kloudspot

Kloudhybrid / Documentation

OKTA Integrations

This document covers

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

SCIM 2.0

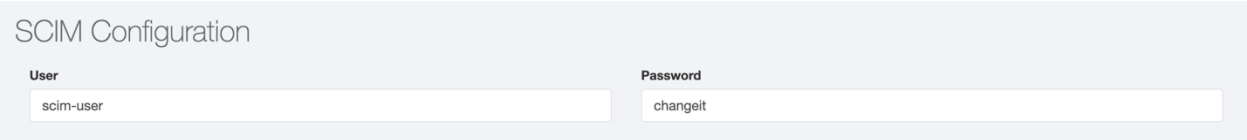
We support an SCIM V2.0 integration with Okta. Set this up as follows:

Get SCIM Credentials from Kloudinsights

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

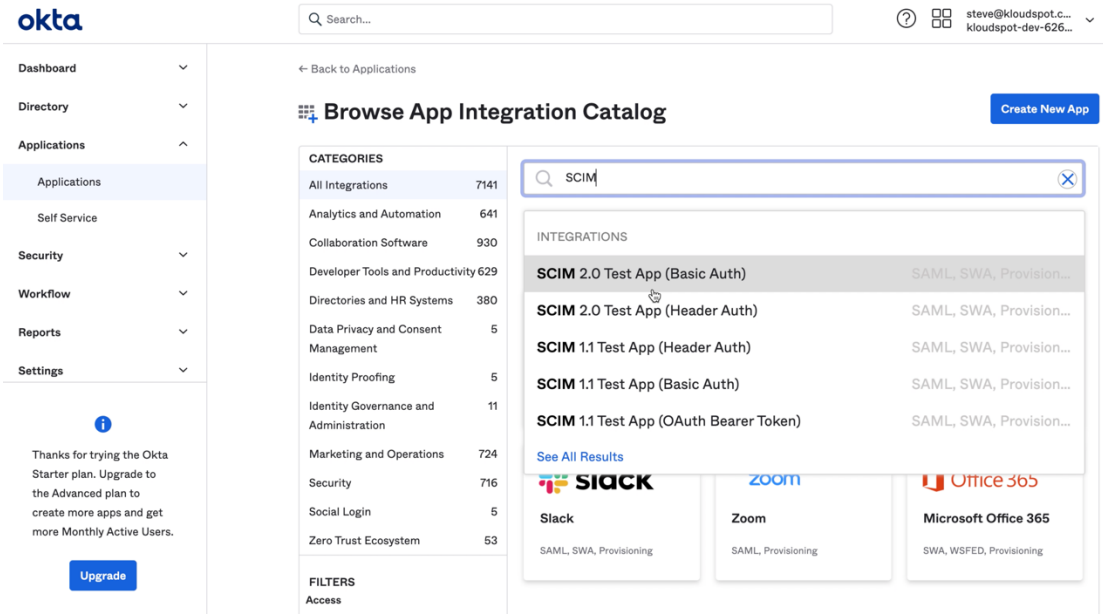
Goto ‘Configuration -> Integrations -> SCIM Configuration’ in the KloudInsights admin menus.

