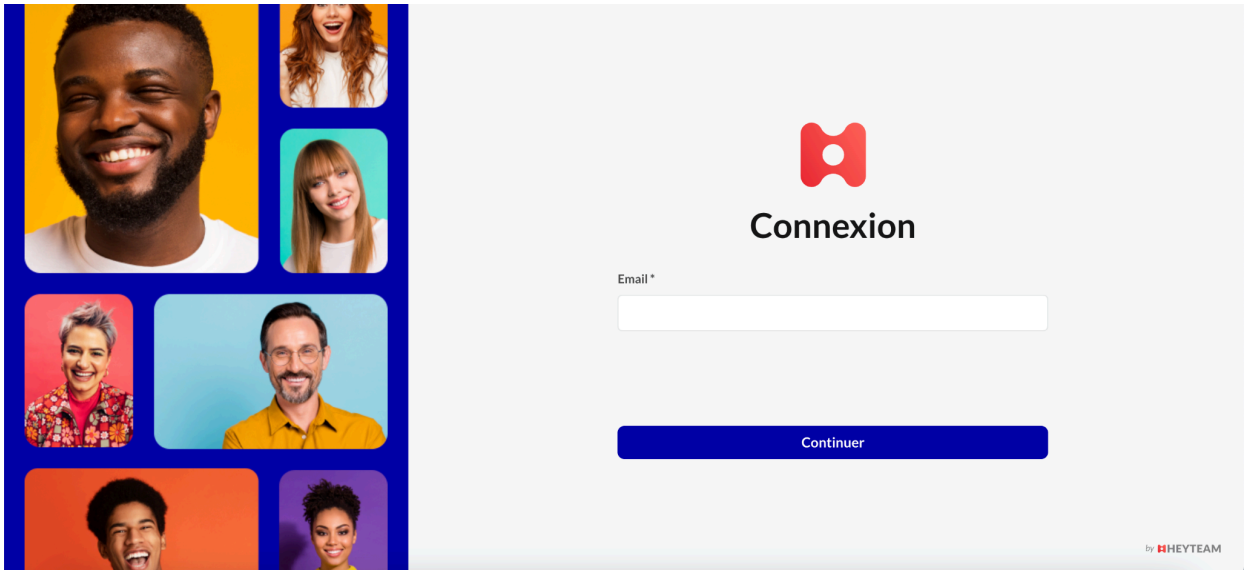
Mise en place du SSO

Microsoft Azure

Son fonctionnement

Pour se connecter via SSO, il faut se connecter via son adresse email professionnelle sur la page de connexion.



La redirection vers votre portail de connexion SSO sera alors effectuée automatiquement.

À noter : Une fois la première connexion effectuée sur votre portail SSO, celui-ci n'apparaîtra plus aux yeux de l'utilisateur et la connexion vers HeyTeam se fera directement.

Pour les nouveaux collaborateurs :

- Un nouveau collaborateur se connecte sur la plateforme HeyTeam via son adresse email personnelle jusqu'à son "jour d'arrivée dans l'entreprise + 1" (cette date est paramétrable sur la plateforme).
- Un passage vers l'adresse professionnelle est automatiquement fait à partir de cette date.

Cela signifie que dans un premier temps le nouveau collaborateur n'aura pas accès au SSO. Il devra créer un mot de passe et se connecter à HeyTeam de manière classique avec son adresse email personnelle.

Autres utilisateurs :

- Excepté les nouveaux collaborateurs, les utilisateurs invités sur HeyTeam se connectent directement avec leur adresse professionnelle, permettant d'accéder dès la première connexion au SSO mis en place.

