

# OKTA Integrations

This document covers

<b>SCIM 2.0</b>	<b>2</b>
<b>SAML</b>	<b>5</b>
<b>OPEN-ID CONNECT</b>	<b>6</b>

**Note:** These instructions will be updated following listing in the Okta application gallery

# SCIM 2.0

We support an SCIM V2.0 integration with Okta. Set this up as follows:

## Get SCIM Credentials from Kloudinsights

First set up some credentials for OKTA to use as an SCIM client:

Goto 'Configuration -> Integrations -> SCIM Configuration' in the KloudInsights admin menus.

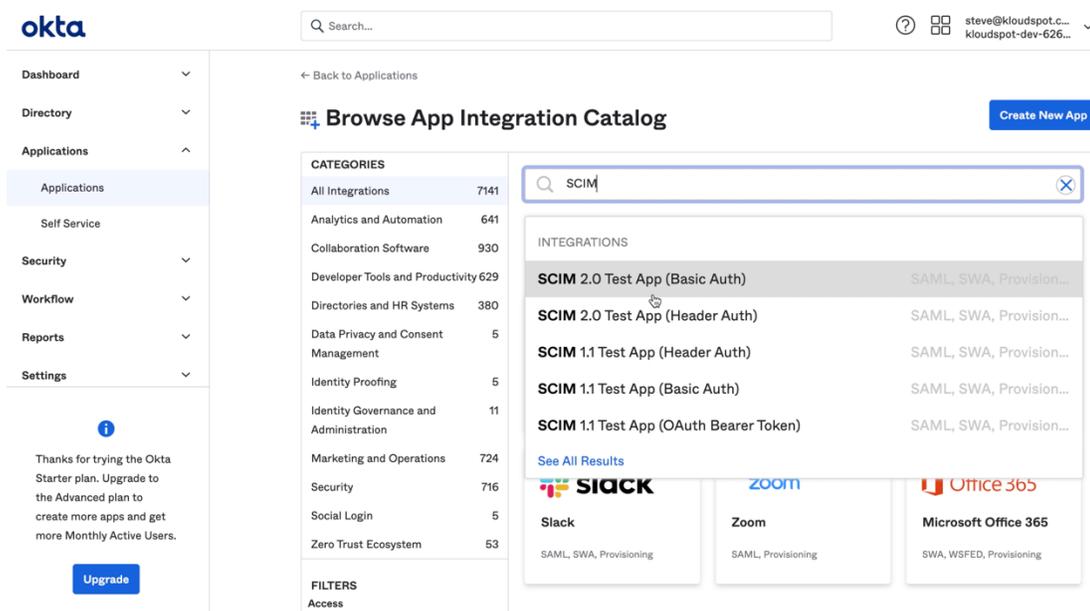
On installation a random password will be generated. You can either use as is or enter you own.

### SCIM Configuration

<b>User</b> scim-user	<b>Password</b> changeit
--------------------------	-----------------------------

