Configuring OneLogin as an Identity Provider

1. Log into your OneLogin account.

2. Go to the "Apps" section and then click the "Add app" button.
   In the filter box type "SAML" and select the "SAML Test Connector (IdP w/attr)" application.
   Change the display name of your app if you wish and click "Save".

3. In your KBPublisher administrator area go to Settings -> Authentication Provider -> SAML.
   Find the "Service Provider" section and open the "Metadata" window.
   On the Configuration tab of your Onelogin app, match the following settings:
   Audience: [Entity Id]
   Recipient: [Entity Id]
   ACS (Consumer) URL Validator: .*.
   ACS (Consumer) URL: [Assertion Consumer Service URL]
   Single Logout URL: [Single Logout Service URL]

   Click on the "Save" button.

4. KBPublisher settings for attributes names default to Onelogin attributes, but you might need to ensure they are equal.

5. Go to the "SSO" tab, then click on the "View Details" link at the "X.509 Certificate" field.
   Copy the certificate contents and paste it into the "Public X.509 Certificate" window in KBPublisher.
   Copy the values of "Issuer URL", "SAML 2.0 Endpoint (HTTP)" and "SLO Endpoint (HTTP)" and paste them into the corresponding KBPublisher fields as shown below.

6. If you don't already have a user on OneLogin go to the "Users" tab and add one.
   Go to the "Applications" tab on the user page and assign the application to him.

7. On your KBPublisher settings page click the "Test / Debug" button.
   If it works, you'll see a greeting message.

8. If click on "App Icon" in Onelogin (or Okta) to login to KBPublisher does not work, fill RelayState field in app settings, it should be full path to your KBPublisher installation (example: https;//domain.com/kb/)

Article ID: 444
Last updated: 12 May, 2022
Updated by: Leontev E.
Revision: 3
KBPublisher 8.0 Knowledge Management Handbook -> Single Sign On -> SAML Authentication -> Configuring OneLogin as an Identity Provider
https://www.kbpublisher.com/kb/entry/444/