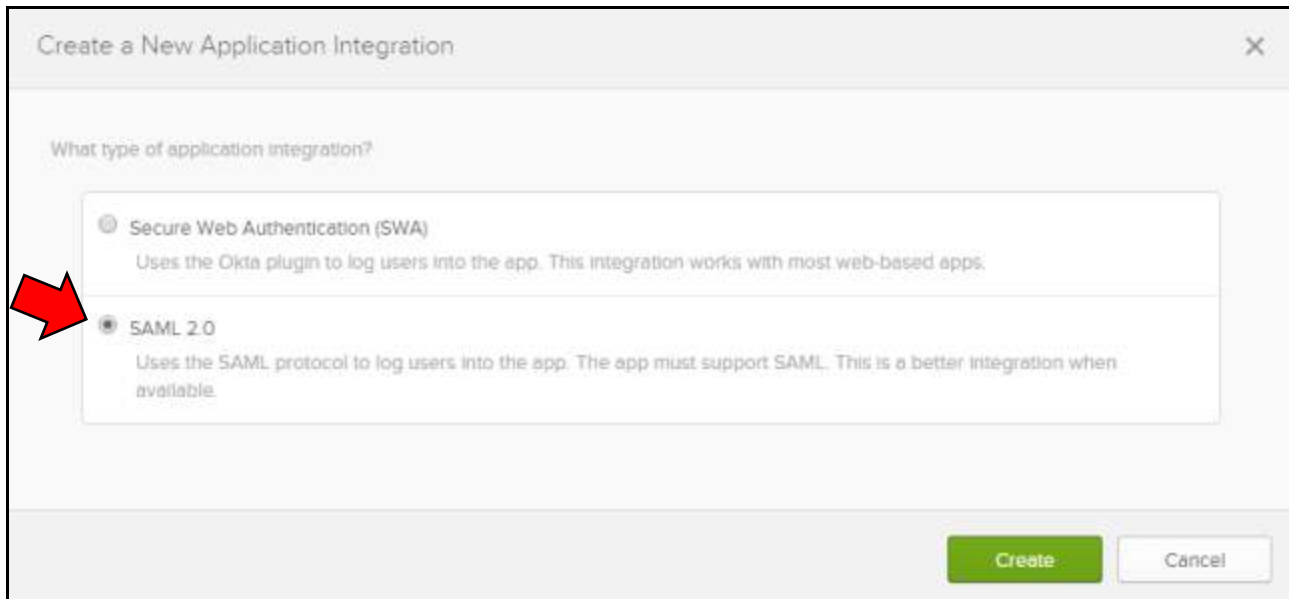# miniOrange

SETUP GUIDE OKTA AS IdP

STEP 1:

- Log into Okta and create a new SAML 2.0 application

STEP 2:

- In General Settings, enter App Name and click Next.
- In SAML Settings, enter the following:

Entity ID	SP-EntityID / Issuer from Step1 of the plugin under Identity Provider Tab.
ACS URL	ACS (AssertionConsumerService) URL from Step1 of the plugin under Identity Provider Tab.
Recipient URL	Recipient URL from Step1 of the plugin under Identity Provider Tab.
Destination URL	Destination URL from Step1 of the plugin under Identity Provider Tab.
Subject Type	Username
Name ID Format	EmailAddress
Single Logout URL	Single Logout URL from Step1 of the plugin under Identity Provider Tab.
Signature Certificate	Upload the certificate provided in Step1 of the plugin under Identity Provider Tab.

Default Relay State	Default Relay State from Step1 of the plugin under Identity Provider Tab.

**STEP 3:**

- After creating and configuring the app go to the **People** tab.
- Here we select the people you want to give access to login through this app. Assign this to the people you would to give access to.

STEP 4:

- After assigning the people to your app go to **Sign On** tab.
- Click on view setup instructions to get the **SAML Login URL (Single Sign on URL), Single Logout URL, IdP Entity ID** and **X.509 Certificate**.
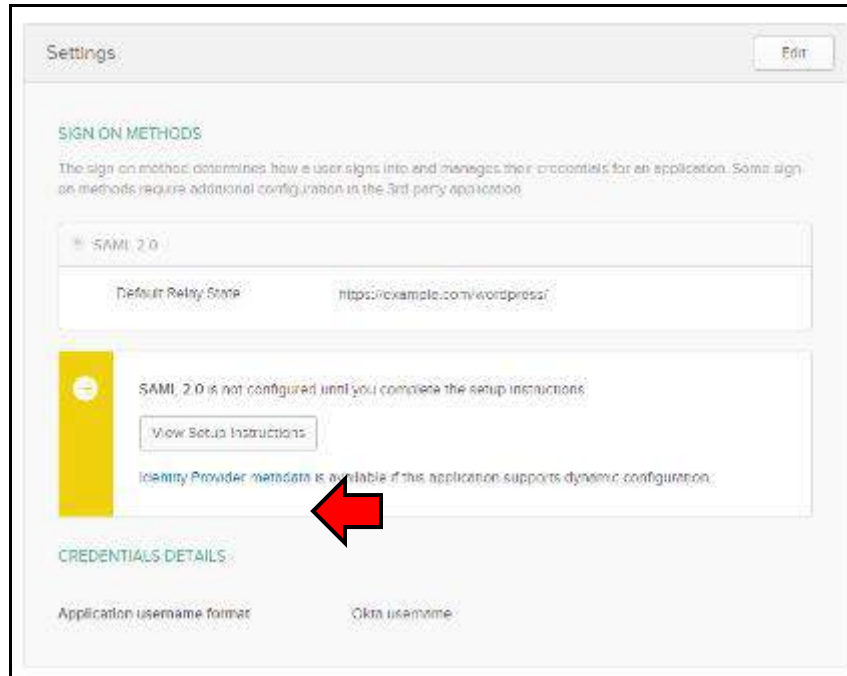
STEP 5:

In miniOrange SAML plugin, go to **Service Provider** tab. Enter the following values:

- **Identity Provider Name:** Okta
- **IdP Entity ID:** Identity Provider Issuer from Okta Setup Instructions
- **SAML Login URL:** Identity Provider Single Sign-On URL from Okta Setup Instructions
- **SAML Logout URL:** Identity Provider Single Logout URL from Okta Setup Instructions
- **X.509 Certificate:** X.509 Certifiacate from Okta Setup Instructions
- **Response Signed:** Checked
- **Assertion Signed:** Checked