SSO and Third-Party Authentication

Theory and Practice

By **Maxi Fernandez**, Software Engineer at Appsembler

appsembler

About me

Maximiliano Fernandez

Organization: **Appsembler**

Role: **Software Engineer**

Location: **Montevideo, Uruguay**

Agenda

Single Sign On (SSO) & edX Third Party Auth (TPA)

What they are, how they're different, and why they matter

SAML Protocol

Open edX - third party auth app

SAML integration Demo

How to accomplish a SSO experience in Open edX

Single Sign On (SSO) - What is it?

SSO is a service that allows the user to use one unique set of credentials (username and password typically) to access multiple applications and typically this is the only access method.

Usually the registration isn’t public, users obtain access to an account after they became members of the organization.

Why is SSO important

- Single set of credentials for many services is crucial for large companies and educational institutions.
- Improves security since the user credentials are stored in one secure place only, not on the services.
- Maximizes user engagement and adoption since it becomes easier for the user to access different services.

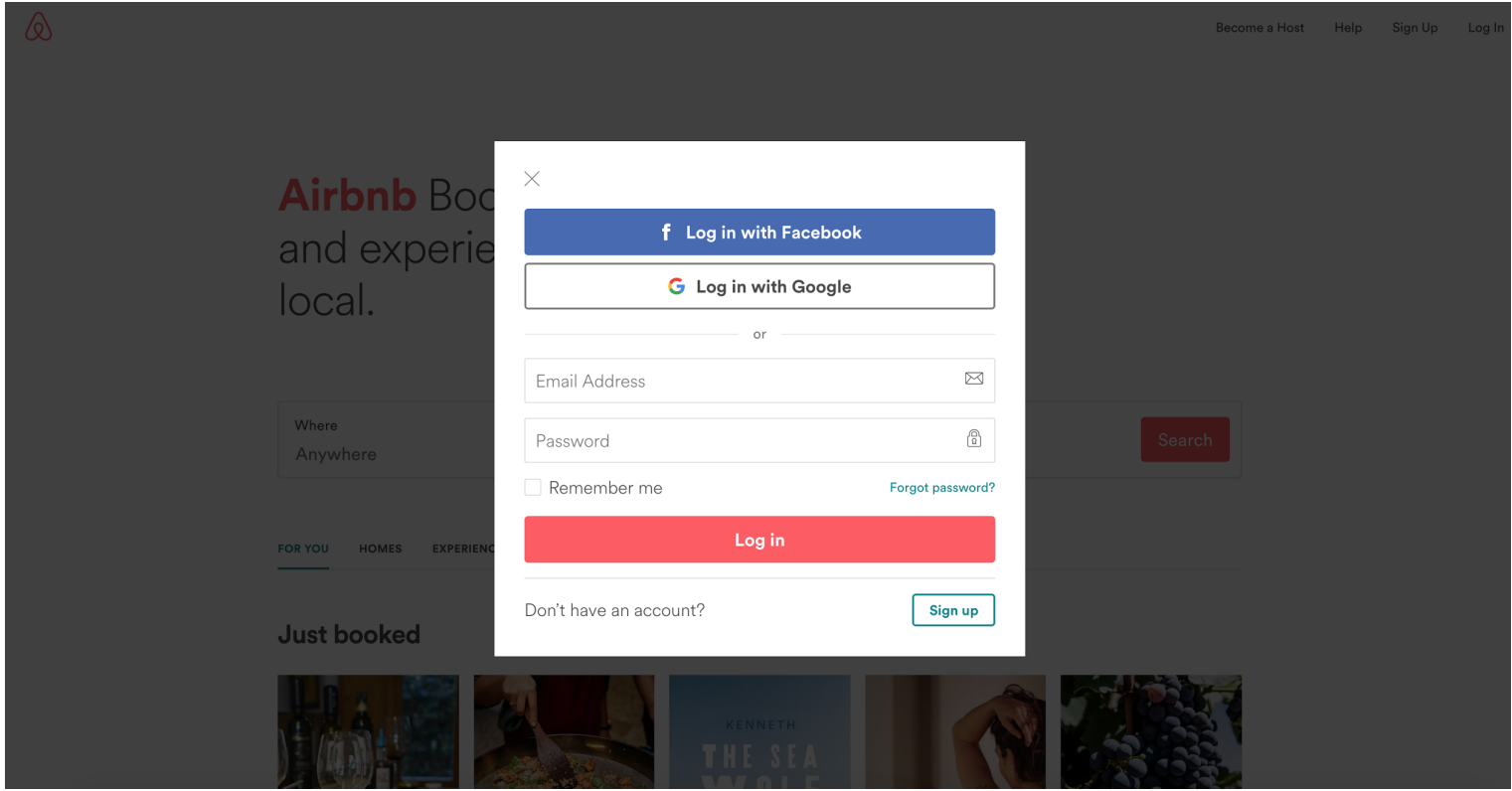
Third Party Authenti-cation (TPA)

Third Party Authentication, like SSO, allows the user to use one unique set of credentials to access multiple applications, but on the application, user also has the option to register a new account creating new credentials.

