SecurEnds

SecurEnds OIDC Configuration Guide

Contents

Supported Features

SecurEnds application supports the following OIDC feature.

- Service Provider (SP)-Initiated Authentication (SSO) Flow

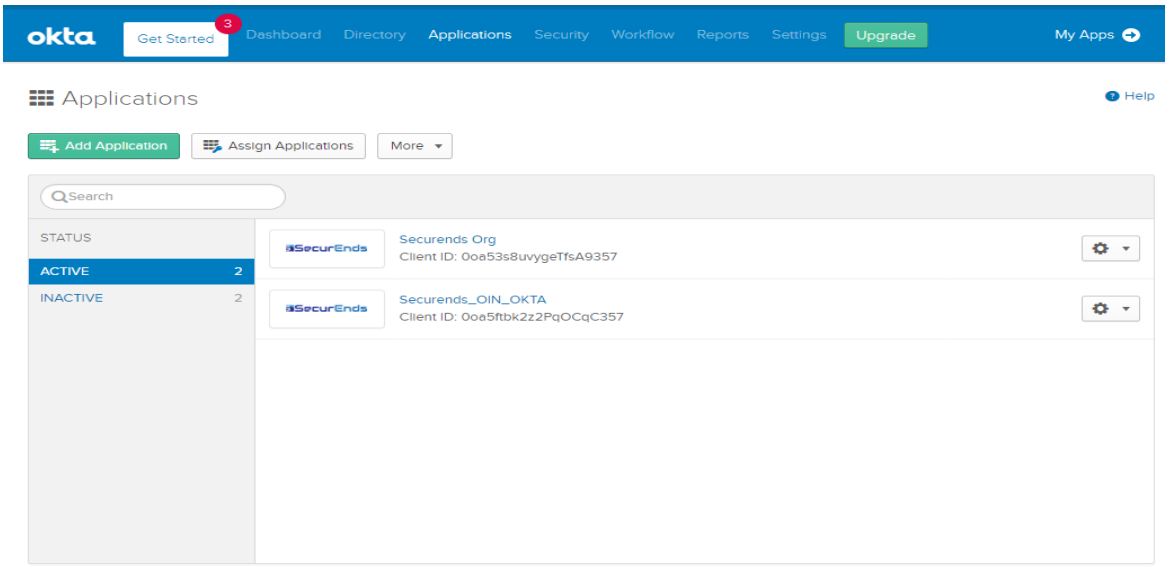
Requirements

Once you have chosen SecurEnds for your Identity Governance needs, please reach out to the SecurEnds team at support@securends.com to get an instance enabled for you.

