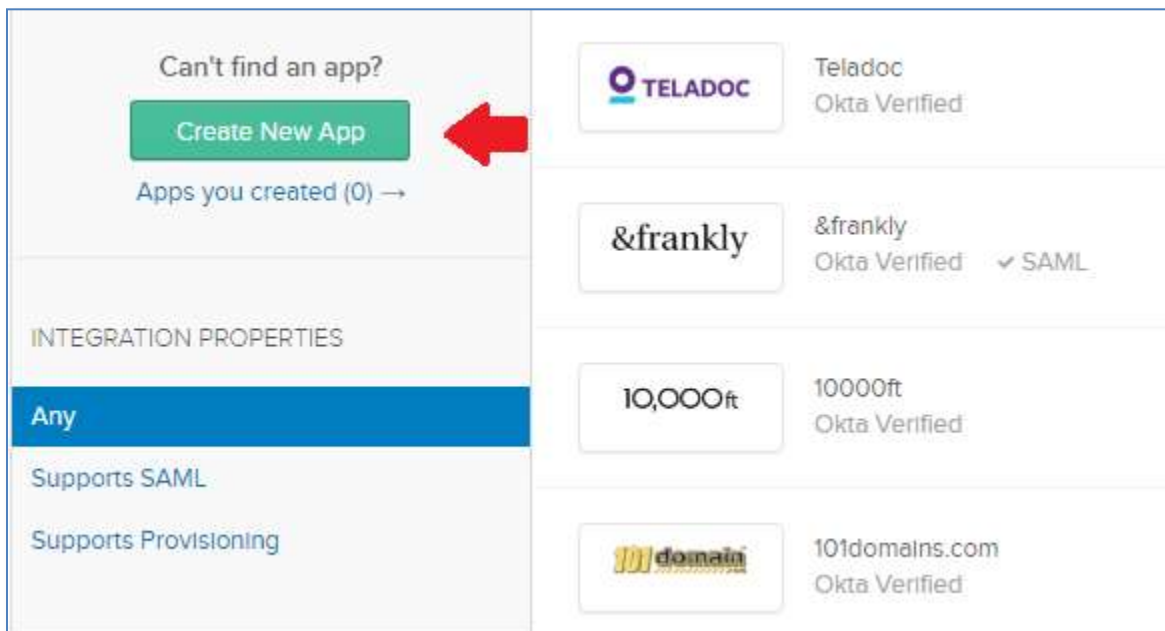
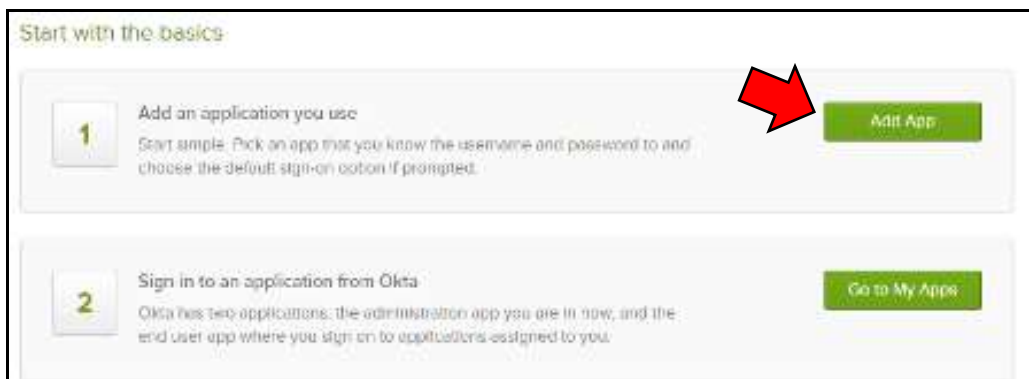


STEP 1:

- Log into Okta and create a new SAML 2.0 application



Create a New Application Integration

What type of application integration?

☐ Secure Web Authentication (SWA)
 Uses the Okta plugin to log users into the app. This integration works with most web-based apps.

☒ SAML 2.0
 Uses the SAML protocol to log users into the app. The app must support SAML. This is a better integration when available.