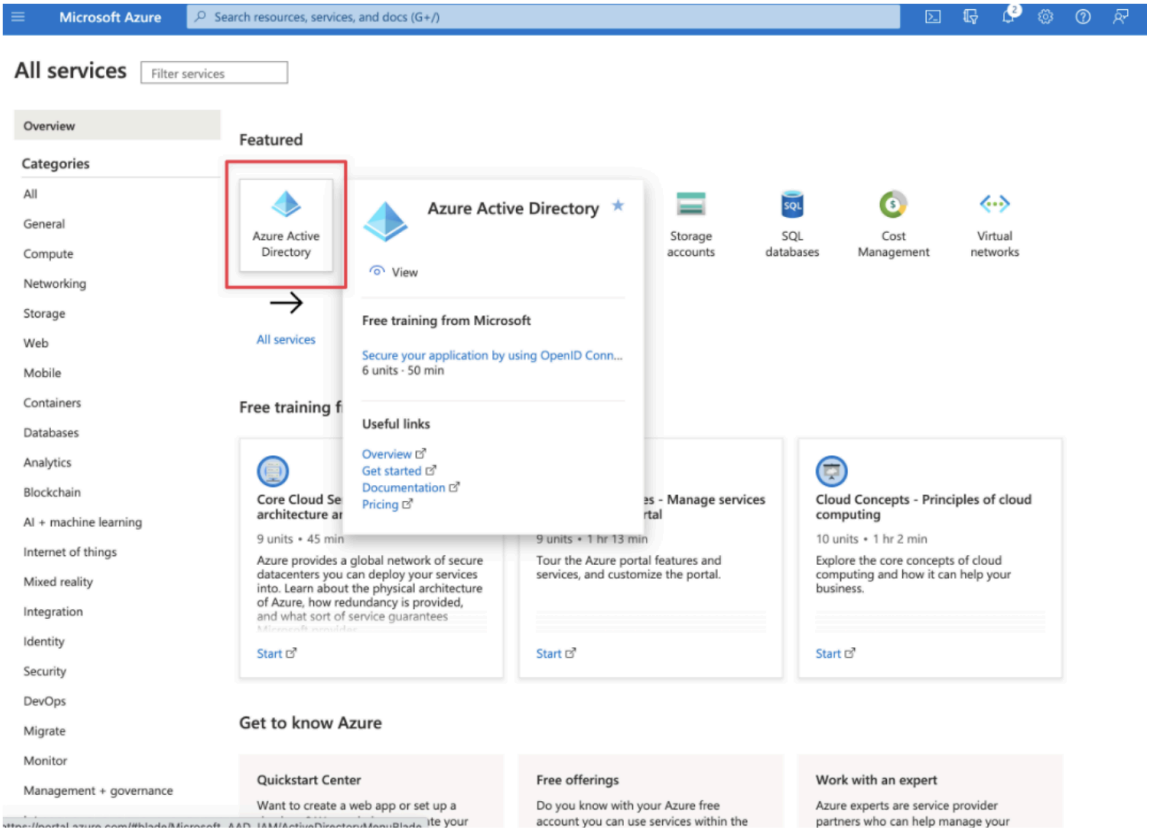
Lors de la première connexion à HeyTeam via le SSO :

- L'onglet "Mot de Passe" dans la section "Mon Compte" n'apparaît plus sur la plateforme HeyTeam. La section "Création du mot de passe" lors de la première connexion disparaît également.

