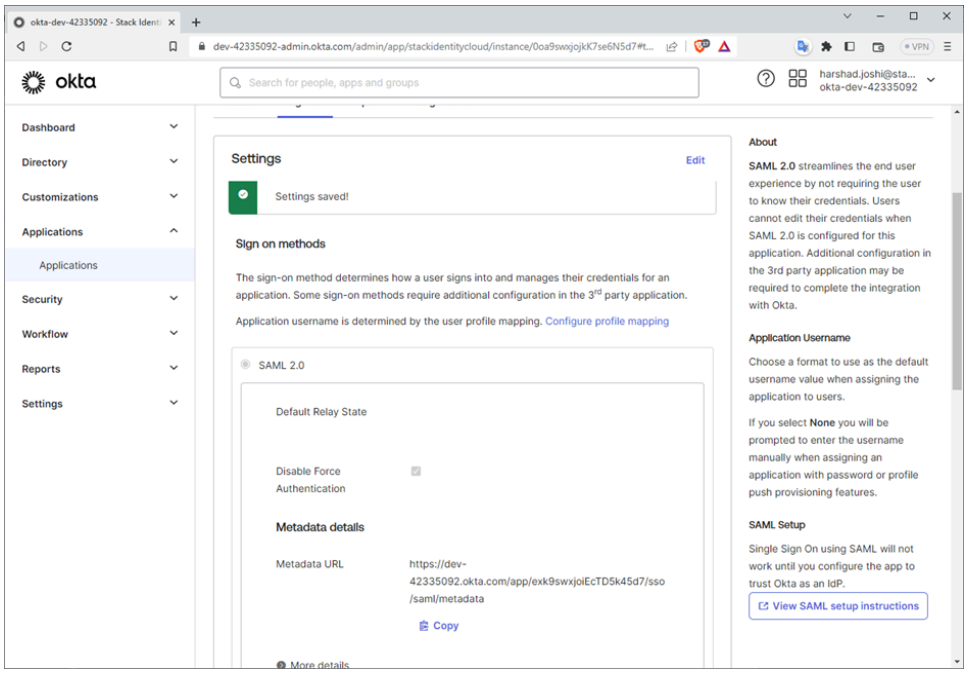
a. Stack Org Id: This is the Id you copied from Stack Identity Settings Page in Step #4.

b. Under ‘Credentials Details’ for ‘Application Username’ choose ‘Email’ from the dropdown.

