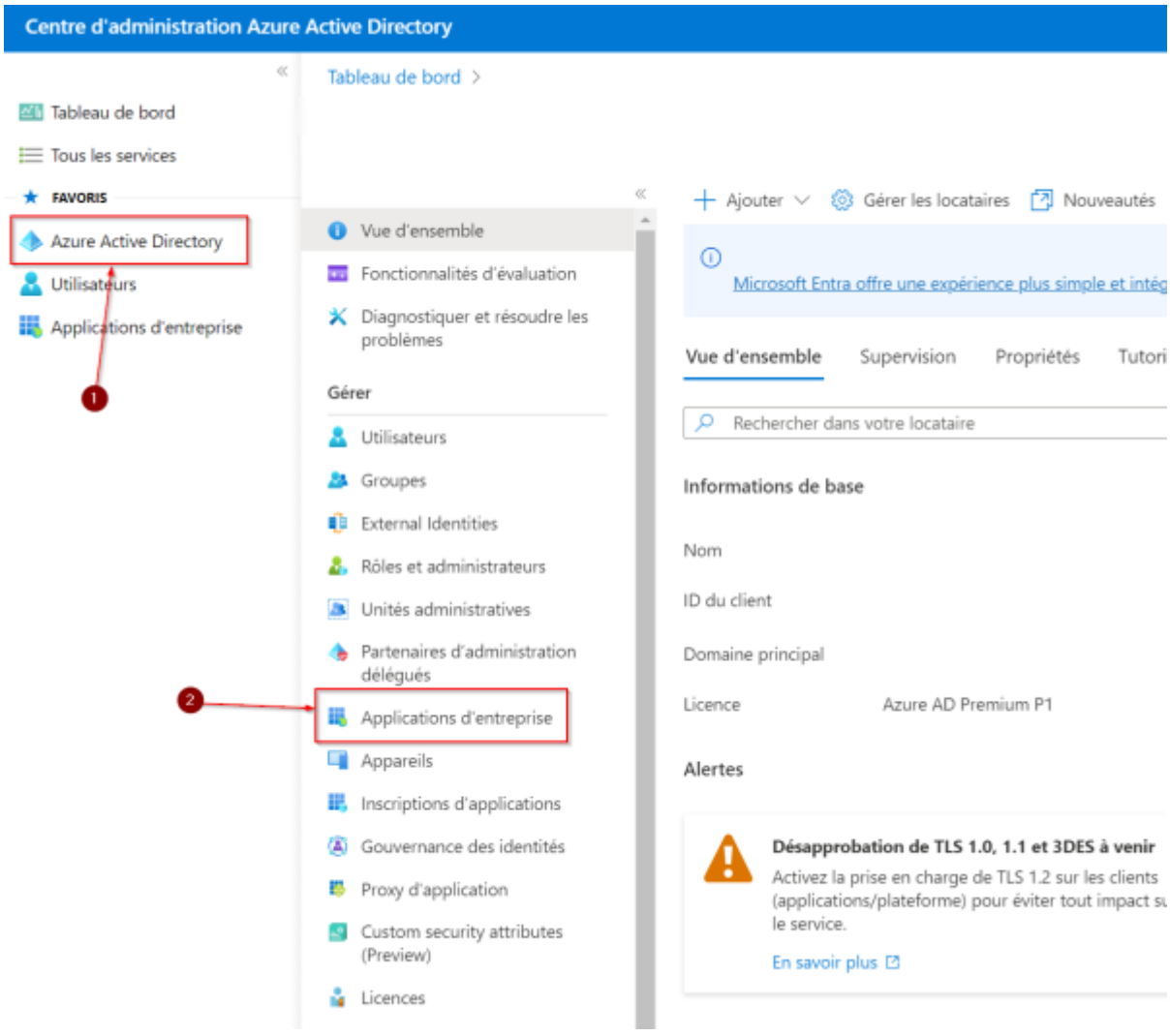
Microsoft Office 365

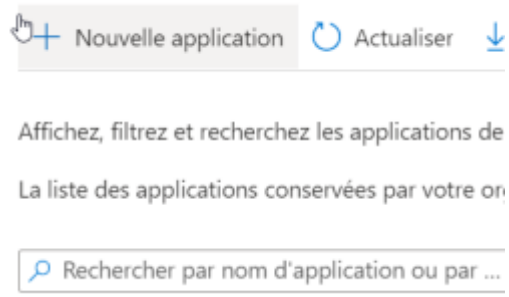
Nous allons voir comment créer et récupérer les éléments permettant de réaliser une liaison entre votre système ESIA et Microsoft Office365

Création de l'application

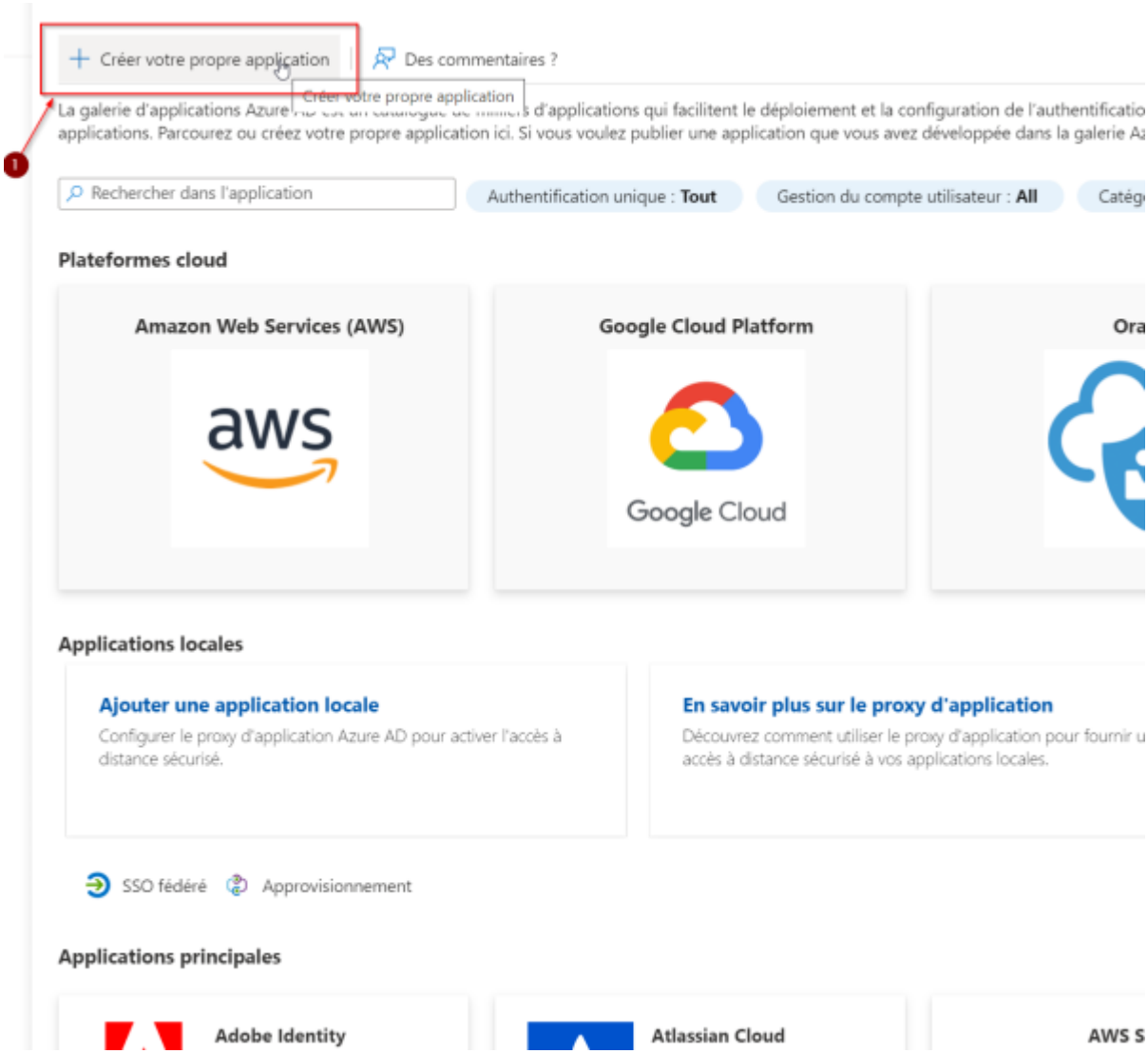
Une fois connecté dans votre centre d'administration Azure Active Directory. Cliquez sur « Azure Active Directory » et ensuite sur « Applications d'entreprise ».