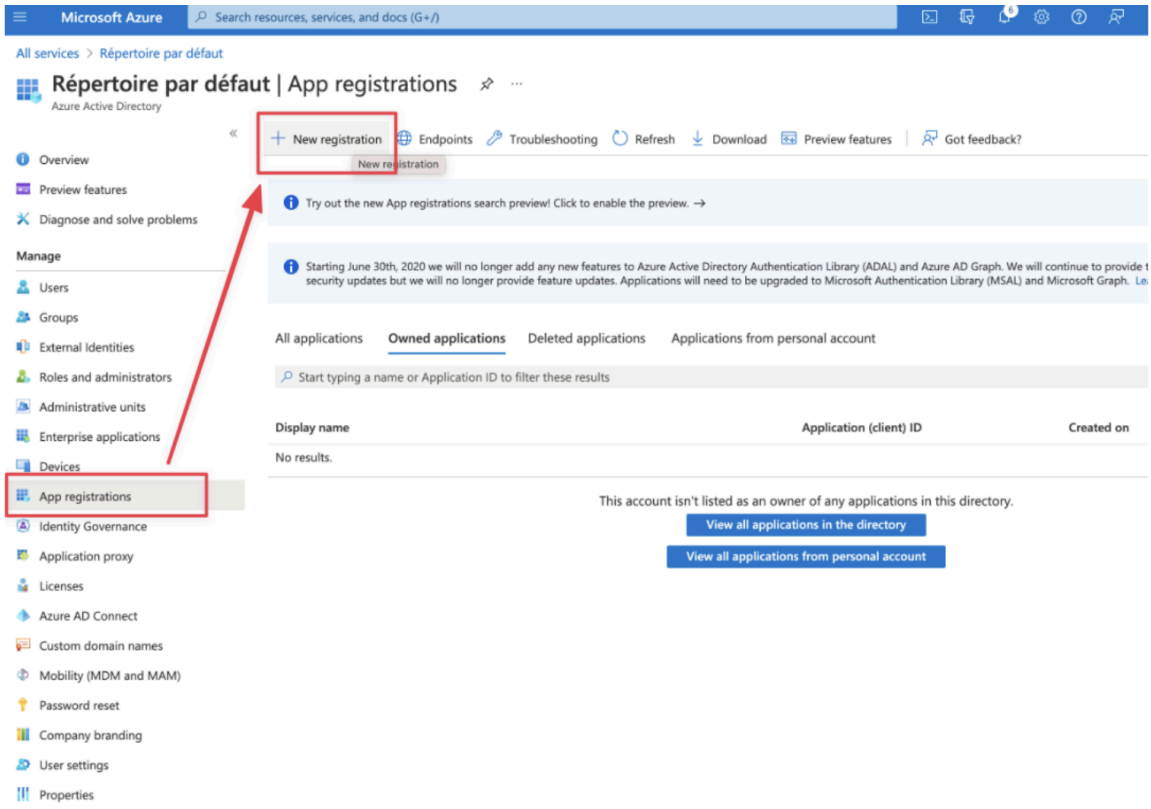
Sa mise en place

Microsoft AZURE