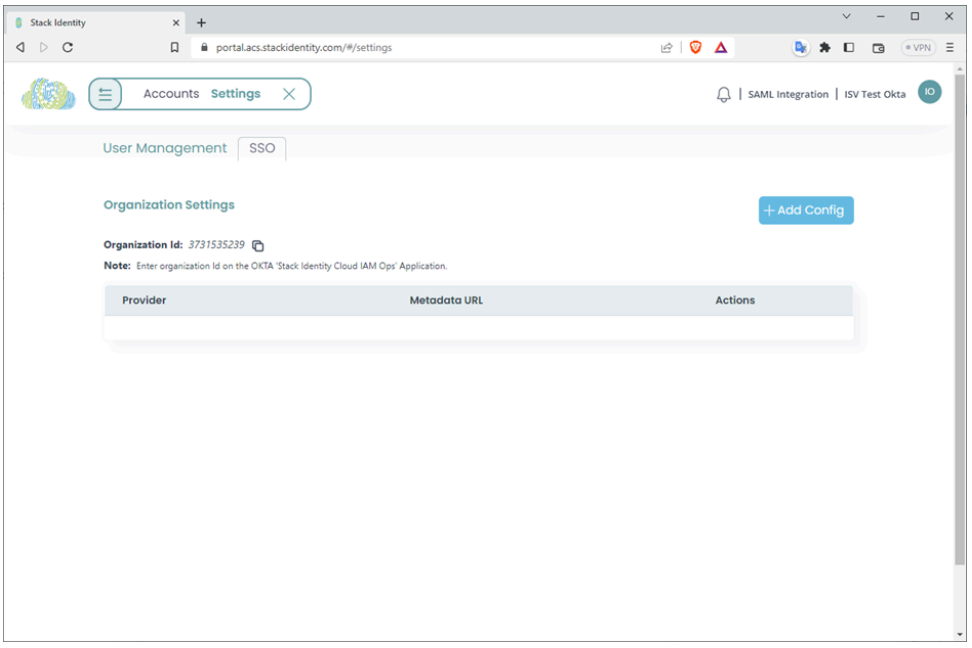


14. Click on Save.

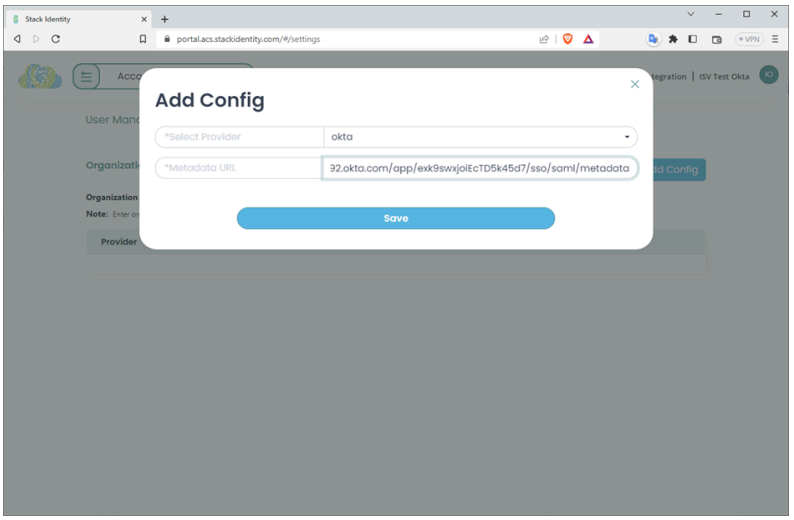
15. After saving you are presented the Settings screen again. At the top in the 'Sign on methods' section under SAML 2.0, the Metadata details are displayed. Click 'Copy' to copy the Metadata URL



16. Switch back to the Stack Identity Website. On the SSO Tab, click the 'Add Config' button



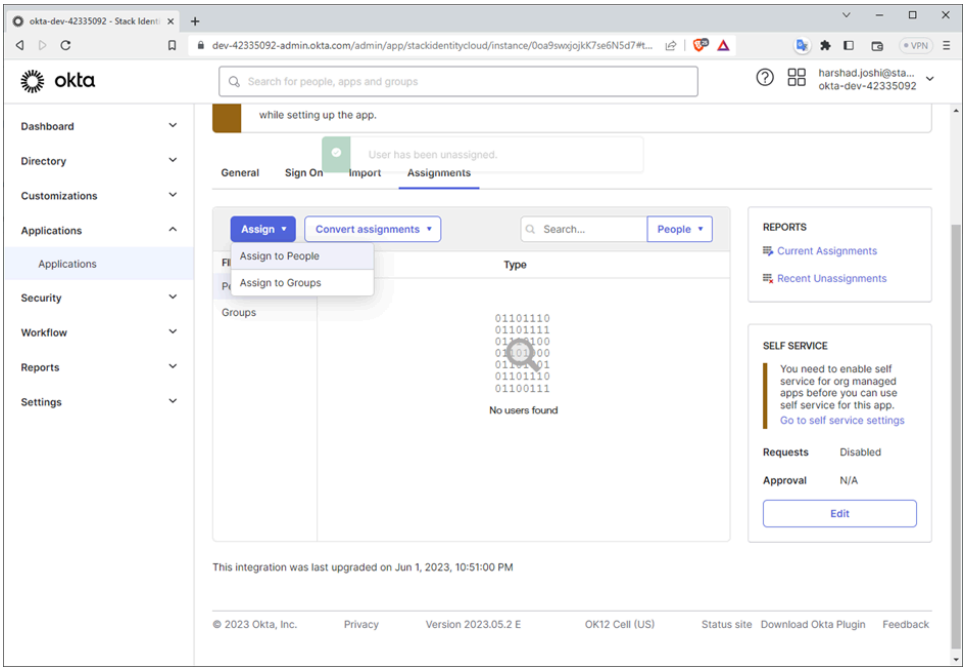
17. On the Add Config Dialog Select Okta as the provider, and paste the metadata URL you copied from the Okta website in step #15



