



# Mise en place SSO via Entra (Leexi)

## Mise en place SSO via Entra (Leexi)

|  |   |
|--|---|
| Procédure de mise en place SSO via Entra (Leexi) ..... | 1 |
| Création de l'application Entra.....                   | 1 |
| Configuration de l'application Entra .....             | 2 |
| Téléchargement du fichier Metadata XML lié .....       | 3 |
| Assigner les utilisateurs à l'application Entra.....   | 4 |
| Forcer le SSO (optionnel) .....                        | 5 |

## Création de l'application Entra

Aller sur le portail entra : [entra.microsoft.com](https://entra.microsoft.com).

Pour ajouter une nouvelle application, aller dans **Applications**, puis **Nouvelle Application**

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a sidebar with links like Favorites, Entra ID, Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps (which is highlighted with a red box), and App registrations. The main area is titled 'Enterprise applications | All applications' and shows a list of applications. At the top right, there's a button labeled '+ New application'. A tooltip message says 'Agent ID (Preview) has been moved to the'. Below the list, it says 'View, filter, and search applications in your org' and 'The list of applications that are maintained by'. There's also a search bar and a note saying '160 applications found'.

Vous avez le choix de créer votre propre application ou d'en chercher une sur le store Entra.  
Nous allons créer notre propre application :

The screenshot shows the Microsoft Entra App Gallery. On the left, there's a sidebar with 'Home > Microsoft Entra > App registrations > Register an application > Enterprise applications | All applications > Browse Microsoft Entra App Gallery'. The main area is titled 'Create your own application'. It has a 'Search application' bar and several filters: Single Sign-on : All, User Account Management : All, Categories : All, and Risk Score. Below these, there's a section for 'Cloud platforms' with links for Amazon Web Services (AWS), Google Cloud Platform, and Oracle. To the right, there's a section titled 'What are you looking to do with your application?' with three radio button options: 'Configure Application Proxy for secure remote access to an', 'Register an application to integrate with Microsoft Entra ID (', and 'Integrate any other application you don't find in the gallery ('. A 'Got feedback?' link is also present.

Nous pouvons ensuite ajouter le nom que nous souhaitons donner à cette application (ici PCM – Leexi SSO).



## Configuration de l'application Entra

Nous allons maintenant nous rendre dans la catégorie **Single Sign-on (SSO)** puis cliquer sur **SAML** et ensuite sur **Configuration** (dans le coin en haut à droite de Basic SAML Configuration)

The screenshot shows the Microsoft Entra app registration interface. On the left, there's a sidebar with navigation links like Home, Microsoft Entra, App registrations, Register an application, Enterprise applications, Overview, Deployment Plan, Diagnose and solve problems, Manage, Properties, Owners, Roles and administrators, Users and groups, Single sign-on (which is highlighted with a red box), Provisioning, Application proxy, Self-service, Custom security attributes, Security, Conditional Access, Permissions, and Token encryption. The main content area is titled 'Basic SAML Configuration'. It includes sections for 'Identifier (Entity ID)', 'Reply URL (Assertion Consumer Service URL)', 'Sign on URL', 'Relay State (Optional)', 'Logout Url (Optional)', 'Attributes & Claims' (with a note to fill out required fields), 'Sign on URL (Optional)', 'Relay State (Optional)', and a 'Save' button at the top.

-Cliquer ensuite sur **Add Identifier**, un champ va apparaître, et nous pourrons y coller la valeur voulu (ici, nous pouvons la récupérer via : <https://app.leexi.ai/en/settings/security>)

**ID d'identité (Entity ID)**

<https://app.leexi.ai/>

Faisons de même pour **Add reply URL** (ici la valeur dont nous avons besoin est <https://api.leexi.ai/users/sso/consume>)

**URL de réponse (ACS)**

<https://api.leexi.ai/users/sso/consume>

-Les autres valeurs peuvent rester sur les valeurs par défaut. Cliquer sur **Save** en haut de la page.



## Téléchargement du fichier Metadata XML lié

Dans l'application, descendre jusqu'à la catégorie **SAML Certificates**

Ensuite cliquer sur le lien pour download le fichier **Federation Metadata XML**

SAML Certificates

Token signing certificate

Status: Active

Thumbprint: [REDACTED]

Expiration: 1/15/2029, 11:17:10 AM

Notification Email: [REDACTED]

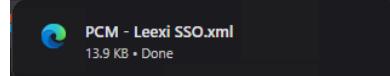
App Federation Metadata Url: https://login.microsoftonline.com/[REDACTED]

Certificate (Base64) [Download](#)

Certificate (Raw) [Download](#)

Federation Metadata XML [Download](#)

Votre navigateur va maintenant télécharger un fichier .xml



*Il vous faut maintenant le déposer à l'endroit prévu dans votre application (ici sur Leexi, dans le champ correspondant)*

Certificat de metadata (XML)

↑

Type de fichiers acceptés: XML



## Assigner les utilisateurs à l'application Entra

Il va maintenant nous falloir assigner des utilisateurs dans l'application Entra que nous avons créée, afin qu'ils puissent utiliser le SSO.

Retourner dans l'application Entra, puis cliquer sur **Users and Groups**, puis Add **User/Group**

The screenshot shows the 'PCM - Leexi SSO | Users and groups' page. On the left, there's a sidebar with options like Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Roles and administrators), and the highlighted 'Users and groups'. A red box highlights the 'Users and groups' link. At the top right, there are buttons for '+ Add user/group', Edit assignment, Remove assignment, Update credential, Refresh, and Manage view. A note says: 'The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.' Below that, it says: 'Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application re...' A search bar says 'First 200 shown, search all users & groups'. A table header includes 'Display name' and 'Object type'. A message at the bottom says 'No application assignments found'.

Cliquer ensuite sur **None Selected**, puis ajouter les utilisateurs/groupes voulus

The screenshot shows the 'Add Assignment' page for the 'PCM SA' role. On the left, under 'Users and groups', the 'None Selected' button is highlighted with a red box. On the right, the 'Users and groups' page is shown with a search bar and a table of results. The table has columns for Name, Type, and Details. It lists three items: a group named '2' (Type: Group), a user named 'AR' (Type: User), and a group named '6' (Type: Group). Each item has a checkbox next to its name.



## Forcer le SSO (optionnel)

Désormais, si toutes les étapes ont été respectées, les utilisateurs qui se connectent sur l'application peuvent toujours s'identifier avec leur email/password comme avant, mais peuvent aussi s'identifier via le SSO que nous venons de configurer (pour les utilisateurs ajoutés dans l'application Entra).

Ici, nous voulons forcer la connexion via SSO, nous pouvons donc directement le faire depuis l'application Leexi :

### Paramètres SSO

Connexion avec le SSO obligatoire



*Attention, vous ne pouvez plus désactiver cette option une fois activée. Contactez-nous si vous devez la désactiver.*

Le SSO est maintenant mis en place entre notre tenant Entra, et l'application Leexi.

Les utilisateurs seront désormais connectés automatiquement via le SSO.

*Pour plus d'informations, voici la documentation officielle :*

[Leexi SSO: Microsoft Entra SAML app + SCIM](#)