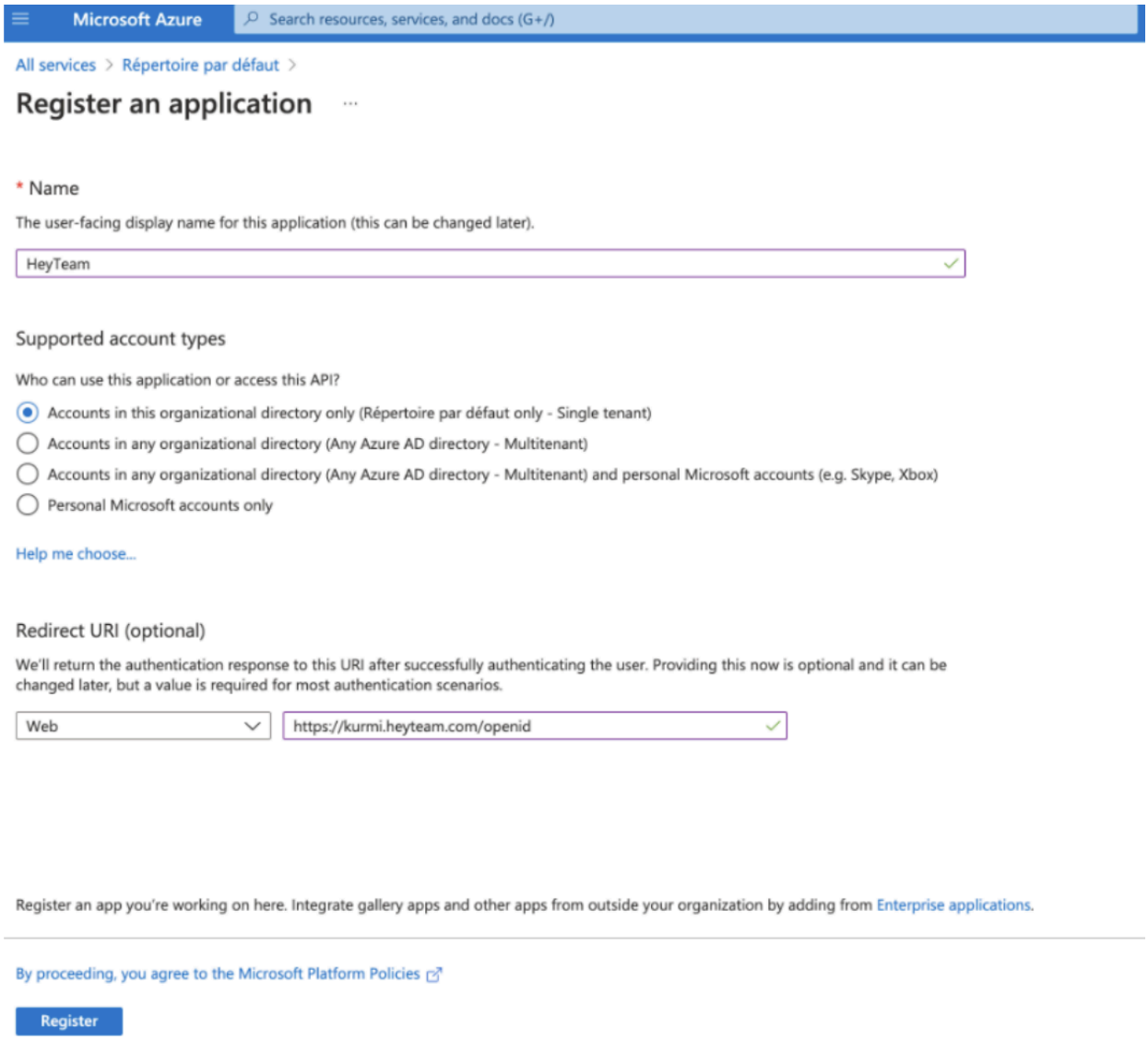
1. **Dans “All services”, cliquez sur “Azure”**