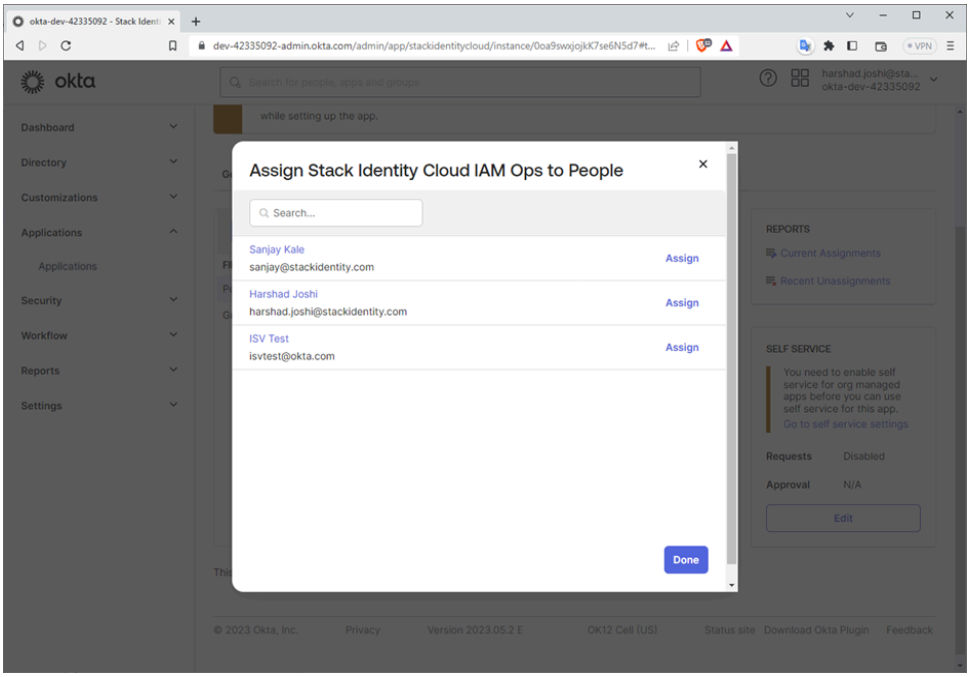
18. Click Save to save your configuration.

