

How to Create Zunos SAML App in Okta

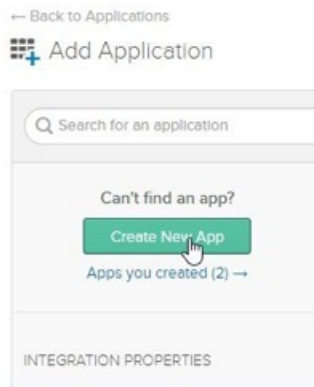
Last Modified on 06/29/2020 3:51 pm EDT

NOTE: This will require you to create an application from within Okta

1. Click on "Add Application" from with the Applications menu in Okta Administration



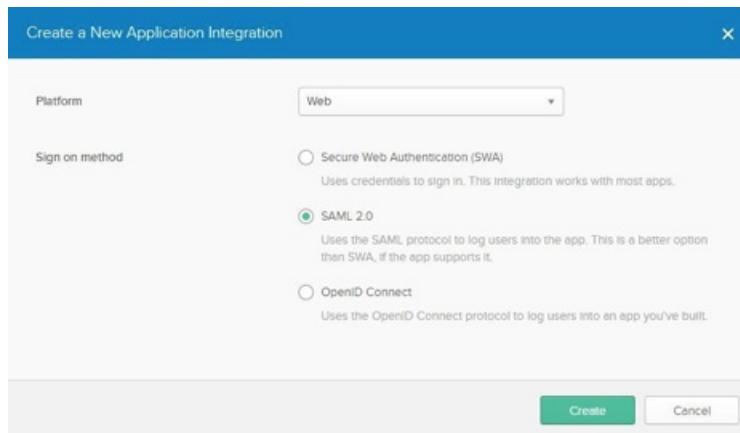
2. Click the "Create New App" button to start the build:



3. Platform: Web

4. Sign on Method: SAML 2.0

5. Click Create



6. App name is customizable, this example displays "Zunos"

7. App logo is also customizable, users can implement the logo used here:




Edit SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

1 General Settings

App name: Zunos

App logo (optional):  Zunos_Logo.png

App visibility:

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

© 2020 Okta, Inc. Privacy Version 2020.04.1 OPI Preview Cert (US) Status site Download Okta Plugin Feedback

This wizard walks you through editing the properties in your SAML app. All of your app's properties are prepopulated in the wizard.

NOTE: App visibility is at user's discretion

8. Click Next

9. Use the following guidelines to fill in the SAML Settings:

Single sign on URL: [https://auth.zunos.com/Saml2/\(OrgName\)/Acs](https://auth.zunos.com/Saml2/(OrgName)/Acs) - (OrgName to be supplied by Bigtincan technical team on setup)

Recipient URL: [https://auth.zunos.com/Saml2/\(OrgName\)/Acs](https://auth.zunos.com/Saml2/(OrgName)/Acs) - (OrgName to be supplied by Bigtincan technical team on setup)

Destination URL: [https://auth.zunos.com/Saml2/\(OrgName\)/Acs](https://auth.zunos.com/Saml2/(OrgName)/Acs) - (OrgName to be supplied by Bigtincan technical team on setup)

Audience URI (SP Entity ID): zunos:saml2

Review the other settings in the screenshot below. They are the default values populated by Okta

SAML Settings		Edit
GENERAL		
Single Sign On URL	https://auth.zunos.com/Saml2/oktadevsaml/Acs	
Recipient URL	https://auth.zunos.com/Saml2/oktadevsaml/Acs	
Destination URL	https://auth.zunos.com/Saml2/oktadevsaml/Acs	
Audience Restriction	zunos:saml2	
Default Relay State		
Name ID Format	EmailAddress	
Response	Signed	
Assertion Signature	Signed	
Signature Algorithm	RSA_SHA256	
Digest Algorithm	SHA256	
Assertion Encryption	Unencrypted	
SAML Single Logout	Disabled	
authnContextClassRef	PasswordProtectedTransport	
Honor Force Authentication	Yes	
SAML Issuer ID	http://www.okta.com/\${org.externalKey}	

10. Click Next

11. Choose "I'm an Okta customer adding an internal app" and click "Finish"

Edit SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

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

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

App type

This is an internal app that we have created

Previous Finish

Why are you asking me this?
This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

© 2020 Okta, Inc. Privacy Version 2020.04.1 OPI Preview Cert (LTS) Status site Download Okta Plugin Feedback

Here is an example assertion:

```
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
```

<http://www.okta.com/Issuer>

userName

zunos:saml2

urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

After setup is complete, users can access the IDP metadata.xml file from the application "Sign On" tab:

← Back to Applications

Zunos application card showing logo, status (Active), and View Logs button.

General Sign On Mobile Import Assignments

Settings panel for Zunos application, including sections for Sign On Methods and Credentials Details.

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](#)

SAML 2.0

Default Relay State

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

[View Setup Instructions](#)

[Identity Provider metadata](#) is available if this application supports dynamic configuration.

CREDENTIALS DETAILS

Application username format: Okta username

Update application username on: Create and update [Update Now](#)

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

About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

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.

Download the "Identity Provider metadata" and supply it to Bigtincan for setup.