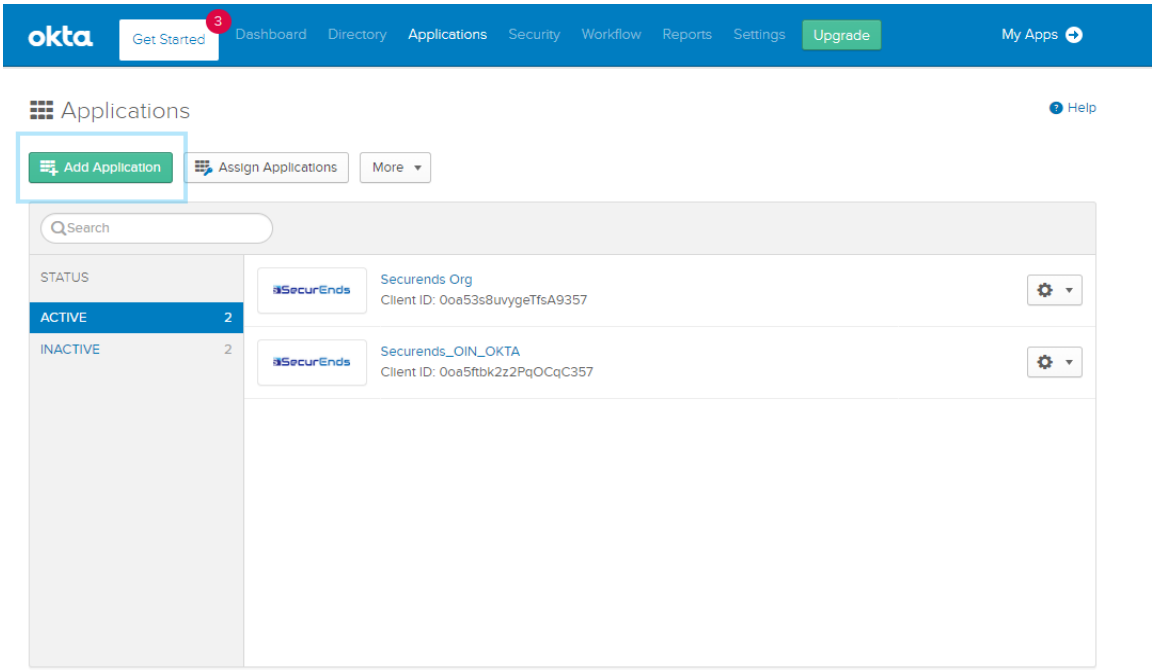
OIDC Configuration Steps

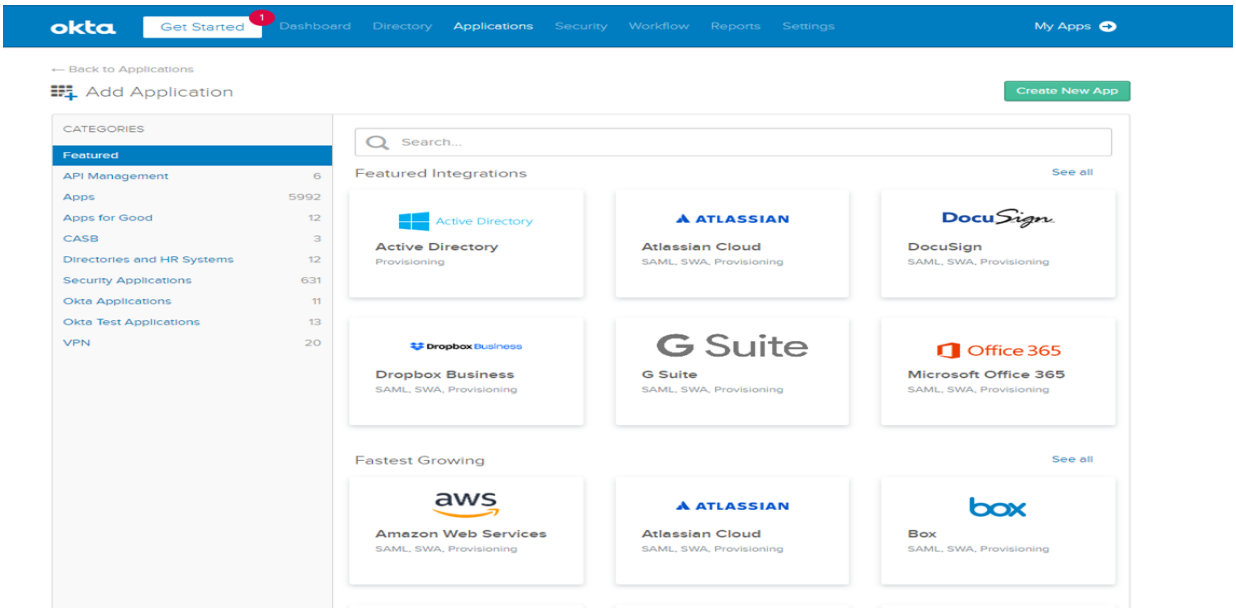
Add SecurEnds Application in Okta dashboard

1) Click on “Applications” link in Okta admin dashboard.