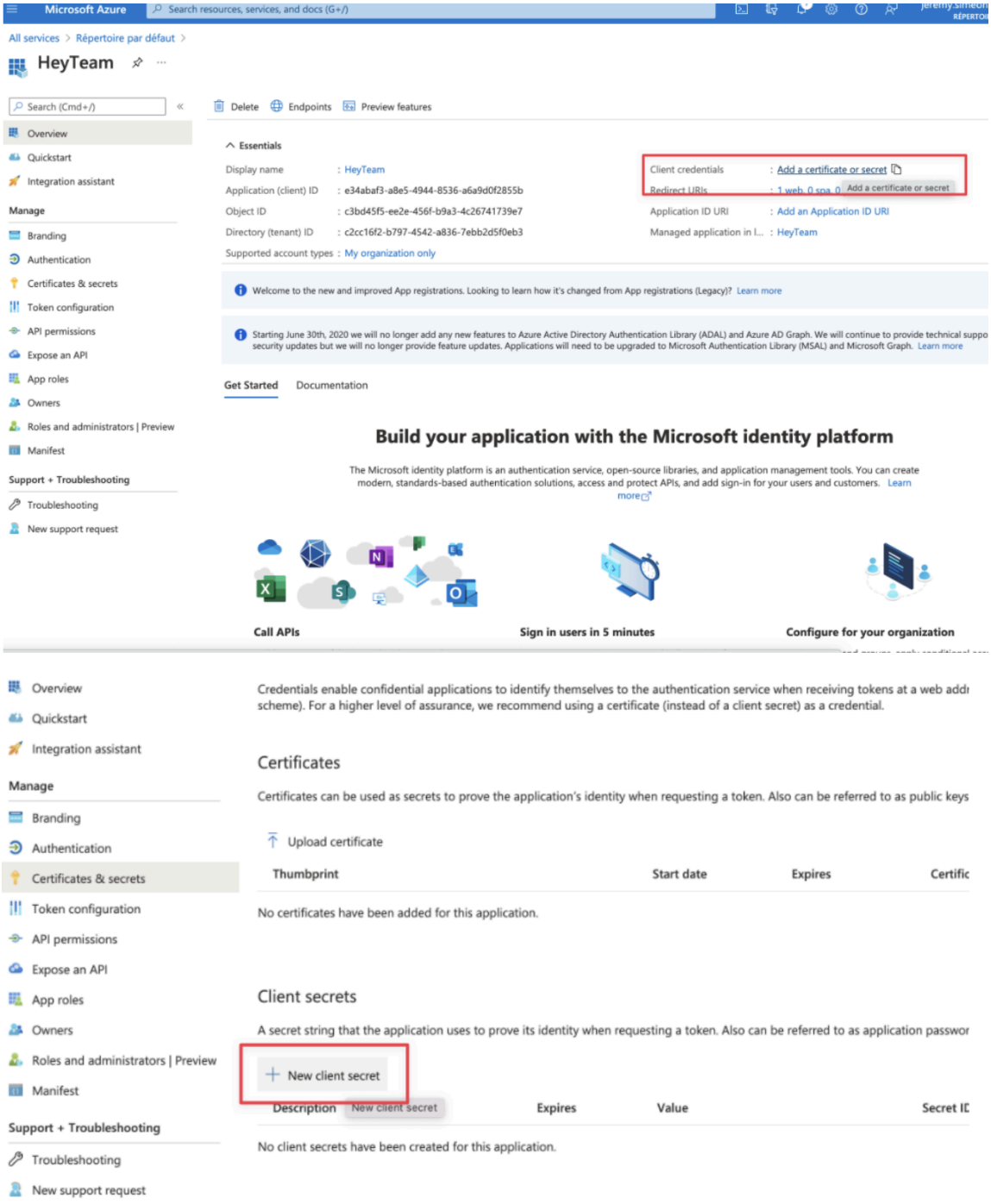
2. **Créer une nouvelle application**



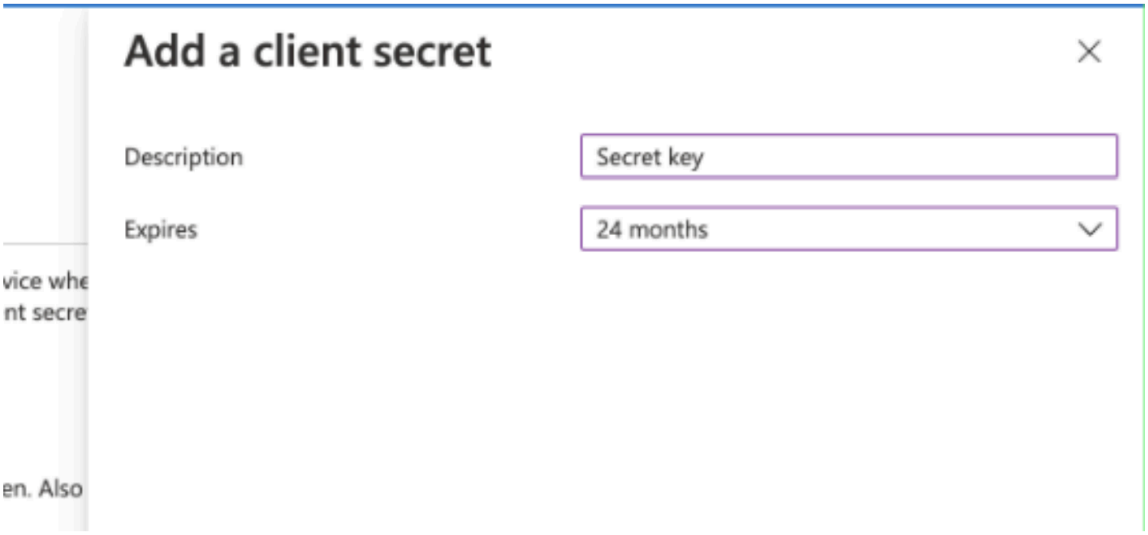
3. **Remplir les paramètres de l'application :**
   Name : HeyTeam
   Redirect URI : vous a été communiqué par HeyTeam. Elle est toujours dans le format suivant https://<domaine>.heyteam.com/openid



4. **Une fois l'application créée, ajouter un client secret**
   "Client credential" > Ajouter un nouveau client secret