Il faut ensuite cliquer sur « Nouvelle application ».

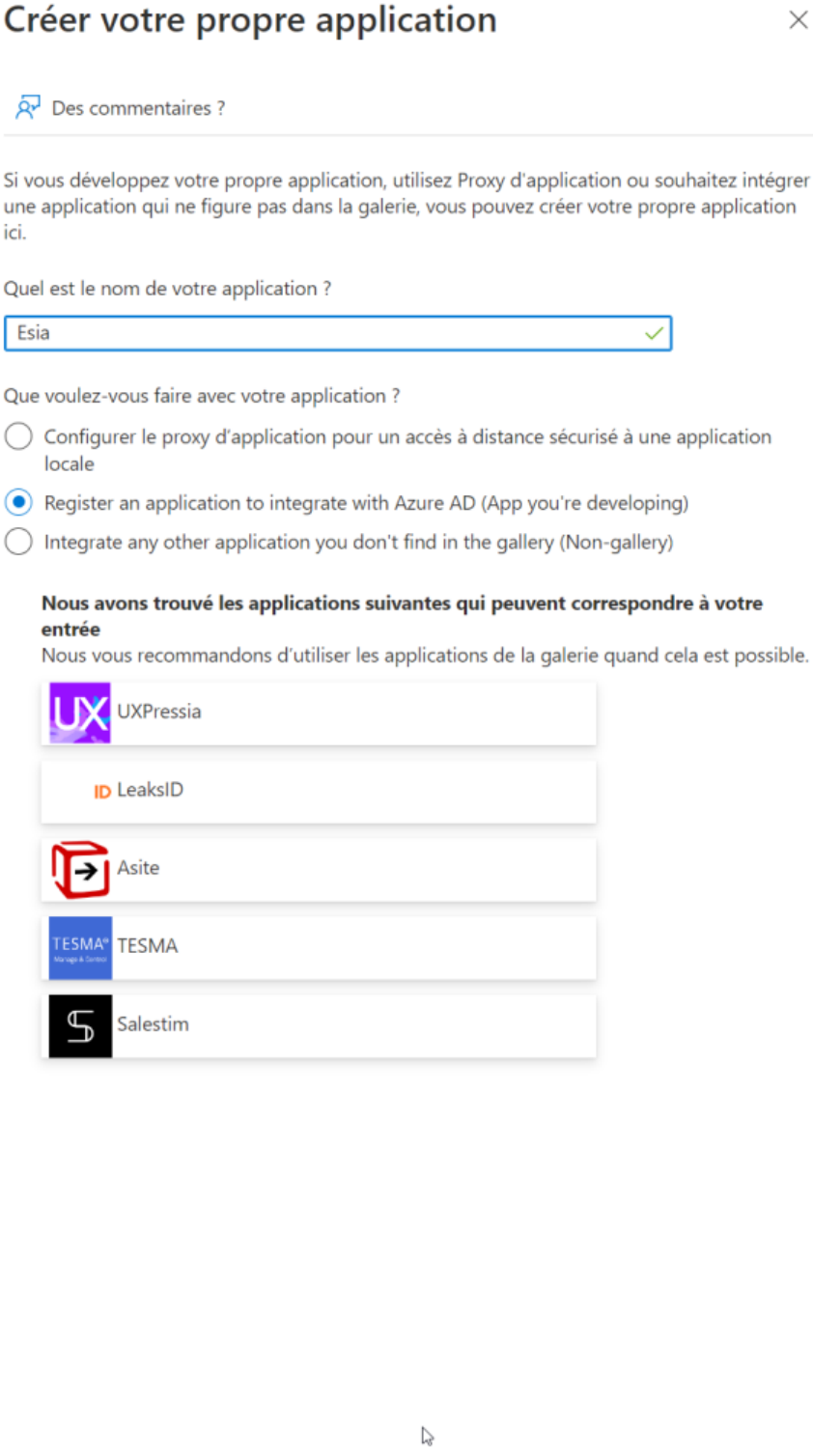


Maintenant, allez sur « Créer votre propre application »

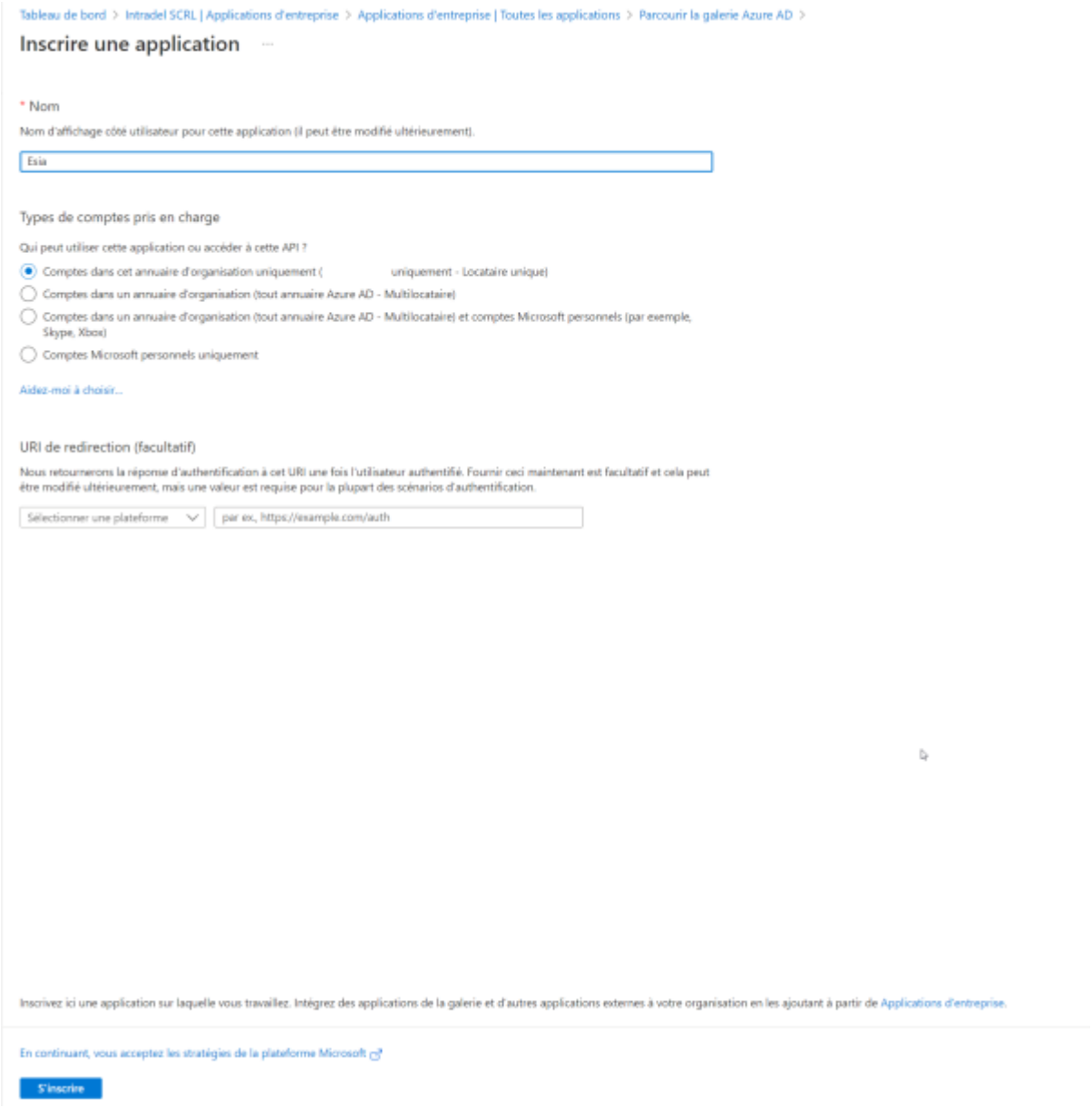


Indiquer le nom de votre application et cocher la case « Register an application to integrate with Azure AD (app you are developing)». Même si votre interface est en français cette option est non traduite actuellement (10 octobre 2022).

