



Better Translation Technology

Okta SAML 2.0 configuration

Published by XTM International Ltd.

© Copyright XTM International Ltd. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying, without prior written consent of XTM International Ltd.

Table of contents

Table of contents	3
Prerequisites	4
Okta configuration	4
XTM configuration	6

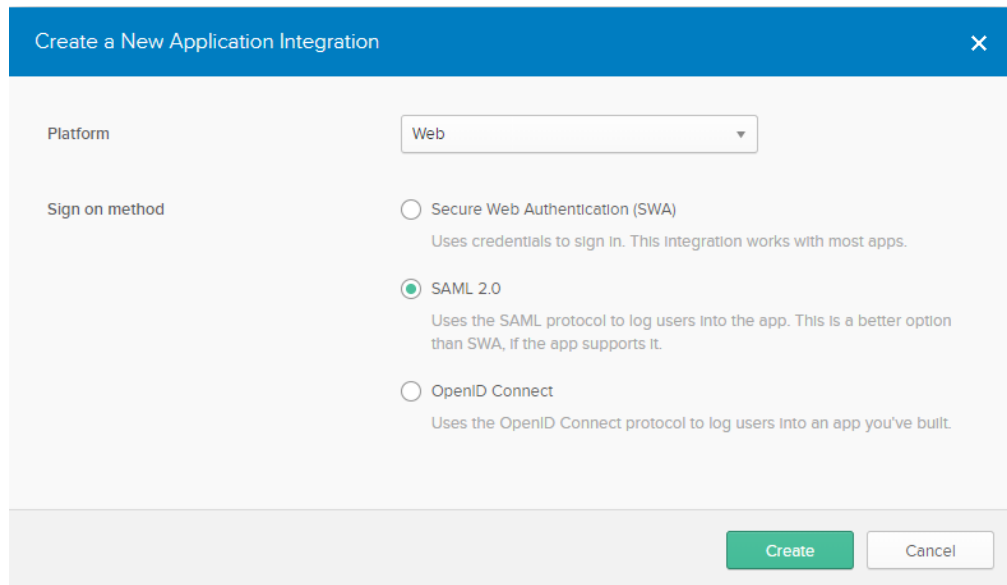
1. Prerequisites

- metadata.xml file from XTM
- Verified okta.com account

2. Okta configuration

2.1. Go to Administrator -> Add Applications -> Create new app

2.2. Choose Platform: *Web* and Sign on method: *SAML 2.0* and click *Create*



Create a New Application Integration

Platform: Web

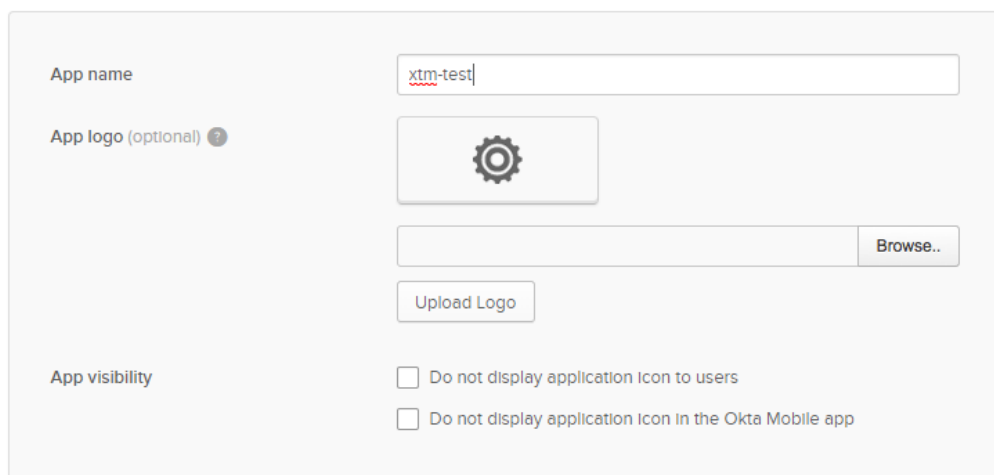
Sign on method:

- Secure Web Authentication (SWA)
Uses credentials to sign in. This integration works with most apps.
- SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.
- OpenID Connect
Uses the OpenID Connect protocol to log users into an app you've built.

Create Cancel

2.3. On *General Settings* screen provide App name and logo.

1 General Settings



App name: xtm-test

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

[Upload Logo]

App visibility:

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

2.4. On *Saml Settings* screen provide following information

2.4.1. **Single sign on URL** - value of the location attribute of

AssertionConsumerService node from the metadata.xml file that should be provided with this manual

2.4.2. Check *Use this for Recipient URL and Destination URL* checkbox

2.4.3. **Audience URI (SP Entity ID)** - value of *entityID* attribute of *EntityDescriptor* node from the metadata.xml file

- 2.4.4. **Default relay state** - leave empty
- 2.4.5. **Name ID format** - EmailAddress
- 2.4.6. **Application username** - Email
- 2.4.7. Add Attribute Statements entry:
 - 2.4.7.1. **Name:** email
 - 2.4.7.2. **Name format:** Basic
 - 2.4.7.3. **Value:** user.email

A 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 ?

Update application username on

[Show Advanced Settings](#)

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

Name	Name format (optional)	Value	
<input type="text" value="email"/>	<input type="text" value="Basic"/>	<input type="text" value="user.email"/>	✕

2.5. Press *Finish*

The following is needed to configure xtm

1 Identity Provider Single Sign-On URL:

https://[REDACTED]/sso/saml

2 Identity Provider Issuer:

http://www.okta.com/[REDACTED]

3 X.509 Certificate:

-----BEGIN CERTIFICATE-----



-----END CERTIFICATE-----

Download certificate

3. XTM configuration

Pass information from screen 2.5 (*Identity Provider Single Sign-on URL*, *Identity Provider Issuer* and *X.509 Certificate*) to XTM staff. SSO will be enabled once XTM finishes their part of the configuration.