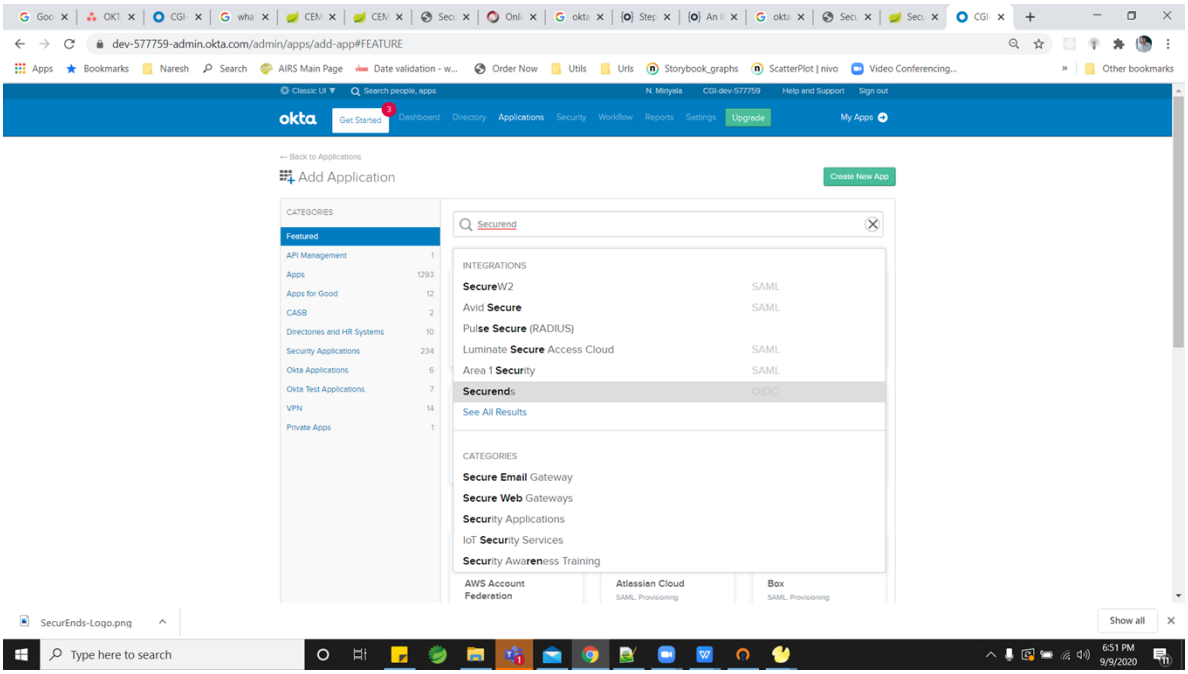


2) Click on “Add Application” button in Okta “Applications” screen

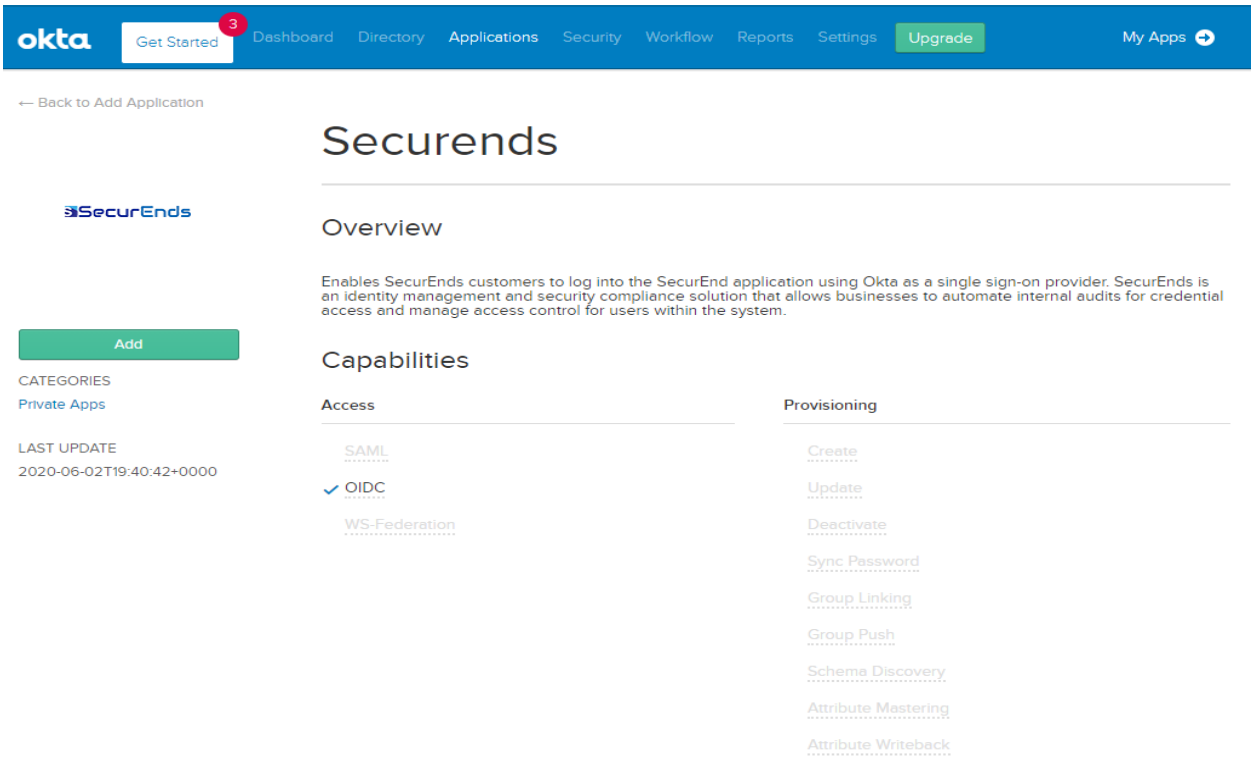




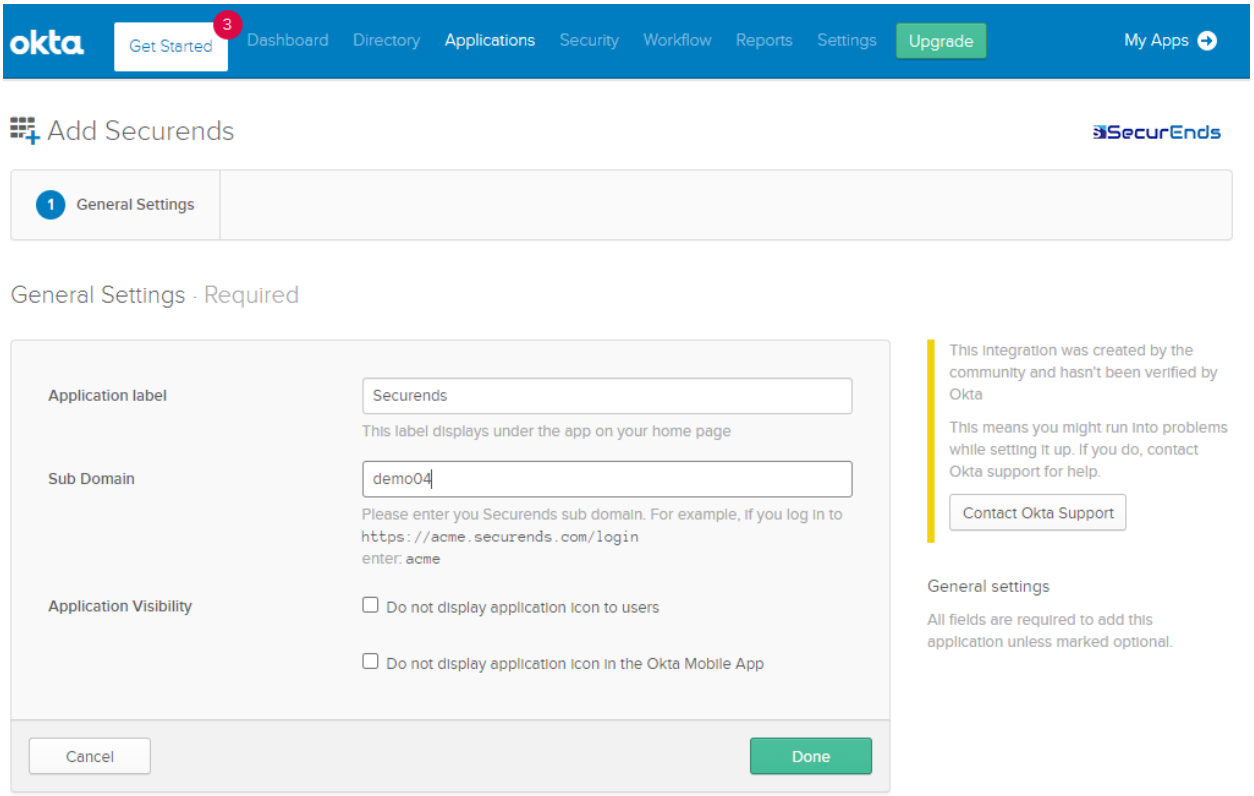
3) Search for “SecurEnds” application and select SecurEnds app from results shown