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



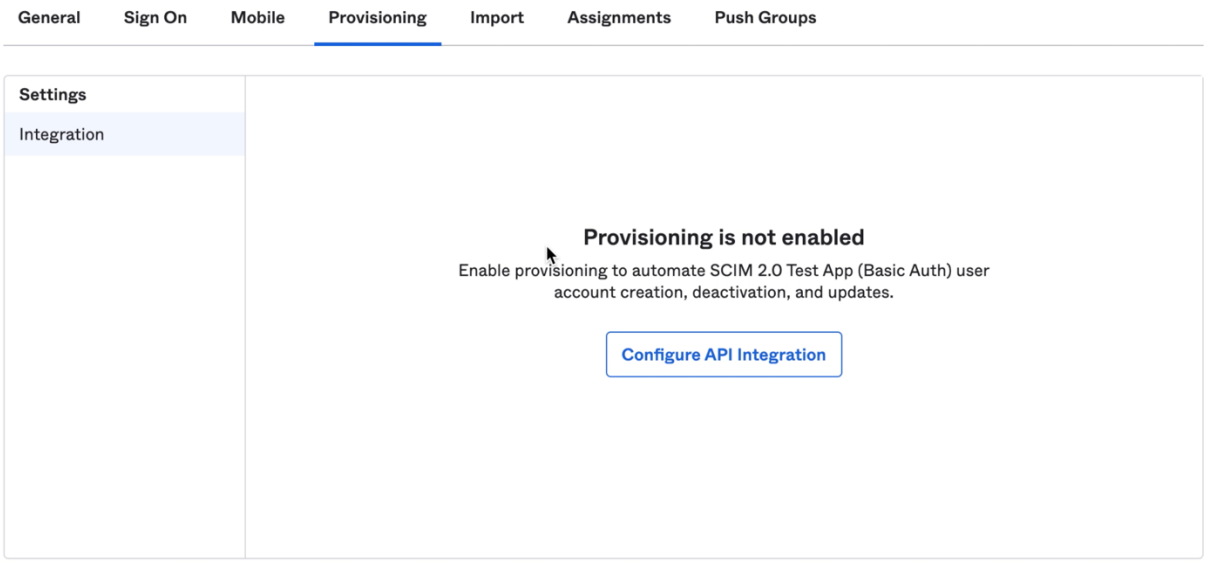
Set up App in Okta

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

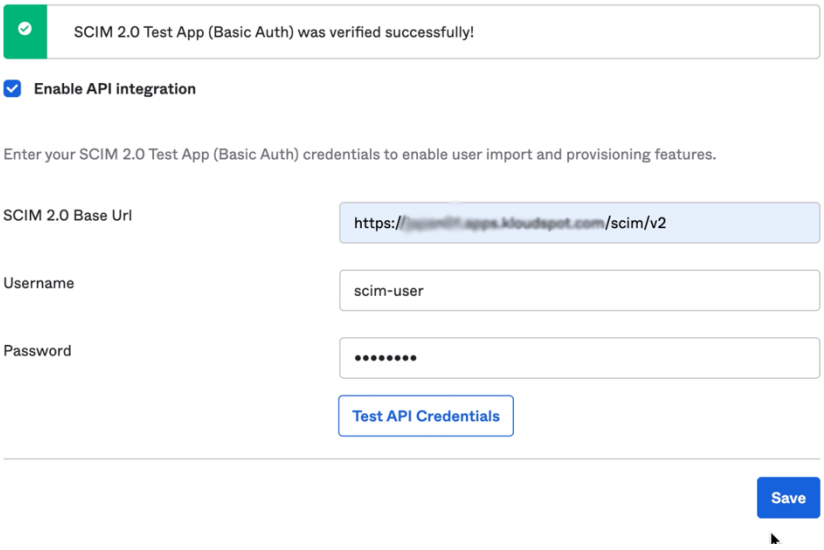


- Click ‘Add’.
- Set a name for the applications. You can safely ignore the other options. Click ‘Next’ and then ‘Done’