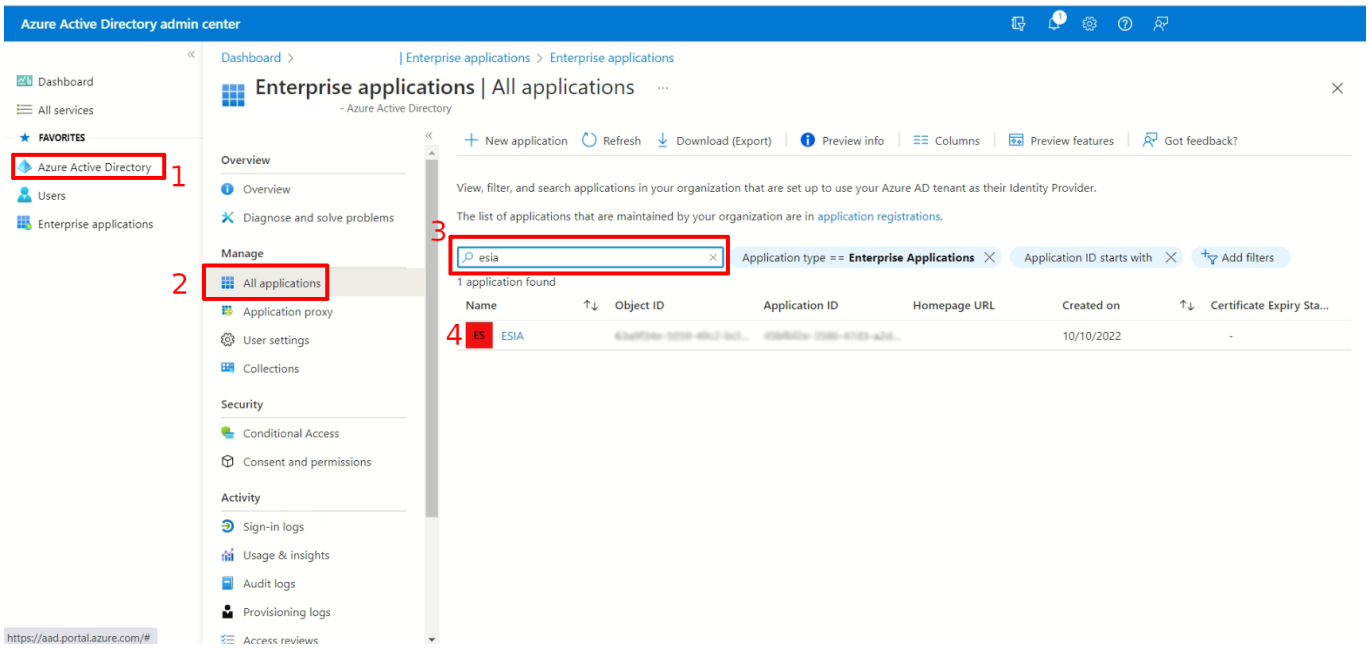
Cliquez ensuite sur « Créer ».


Créer votre propre application
Des commentaires ?
Si vous développez votre propre application, utilisez Proxy d'application ou souhaitez intégrer une application qui ne figure pas dans la galerie, vous pouvez créer votre propre application ici.
Quel est le nom de votre application ?
Esia
Que voulez-vous faire avec votre application ?
Configurer le proxy d'application pour un accès à distance sécurisé à une application locale
Register an application to integrate with Azure AD (App you're developing)
Integrate any other application you don't find in the gallery (Non-gallery)
Nous avons trouvé les applications suivantes qui peuvent correspondre à votre entrée
Nous vous recommandons d'utiliser les applications de la galerie quand cela est possible.
UXPressia
LeaksID
Asite
TESMA
Salestim
Créer

Sélectionner le type de compte « Compte dans cet annuaire d'organisation uniquement (XXXXX uniquement – Locataire unique) ».

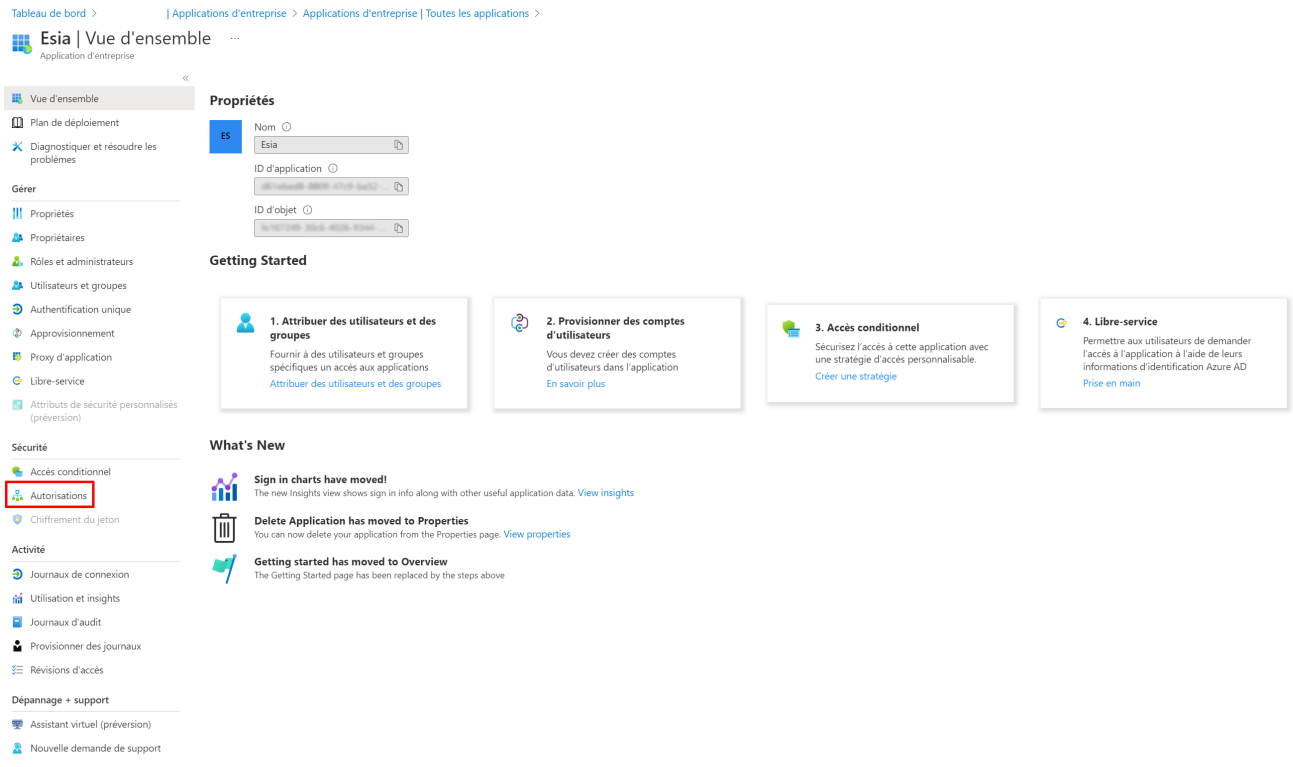


Il faut maintenant configurer les autorisations de l'application, Cliquez sur “Azure Active Directory”, “All application”. Dans le champ de recherche, indiquez le nom de l'application (ici: esia) et pour terminer cliquez sur votre application.

