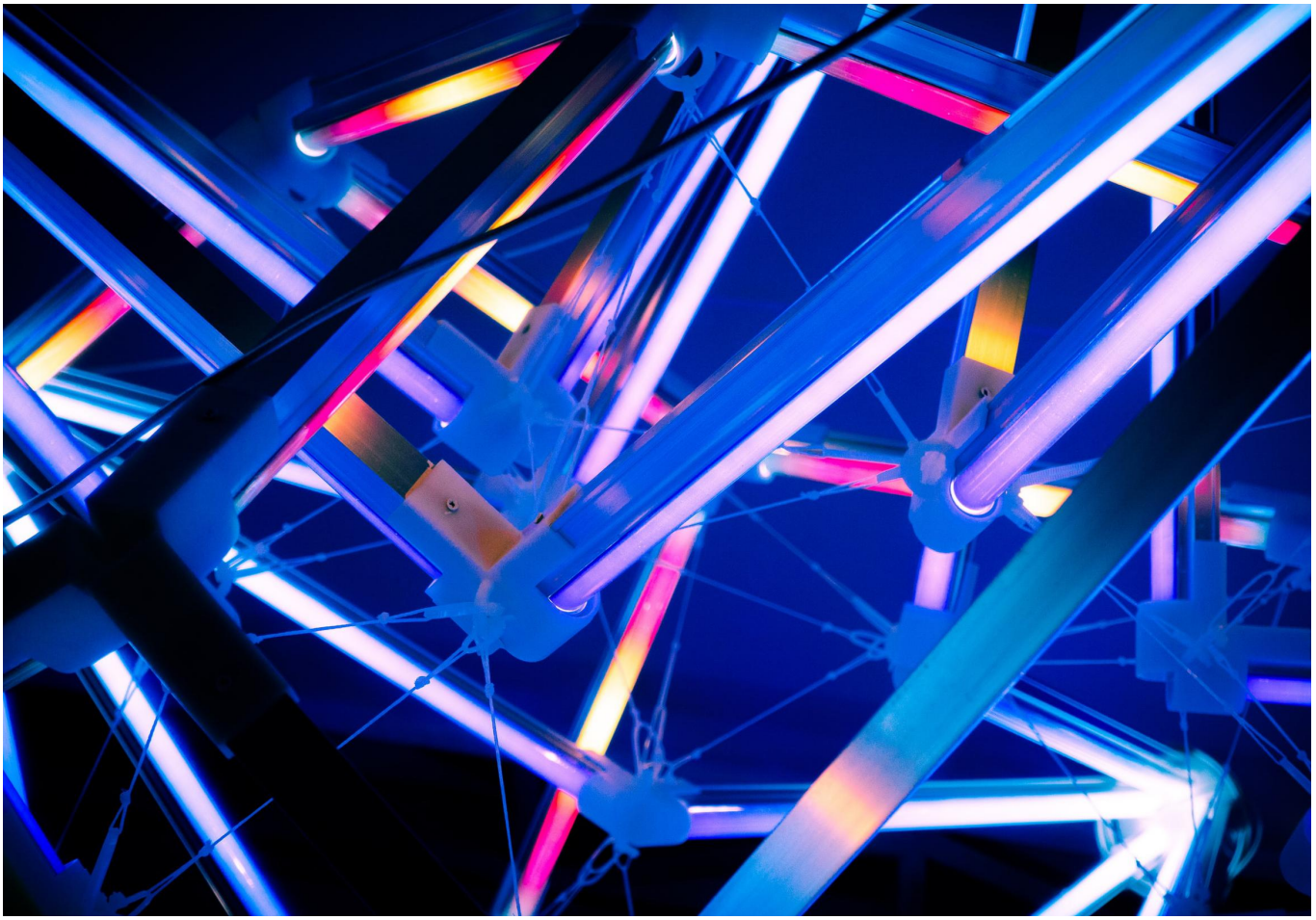
360Learning

LMS & CORPORATE **UNIVERSITIES**

Technical Guide
SSO SAML Azure AD

version 1.2



👉 At **360Learning**, we don't make promises about technical solutions, we make commitments. This technical guide is part of our Technical Documentation.

360Learning

360LEARNING IS A LEADING EUROPEAN CLOUD SOLUTION PROVIDER

> As a leading Cloud Solution Provider, we are strongly committed to providing our clients with high levels of security, SLAs and privacy, both in the contractual engagements we make and the technical infrastructure we build. We comply with French Laws requirements which are the most restrictive in terms of Data, Security & Privacy.

Nicolas Hernandez
CEO, 360Learning

👉For more information, please contact us:

product@360learning.com | www.360learning.com

Table of contents👇

Introduction

Single Sign-On (SSO) is an authentication mechanism that allows users to access several applications with only one set of login credentials.

By enabling SSO for your 360Learning application, you become responsible for the authentication of your users: they get authenticated through your own login portal and do not need an additional set of login / password anymore.

Communication between your authentication system and 360Learning can be handled by several technologies including SAML (Secure Assertion Markup Language), a format based on XML.

SAML is supported by many services and can be easily integrated with your corporate authentication system, for example Windows Active Directory.

Process

Let's compare the local login process and the SSO process to understand their differences.

Local login process (credentials managed by 360Learning)

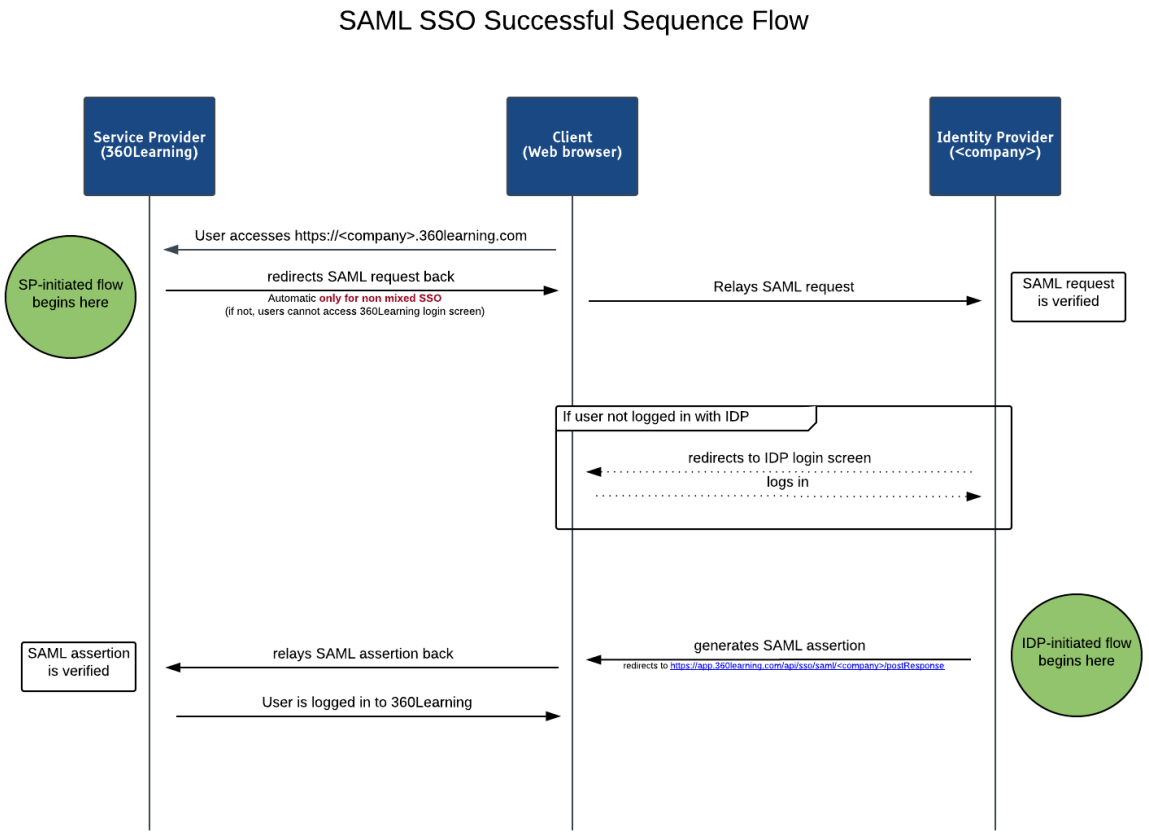
1. An unauthenticated user requests access to your 360Learning space.
2. The user is redirected to the login page of your 360Learning space where he can provide his login and password.
3. 360Learning grants him permission and redirects him to your space.

SAML SSO process (credentials managed by you)

While using SSO, the process involved is slightly different and requires several browser redirections and message exchanges using SAML standard.

1. An unauthenticated user requests access to your 360Learning space.
2. 360Learning redirects him to your own login portal.
3. The user gets authenticated using your own authentication process.
4. A secured SAML payload (“SAML assertion”) containing information about the user is created.
5. The user gets redirected to our endpoint with the SAML payload.
6. 360Learning analyzes the payload, grants the user permission and redirects him to your 360Learning space.

This process is illustrated in the following sequence diagram :



Please note that the process can be initiated by the “Service Provider” (360Learning) as well as the “Identity Provider” (you).

Service provider initiated flow

This is the case when the SSO flow is triggered by 360Learning. : our login page redirect the user to your servers with appropriate SAML payload.

Identity provider initiated flow

This is typically the case when you integrate a link in your intranet to reference 360Learning. Please note that this is no standard link : you have to generate the SAML assertion as illustrated in the above diagram.

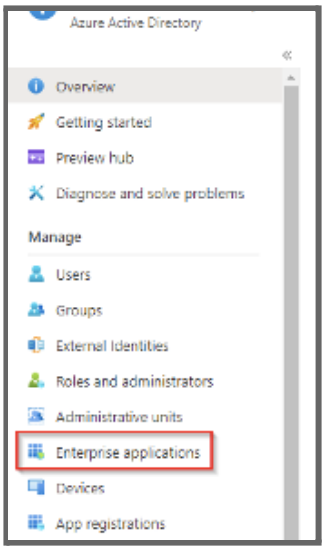
Configuration

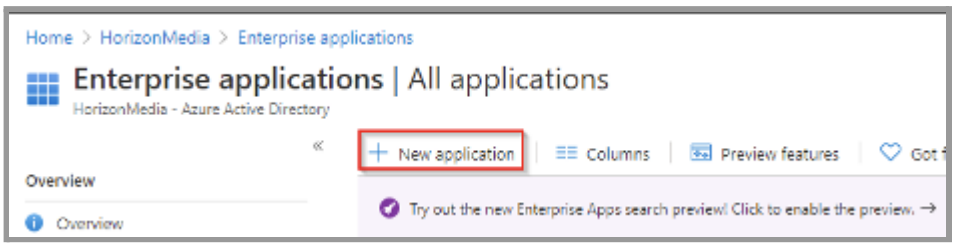
In this part, we focus on how to configure SSO with Azure AD (Microsoft Azure Active Directory).

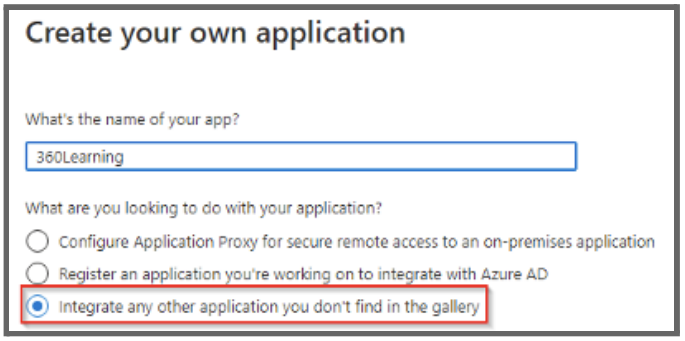
To enable SSO for your 360Learning space, first contact your designated solution architect: he will guide you through the entire integration process and give you the Reply URL required to configure your Azure AD.

Adding an unlisted application

→ To connect an application using an app integration template, sign into the Azure management portal using your Azure Active Directory administrator account, and browse to the **Azure Active Directory > Enterprise Applications** section, select **New Application**, and then **create your own application**.

