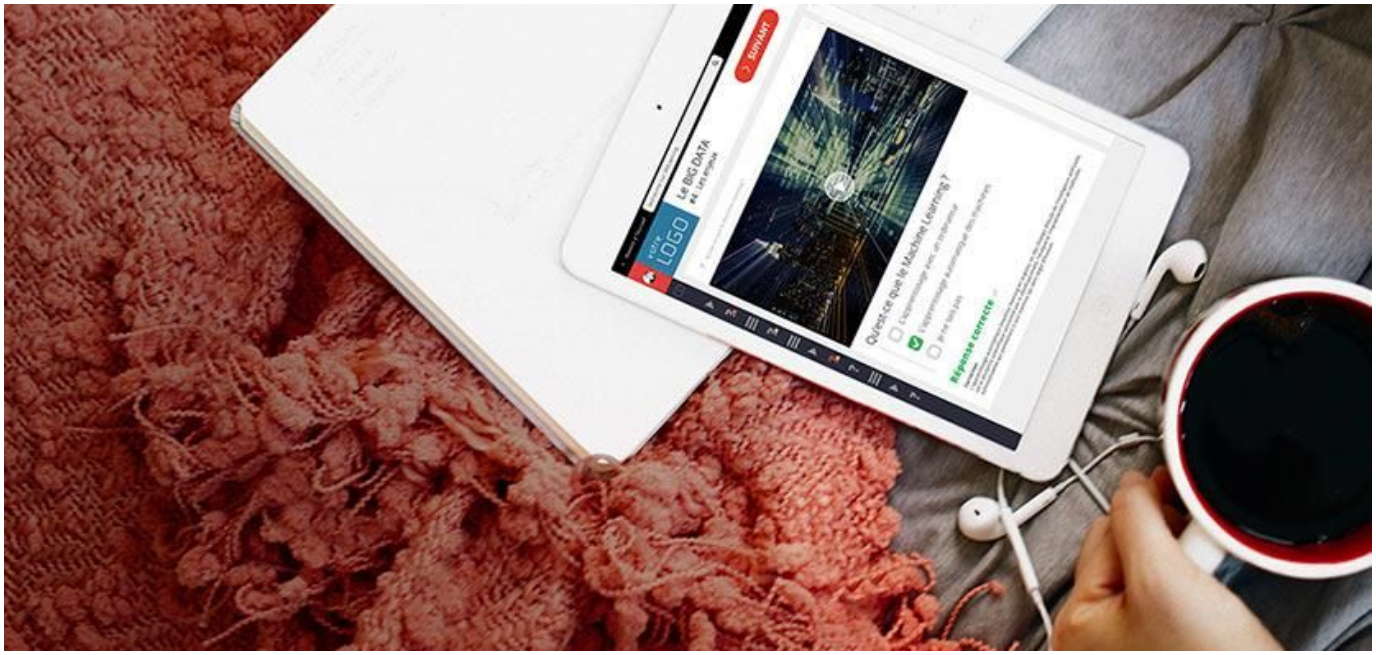
360Learning
LMS & Corporate **Universities**

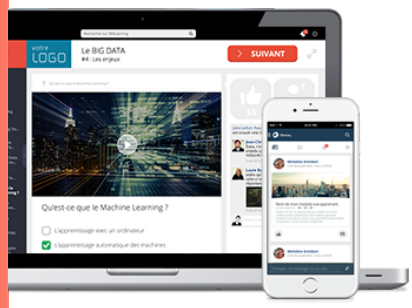


TECHNICAL GUIDE SSO SAML

At 360Learning, we don't make promises about technical solutions, we make commitments.

This technical guide is part of our Technical Documentation.

Version 1.3



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

orange
Dior
HEC PARIS
Pernod Ricard
SciencesPo EXECUTIVE EDUCATION
HAVAS MEDIA
StanleyBlack&Decker
ESSEC BUSINESS SCHOOL
DANONE
Capgemini CONSULTING.TECHNOLOGY.OUTSOURCING
BNP PARIBAS La banque d'un monde qui change

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, such as 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)