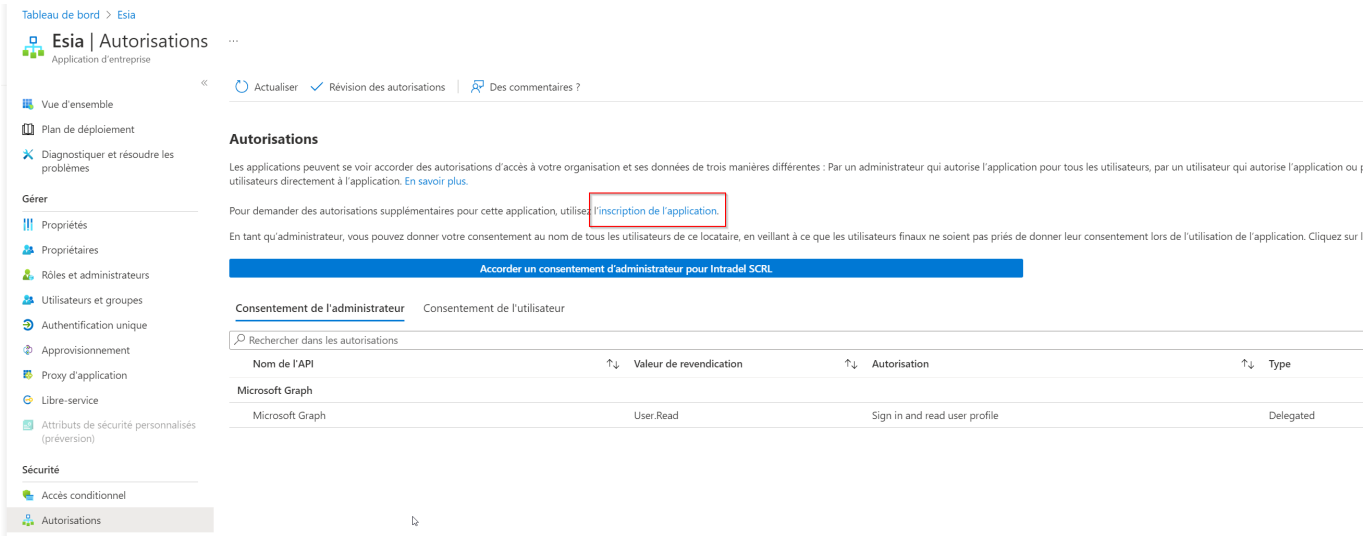


Autorisations

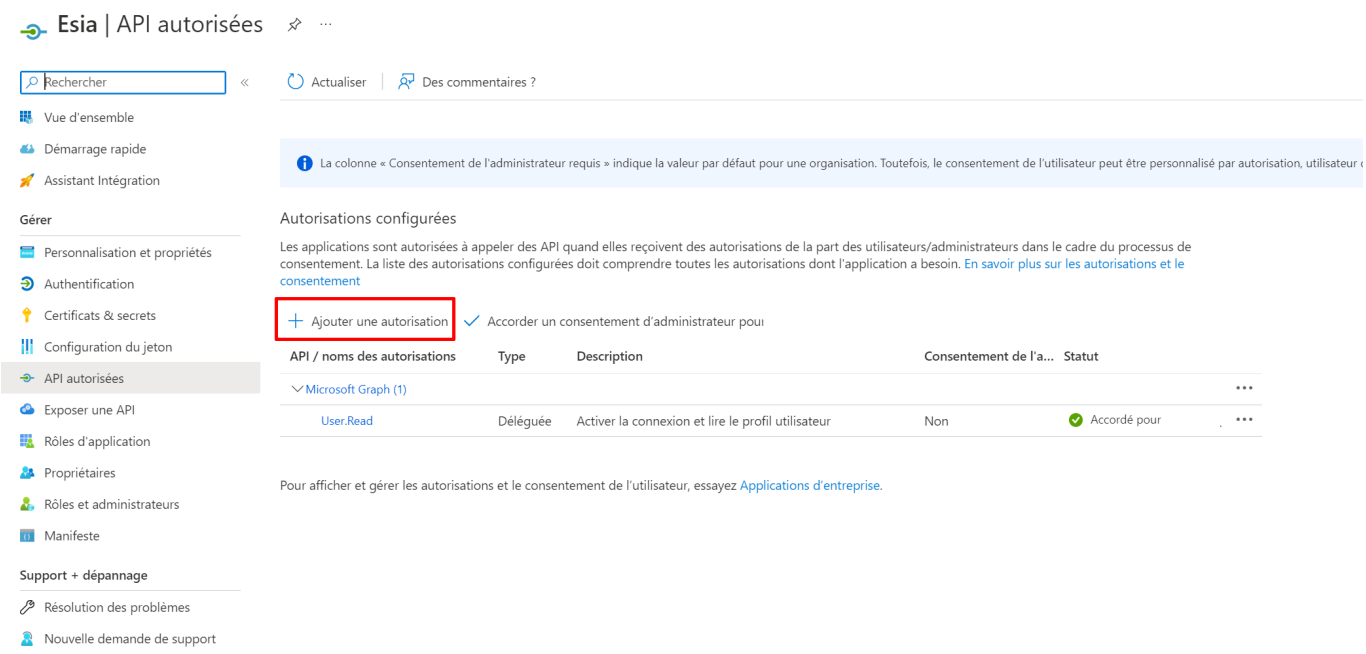
Vous voilà maintenant dans la vue d'ensemble de l'application. Cliquez sur « Autorisations »



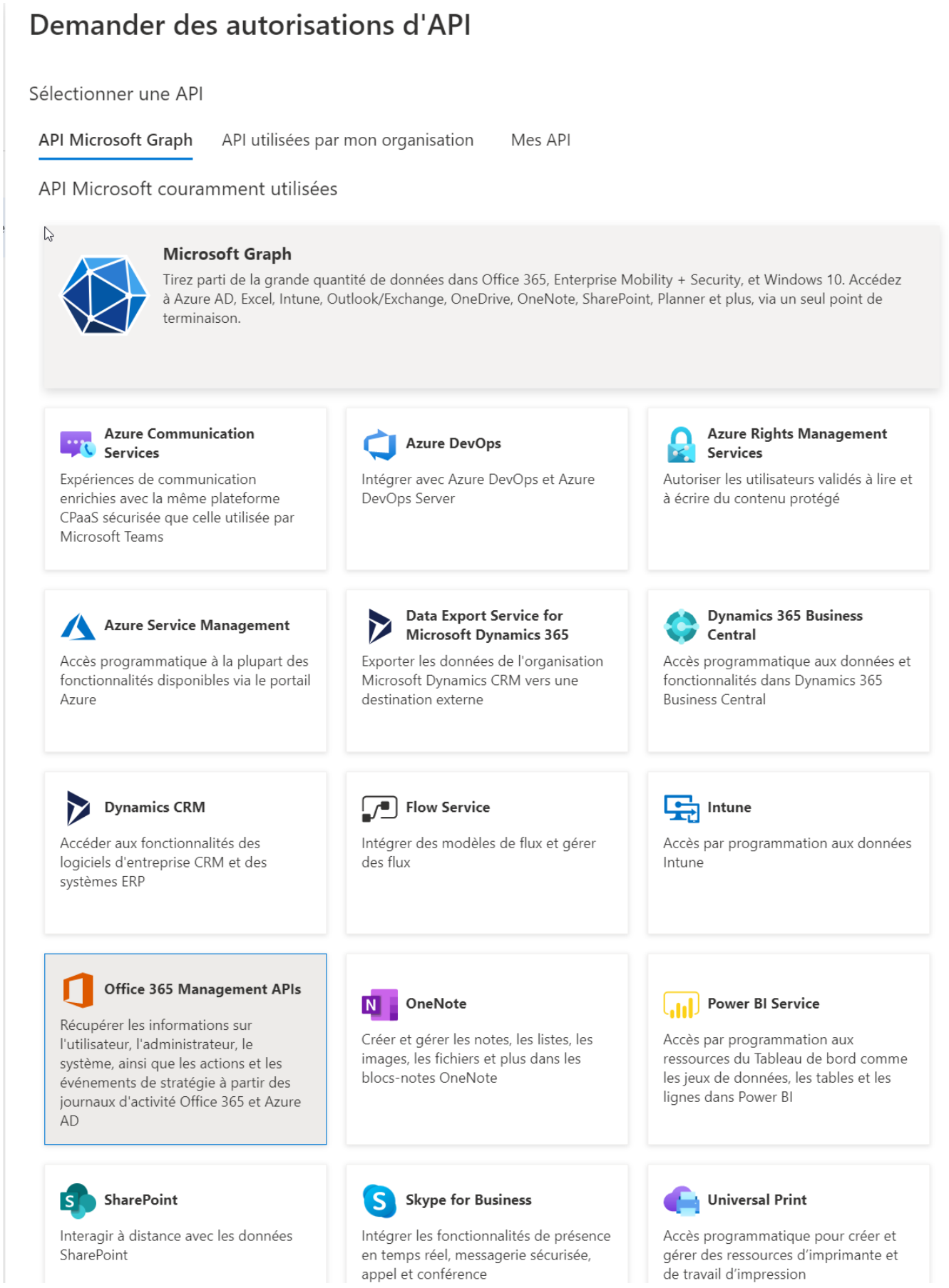
Maintenant, cliquez sur « Inscription de l'application » afin de lui donner les droits correspondants.