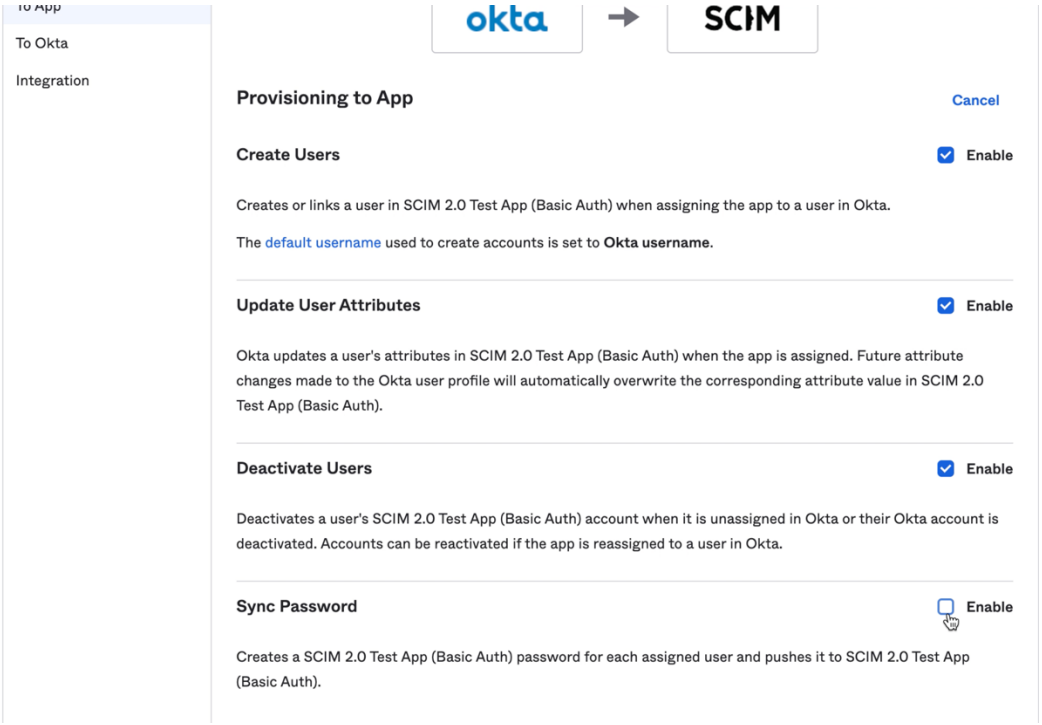
- Then click on ‘Provisioning’ and ‘Configure API Integration’:



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



- 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’.



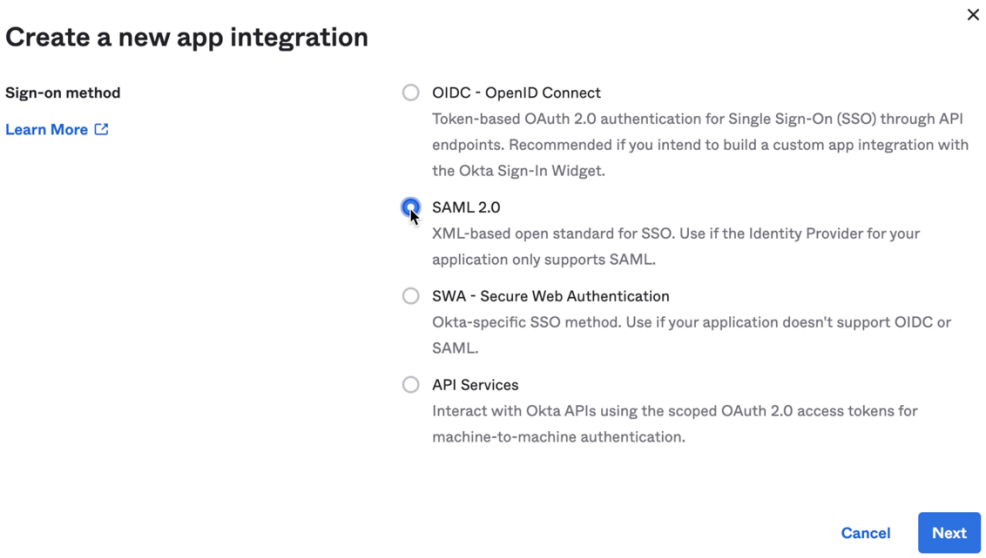
- Finally scroll down to the ‘Attribute Mappings’ section and remove any sensitive mappings. We recommend that all of the address related mappings are deleted. The application will make use of the name, email and phone number related mappings as well as the organizational hierarchy mappings.

- You are now finished with configuration and can assign users and groups to the app.