Main Aspects of TPA

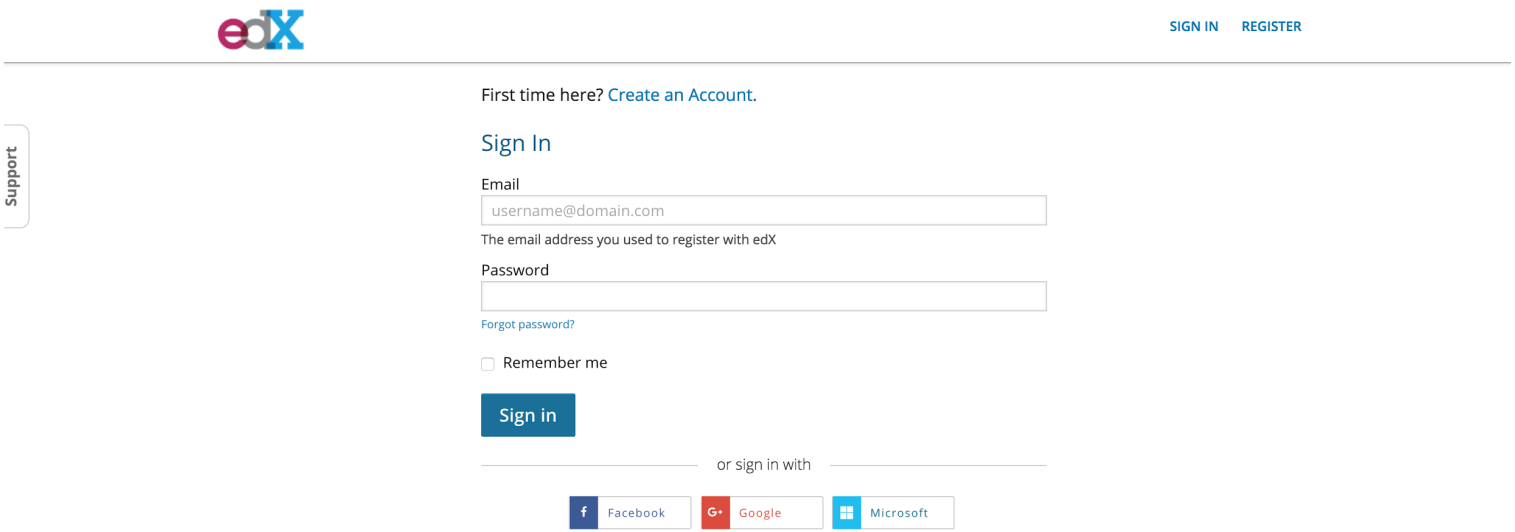
- TPA is better for sites and platforms with open registration.
- In TPA, the User can choose to use or create platform credentials or TPA.
- Usually we have more than external authentication service available.
- More accessible, better for attracting users and quick adaption.