Cliquez sur « Ajouter une autorisation »



Sélectionnez « Office 365 management APIs ».



Cliquez sur « Autorisation d'application » et sélectionnez les droits suivants :

- ActivityFeed.Read
- ActivityFeed.ReadIp

- ServiceHealth.Read

Cliquez sur « Ajouter des autorisations ».

Demander des autorisations d'API

‹ Toutes les API

Office 365 Management APIs

https://manage.office.com/ Documents

Quel type d'autorisation votre application nécessite-t-elle ?

Autorisations déléguées
Votre application doit accéder à l'API en tant qu'utilisateur connecté.

Autorisations d'application
Votre application s'exécute en tant que service en arrière-plan ou démon sans utilisateur connecté.

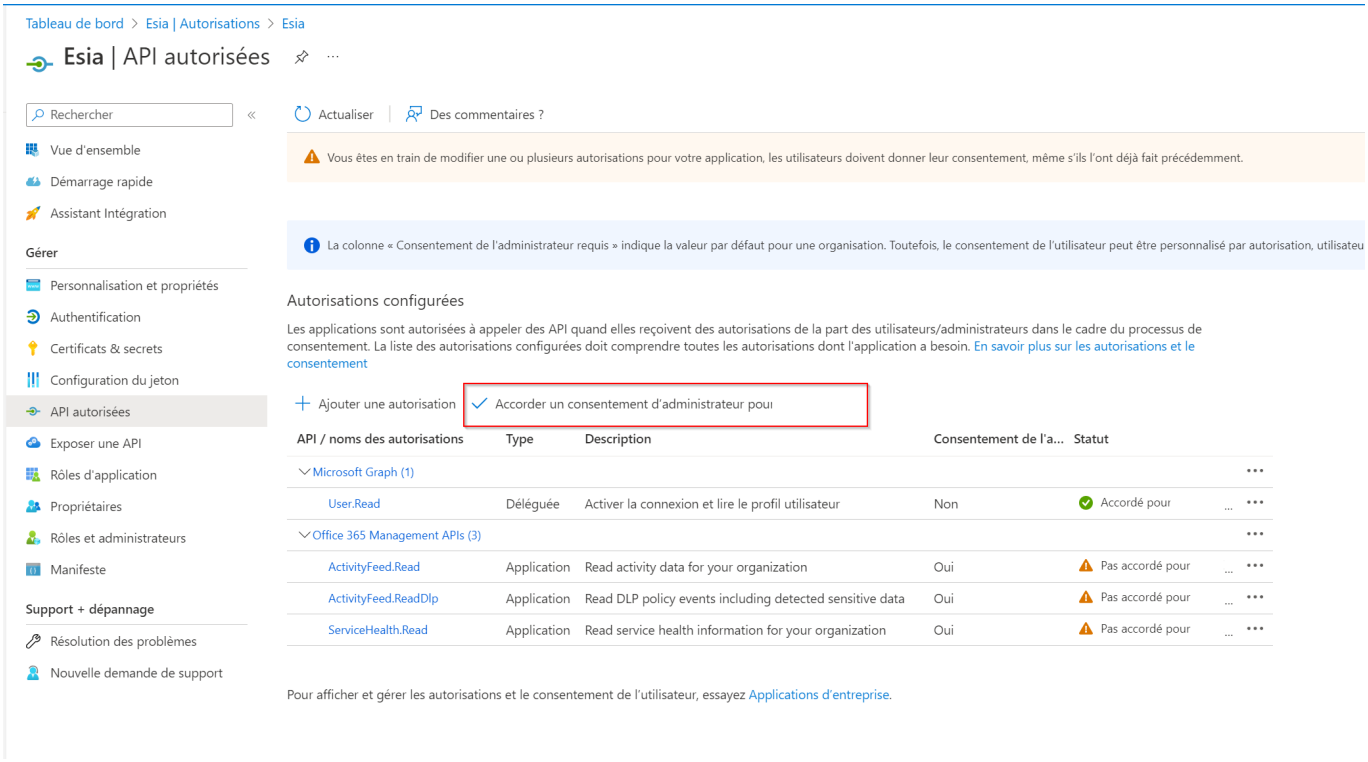
Sélectionner des autorisations développer tout

Commencez à taper une autorisation pour filtrer ces résultats

Autorisation	Consentement de l'administrateur r...
ActivityFeed (2)	
ActivityFeed.Read Read activity data for your organization	Oui
ActivityFeed.ReadDlp Read DLP policy events including detected sensitive data	Oui
ServiceHealth (1)	
ServiceHealth.Read Read service health information for your organization	Oui

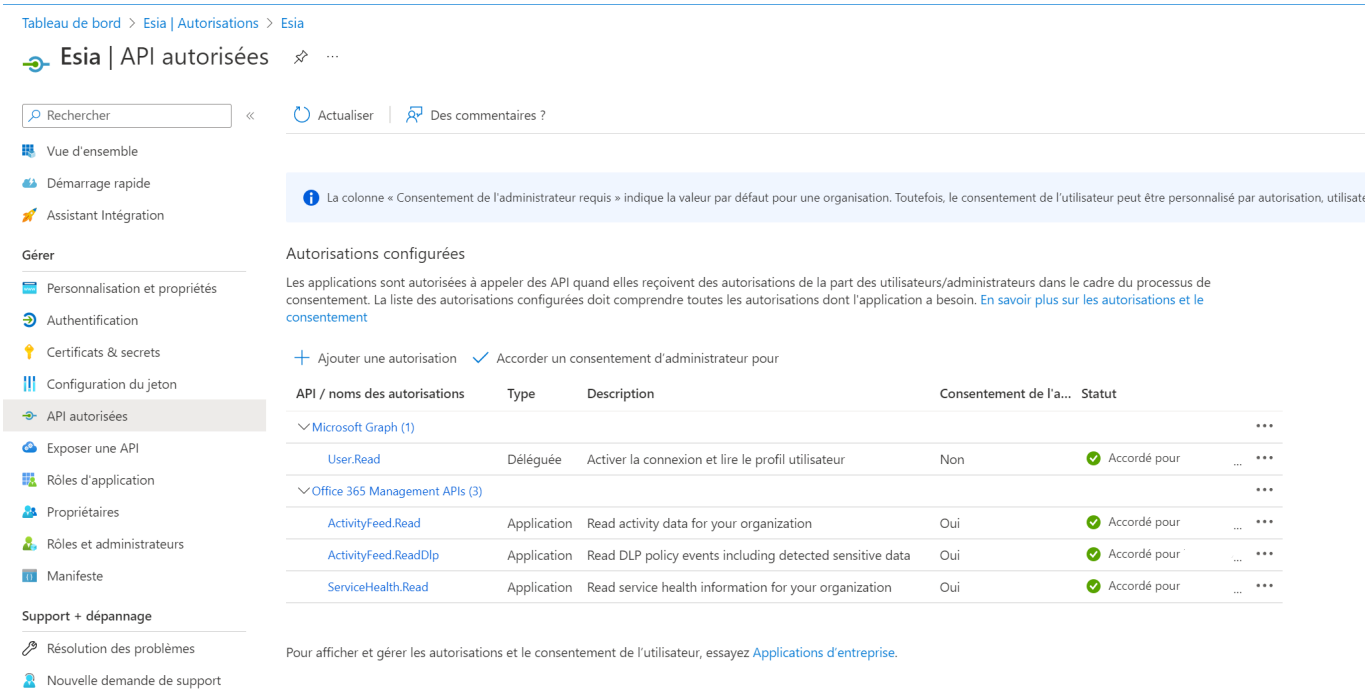
Ajouter des autorisations Abandonner

Cliquez sur « Accorder un consentement d'administrateur »



Répondez « oui » pour appliquer les droits.