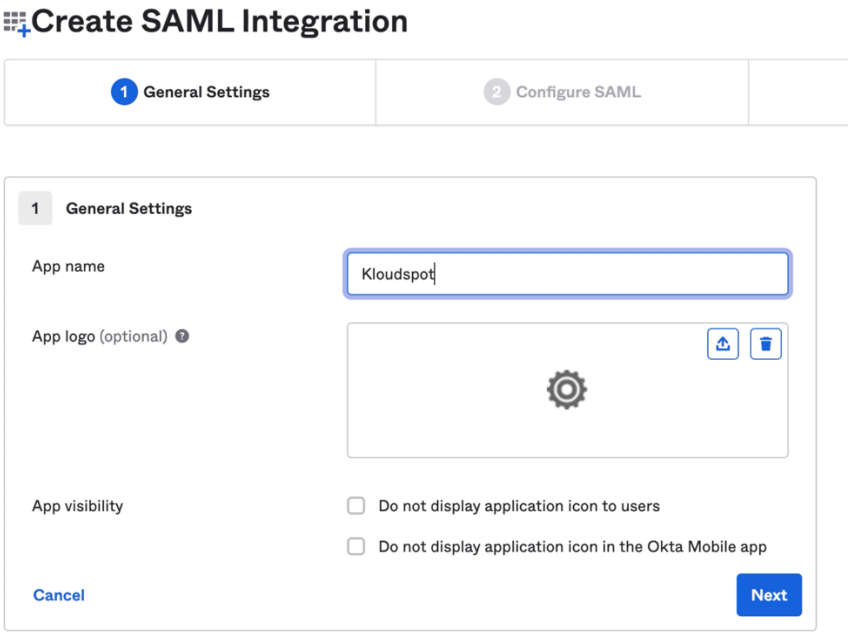
SAML

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:



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



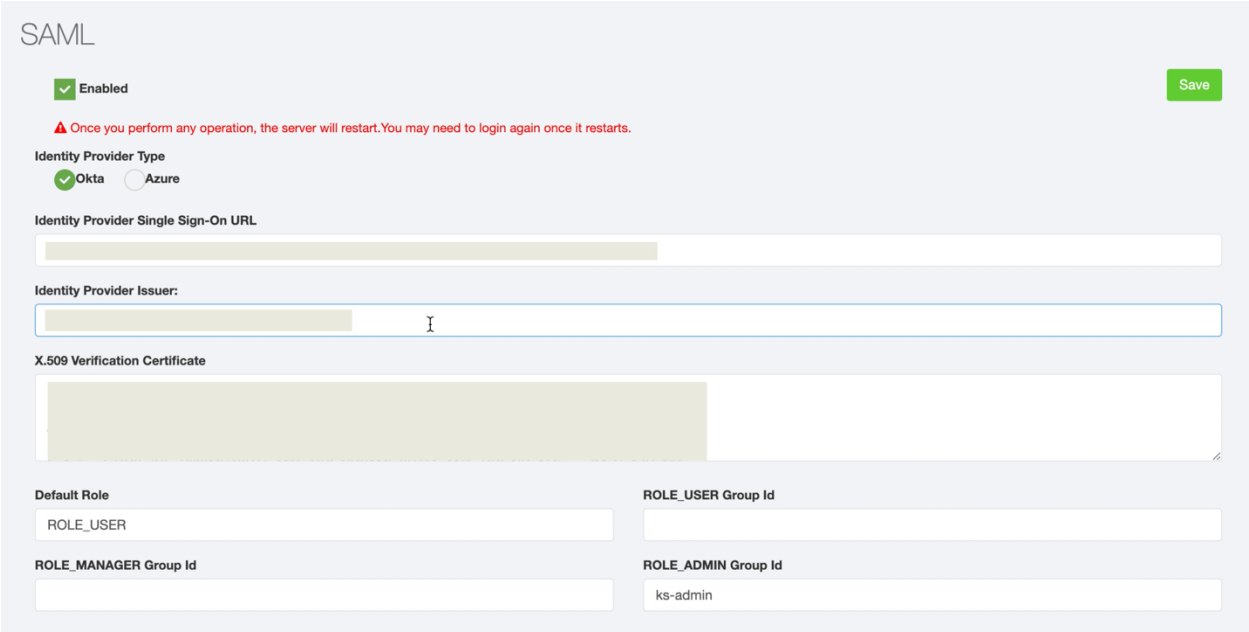
- Then enter the Single Sign-on URL and the Audience URI as follows:
  - **Single Sign-on URL**: https://<server>/login/saml2/sso/okta
  - **Audience URI**: https://<server>/saml2/service-provider-metadata/okta
- Then scroll down to the 'Group attributes' and enter a selector for the groups attribute.