TPA example - Airbnb



appsembler

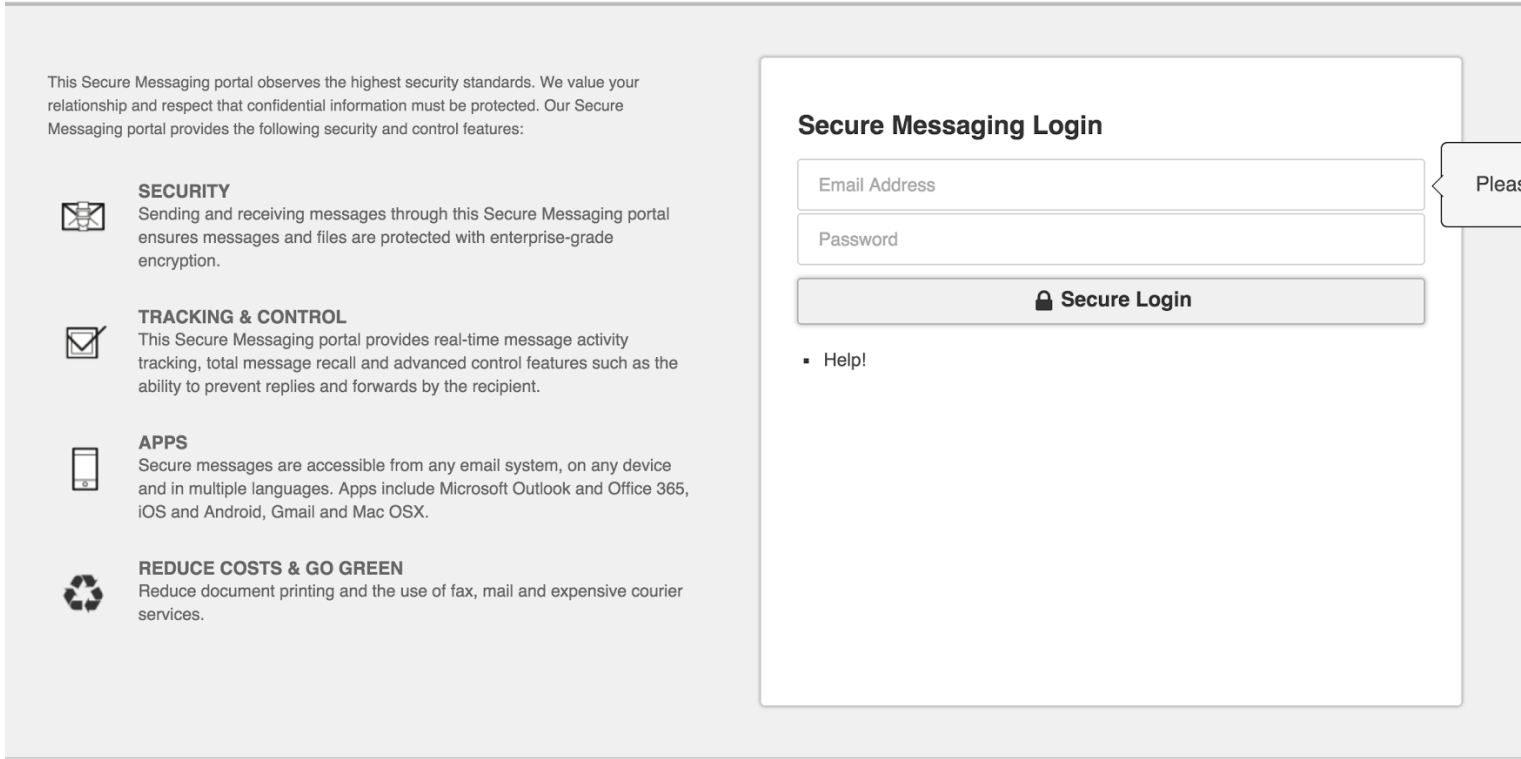
TPA example - edX



Main Aspects of SSO

- In SSO, there is only one login option available. A single identity is used for all services
- Used primarily for educational and private institutions who want a streamlined login process
- Good for systems with shared credentials such as the Google ecosystem.

SSO example - Secure Messaging App



appsembler

SSO and TPA - What do they have in common?

- They use the same protocols for authentication and encryption
- They are both used for authentication on a site with a different source of truth
- Both for authentication on websites without creating any new user credentials

Authenti-cation Protocols - Overview

Authentication protocols are communications or cryptographic protocols that are created specifically for transferring authentication data between two entities.

The two most popular Authentication Protocols in use today are OAuth and SAML

OAuth - What is it?

OAuth is an open standard authorization protocol used to authorize websites or applications to access users' information on other websites without giving them the passwords.

It is the most extended protocol, being used by Google, Twitter, Facebook, among others to provide external authentication.

Open edX uses Oauth both as an identity provider and as a service provider.

SAML - Security Assertion Markup Language

Principles

Design

Workflow

SAML - Principles

Roles:

Principal - Typically a user

IdP - Identity Provider

SP - Service Provider

Relying parties

A Service Provider and an Identity Provider became relying parties after a metadata exchange.

During the metadata exchange the most important information that is shared between the relying parties is:

- Entities IDs
- Bindings (URLs)
- Certificates

SAML - Design

Extensible Markup Language (XML)

XML Schema (XSD)

XML Signature

XML Encryption

Hypertext Transfer Protocol (HTTP)

SAML - Design

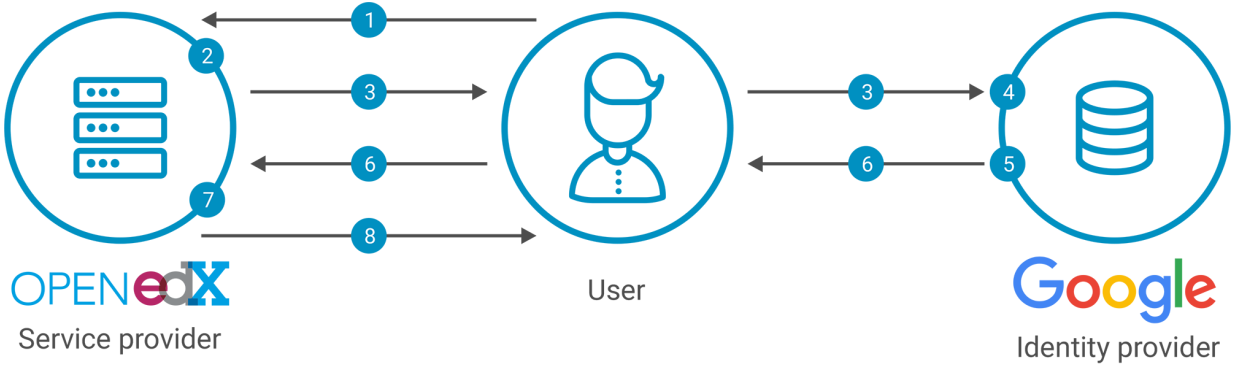
SAML is based on:

Assertions

Bindings

Profiles

How does SAML work?