Vous devriez avoir le panneau des autorisations qui ressemble à ceci :

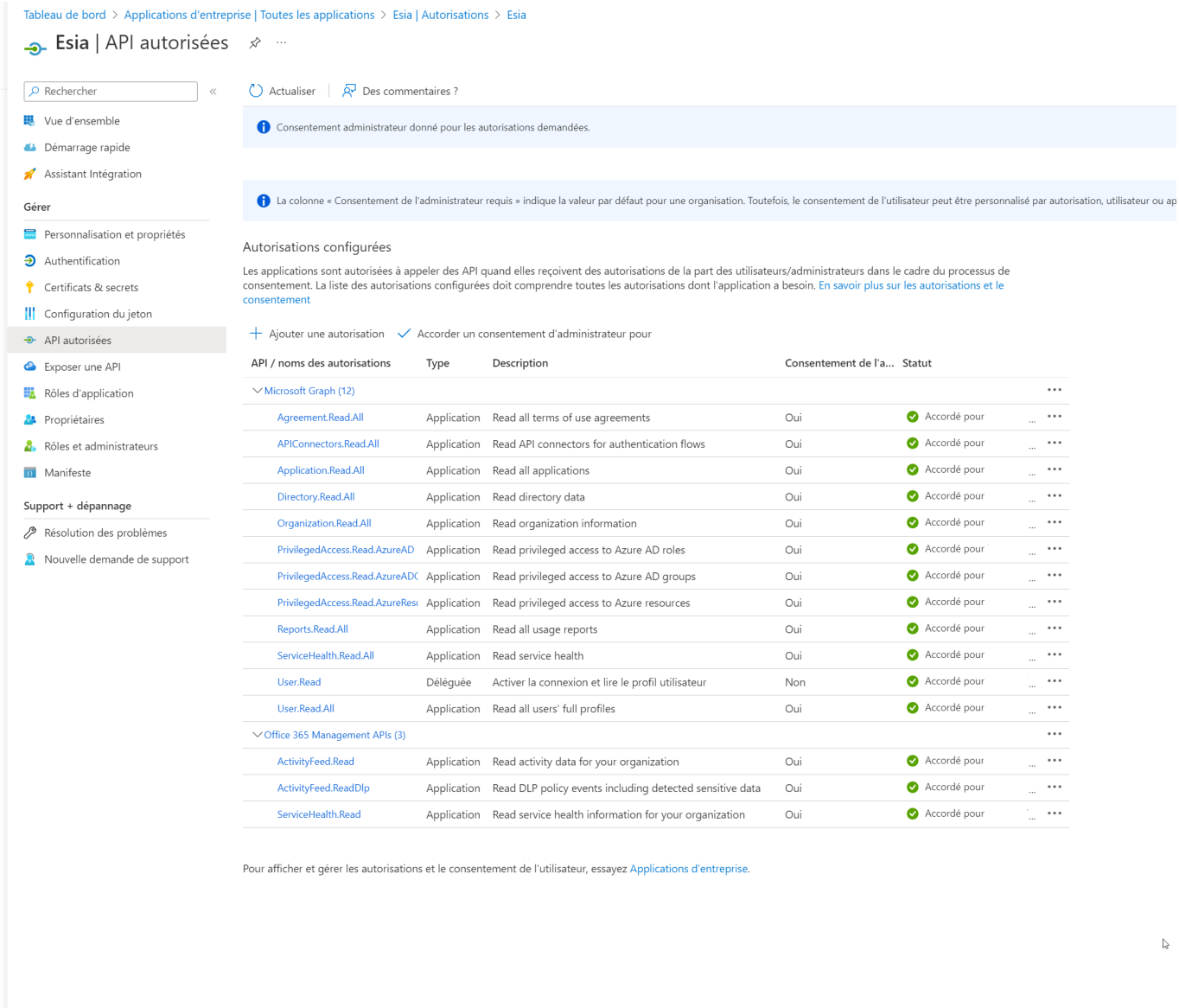


Recommencez l'opération d'application des autorisations, mais afin d'ajouter les droits d'accès à l'API des graphiques.

Cliquez sur « Ajouter une autorisation » et sélectionnez « Microsoft Graphique ». Les droits suivants sont nécessaires :

- Agreement.Read.All
- APIConnectors.Read.All
- Application.Read.All
- Directory.Read.All
- Organization.Read.All
- Reports.Read.All
- ServiceHealth.Read.All
- User.Read.All

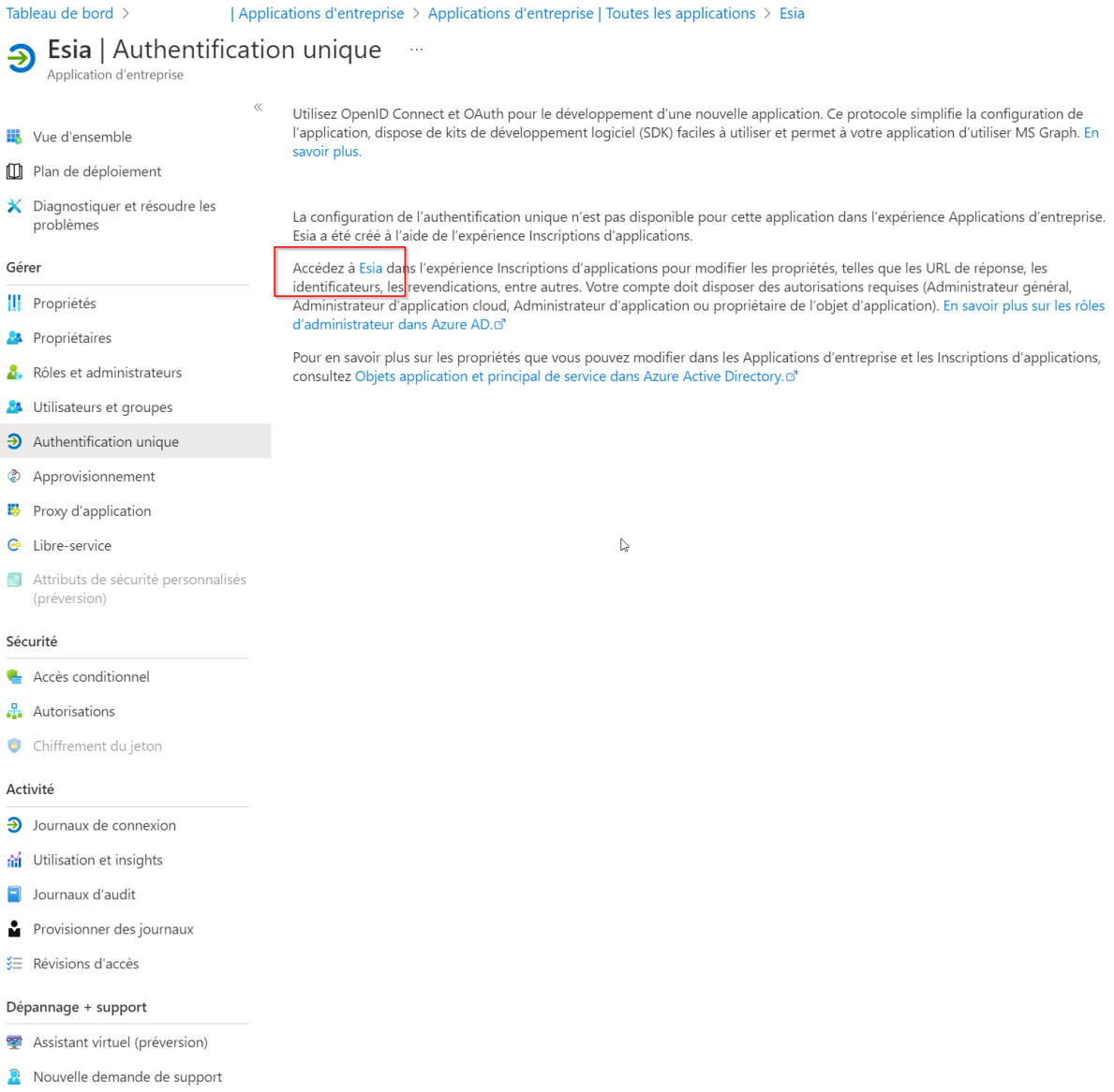
Au final votre panneau ressemblera à ceci:



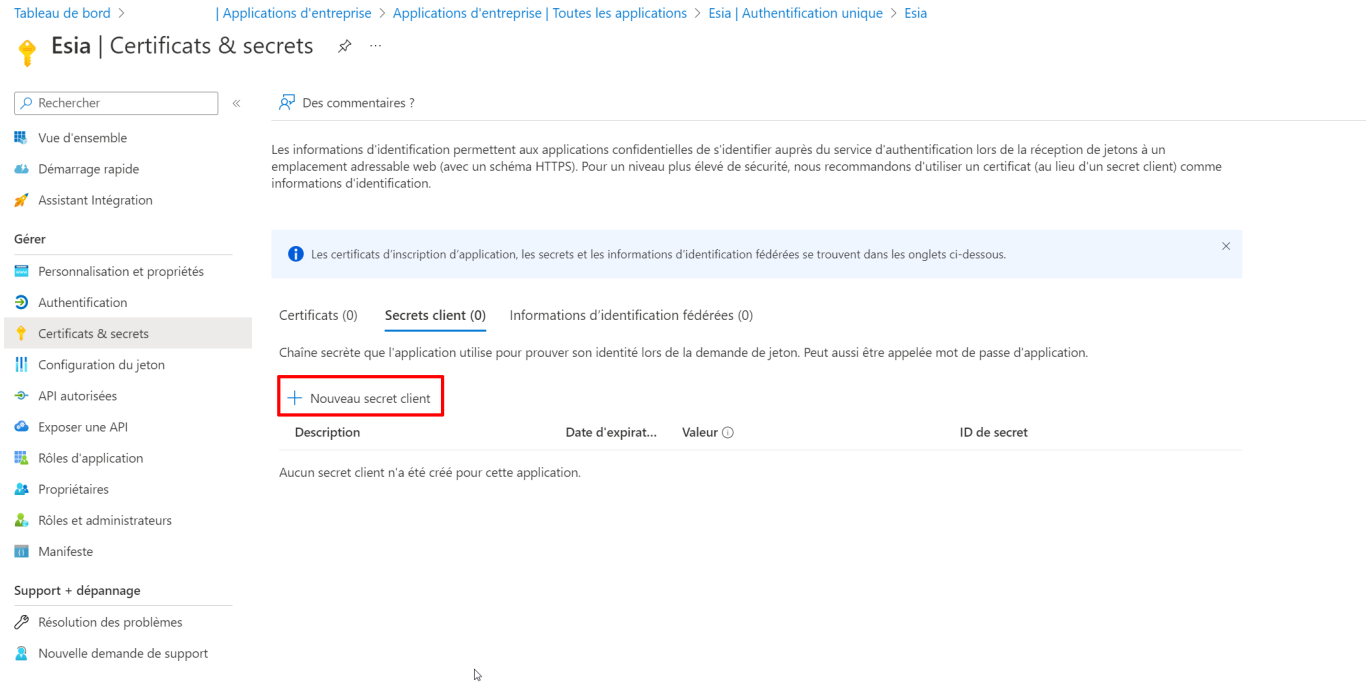
Les droits sont maintenant configurés.

Tenant ID, client ID et clé d'API

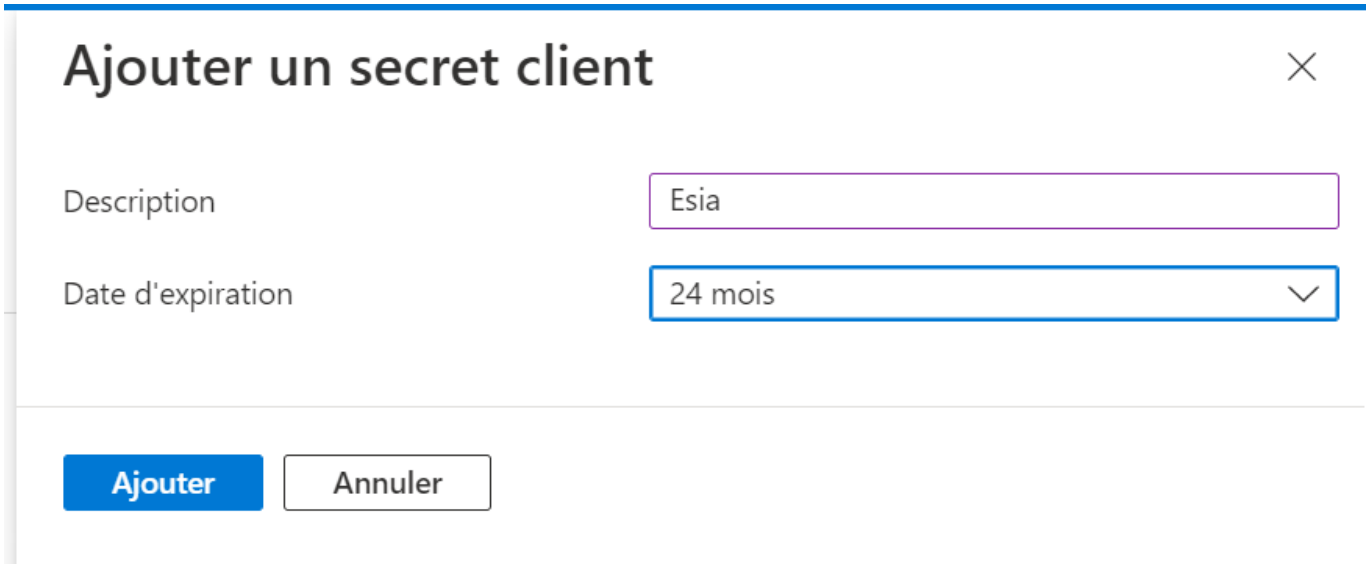
Il faut configurer maintenant la clé d'application afin de pouvoir se connecter. Cliquez dans le menu sur « Authentification unique » et chercher le nom de votre application (ici : « esia ») et cliquez dessus (encadré rouge dans la capture d'écran).



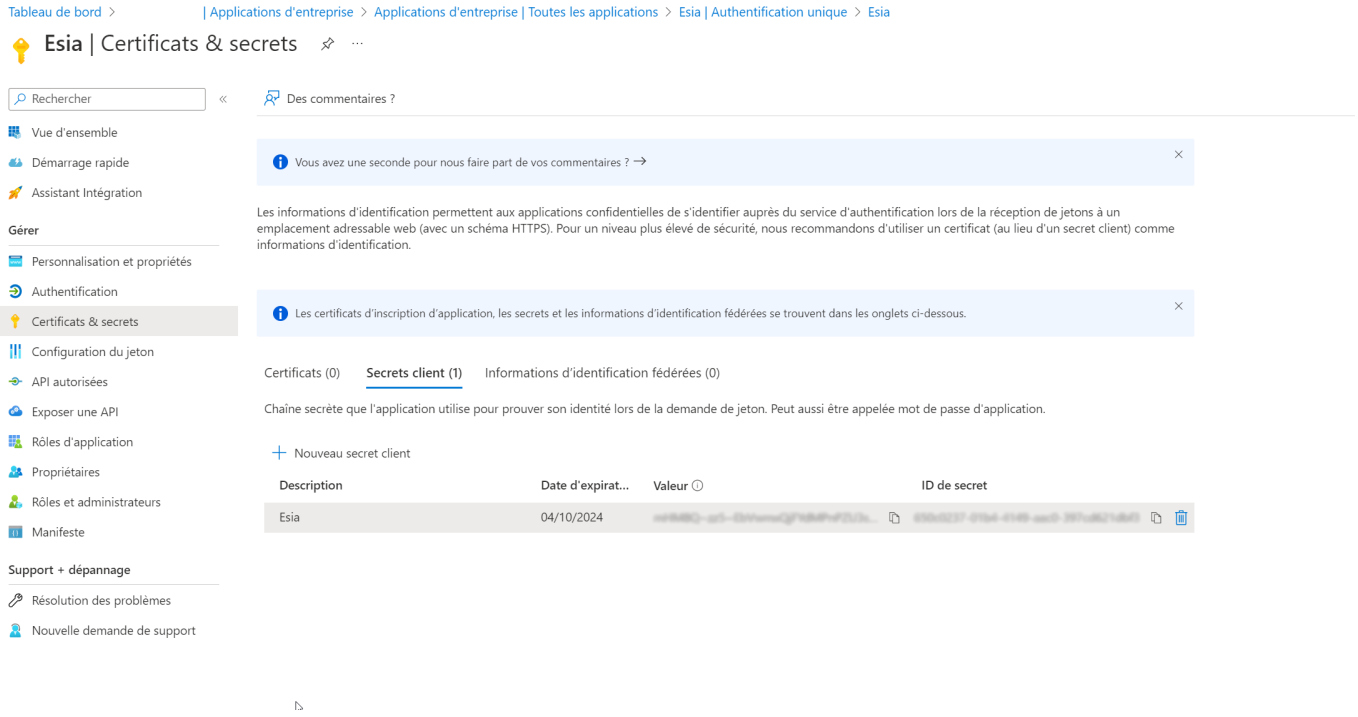
Cliquez sur « certificats & secrets » et ensuite sur « nouveau secret client ».