## Set up App in Okta

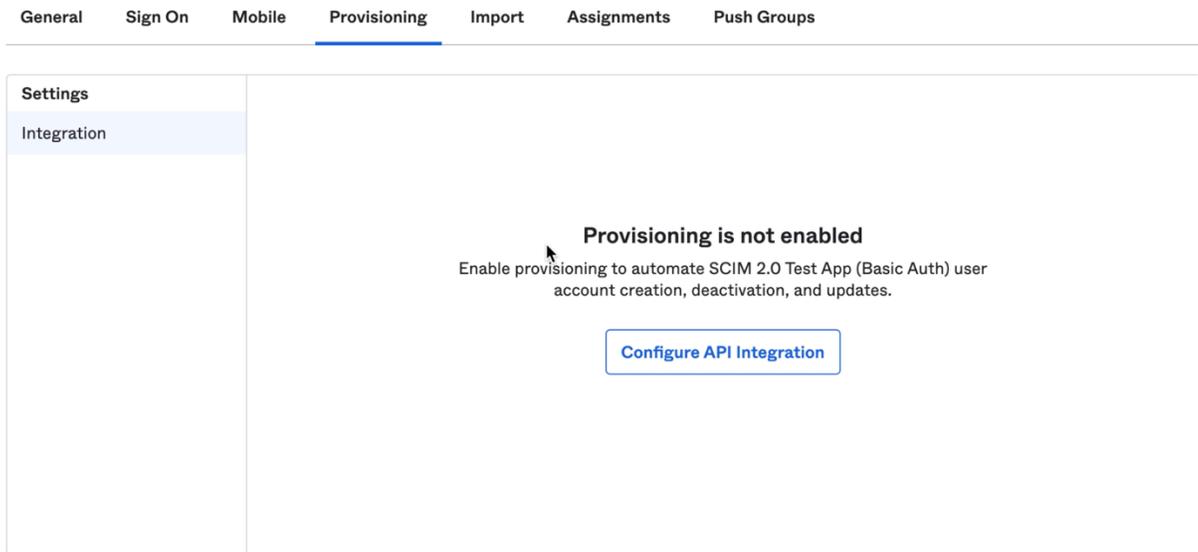
- Go to Applications -> 'Browse App Catalog'.
- Select SCIM 2.0 Test App (Basic Auth)



The screenshot shows the Okta Admin Console interface. On the left is a navigation sidebar with 'Applications' selected. The main content area is titled 'Browse App Integration Catalog'. A search bar at the top contains the text 'SCIM'. Below the search bar, a list of integrations is displayed, with 'SCIM 2.0 Test App (Basic Auth)' highlighted. To the right of the search results are three app cards for Slack, Zoom, and Microsoft Office 365. The Slack card shows 'SAML, SWA, Provisioning'. The Zoom card shows 'SAML, Provisioning'. The Microsoft Office 365 card shows 'SWA, WSFED, Provisioning'.

- Click 'Add'.
- Set a name for the applications. You can safely ignore the other options. Click 'Next' and then 'Done'

- Then click on 'Provisioning' and 'Configure API Integration':



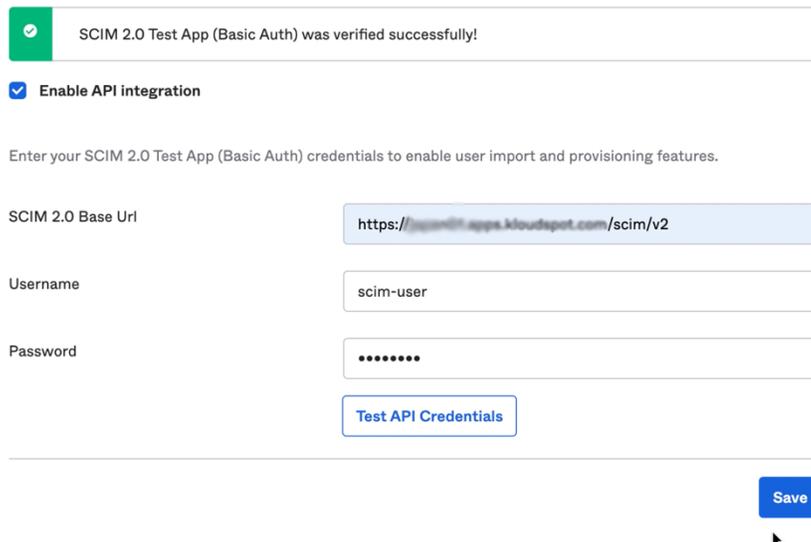
General Sign On Mobile **Provisioning** Import Assignments Push Groups

Settings  
Integration

**Provisioning is not enabled**  
Enable provisioning to automate SCIM 2.0 Test App (Basic Auth) user account creation, deactivation, and updates.

[Configure API Integration](#)

- Enter the URL which will be of the form '**https://<server>/scim/v2**' and the credentials from above and then click 'Test API Credentials'.



SCIM 2.0 Test App (Basic Auth) was verified successfully!

Enable API integration

Enter your SCIM 2.0 Test App (Basic Auth) credentials to enable user import and provisioning features.