19. Back in Okta you can now Assign your Application to your Users.

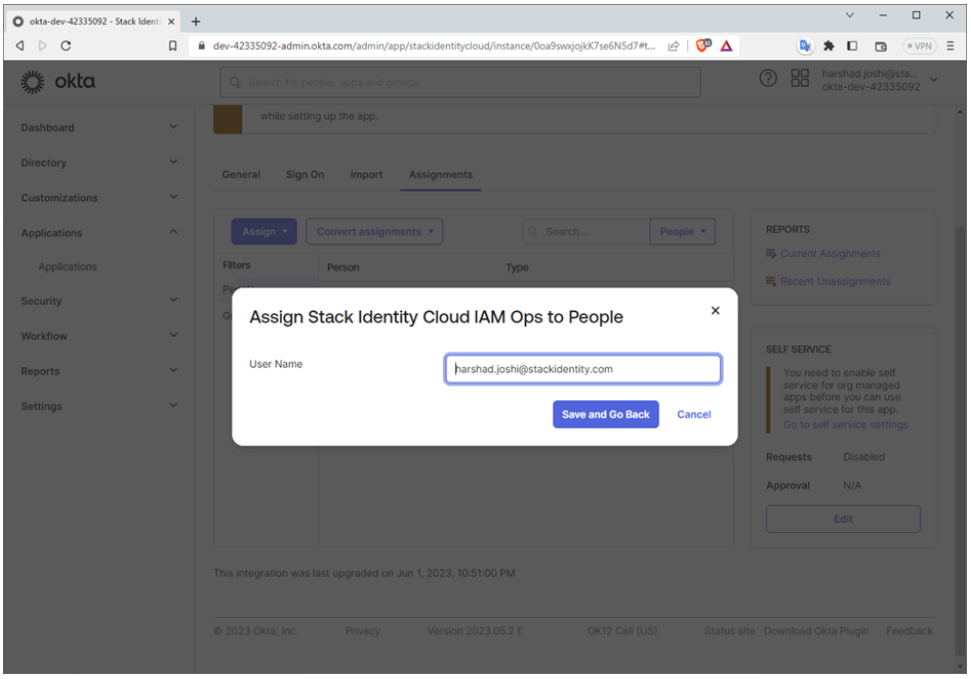
20. From the Assignments Tab choose Assign >> Assign to People.



21. Choose the Users you want to assign the Application to.

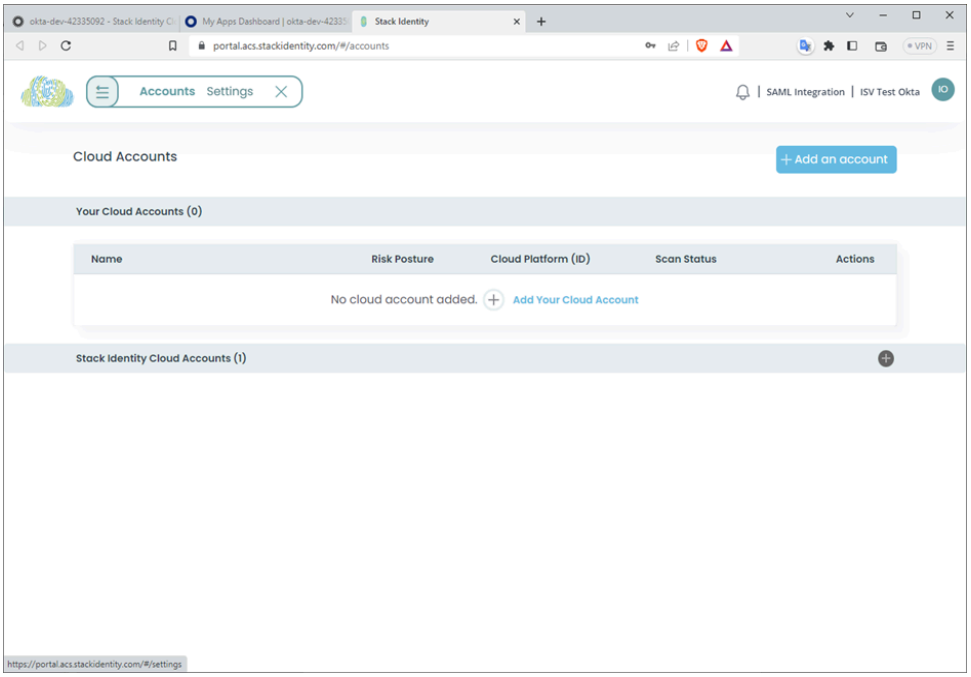


22. Keep the value of the ‘User Name’ field as the email address. This is the default value displayed, do not change this.



23. Click on Save and Go back.

24. To test the integration, go to your End User Dashboard and click on the Stack Identity tile, if your StackIdentity Account is with the same Email address as your OKTA email, you will be logged in to the StackIdentity Website in a new window.



Troubleshoot

For any help in configuration or integration of a SAML Identity Provider with your StackIdentity account, please get in touch with support@stackidentity.com.