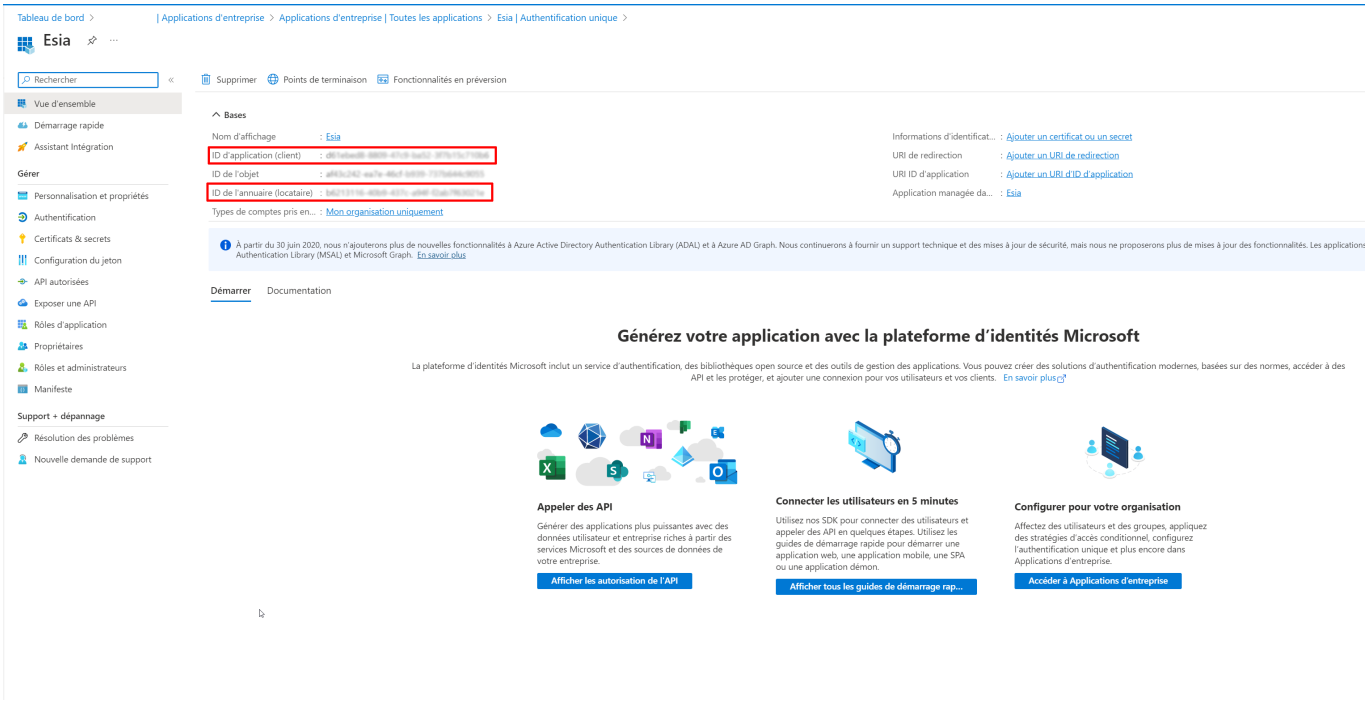
Sélectionnez la Date d'expiration de la clé (maximum 24 mois).



Sauvegarder la « Valeur de la clé » dans un fichier texte, il faudra la renseigner dans Esia.



Cliquez sur « vue d'ensemble » et copiez dans votre fichier l'ID d'application (ClientID) et ID de l'annuaire (TenantID).



Nous avons maintenant toutes les données pour créer la liaison avec Esia.

Vous pouvez vous rendre sur le tuto suivant afin de terminer la configuration:

Installation & Configuration du module Office 365

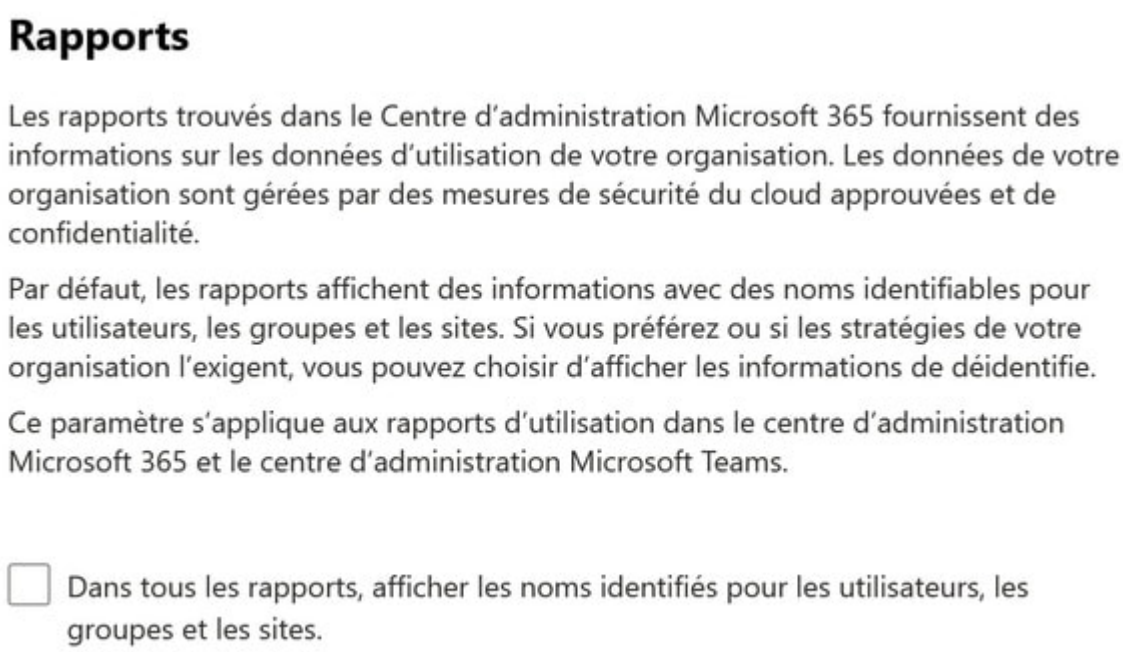
Afficher les adresses mails et pas les hashs

Afin de respecter le GDPR, Microsoft a caché par défaut les informations utilisateurs,consulter votre

DPO ou mettez à jour vos conditions d'utilisation..

Pour les afficher, aller dans “Centre d'administration” ensuite “Paramètres” puis “Paramètres de l'organisation ”, puis “Services” et enfin “Rapports.”.

Assurez vous que la case est bien décocher, la traduction peut prêter à confusion.



Au prochain test d'esia les données sont rechargées (+- 30 min), si vous ne souhaitez pas attendre, vous pouvez supprimer le cache.

```
rm /tmp/o365/*
```