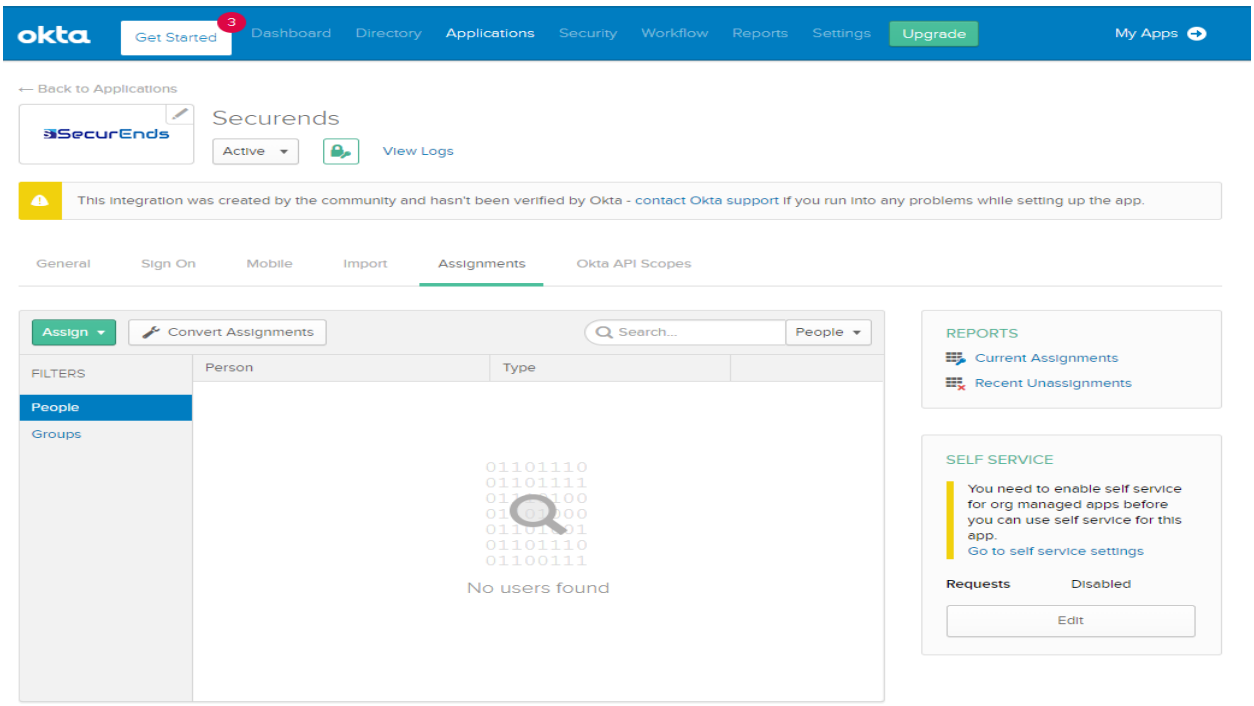
4) Click on “Add” button in “Add Application” screen.



