

# SSO Login via Okta to Markit

Markit users who have enterprise login can start using Okta as their login provider. This document describes the initial setup steps.

## 1. Supported features

- Single Sign-On (OpenID Connect) initiated with Okta from the application.

## 2. Requirements

In order to proceed with configuring, you must:

- If you haven't already, sign-up as a user in Markit
- The Okta Single Sign-On integration is only available for Markit Enterprise login users. This can be obtained by contacting your account manager in Markit.

## 3. Configuration steps

1. Download 'Markit Procurement Service' app from Okta's catalogue & enter the Sign-in redirect

URI that is associated with your Markit Enterprise login (if you do not know it then contact your account manager).

[View Setup Instructions](#)

OpenID Provider Metadata is available if this application supports dynamic configuration.

### Advanced Sign-on Settings

These fields may be required for a Markit Procurement Service proprietary sign-on option or general setting.

Sign-in redirect URI

Please enter your Sign-in redirect URI. Refer to the Setup Instructions to obtain this value.

### Credentials Details

Application username format: Okta username

Update application username on: Create and update

Password reveal:  Allow users to securely see their password (Recommended)

[Save](#)

2. After successful download, in the Okta admin page, click on the 'Markit Procurement Service' application and then navigate to the Sign On tab.

3. Copy the values of Client ID and Client secret (click the eye button to toggle the visibility).

General **Sign On** Mobile Import Assignments Okta API Scopes Application Rate Limits

**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 3<sup>rd</sup> party application. Application username is determined by the user profile mapping. [Configure profile mapping](#)

OpenID Connect

**Client ID**  [Edit](#)

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

**Client secret**  [Edit](#)

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.

**About**

**OpenID Connect** allows users to sign-on to applications using the OpenID Connect protocol.

**Application Username**

Choose a format to use as the default username value when assigning the application to users.

If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

4. Find the Okta Domain (or Issuer URI), which is the URI at which you are accessing your Okta tenant (https://example.okta.com).

## 4. After gathering information

Once you have all the information send the 'Client ID', 'Client Secret' & 'Issuer URI' to your Markit account manager.

NB! Do not send secrets as plain text via email.

## 5. Finally

Wait for the answer from your Markit account manager and continue as instructed.

Each customer in Markit who has enterprise login has their own login portal. Login portal URL will be provided by your account Manager in Markit if you do not know it already. NB! Okta login is only possible through your enterprise login portal.

If you have any extra questions, ask your Markit account manager.