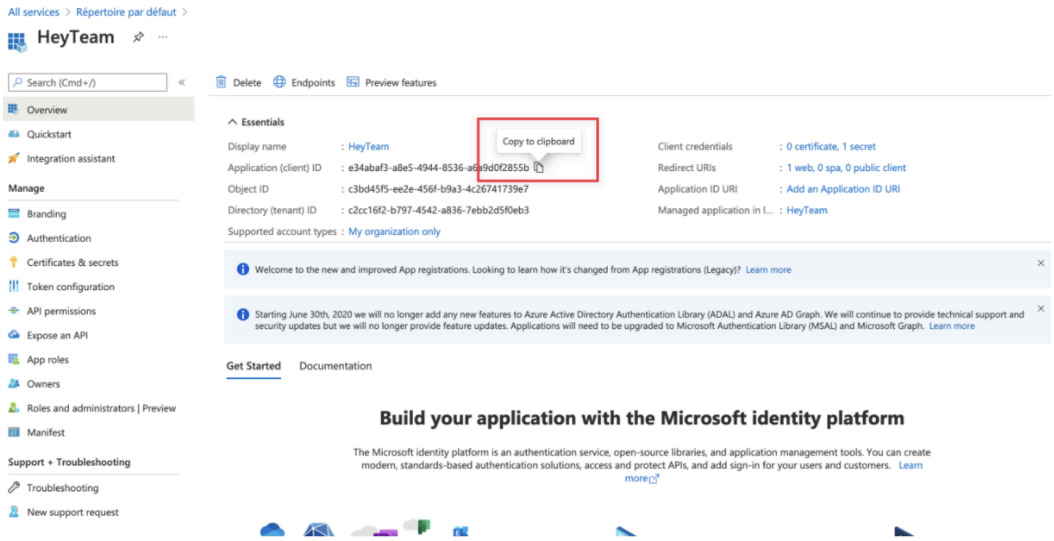


Préciser ensuite la durée de validité et vous pouvez ensuite valider.

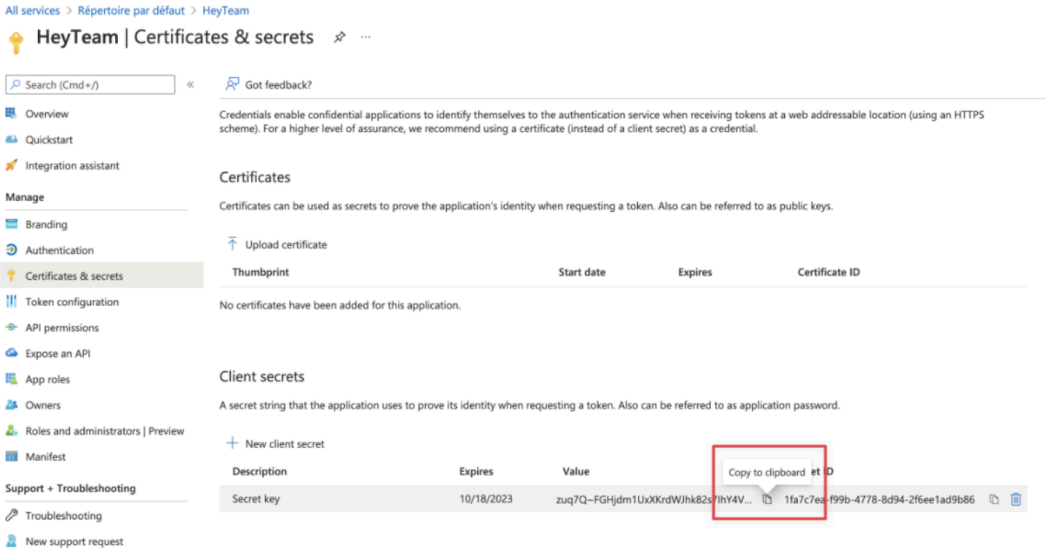


5. **Il est temps ensuite de copier les données dans l'interface HeyTeam.**
   Vous aurez besoin de :
   a. Client ID
   b. Client Secret
   c. Le "well-knwon"