SCIM 2.0 Base Uri

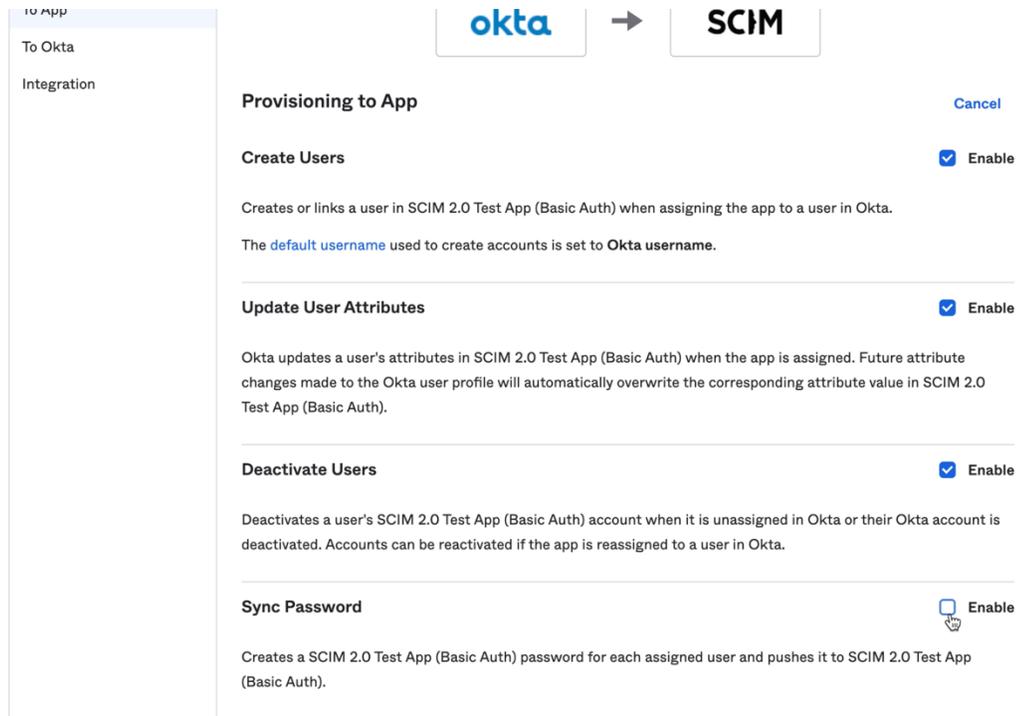
Username

Password

[Test API Credentials](#)

[Save](#)

- If the connection is verified, click 'Save'.
- Now we need to configure the provisioning:
  - Click edit and enable 'Create Users', 'Update User Attributes' and 'Deactivate Users'. Do not enable 'Sync Password'.
  - Click 'Save'.



**Provisioning to App** Cancel

**Create Users**  Enable

Creates or links a user in SCIM 2.0 Test App (Basic Auth) when assigning the app to a user in Okta.

The **default username** used to create accounts is set to **Okta username**.

**Update User Attributes**  Enable

Okta updates a user's attributes in SCIM 2.0 Test App (Basic Auth) when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in SCIM 2.0 Test App (Basic Auth).

**Deactivate Users**  Enable

Deactivates a user's SCIM 2.0 Test App (Basic Auth) account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.

**Sync Password**  Enable

Creates a SCIM 2.0 Test App (Basic Auth) password for each assigned user and pushes it to SCIM 2.0 Test App (Basic Auth).

- Finally scroll down to the 'Attribute Mappings' section and remove any sensitive mappings. We recommend that all of the address related mappings are deleted. The application will make use of the name, email and phone number related mappings as well as the organizational hierarchy mappings.
- You are now finished with configuration and can assign users and groups to the app.

