Integrate the first application to Ubisecure SSO

This article instructs on creating the first application on top of Ubisecure SSO.

Installation

One option is to use SAML as a service provider for the application. See the manual for integrating the application using SAML at Install Sample SAML service provider application for Java.
OAuth 2.0 or OpenID can alternatively be used as the service provider.

Delivering user attributes

The user attributes sent from SSO to the application can be managed through the application's authorization policy.
The process of creating and adjusting the policy is described in the article Manage authorization policies.

Directory user mapping

The application can use the data of the authenticating user to fetch their data from a third-party identity provider. This is achieved by mapping the users in the directories.
Below is a manual for directory user mapping for the TUPAS methods with practical examples :
Management UI Traditional Directory User Mappings - SSO
For SQL databases, some specific configurations are needed:
Use Directory User Mapping with SQL databases

Related articles

- Use an unsolicited SSO or an IDP initiated SSO
- Integrity verification failed on token endpoint
- SAML Compatibility Flags
- How to log a user in based on an existing session
- Configure OpenID Connect Google login