

---

# Okta Integration Guide

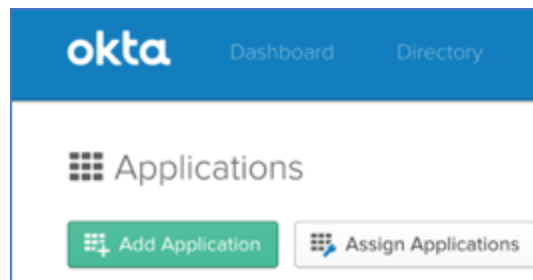
## Cloudflare Area 1 Overview

Area 1 fully supports Single Sign-On (SSO) today via IdP-initiation. One of the most popular distributions is Okta. In this document, all necessary steps to hook into Okta will be outlined.

When SSO is correctly configured, your authorised employees may connect to the Area 1 Customer Portal using a familiar username & password.

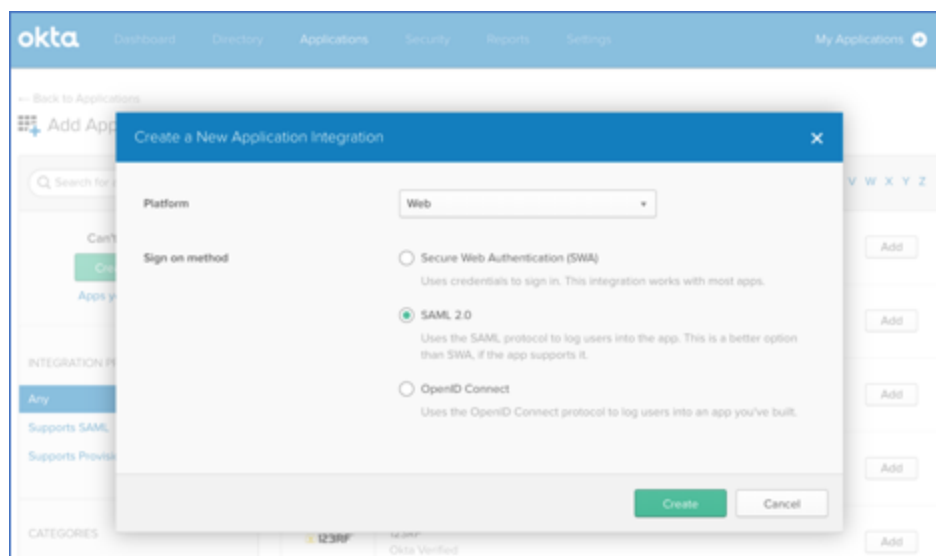
# Creating an Area 1 App in Okta

An app for Area 1 will need to be created manually in Okta. To start, log into Okta as an administrator and go to *Add Application*:



Next, you'll need to create a new SAML 2.0 app:

*Create New App > SAML 2.0 > Create*



Name the app "**Area 1**" and Next:

**Create SAML Integration**

1 General Settings | 2 Configure SAML

1 General Settings

App name: Area 1

App logo (optional): [Gear icon] [Browse...]

Upload Logo

App visibility:

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

Cancel | Next

Enter in all the info below (including *Single Sign-On URL, Audience URI, Default RelayState, Name ID Format, Application Username, Attribute Statements*) and press Next:

Single sign on URL	https://portal.area1security.com/api/users/saml
Audience URI	https://portal.area1security.com/api/users/saml
Default RelayState	https://portal.area1security.com
Name ID format	EmailAddress
Application username	Email
Attribute Statements / Name	email
Attribute Statements / Value	user.email

**SAML Settings**

**GENERAL**

Single sign on URL   
 Use this for Recipient URL and Destination URL  
 Allow this app to request other SSO URLs

Audience URI (SP Entity ID)

Default RelayState   
If no value is set, a blank RelayState is sent

Name ID format

Application username

[Show Advanced Settings](#)

---

**ATTRIBUTE STATEMENTS (OPTIONAL)** [LEARN MORE](#)

Name	Name format (optional)	Value
<input type="text" value="email"/>	<input type="text" value="Unspecified"/>	<input type="text" value="usec.email"/>

Next

Define as an internal app and press Finish:

3 Help Okta Support understand how you configured this application

Are you a customer or partner?  I'm an Okta customer adding an internal app  
 I'm a software vendor. I'd like to integrate my app with Okta

**i** The optional questions below assist Okta Support in understanding your app integration.

App type **i**  This is an internal app that we have created

Previous Finish

Click the Identity Provider link here:

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.