1. User tries to reach Open edX
2. Open edX generates SAML request
3. Open edX redirects browser to SSO URL
4. Google parses SAML request, authenticates user
5. Google generates SAML response
6. Google returns encoded SAML response to browser, who in turn sends it to Access Control Service
7. Access Control Service verifies SAML response
8. User is logged in to Open edX

Popular hosted SAML providers

Shibboleth

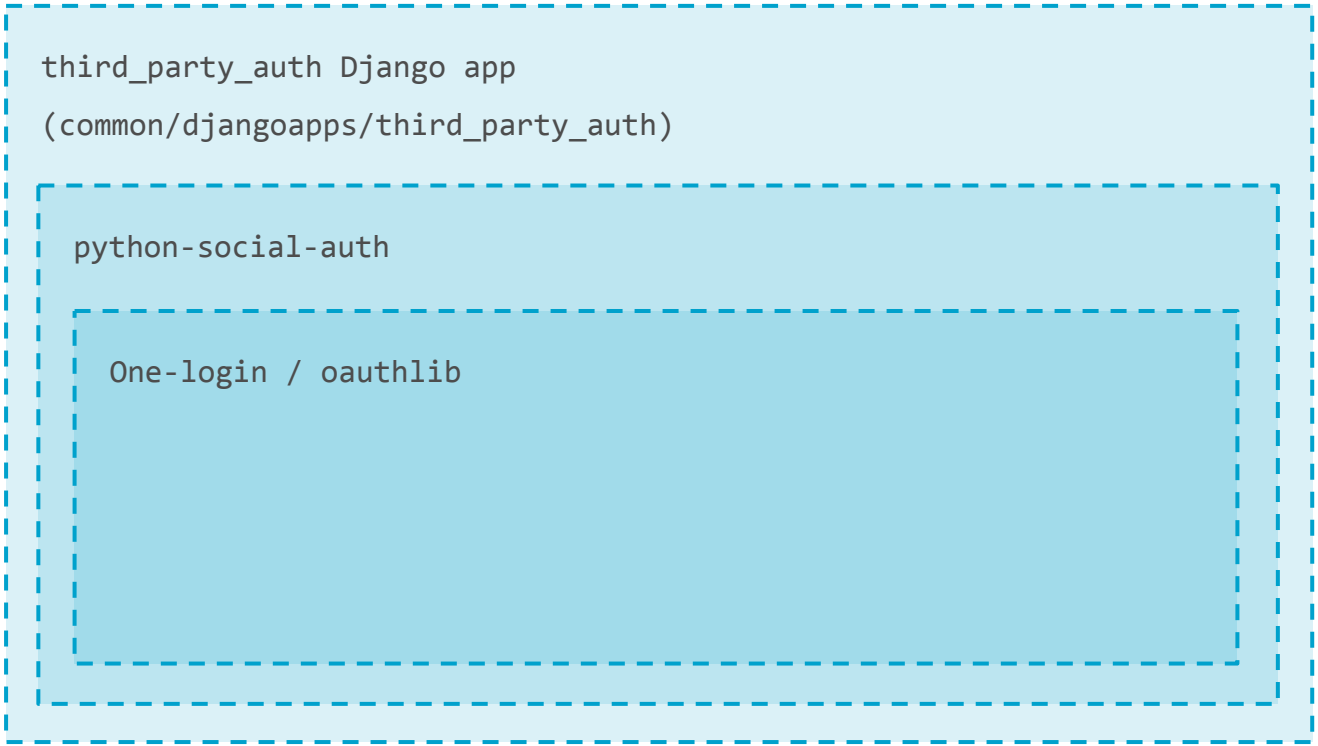
Open Source

Hard to deploy but very flexible

Doesn’t provide User interface for configuration.

