SSO Implementation

You can add SAML security to your KCCP implementation and enforce Single Sign On (SSO) to improve security.

This guide provides a high level overview of how to set up SSO for your Admin interface users. The information here does not apply for shopper accounts on the storefront. You can implement SSO for shoppers with a custom integration using API Extensions.

Development Requirements

First you must configure your identity provider (IdP). Create a service provider (SP) metadata file using the below templates, replacing [NAME] with a short, web-safe name for your company.

Metadata file for US tenants:

```
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
validUntil="2030-03-20T17:10:46Z"
entityID="http://www.kibocommerce.com/sso/prod">
<md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false" protocolSupp
ortEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://www.mozu.com/login/Home/Logout" />
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://www.mozu.com/login/WsFed/Signin/[NAME]"
index="1" />
</md:SPSSODescriptor>
</md:EntityDescriptor>
```

Metadata file for EU tenants:

```
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
validUntil="2030-03-20T17:10:46Z"
entityID="http://www.kibocommerce.com/sso/prod">
<md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false" protocolSupp
ortEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://www.euw1.kibocommerce.com/login/Home/Logout" />
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://www.euw1.kibocommerce.com/login/WsFed/Signin/[NAME]"
index="1" />
</md:SPSSODescriptor>
</md:EntityDescriptor>
```

Import the SP file into your IdP, including the following claims.

- The first is used to find the user by email address, and must be from a set of specified domains:

  `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`

- The second is used to create the user's surname in the system if the user is unknown:

  `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname`

- The third is used to create the user's given name in the system if the user is unknown:

  `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname`

Export IdP File

After adding and configuring the Kibo Service Provider in your identity provider, export an IdP Metadata or Federation Metadata file.

Submit a Ticket

Submit a ticket with the exported file along with a set of test credentials and optional login endpoint on your system to validate. Kibo will update the system with your configuration and validate the connection.

After submitting your ticket, please plan on four to six weeks of implementation time.