SAML 2.0

Default Relay State <https://portal.area1security.com>

**i** SAML 2.0 is not configured until you complete the setup instructions.

View Setup Instructions

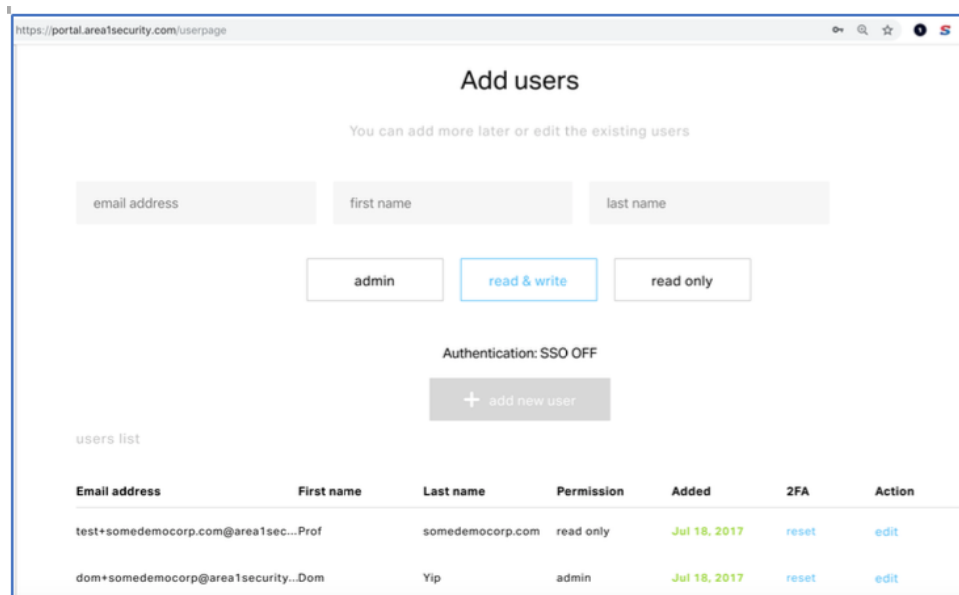
**Identity Provider metadata** available if this application supports dynamic configuration.

Copy the URL in your browser's address bar (CTRL+C). **Important:** You'll need to paste this into your Area 1 configuration later.

## Configuring Area to Connect to Okta

Go to your Area 1 Customer Portal (<http://portal.area1security.com>) and add the email addresses of all your authorised administrators:

*Settings > User Management*



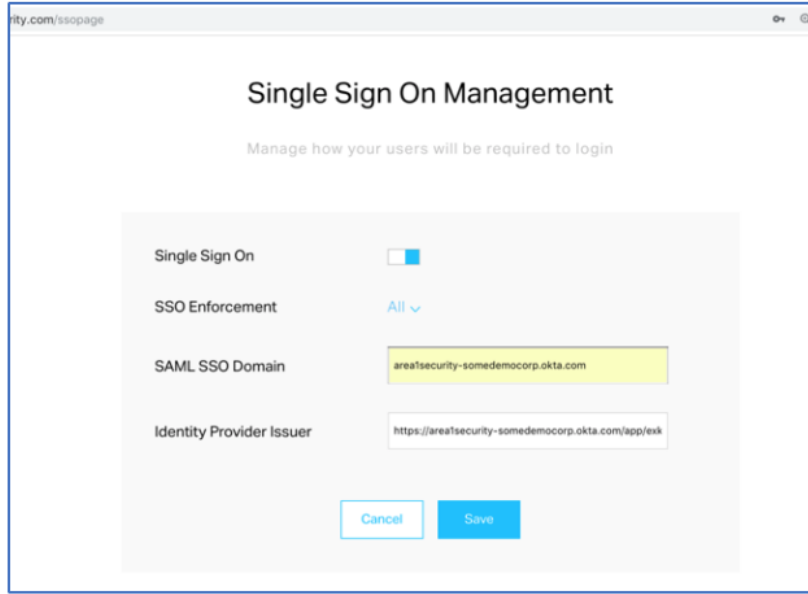
The screenshot shows the 'Add users' interface. At the top, there are three input fields for 'email address', 'first name', and 'last name'. Below these are three buttons for permissions: 'admin', 'read & write', and 'read only'. The 'read & write' button is highlighted. Underneath, it says 'Authentication: SSO OFF' and there is a '+ add new user' button. At the bottom, there is a 'users list' table with the following data:

Email address	First name	Last name	Permission	Added	2FA	Action
test+somedemocorp.com@area1sec...Prof		somedemocorp.com	read only	Jul 18, 2017	reset	edit
dom+somedemocorp@area1security...Dom		Yip	admin	Jul 18, 2017	reset	edit

Next, go to :

*Settings > SSO Settings.*

Toggle on the Single Sign On switch, then set enforcement as needed. Enter in your SAML SSO Domain and paste (CTRL+V) that URL string from earlier into Identity Provider Issuer:



## Success!

Log out of any Customer Portal sessions. You may now log into Area 1 through your Okta tiles:

