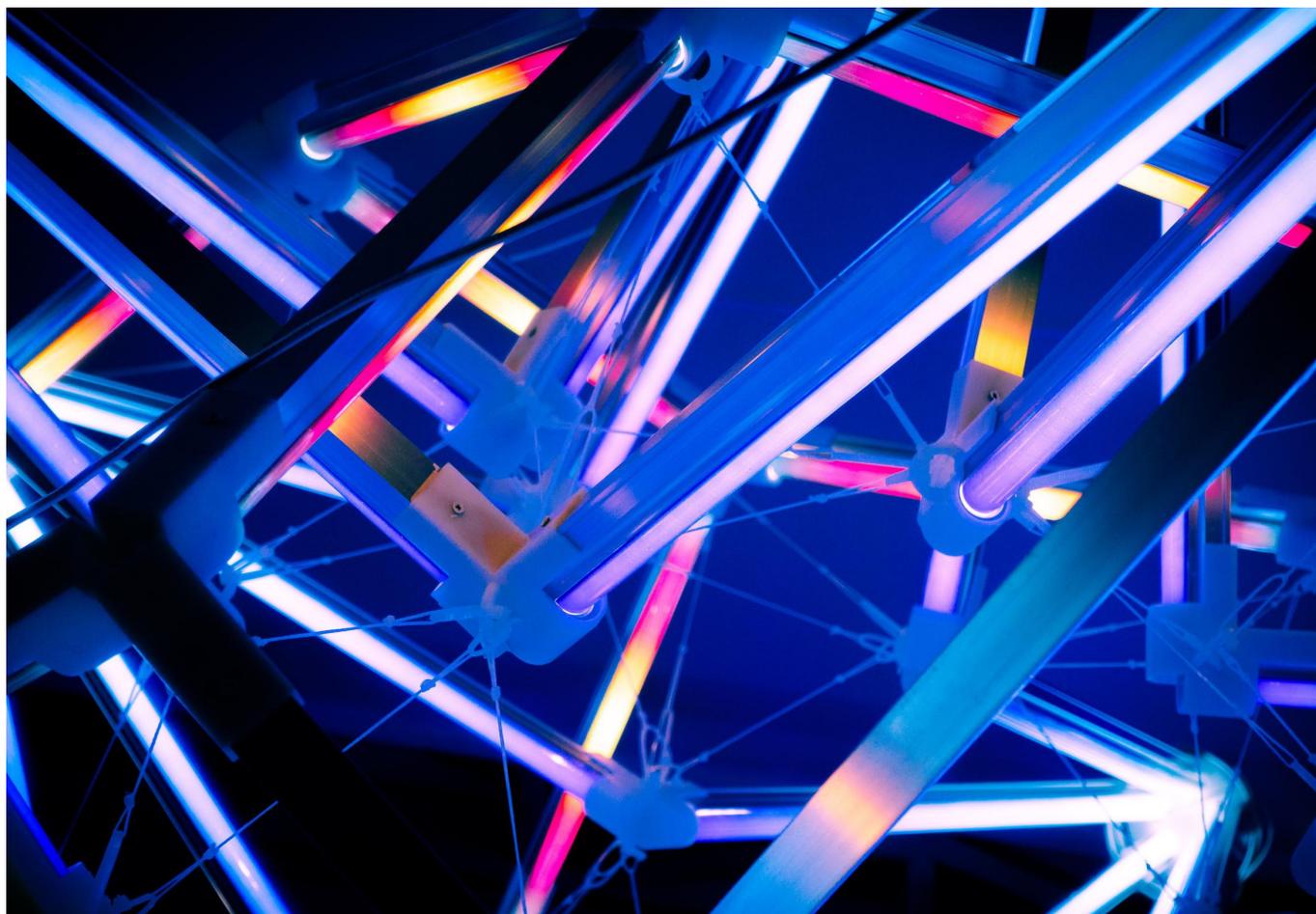


Technical Guide

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 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	4
Process	4
Local login process (credentials managed by 360Learning)	4
SAML SSO process (credentials managed by you)	5
Service provider initiated flow	6
Identity provider initiated flow	6
Configuration	6
Adding an unlisted application	6
Assigning users and groups to your SAML application	9

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.

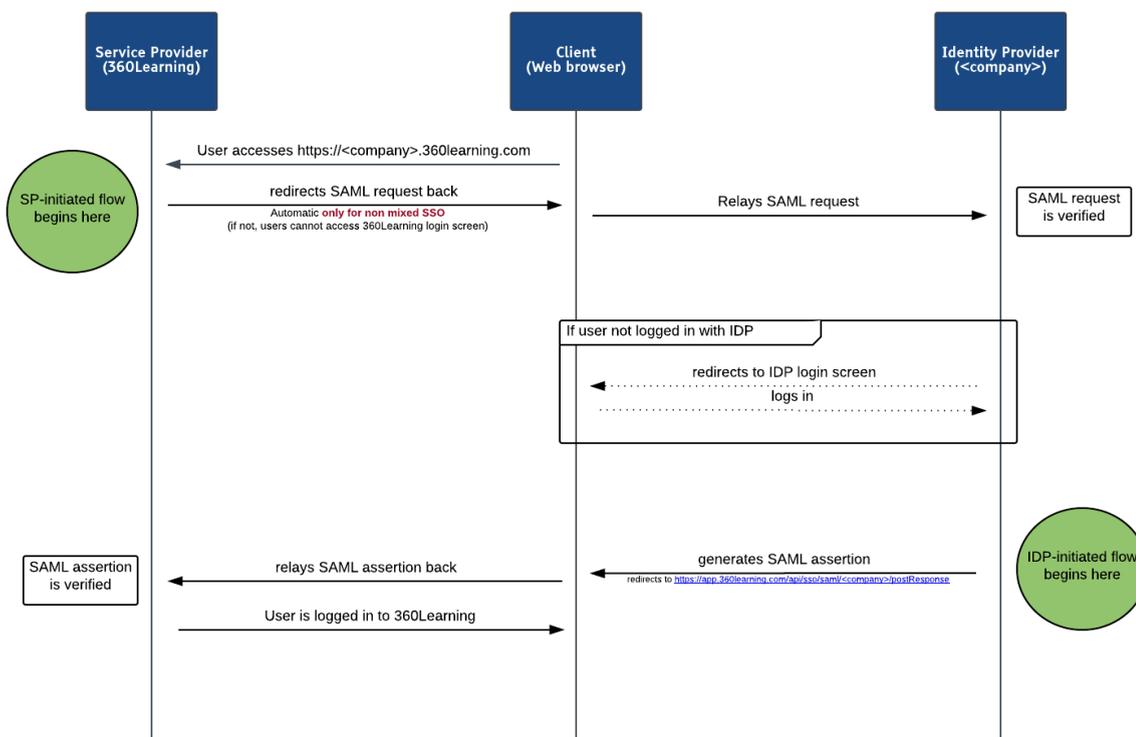
→ SAML SSO process (credentials managed by you)

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 :

SAML SSO Successful Sequence Flow



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.

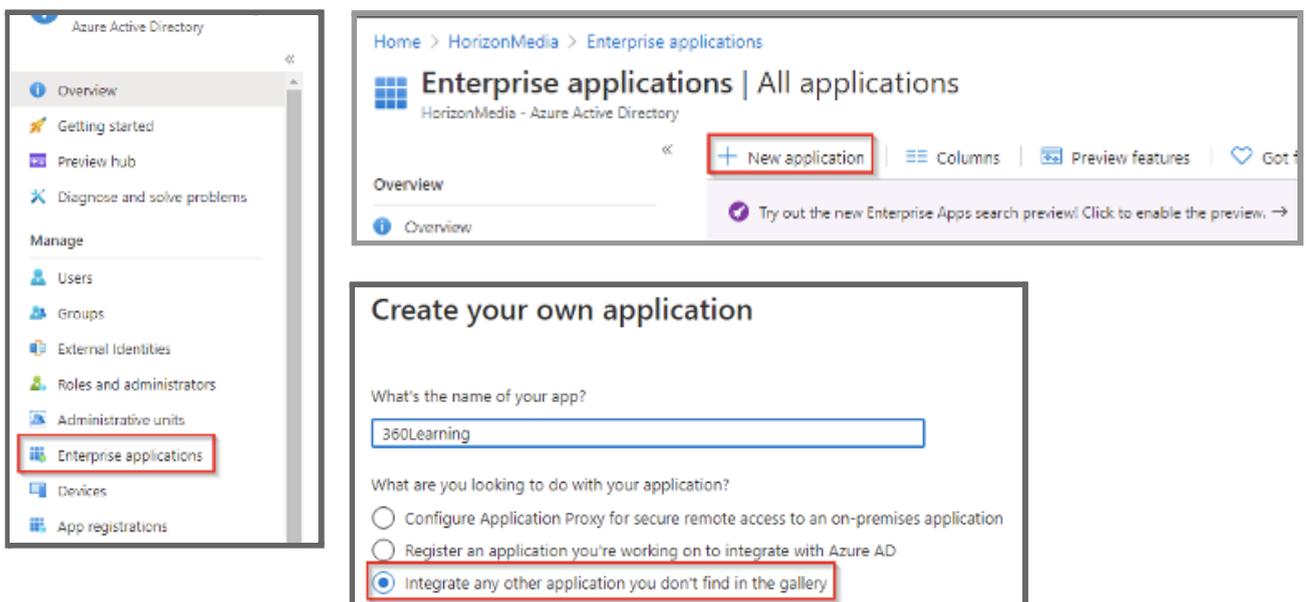
Configuration

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**.

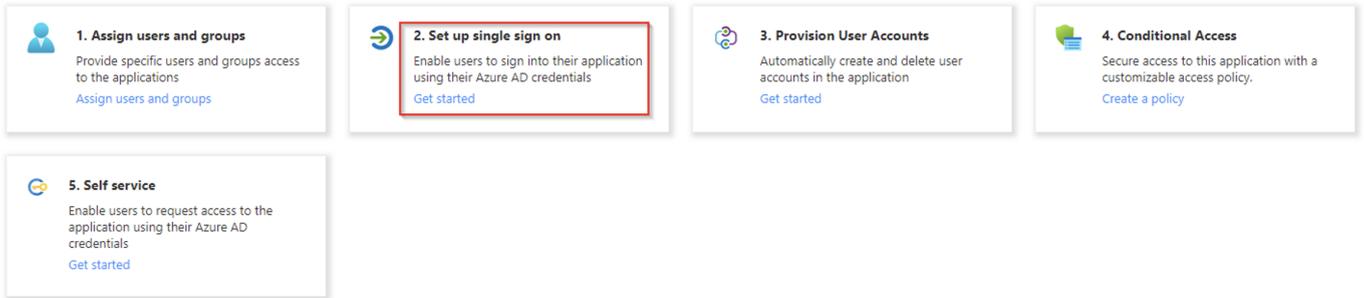


The image shows two screenshots from the Azure Active Directory portal. The left screenshot shows the navigation menu with 'Enterprise applications' highlighted. The right screenshot shows the 'Enterprise applications | All applications' page with a '+ New application' button highlighted. Below it is a 'Create your own application' form with the following fields and options:

- What's the name of your app? (Text input: 360Learning)
- What are you looking to do with your application?
 - Configure Application Proxy for secure remote access to an on-premises application
 - Register an application you're working on to integrate with Azure AD
 - Integrate any other application you don't find in the gallery

→ 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)



1. Assign users and groups
Provide specific users and groups access to the applications
[Assign users and groups](#)

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
[Get started](#)

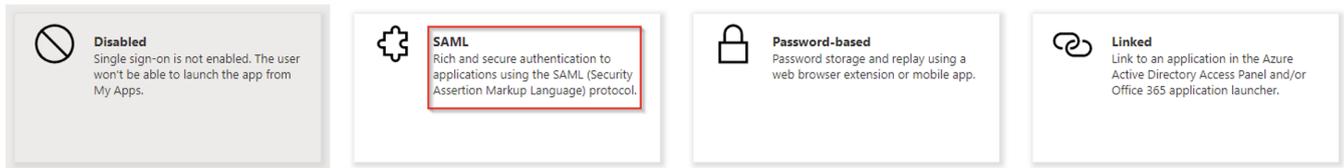
3. Provision User Accounts
Automatically create and delete user accounts in the application
[Get started](#)

4. Conditional Access
Secure access to this application with a customizable access policy.
[Create a policy](#)

5. Self service
Enable users to request access to the application using their Azure AD credentials
[Get started](#)

→ Select the SAML single sign-on method

Select a single sign-on method [Help me decide](#)



Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

→ Edit the Basic SAML Configuration

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating 360Learning.

1

✎ Edit

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

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

```

team.360learning.com/api/sso/saml/test/metadata
This XML file does not appear to have any style information associated with it. The document tree is shown below.
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="https://app.360learning.com">
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Certificate>MlICeDCCAZgCQCcvZXX/G521TANBqkqkhiG9w0BAQeFADAAmRgWpFgYDVOQDEw9h cHauMzYwbW9vYy5jb20wHhcNMTYwMjAyMTE0OTUzWjc0MTE0OTUzWjAa MRgwFgYDVOQDEw9h
DwAwgEKAoIBAQQgPh7b4TVVfOfyVVKRumV0951YAsf7C377idoyGEaa7WS0lwnQ wYrhkCoTwxPTJkwpP57Jadgn15xqxMBcwgG4p8FzgvYd5fzcoq25EPBek7tqW9 CV0IHddRoUgPHNPkhKY7H1wzLUnMMLKwUDrSI
LG5XSVt+zLwWaw2TjIqNa3T0N6GQKQo+MwVM4PpKLV6WmGwCn/JLhM6scdiMq6D U5yac4czoudrq1VbBzV1DQayvX2f0naXxIq8BMFhazIjDB2Tfso+xismjBbp L8wBv1u928K/DdZwjGca0JPDHd9xw0tw6/qvi
ggEBANoCM1Rx2qKNEW5pLxPFL0b2TVnWPhsoB1514rtheZoj2q3J+OtsCqXok05 PGzX7j25Uu6zr+ecaJ5E1UEKrcLE4TQPuHgzf2JekKHibK7PC2Bmt1LS4v0wNKGz 7kxnQgm2IzhX4s1jm8owz1VmxUnGvt4zXp:
bBpQs3MvhV5Q0y9Stu+8B3RBkA2RFXI5m0bEIS1deH0MyJWON+lud9nsdPIL7Y90 eZht409Nj4DG09+J61b8SiXh0dRhkQIamjsL6evmcTbLg2R41r4hHEFCR1aJ0m1Y C0cX1AX2ma8jvb804t0mvsxn9vw=</ds:X509Certificate>
      </ds:KeyInfo>
    </KeyDescriptor>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://app.360learning.com/api/sso/saml/test/logout/">
    </SingleLogoutService>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://app.360learning.com/api/sso/saml/test/postResponse" index="0"/>
  </SPSSODescriptor>
</EntityDescriptor>

```

- 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).

Manage

- Properties
- Owners
- Users and groups
- Single sign-on
- Provisioning

3
SAML Signing Certificate
✎

Status	Active
Thumbprint	2A36 [redacted] 89C23
Expiration	9/21/2021, 9:03:57 AM
Notification Email	[redacted]
App Federation Metadata Url	https://login.microsoftonline.com/[redacted] 📄
Certificate (Base64)	Download

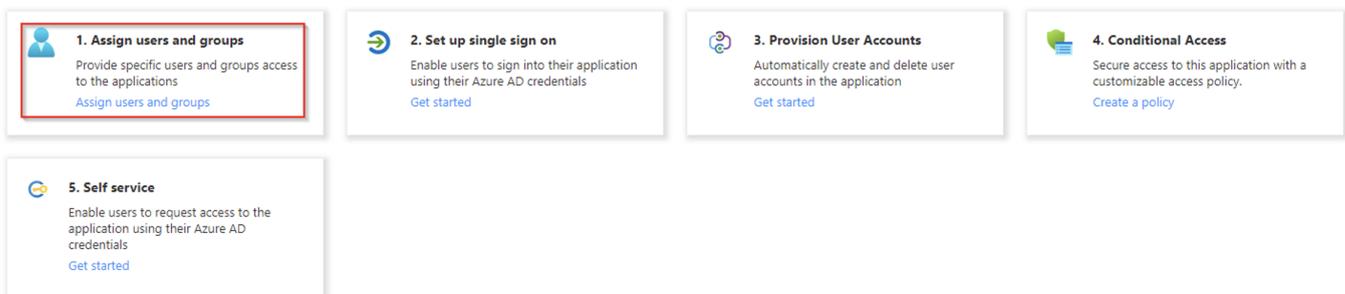
→ Set the following parameters (which may have been pre-filled by Azure AD):

- **Issuer url:** the entityID in your Federation metadata
- **Single sign-on service url:** the SingleSignInService 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.



- 1. Assign users and groups**
Provide specific users and groups access to the applications
[Assign users and groups](#)
- 2. Set up single sign on**
Enable users to sign into their application using their Azure AD credentials
[Get started](#)
- 3. Provision User Accounts**
Automatically create and delete user accounts in the application
[Get started](#)
- 4. Conditional Access**
Secure access to this application with a customizable access policy.
[Create a policy](#)
- 5. Self service**
Enable users to request access to the application using their Azure AD credentials
[Get started](#)

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.