

Okta Integration with Sclera

Log in to Sclera using Okta Single Sign-On (SSO)

Sclera users have an option of signing in to their Sclera accounts using Okta Single Sign-On (SSO) option and access all the services of Sclera. Okta SSO renders greater control to the business owners and administrators over managing Sclera account and features. It gives the users an advantage of signing in their accounts without having to remember their Sclera user name and password.

You can use the following steps to configure Okta as primary identity provider and facilitate SSO with Sclera application:

Supported Features

Service Provider-Initiated (SP) Authentication (SSO) Flow: This authentication flow occurs when a user attempts to log in to Sclera from Okta.

Requirements

In order to configure Okta login with SSO, you must:

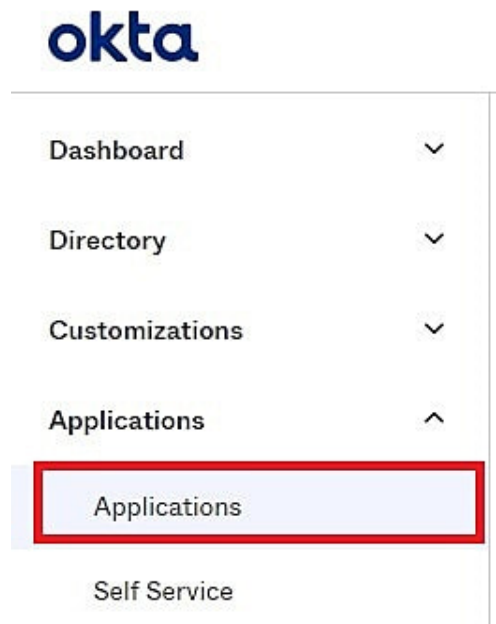
- i) Have access to an Okta user account
- ii) Be an Okta administrator to that user account
- iii) Make sure that the emails of the Sclera users exactly match their Okta accounts
- iv) Have received a Welcome to Sclera email invitation

If you have not received a Welcome to Sclera email invitation, please email support@sclera.com to request an invite.

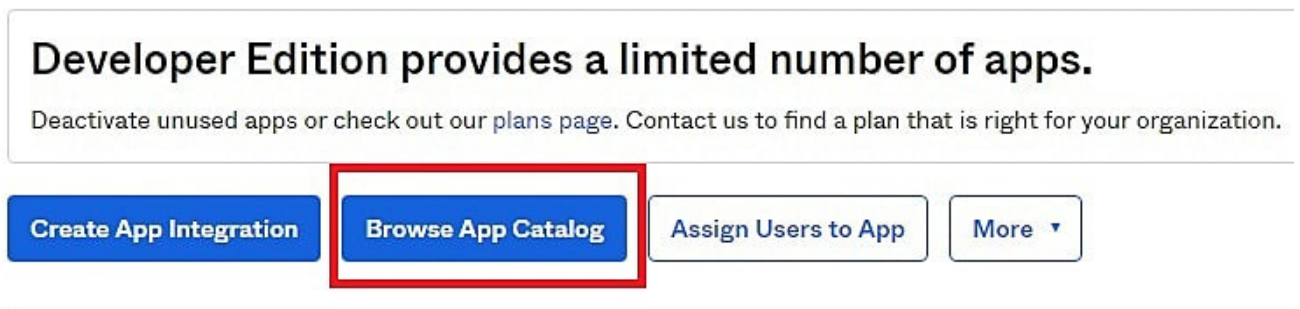
Configuration Steps

The administrators need to configure Okta before they can integrate it with Sclera and give users its access to sign in to their Sclera accounts. To configure Okta, they need to perform the following steps:

Step 1 Click **Applications**.



Step 2 Click **Browse App Catalog** in the Okta dashboard.



Step 3 Click **OIDC** (OpenID Connect) check box in the **Functionality** of **Browse App Integration Catalog** page.

Functionality

- Workflows Connectors
- Workflow Templates
- SAML
- OIDC**
- SWA
- SCIM
- API

Step 4 Click on the search window and type Sclera.