   a. **Le client ID se trouve dans le champ "Application (client) ID" :**



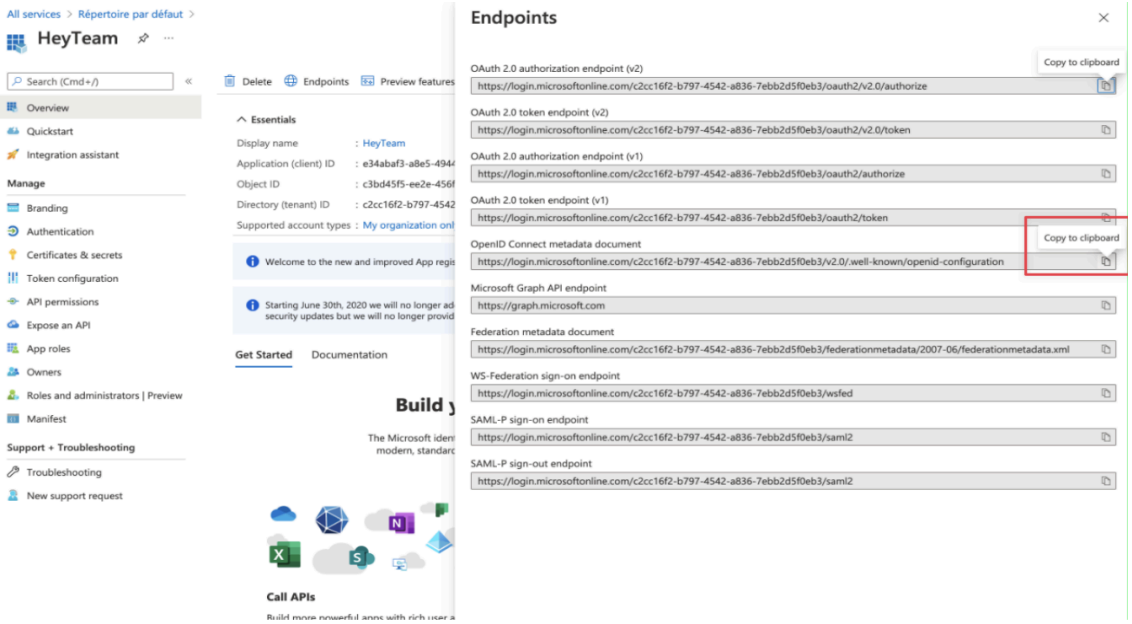
b. **Le secret ID se trouve dans la partie Certificates :**



c- L'authentification URI, le token URI ainsi que le User URI se trouvent dans vos metadata via le lien du .well_known.

Ces informations sont accessibles dans la partie "Overview" > "Endpoints".
Pour récupérer les 3 liens, vous pouvez faire une recherche des 3 informations :