Can connect to authentication control services such as LDAP, Kerberos, JAAS

Open edX Third Party auth



Integrating Open edX with SAML Identity Provider

SAML Attributes

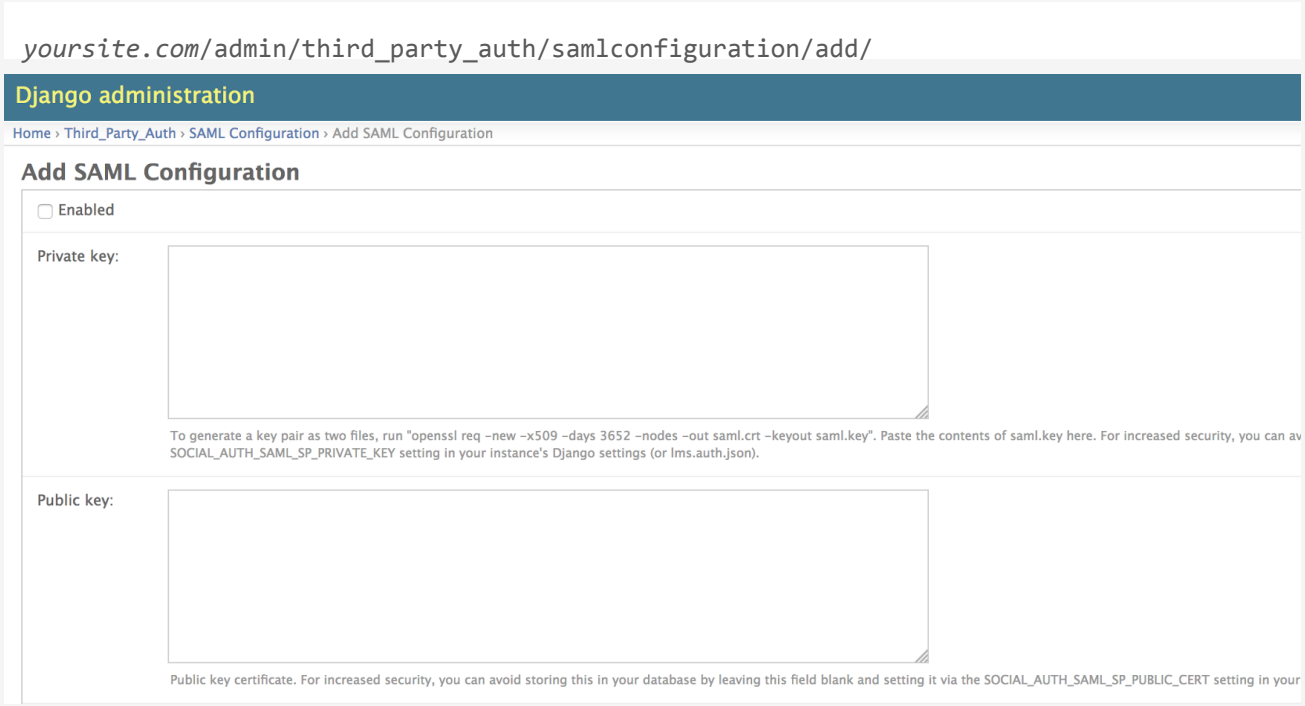
```
<saml:AttributeStatement>
  <saml:Attribute Name="uid" NameFormat="urn:oasis:names:tc:SAML:
2.0:attrname-format:basic">
    <saml:AttributeValue xsi:type="xs:string">test</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="mail" NameFormat="urn:oasis:names:tc:SAML:
2.0:attrname-format:basic">
    <saml:AttributeValue xsi:type="xs:string">test@example.com</
saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="eduPersonAffiliation"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml:AttributeValue xsi:type="xs:string">users</saml:AttributeValue>
    <saml:AttributeValue xsi:type="xs:string">examplerole1</
saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
```

Enabling Third Party Auth

```
/edx/app/edxapp/lms.env.json

"FEATURES" : {

    ...

    "ENABLE_COMBINED_LOGIN_REGISTRATION": true,

    "ENABLE_THIRD_PARTY_AUTH": true

}

# Restart edxapp: services

# Ensure that third_party_auth.saml.SAMLAuthBackend is enabled in
THIRD_PARTY_AUTH_BACKENDS
```

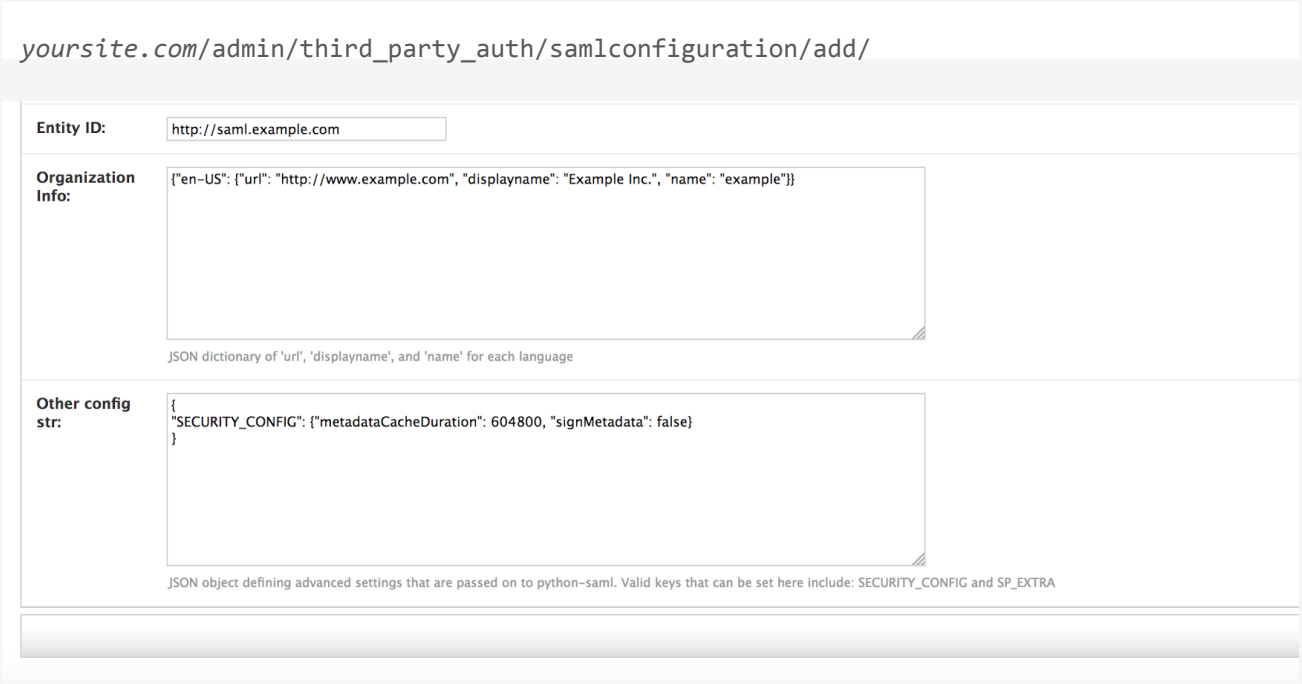
Configuring Open edX as SAML Service Provider