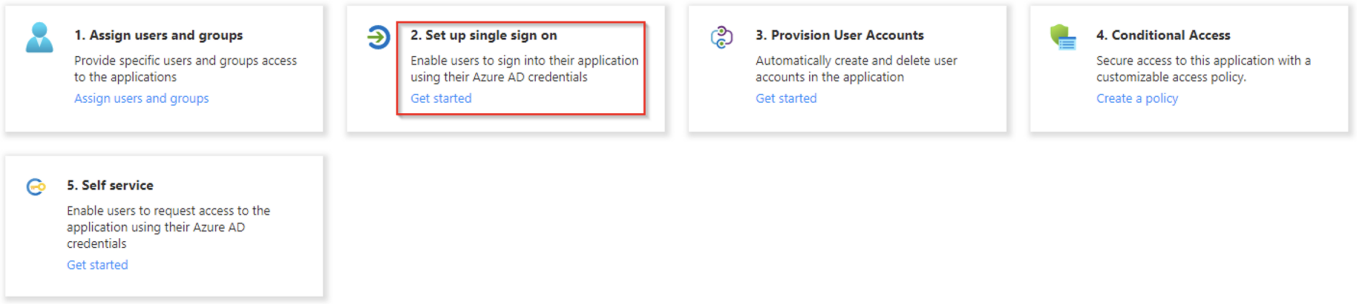




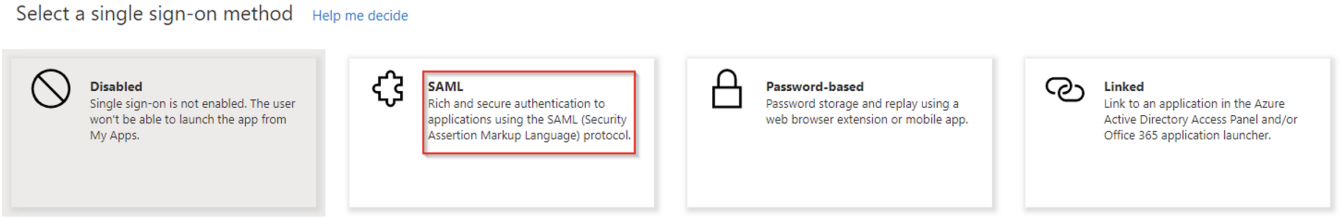


→ Back at the application configuration page, select “Set up single sign-on”

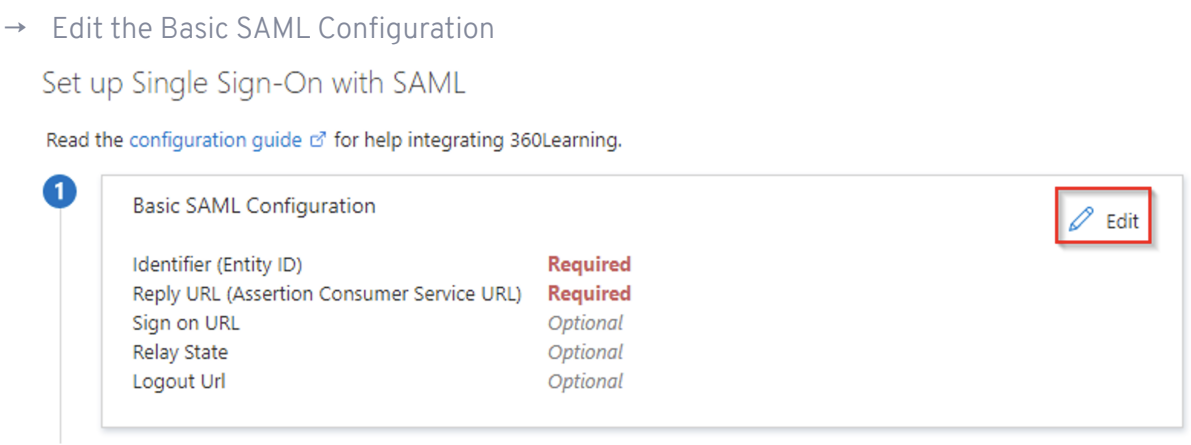
(if you do not see these options on your screen, please contact your Azure AD admin)