# SAML

The SAML support is configured as follows:

- Go to the 'Applications' menu in Okta and click 'Create App Integration'.
- Select 'SAML 2.0' as the Sign-on method:

### Create a new app integration ×

Sign-on method [Learn More](#)

- OIDC - OpenID Connect**  
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**  
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**  
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**  
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

[Cancel](#) [Next](#)

- Enter a name for the app and click 'Next':

## ⚙️ Create SAML Integration

1 General Settings      2 Configure SAML

1 General Settings

App name

App logo (optional)   

App visibility  Do not display application icon to users  
 Do not display application icon in the Okta Mobile app

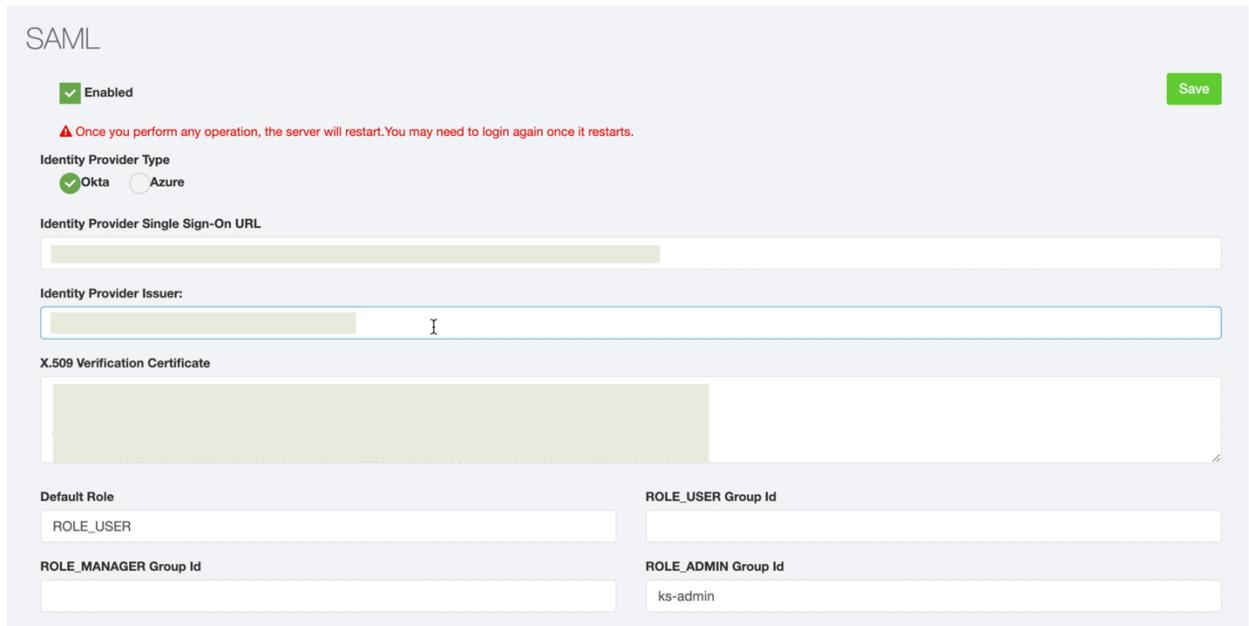
[Cancel](#) [Next](#)

- Then enter the Single Sign-on URL and the Audience URI as follows:
  - **Single Sign-on URL:** <https://<server>/login/saml2/sso/okta>
  - **Audience URI:** <https://<server>/saml2/service-provider-metadata/okta>
- Then scroll down to the 'Group attributes' and enter a selector for the groups attribute.

- Then click 'Next' and 'Finish'.
- Then scroll down to the 'Setup Instruction' which will give you the information enter into KloudInsights:

Now login to KloudInsights and perform the following steps:

- Go to 'Configuration -> Integrations -> External Authentication' in the KloudInsights admin menus and enable 'SCIM':
- Select 'Okta' as the Identity Provider and cut and paste the information from the Okta instructions:



SAML

Enabled Save

▲ Once you perform any operation, the server will restart. You may need to login again once it restarts.