Part 2



appsembler

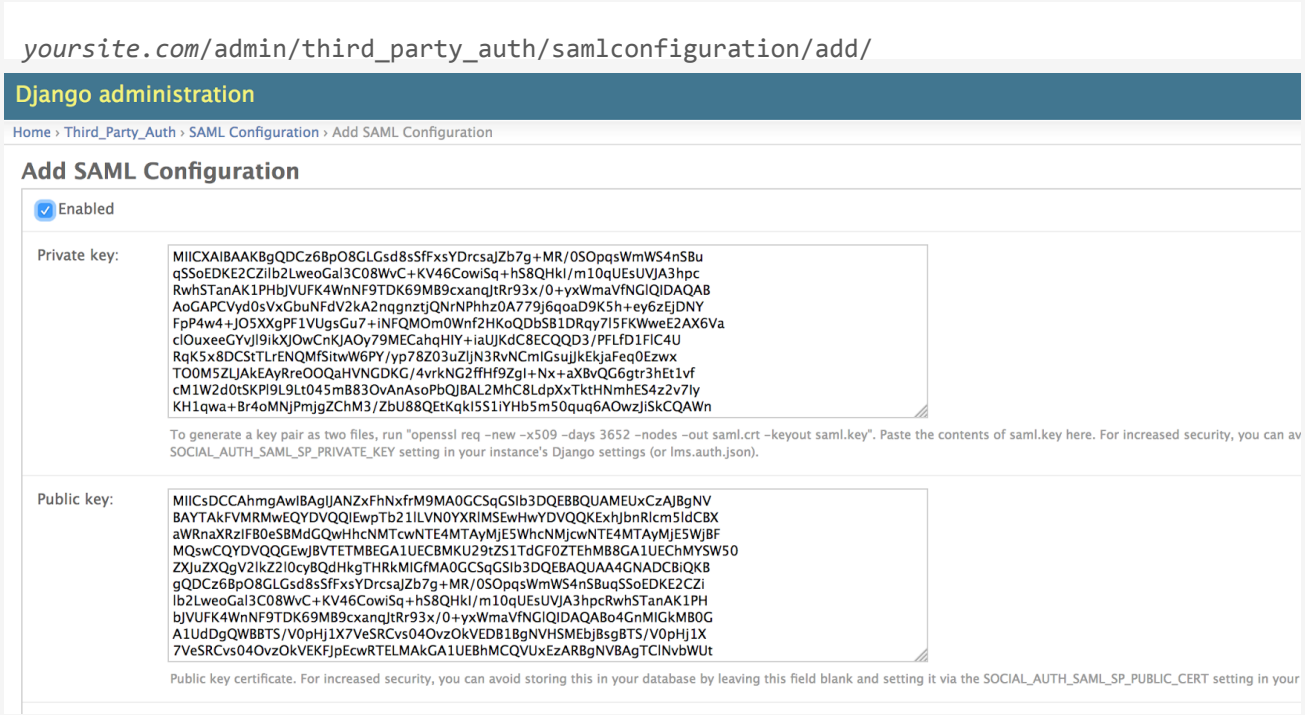
Configuring Open edX as SAML Service Provider



Generate Public and Private Keys

```
$ openssl req -new -x509 -days 3652 -nodes -out sso-workshop-saml.crt
-keyout sso-workshop-saml.key

$ cat sso-workshop-saml.crt
-----BEGIN CERTIFICATE-----
MIICsDCCAhmgAwIBAgIJANZxFhNxfrM9MA0GCSqGSIb3DQEBBQUAMEUxCzAJBgNV
. . .
tA0pas1P4pNGnY99obhXOl6KAk0=
-----END CERTIFICATE-----

$ cat sso-workshop-saml.key
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDCz6BpO8GLGsd8sSfFxsYDrcsaJZb7g+MR/0SOpqsWmWS4nSBu
. . .
kU7OyjUJms+YhDsP/rmBSsVqoGAf9Uuo4lLzNpiHHLo=
-----END RSA PRIVATE KEY-----
```

Service Provider Configura-tion Finished



appsembler

Service Provider Configuration Finished

Part 2

yoursite.com/admin/third_party_auth/samlconfiguration/add/

Entity ID: http://saml.sso-workshop.appsembler.cc

Organization Info:

```
{
    "en-US": {
        "url": "http://www.sso-workshop.appsembler.com",
        "displayname": "SSO Workshop",
        "name": "sso workshop"
    }
}
```