→ Select the SAML single sign-on method

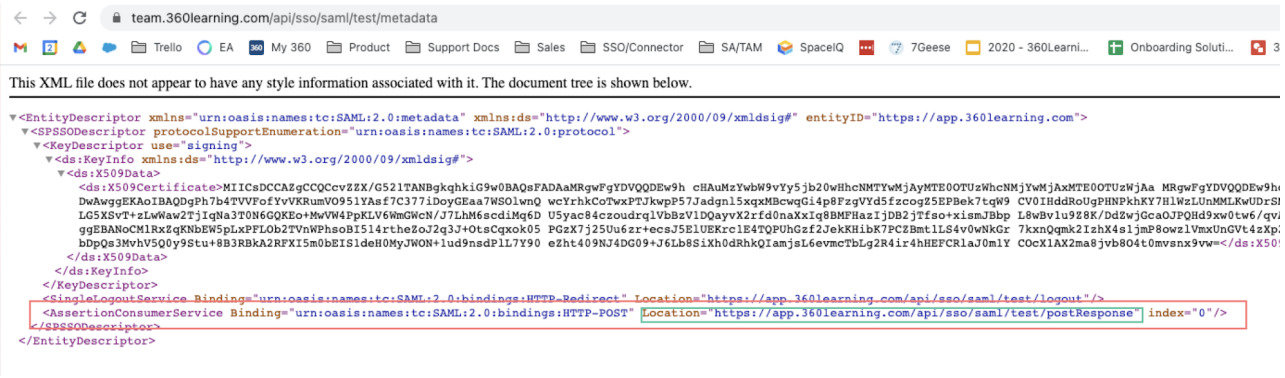


→ Edit the Basic SAML Configuration



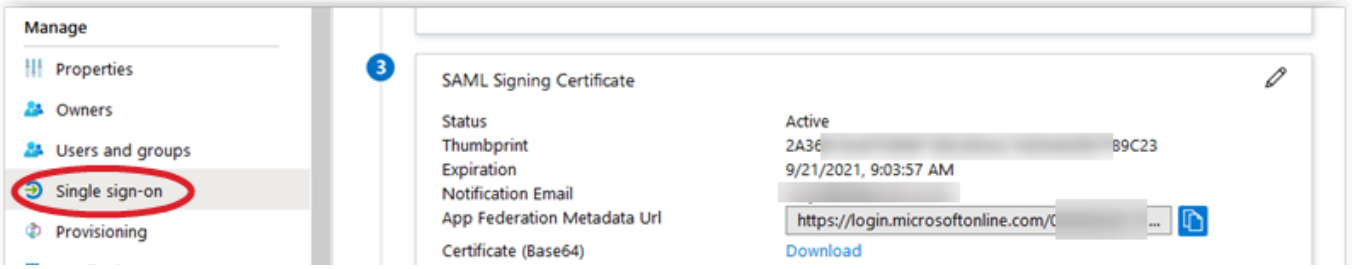
Set the following parameters:

- **Sign on url :** https://yoursubdomain.360learning.com (please check that a sub-domain has already been defined in your 360learning application settings)
- **Identifier (Entity ID)** : https://app.360learning.com
- **Reply url (ACS URL)** : the reply URL (ACS URL) that you can find in the metadata URL that the solution architect sent to you



→ After these have been entered, click **Next** to proceed to the next screen

→ Download the **certificate** (base64) and copy your **App Federation Metadata URL** and save it on your disk (you will need to send it to your solution architect).



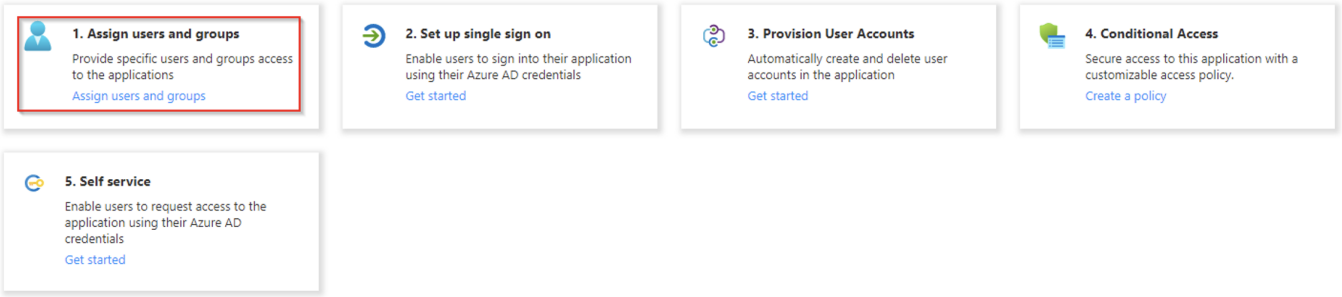
→ Set the following parameters (which may have been pre-filled by Azure AD):

- **Issuer url**: the entityID in your Federation metadata
- **Single sign-on service url**: the SingleSignOnService Location url in your Federation metadata
- **Single sign-out service url**: the SingleLogoutService Location url in your Federation metadata

Click the **Next** button and then the **Complete** to close the dialog box.

Assigning users and groups to your SAML application

As a security control, Azure AD will not issue a token allowing them to sign into 360Learning unless they have been granted access using Azure AD. Users may be granted access directly, or through a group that they are a member of.



To assign a user or group to 360Learning, click the **Assign Users** button. Select the user or group you wish to assign, and then select the **Assign button**.

Assigning a user will allow Azure AD to issue a token for the user, as well as causing a tile for 360Learning to appear in the user's Access Panel. An application tile will also appear in the Office 365 application launcher if the user is using Office 365.

Your application is now ready for testing. **Please send your metadata URL and the certificate** to your solution architect who will get back to you for the next steps.