[Applications](#) > [Catalog](#) > All Integrations







Browse App Integration Catalog

[Create New App](#)

Use Case	
All Integrations	7496
Apps for Good	9
Automation	26
Centralized Logging	11
Directory and HR Sync	20
Bot or Fraud Detection	3
Identity Proofing	10
Identity Governance and Administration (IGA)	7

Search: sclera

POPULAR SEARCHES : [Bookmark App](#) [SCIM 2.0 Test App](#) [Okta Org2Org](#) [Template App](#)

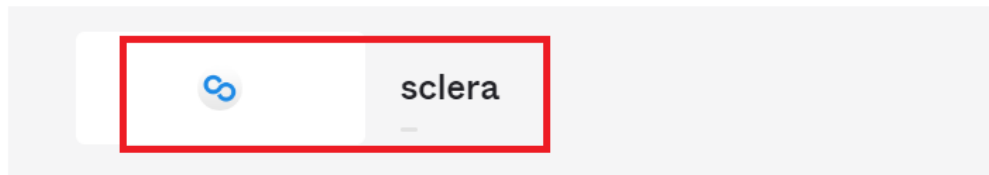
 SkyClerk SWA	 Valera Global SWA
 Georgia Clerks Authority SWA	 FannieMae DUS Disclose SWA
 Doppler SAML	 sclera

Step 5 Once the Sclera icon shows up, click on the icon and **Add Integration**.

[Applications](#) > [Catalog](#) > [Private Apps](#) > sclera

Last updated: February 2, 2023

[+ Add Integration](#)



Use Case

Overview

[Private Apps](#)

Functionality

sclera is an IT and OT asset monitoring and management software that transforms the way businesses manage the assets in their property. It leverages on its robust functionality, flexibility and scalability to centralize control of the assets and bring ease to the property management. It seamlessly works across devices and streamlines asset management by using remote monitoring to bring down waste of time, efforts, resources and expenses. Users may use Okta as a single sign-on provider to safely log into their sclera account and access the same functionalities of the app.

Step 6 Click **Sclera** and navigate to the **Sign On** tab.

sclera

[Active](#) [View Logs](#) [Monitor Imports](#)

[General](#) **[Sign On](#)** [Import](#) [Assignments](#) [Okta API Scopes](#)

[Assign](#) [Convert assignments](#) [People](#)

Filters	Person	Type
People		

Step 7 Copy the **Client ID** and **Client Secret**.

You will also be able to find your organization's domain in your Okta profile. Once you have these details you need to send an email to support@sclera.com. Sclera support will handle your request and get back to you once the integration is configured.

General **Sign On** Import Assignments Okta API Scopes

Settings Edit

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

OpenID Connect

Client ID

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

Client secret

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.

Q Search...

Applications

Developer Edition provides a limited number of apps.

Deactivate unused apps or check out our [plans page](#). Contact us to find a plan that is right for your organization.

[Create App Integration](#) [Browse App Catalog](#) [Assign Users to App](#) [More](#)

derryl@*****.io
okta-dev-46 *****

Derryl Murray

derryl@*****.io
dev-46 *****.okta.com

[My settings](#)

[Sign out](#)

Step 8 Click the **Assignments** tab in the configured Sclera app to give people or groups access to the Sclera application.

The screenshot shows the Sclera app configuration interface. At the top, there is a header with the Sclera logo, an 'Active' status indicator, and links for 'View Logs' and 'Monitor Imports'. Below this is a navigation bar with tabs for 'General', 'Sign On', 'Import', 'Assignments', and 'Okta API Scopes'. The 'Assignments' tab is highlighted with a red box. Below the navigation bar, there is a section with a search bar and a 'People' dropdown. A dropdown menu is open under the 'Assign' button, showing options for 'Assign to People' and 'Assign to Groups'. The 'Assign to Groups' option is highlighted with a red box. Below the dropdown, there is a table with a 'Type' column and three rows of binary strings: '01101110', '01101111', and '01101100'.

Step 9 Click **Assign** to complete the integration procedure.

The screenshot shows a dialog box titled 'Assign Sclera to Groups' with a close button (X) in the top right corner. At the top of the dialog is a search bar with the placeholder text 'Search...'. Below the search bar, there is a list of three options, each with a radio button and an 'Assign' button. The first option is 'Everyone' with the description 'All users in your organization' and its 'Assign' button is highlighted with a red box. The second option is 'Group A' and the third is 'Group B'. At the bottom right of the dialog, there is a 'Done' button, which is also highlighted with a red box.

Assign Sclera to People



Rachel Hunter

rachel@*****.io

Assign

Lisa David

lisa@*****.io

Assign

Ensuring access to valid users

Okta SSO provides an option to give an easy sign in option to individuals and groups. The administrator needs to make sure the assigned user name and email are valid before providing access.

Once users get access to Okta, they will be able to log in to their Sclera accounts through Sclera app using SSO on Okta dashboard.

SP-initiated SSO

- Step 1** Navigate to SSO page from your browser (<https://app.sclera.com/signin>).
- Step 2** Click Sign-in with Okta.
- Step 3** Enter your Okta user name and password in Okta Sign-in window.
- Step 4** Click Next.
- Step 5** You will be directed to Sclera dashboard in case you have entered valid credentials.

Known Issues / Troubleshooting

Please reach our team at support@sclera.com if you encounter any issue.