JSON dictionary of 'url', 'displayname', and 'name' for each language

Other config str:

```
{
    "SECURITY_CONFIG": {
        "signMetadata": false,
        "metadataCacheDuration": ""
    }
}
```

JSON object defining advanced settings that are passed on to python-saml. Valid keys that can be set here include: SECURITY_CONFIG and SP_EXTRA

SP Metadata

yoursite.com/auth/saml/metadata.xml

```
<md:EntityDescriptor entityID="http://saml.sso-workshop.appsembler.com"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>
            MIICsDCCAhmgAwIBAgIJANZxFhNxfrM9MA0GCSqGSIb...
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:KeyDescriptor use="encryption" xmlns:ds="http://www.w3.org/2000/09/
xmldsig#">
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>
            MIICsDCCAhmgAwIBAgIJANZxFhNxf...
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
```

SP Metadata

yoursite.com/auth/saml/metadata.xml

```
 <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="http://sso-workshop.ngrok.io/auth/complete/tpa-saml/" index="1"/>
  </md:SPSSODescriptor>
  <md:Organization>
    <md:OrganizationName xml:lang="en-US">sso workshop</md:OrganizationName>
    <md:OrganizationDisplayName xml:lang="en-US">SSO Workshop</
md:OrganizationDisplayName>
    <md:OrganizationURL xml:lang="en-US">http://www.sso-workshop.appsembler.com</
md:OrganizationURL>
  </md:Organization>
  <md:ContactPerson contactType="technical">
      <md:GivenName>SSO Workshop Support</md:GivenName>
      <md:EmailAddress>technical@example.com</md:EmailAddress>
  </md:ContactPerson>
  <md:ContactPerson contactType="support">
      <md:GivenName>SSO Workshop Support</md:GivenName>
      <md:EmailAddress>technical@example.com</md:EmailAddress>
  </md:ContactPerson>
</md:EntityDescriptor>
```

Identity Provider Configura-tion

yoursite.com/admin/third_party_auth/samlproviderconfig/add/

Django administration

Home › Third_Party_Auth › Provider Configuration (SAML IdPs) › Add Provider Configuration (SAML IdP)

Add Provider Configuration (SAML IdP)

Enabled

Icon class: fa-sign-in

The Font Awesome (or custom) icon class to use on the login button for this provider. Examples: fa-google-plus, fa-facebook, fa-linkedin, fa-sign-in, fa-university

Icon image: Browse... No file selected.

If there is no Font Awesome icon available for this provider, upload a custom image. SVG images are recommended as they can scale to any size.

Name:

Name of this provider (shown to users)

Secondary

Secondary providers are displayed less prominently, in a separate list of "Institution" login providers.

Skip registration form

If this option is enabled, users will not be asked to confirm their details (name, email, etc.) during the registration process. Only select this option for trusted providers that are known to provide accurate user info

Skip email verification

If this option is selected, users will not be required to confirm their email, and their account will be activated immediately upon registration.

Backend name: tpa-saml

Idp slug:

A short string uniquely identifying this provider. Cannot contain spaces and should be a usable as a CSS class. Examples: "ubc", "mit-staging"

Entity ID:

Example: https://idp.testshib.org/idp/shibboleth

Metadata source:

URL to this provider's XML metadata. Should be an HTTPS URL. Example: https://www.testshib.org/metadata/testshib-providers.xml

Identity Provider Configura-tion

Part 2

yoursite.com/admin/third_party_auth/samlproviderconfig/add/

User ID Attribute:

URN of the SAML attribute that we can use as a unique, persistent user ID. Leave blank for default.

Full Name Attribute:

URN of SAML attribute containing the user's full name. Leave blank for default.

First Name Attribute:

URN of SAML attribute containing the user's first name. Leave blank for default.

Last Name Attribute:

URN of SAML attribute containing the user's last name. Leave blank for default.

Username Hint Attribute:

URN of SAML attribute to use as a suggested username for this user. Leave blank for default.

Email Attribute:

URN of SAML attribute containing the user's email address[es]. Leave blank for default.

Advanced settings:

For advanced use cases, enter a JSON object with addtional configuration. The tpa-saml backend supports only {"requiredEntitlements": ["urn:..."]} which can be used to requir

Identity Provider Configura-tion Finished

yoursite.com/admin/third_party_auth/samlproviderconfig/add/

Django administration

Home › Third_Party_Auth › Provider Configuration (SAML IdPs) › Add Provider Configuration (SAML IdP)

Add Provider Configuration (SAML IdP)

Enabled

Icon class: fa-sign-in
The Font Awesome (or custom) icon class to use on the login button for this provider. Examples: fa-google-plus, fa-facebook, fa-linkedin, fa-sign-in, fa-university

Icon image: Browse... No file selected.
If there is no Font Awesome icon available for this provider, upload a custom image. SVG images are recommended as they can scale to any size.

Name: Onelogin
Name of this provider (shown to users)

Secondary
Secondary providers are displayed less prominently, in a separate list of "Institution" login providers.