Identity Provider Type

Okta  Azure

Identity Provider Single Sign-On URL

Identity Provider Issuer:

X.509 Verification Certificate

Default Role: ROLE\_USER

ROLE\_USER Group Id

ROLE\_MANAGER Group Id

ROLE\_ADMIN Group Id: ks-admin

- Click on save which will restart the server with the new login configuration.
- The integration is now set up and you can assign groups and users to it.
- Note that you can use these groups to select the role used in KloudInsights. To do this enter the mapping into the relevant fields above.

## Open-ID Connect

The Open-ID connect support is configured as follows:

- Go to the 'Applications' menu in Okta and click 'Create App Integration'.
- Select 'OIDC – OpenID Connect' as the Sign-on method and 'Web Application' as the Application type and then click 'Next'

## Create a new app integration

### Sign-on method

[Learn More](#)

- OIDC - OpenID Connect**  
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**  
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**  
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**  
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

### Application type

What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

- Web Application**  
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)
- Single-Page Application**  
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)
- Native Application**  
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

[Cancel](#)

[Next](#)

- Set a name for the App.
- Set the Sign-in redirect URIs and Sign-out redirect URIs:
  - Sign-in redirect URIs: `https://<server>/login/oauth2/code/okta`
  - Sign-out redirect URIs: `https://<server>/logout`
- Then click 'Save'. The screen will now show the properties needed to configure KloudInsights:

General Sign On Assignments Okta API Scopes

### Client Credentials Edit

Client ID Ooa2j8nkqgwDHPu7t5d6 Copy

Public identifier for the client that is required for all OAuth flows.

Client secret ..... Copy

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

### General Settings Edit

Okta domain dev-6265734.okta.com Copy

Finally, you need to determine which groups get exposed by Okta. You do this by adding the groups claim and setting the filter appropriately. Typically, you would create groups for the different user roles prefaced by something (for example 'ks-') and then edit the Open Id Connect Token in the 'Sign On' tab:

### OpenID Connect ID Token Edit

Issuer https://dev-6265734.okta.com

Audience Ooawd3466K95IbIID5d6

Claims Claims for this token include all user attributes on the app profile.

Groups claim type Filter

Groups claim filter ? groups Starts with ks-

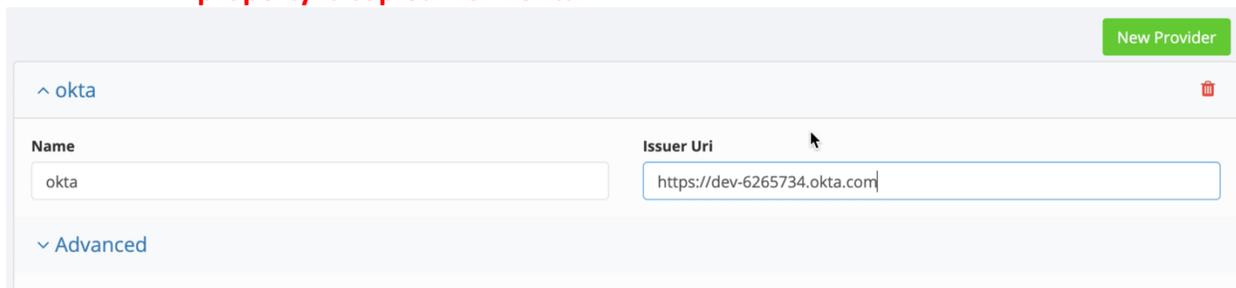
[Using Groups Claim](#)

Okta is now set up. Now login to KloudInsights and perform the following steps:

- Go to 'Configuration -> Integrations -> External Authentication' in the KloudInsights admin menus and enable 'OAuth2 / OpenID Connect'.
- Click 'New Provider' and set the following properties:

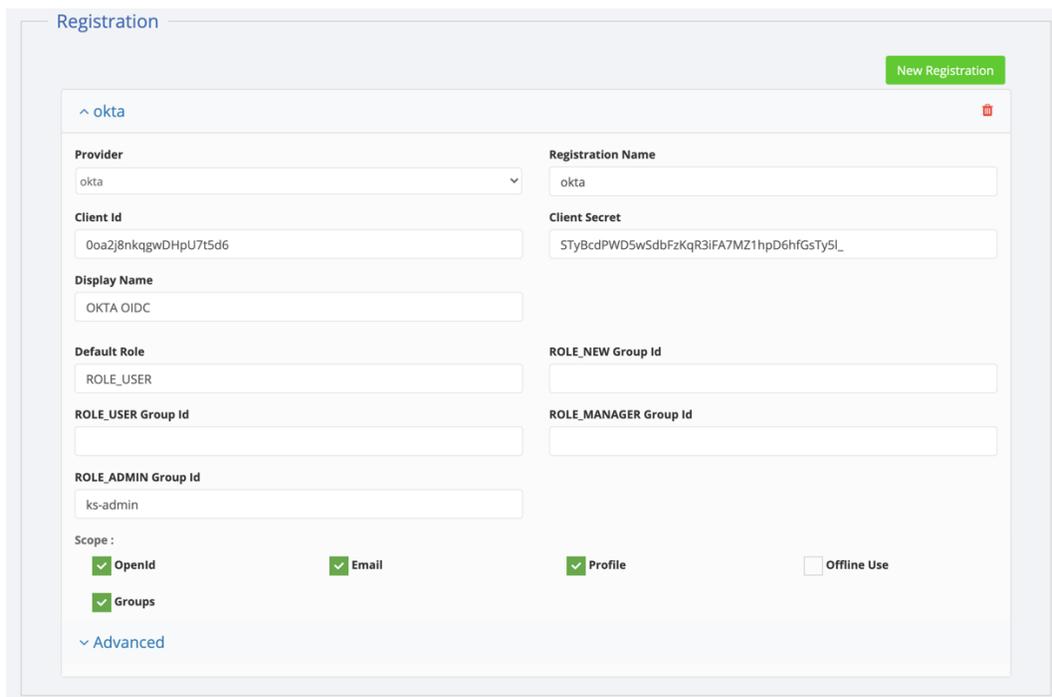
- Name: Set this to 'okta'
- Issuer Uri: Set this using the 'Okta domain'.

**Note that you need to add the 'https://' since this is not present when the property is copied from Okta.**



The screenshot shows the 'New Provider' configuration form for Okta. The 'Name' field is set to 'okta' and the 'Issuer Uri' field is set to 'https://dev-6265734.okta.com'. There is a 'New Provider' button in the top right corner and an 'Advanced' section below the main fields.

- Next click 'New Registration' and set the following properties:
- **Registration Name:** Set to 'Okta'
  - **Client Id:** Cut and paste from OKTA
  - **Client Secret:** Cut and paste from OKTA
  - **Display Name:** Use an appropriate 'friendly' name – this is what is displayed on the login screen.
  - Ensure that the 'OpenId', 'Email', 'Profile' and 'Groups' scopes are selected.
  - **'Offline Use' must not be selected.**
  - Enter any group mappings as needed to match those setup above.



The screenshot shows the 'New Registration' configuration form for Okta. The 'Provider' is set to 'okta' and the 'Registration Name' is 'okta'. The 'Client Id' is '0oa2j8nkqgwdHpU7t5d6' and the 'Client Secret' is 'STyBcdPWD5wsdbFzKqR3iFA7MZ1hpD6hfGsTy5L\_'. The 'Display Name' is 'OKTA OIDC' and the 'Default Role' is 'ROLE\_USER'. There are fields for 'ROLE\_USER Group Id', 'ROLE\_ADMIN Group Id', 'ROLE\_NEW Group Id', and 'ROLE\_MANAGER Group Id'. The 'Scope' section has checkboxes for 'OpenId', 'Email', 'Profile', and 'Offline Use', with 'OpenId', 'Email', and 'Profile' checked. There is a 'New Registration' button in the top right corner and an 'Advanced' section below the main fields.

- Now click 'Save'. The server will restart. Wait for 15-30 seconds for this to complete and then refresh the screen.
- Whilst the server is restarting, go to the Okta Ui and assign groups/users to the App that you want to be able to access Kloudspot.
- Once the server is restarted, you should be able to see the Okta OIDC login button on the main login screen.