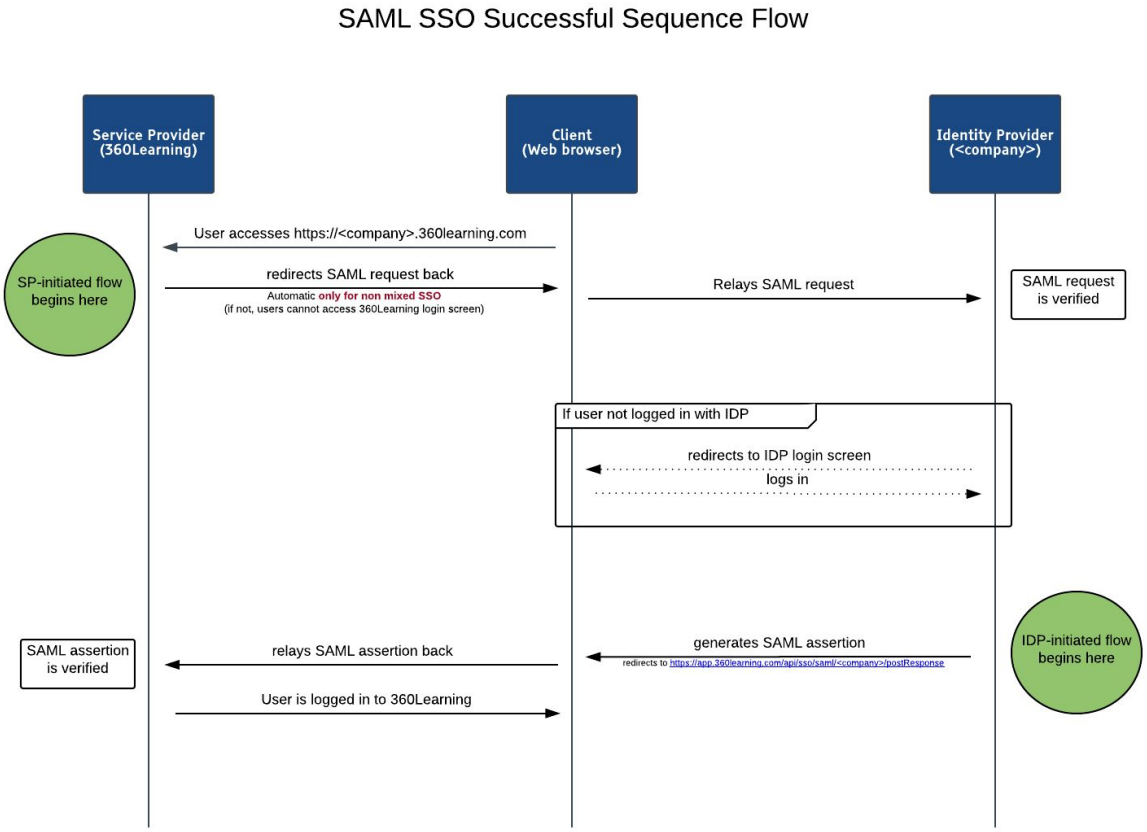
1. An unauthenticated user requests access to your 360Learning space.
2. The user is redirected to the login page of your 360Learning space where he can provide his login and password.
3. 360Learning grants him permission and redirects him to your space.

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.

Mixed or forced SSO ?

SSO come in two flavours at 360Learning. The best option depends on your situation.

Mixed SSO

In this configuration, you users have two different ways to log in :

- via the 360Learning login page (with their 360Learning credentials).
- via your login portal

Pros : you retain the ability to invite users external to your organization.
Cons : Users not used to SSO may be confused by the process and mix up their credentials.

Forced SSO

With this configuration, you users can only log in via your login portal. You are in control of ALL the logins of your users.

Pros : seamless integration
Cons : all your users must be able to log in via your corporate portal. (It will probably not be the case for freelances, consultants, clients, partners…).

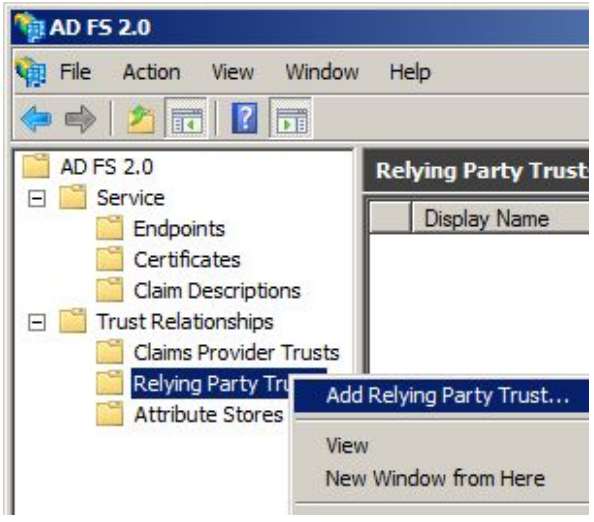
Configuration with ADFS 2.0

In this part, we focus on how to configure SSO with ADFS 2.0 (Microsoft Active Directory Federation Services).
For other tools, the configuration process should be quite similar.

To enable SSO for your 360Learning space, first contact your designated account manager: he will guide you through the entire integration process and give you a federation file required to configure your ADFS.

Relying Party Trust Configuration

- In your ADFS, select the *Add Relying Party Trust* option located under *Trust Relationships* / *Relying Party Trusts* in the left panel.