- 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:

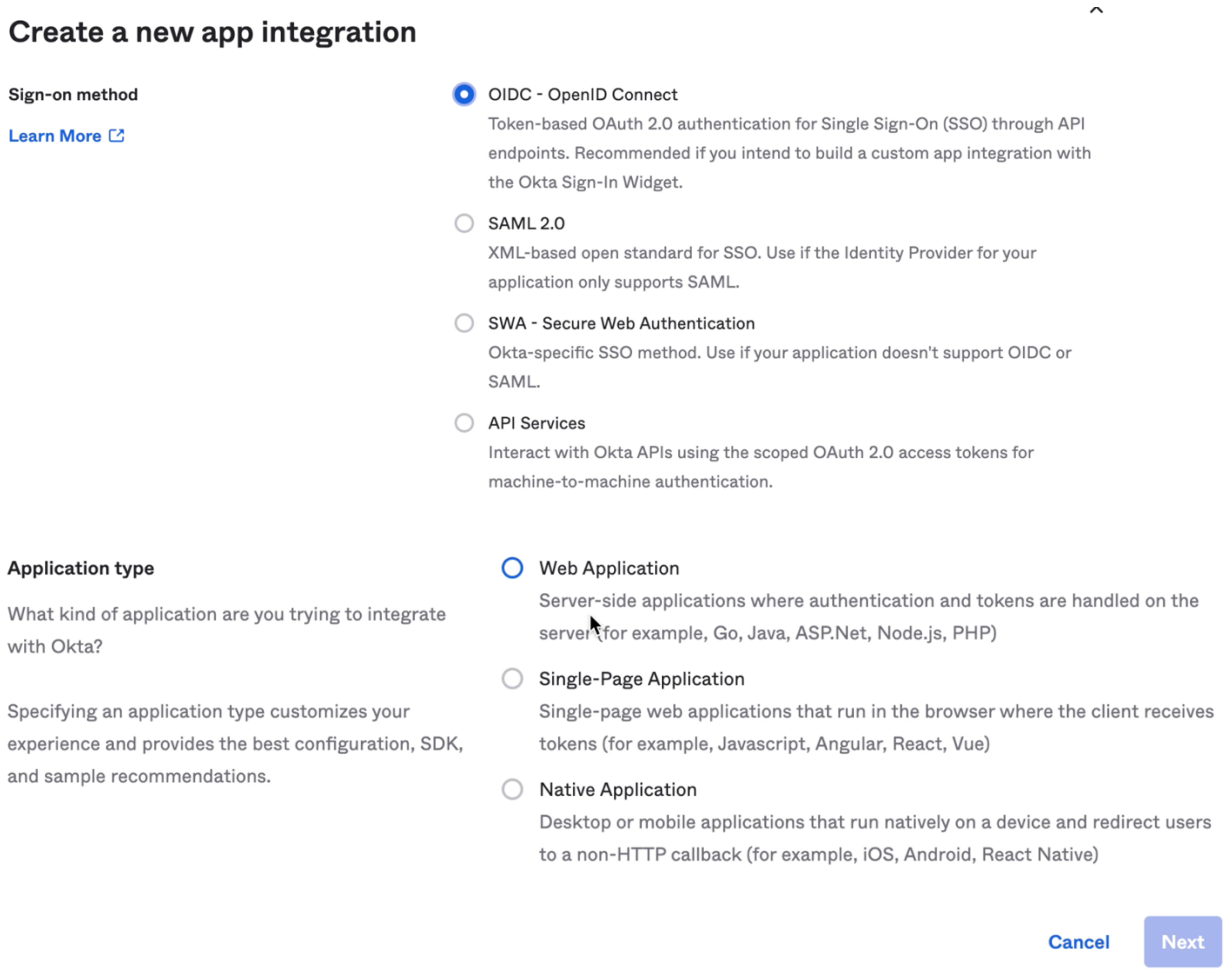


- Click on save which will restart the server with the new login configuration.
- The integration is now set up and you can assign groups and users to it.
- Note that you can use these groups to select the role used in KloudInsights. To do this enter the mapping into the relevant fields above.