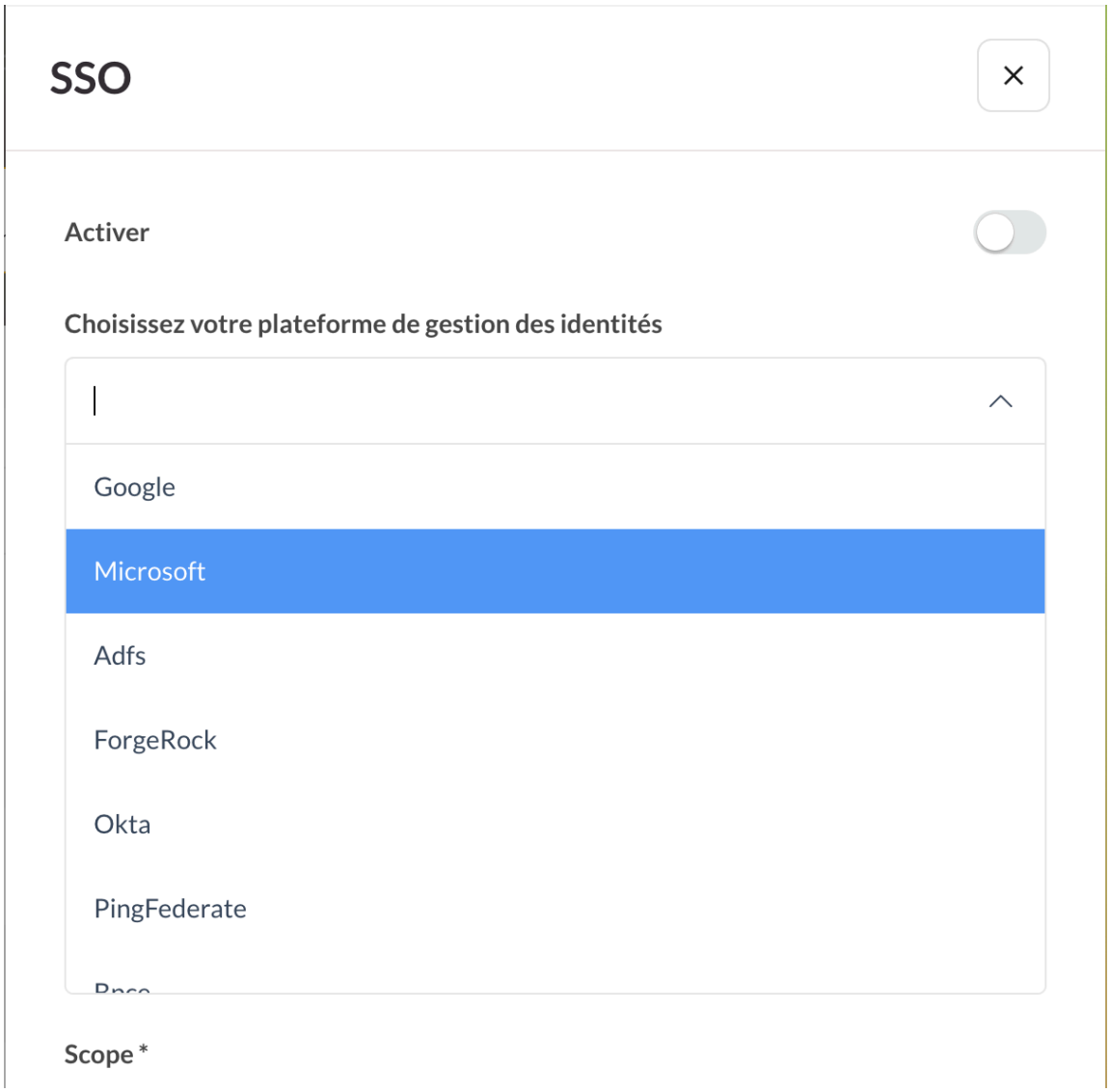
- Auth uri = l'url se termine par "/authorize"
- Token uri = l'url se termine par "/token"
- User uri = l'url se termine par "userinfo"



6. **Dans HeyTeam, se rendre dans Paramètres > Sécurité & confidentialité > SSO**


Retour au menu
Utilisateurs
Rôles
Entités
Plateforme
Page(s) entreprise
Notifications
Chatbot d'accueil
Communication
Langues
Intégration
Analyse de données
Sécurité & confidenti...
Champs personnalis...
Logs
Erwan
Rechercher
NAME
Mot de passe
SSO
Temps de session
Membres d'équipe
Suppression des données
Double authentification (2FA)
SSO
Activer
Choisissez votre plateforme de gestion des identités
Microsoft
Auth uri *
https://login.microsoftonline.com/common/oauth2/v2.0/authorize
Token uri *
https://login.microsoftonline.com/common/oauth2/v2.0/token
User uri *
https://graph.microsoft.com/oidc/userinfo
Scope *
openid profile email
Client id *
your-client-id
Client secret *
Domains Optionnel

7. **Sélectionner ensuite le service “Microsoft”**



8- Puis copier-coller les informations de Microsof Azure sur HeyTeam en renseignant :

a. Auth uri : à récupérer dans le .well_known
b. Token uri : à récupérer dans le .well_known
c. User uri : à récupérer dans le .well_known
d. Scope : toujours indiquer : “openid profile email”
e. Client ID : à récupérer directement dans vos endpoint
f. Client Secret : à récupérer directement dans vos endpoint

Vous pouvez également rajouter de manière optionnelle un domaine, par exemple heyteam.com. Cela veut dire que toutes les adresses mail se terminant avec ce nom de domaine seront associées au SSO.

9- Vous pouvez cliquer sur “Tester la configuration” pour vous assurez que tout est OK.