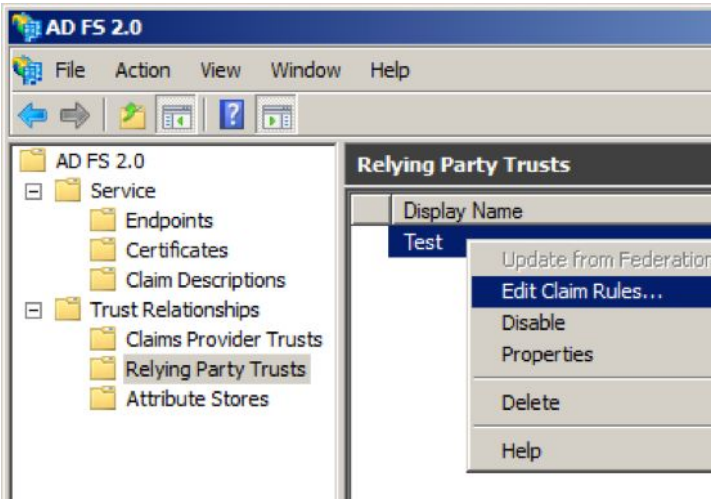
- Click on the *Start* button and import your federation file (the XML file you received from your presales engineer) using the *Import data about the relying party from a file* option.
- Click on *Next*, and provide a *Display Name* (for example 360Learning).
- Click on *Next* again and select *Permit all users to access the relying party* in the *Choose Issuance Authorization Rules* panel.
- Finish the configuration.

Certificate

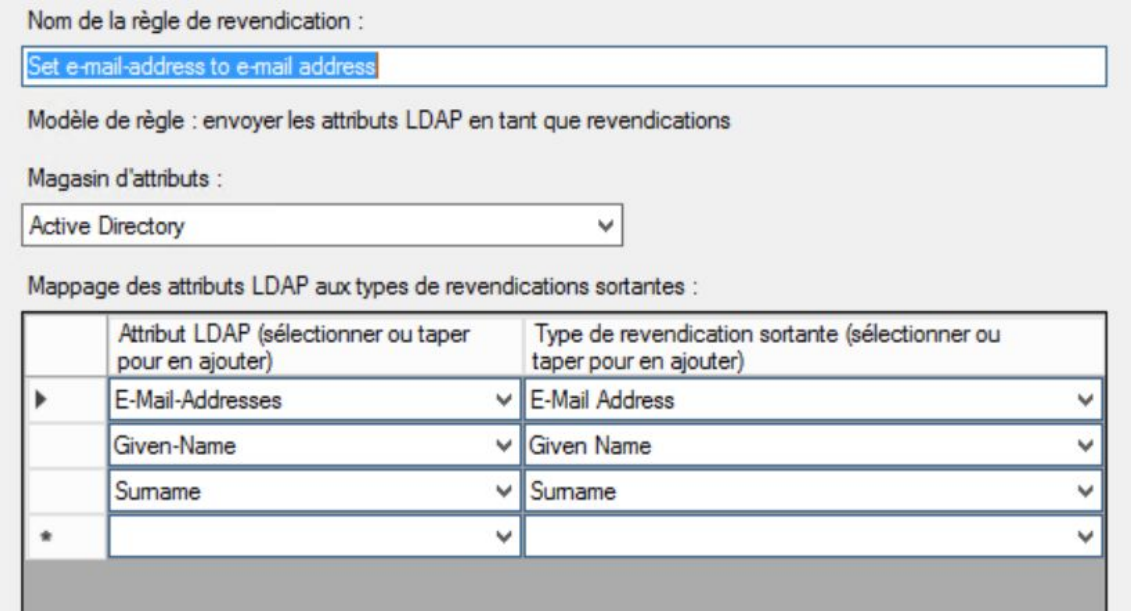
- In the left panel, under *Services* / *Certificates*, right-click on the *Token-signing* Certificate and select *View Certificate…*
- In the *Certificate* window, open the *Details* tab and click on the *Copy to File* button.
- In the *Export* popin, click on *Next* and select *DER encoded base64 X.509 (.cer) format*.
- Click on Next and select where you want to save the certificate on your disk (you will need it later).

Claim Rules Configuration

- From the left panel, go to *Trust Relationships* / *Relying Party* Trusts and right-click on the 360Learning relying trust (the one your create during the first step). Select *Edit Claim Rules…*



- *Add Rules* using the *Send LDAP Attributes as Claims* template.
- Set a name for the rule, select the *Active Directory* option and create the mapping:
  - LDAP Attribute: E-Mail-Addresses / Outgoing Claim Type: emailaddress
  - LDAP Attribute: Given-Name / Outgoing Claim Type: givenname
  - LDAP Attribute: Surname / Outgoing Claim Type: surname



- *Finish* the configuration of this rule.
- Add another rule. This time, select the *Transform an incoming Claim* option and click on *Next*.
- Set a name for the rule (Email to NameID). Set the parameters:
  - Incoming claim type: E-Mail Address
  - Outgoing claim type: Name ID
  - Outgoing name ID format: Email
- *Finish* the configuration of this rule.

Now, send the certificate, along with the URL of your login portal (for example https://fs.mycompany.com/adfs/ls) to your presales engineer!

Access control with SSO

Account provisioning with first SSO login

We will create an account on the fly on our platform for the users who successfully log in via SSO if they were previously unknown to us.

Managing specific access to 360Learning

You can configure your ADFS to restrict access to 360Learning to specific groups of your organization.