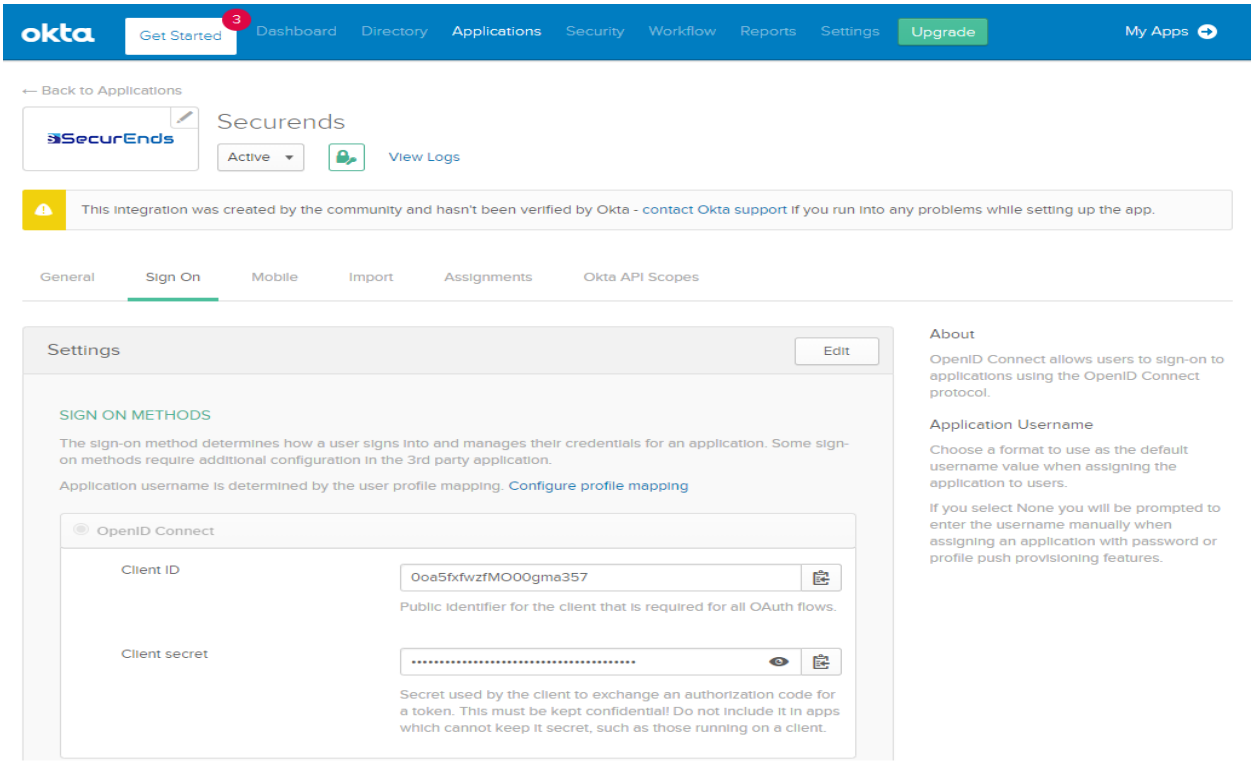
5) Give “Application label” and “Sub Domain” details and click on “Done” button.



6) You will be redirected to view SecurEnds application details.



7) Click on “Sign On” tab, then copy “Client Id” and “Client secret” values that need to be configured within your organization’s SecurEnds application to enable SSO.



SecurEnds application requires below details to enable Okta SSO.

1) Client Id
2) Issuer
3) Client Secret

Test your integration:

Assign users

First you must assign your integration to one or more test users in your org:

1. Click on **“Assignments”** tab.
2. Click on **“Assign”** and then select either “**Assign to People**” or “**Assign to Groups**”.
3. Enter the appropriate people or groups that you wish to enable Single Sign-On into your application, and then click “**Assign**” for each.

4. For any people that you added, verify the user-specific attributes, and then select "**Save and Go Back**".
5. Click on "**Done**".

Test Single Sign-On

1. Sign out of your administrator account in your development org. Click on "**Sign out**" in the upper-right corner of the Admin Console.
2. Sign in to the Okta End-User Dashboard as the regular user who was assigned the SecurEnds integration.
3. In your dashboard, click the Okta tile for the integration and confirm that the user is signed in to SecurEnds application.

Notes

User can access SecurEnds application using OIDC features in following ways.

1) Customer can login to their okta org url

a) After authentication, customer can click on the SecurEnds App available in the dashboard and will be redirected to the SecurEnds application.

2) Access SecurEnds instance url directly

a) Customer will be redirected to their okta org for authentication and after authentication customer will be redirected back to SecurEnds application.

Troubleshooting and Tips

If you run into issues with your sign-in process, you can try the following to troubleshoot the issues:

1. In the Admin Console of your Okta development org, navigate to Reports > System Log and examine any failure messages reported.
2. Open the developer console of your web browser and examine any status messages related to your authentication request. The console errors have status codes in the 4XX range. Investigate and resolve any error messages generated by your sign-on request.
3. Please reach out to the SecurEnds SPOC in case further help is required.