Create

Cancel

STEP 2:

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

Single Sign On URL	ACS (Assertion Consumer Service) URL from Step1 of the plugin under Configure IDP Tab.
Audience URI(SP Entity ID)	SP-EntityID / Issuer from Step1 of the plugin under Configure IDP Tab.
Default Relay State	Default Relay State from Step1 of the plugin under Configure IDP Tab.
Name ID Format	Email Address
Application Username	Okta username

A

SAML Settings

GENERAL

Single sign on URL ⓘ

☒ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) ⓘ

Default RelayState ⓘ

If no value is set, a blank RelayState is sent

Name ID format ⓘ

EmailAddress ▾

Application username ⓘ

Okta username ▾

Response ⓘ

Signed ▾

Assertion Signature ⓘ

Signed ▾

Signature Algorithm ⓘ

RSA-SHA256 ▾

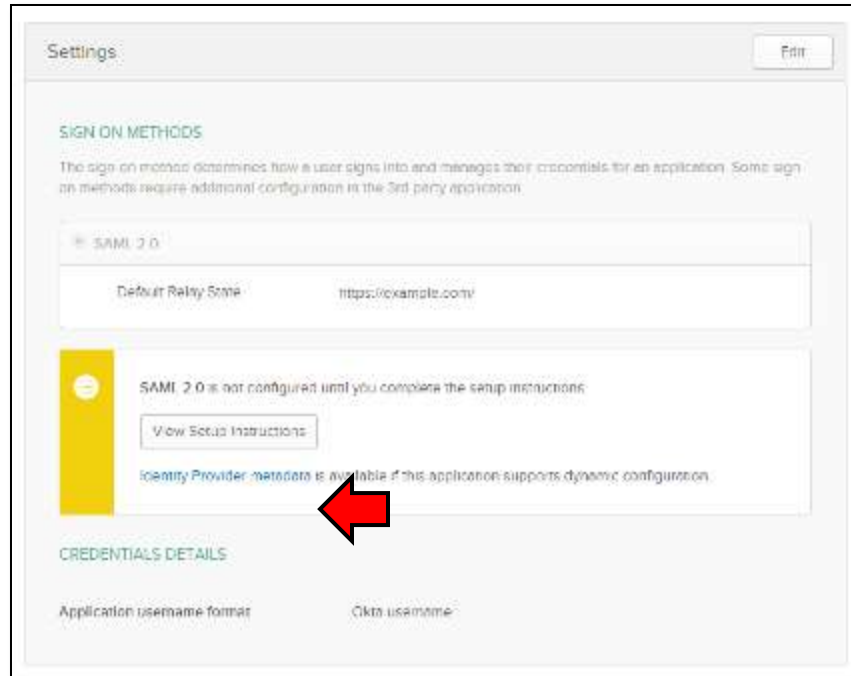
Hide Advanced Settings

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 **Configure SP** tab. Enter the following values:

- **IDP Entity ID:** Identity Provider Issuer from Okta Setup Instructions
- **Single Sign On URL:** Identity Provider Single Sign-On URL from Okta Setup Instructions
- **Single Logout URL:** Identity Provider Single Logout URL from Okta Setup Instructions
- **X.509 Certificate:** X.509 Certificate from Okta Setup Instructions

STEP 6:

In miniOrange SAML plugin, go to **Attribute Mapping** tab. Enter the following values:

- **Username:** Name of the username attribute from IDP (Keep NameID by default)
- **Email:** Name of the email attribute from IDP (Keep NameID by default)
- **FirstName:** Name of the firstname attribute from IDP
- **LastName:** Name of the lastname attribute from IDP

Attribute Mapping

Username: *

Enter the Attribute Name that contains Confluence Username. Use *NameID* if Username is in Subject element.

Email: *

Enter the Attribute Name that contains Email. Use *NameID* if Email is in Subject element.

Full Name Attribute:

Enter the Attribute Name that contains Full Name.

Separate Name
Attributes:☐ (Select this if your IDP is sending First name and Last name as separate attributes.)

First Name:

Enter the Attribute Name that contains First Name.

Last Name:

Enter the Attribute Name that contains Last Name.

STEP 7:

Go to **Role Mapping** tab. Enter the following values:

- **Role Mapping:** Name of the Role attribute from IDP

You can check the **Test Configuration Results** to get a better idea as to which values to map here.

Under the Role Mapping Section configure which GROUP value coming in the SAML response needs to be mapped to which role. The Group value coming in the SAML response will be mapped to the Role assigned here and the user will be assigned that role.

Role Mapping

Role Attribute:

Enter the Attribute Name that contains Roles of the User.

Create Users: ☐ If checked, Users will be created only if roles are mapped.

Default Group:*

Select Default Group to assign to new Users.

confluence-administrators:

confluence-users:

Note: Enter semi-colon separated list of role values in the textbox.

Save

STEP 8:

Go to **Sign In Settings** tab. Enable auto-redirect to IDP using **Disable Confluence login** option.

Sign In Settings

Login Button Text:*

Disable Confluence login: ☒

Enable backdoor: ☒ Use `http://localhost:8091/login.action?saml_sso=false`
For administrative tasks use `http://localhost:8091/authenticate.action?saml_sso=false`

Save