Skip registration form
If this option is enabled, users will not be asked to confirm their details (name, email, etc.) during the registration process. Only select this option for trusted providers that are known to provide accurate user infor

Skip email verification
If this option is selected, users will not be required to confirm their email, and their account will be activated immediately upon registration.

Backend name: tpa-saml

Idp slug: one-login
A short string uniquely identifying this provider. Cannot contain spaces and should be a usable as a CSS class. Examples: "ubc", "mit-staging"

Entity ID: https://app.onelogin.com/saml/metadat
Example: https://idp.testshib.org/idp/shibboleth

Metadata source: https://app.onelogin.com/saml/metadat
URL to this provider's XML metadata. Should be an HTTPS URL. Example: https://www.testshib.org/metadata/testshib-providers.xml

Identity Provider Configura-tion Done

Part 2

yoursite.com/admin/third_party_auth/samlproviderconfig/add/

Metadata source: https://app.onelogin.com/saml/metadat

URL to this provider's XML metadata. Should be an HTTPS URL. Example: https://www.testshib.org/metadata/testshib-providers.xml

User ID Attribute: User.email

URN of the SAML attribute that we can use as a unique, persistent user ID. Leave blank for default.

Full Name Attribute: User.FirstName

URN of SAML attribute containing the user's full name. Leave blank for default.

First Name Attribute: User.FirstName

URN of SAML attribute containing the user's first name. Leave blank for default.

Last Name Attribute: User.FirstName

URN of SAML attribute containing the user's last name. Leave blank for default.

Username Hint Attribute: User.Username

URN of SAML attribute to use as a suggested username for this user. Leave blank for default.

Email Attribute: User.email

URN of SAML attribute containing the user's email address[es]. Leave blank for default.

Advanced settings: {}

For advanced use cases, enter a JSON object with addtional configuration. The tpa-saml backend supports only {"requiredEntitlements": ["urn:..."]} which can be used to require the presence of a s

SAML Pull Metadata

```
## In case we make a change to configuration but the SAML Metadata
## doesn’t update automatically as it should, we can do the following
## to trigger the process manually.

$ sudo su edxapp -s /bin/bash
$ source /edx/app/edxapp/edxapp_env
$ cd ~/edx-platform
$ python manage.py lms --settings=<devstack/aws> saml --pull
```

Tools

Onelogin - https://www.onelogin.com

Firefox SAML trace - https://addons.mozilla.org/es/firefox/addon/saml-tracer/

Theming changes for SSO

```
<%
import third_party_auth
from third_party_auth import pipeline

try:
   tpa_idp = third_party_auth.provider.Registry.accepting_logins()[0]
   custom_login_url = pipeline.get_login_url(tpa_idp.provider_id,
pipeline.AUTH_ENTRY_REGISTER, redirect_url=request.path)
except:
    custom_login_url = '/login'

try:
    tpa_idp = third_party_auth.provider.Registry.accepting_logins()[0]
    custom_logout_url = pipeline.get_logout_url(tpa_idp.provider_id,
pipeline.AUTH_ENTRY_REGISTER)
except:
    custom_logout_url = '/logout'
%>
```

Nginx rules for SSO

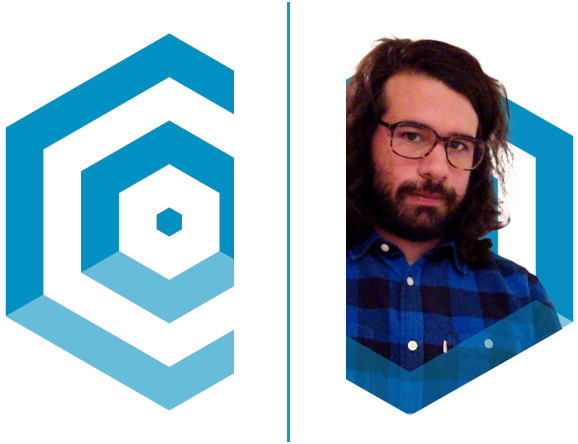
```
server {
  ...
  location = /login {
    try_files $uri $SSO_restrictions_proxy_loc;
  }

  location = /register {
    try_files $uri $SSO_restrictions_proxy_loc;
  }

  location = /account/settings {
    return 302 https://appsembler.onelogin.com/profile;
  }

  location @redirect_to_idp_login {
    return 302 http://sso-workshop.appsembler.com/auth/login/tpa-saml/?
auth_entry=register&next=%2F&idp=one-login;
  }
  ...
}
```

Nginx rules for SSO

```
map $http_referer-$uri?$query_string $SSO_restrictions_proxy_loc {
  # default to redirect
  # some referers
  default @redirect_to_idp_login;
  ~^https\:\/\/appsembler\.onelogin\.com\/trust\/saml2\/http-redirect\/sso(.*)
@proxy_to_lms_app;
}
```

Recap - Key Takeaways

- Basic concepts about SAML protocol
- How to integrate Open edX with a SAML Identity Provider
- How to customize Open edX to get a SSO experience



Thank you!