# SSO / SAML 2.0

- Integrations
- Microsoft Azure - Exchange of Metadata: Basic Guideline

# Integrations

Security Assertion Markup Language (SAML) is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP).

SAML transactions use Extensible Markup Language (XML) for standardized communications between the identity provider and service providers. SAML is the link between the authentication of a user’s identity and the authorization to use a service.

| Integration | Description |
| --- | --- |
| Microsoft Azure | SAML 2.0 integration over Azure Active Directory admin portal |

# Microsoft Azure - Exchange of Metadata: Basic Guideline

## Preparation

1. Go to Azure Active Directory admin portal
2. Go to *Enterprise Applications*
3. create a *new application* (*create your own application*)
   - Name: "Swiss Learning Hub" or something that helps you recognize this configuration again
   - Select: **Integrate any other application you don't find in the gallery (Non-gallery)**
4. Go to *Single sign-on* and choose SAML
   1. On step 2 (Attributes & Claims): change the *Attributes & Claims* if necessary. As *Unique User Identifier (Name ID)* the same variable must be used, which contains the value that is identical to the Swiss Learning Hub username.
   2. On step 3 (SAML Certificates): Copy the *App Federation Metadata URL*. **Send this link (or Metadata XML behind this link) to your Swiss Learning Hub contact**.
5. Go to *Users and groups* and add users or groups to be authorized for authentication.

## Receive the metadata of Swiss Learning Hub

1. Go to Azure Active Directory admin portal
2. Go to *Enterprise Applications*
3. Choose the Swiss Learning Hub application
4. Go to *Single sign-on* and choose *SAML*
5. Upload the received metadata file.