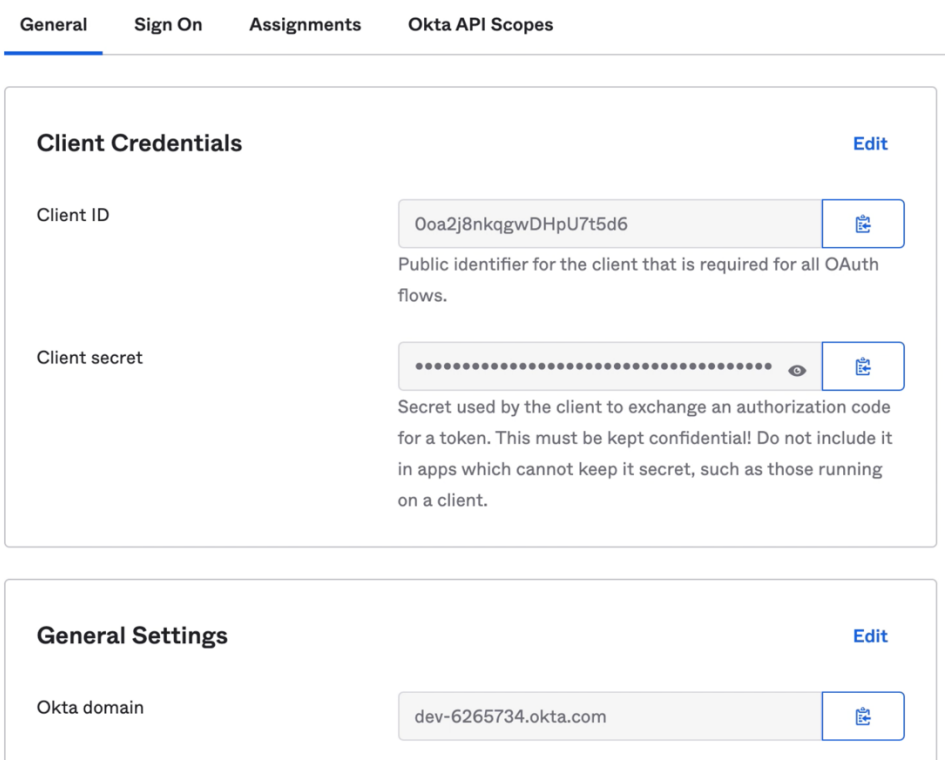
Open-ID Connect

The Open-ID connect support is configured as follows:

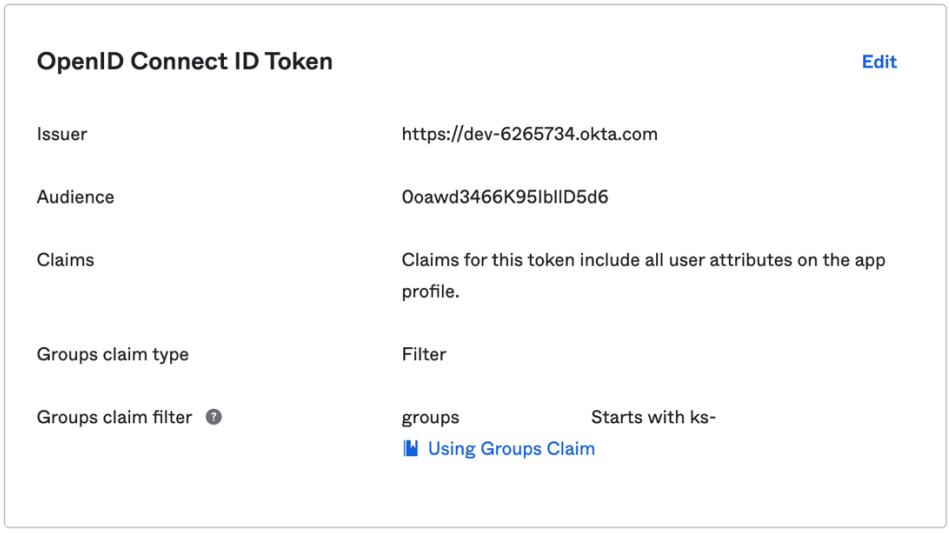
- Go to the ‘Applications’ menu in Okta and click ‘Create App Integration’.
- Select ‘OIDC – OpenID Connect’ as the Sign-on method and ‘Web Application’ as the Application type and then click ‘Next’



- 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:

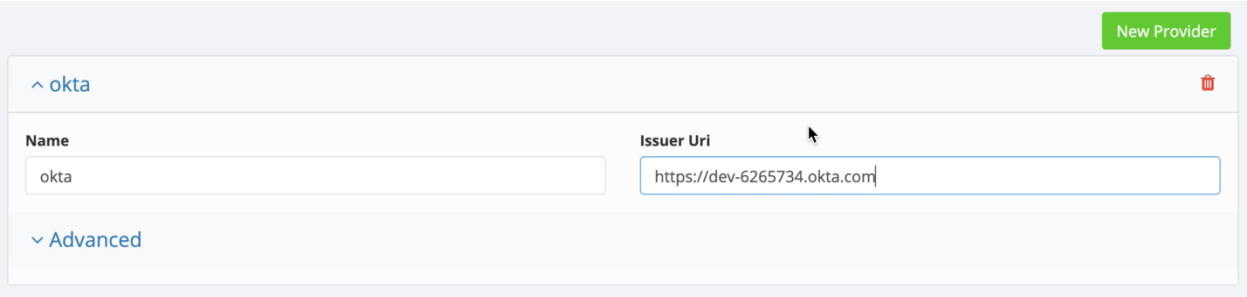


Finally, you need to determine which groups get exposed by Okta. You do this by adding the groups claim and setting the filter appropriately. Typically, you would create groups for the different user roles prefaced by something (for example 'ks-') and then edit the Open Id Connect Token in the 'Sign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

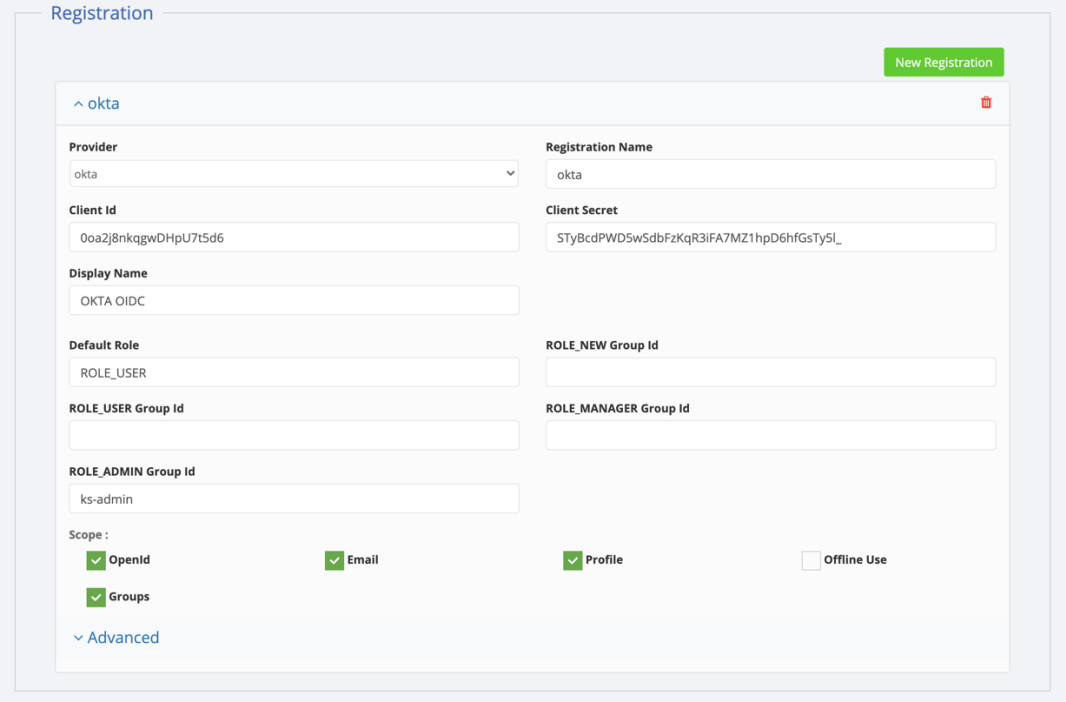


Okta is now set up. Now login to KloudInsights and perform the following steps:

- 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.



- 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.



- 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.