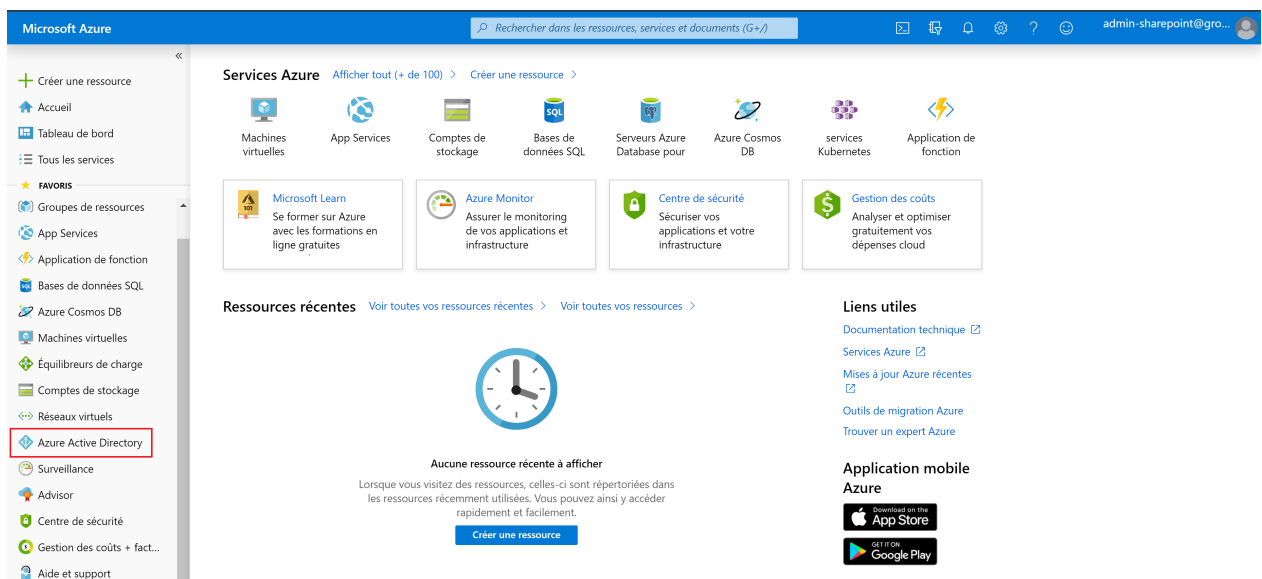


# Ajouter l'application RDD sur le tenant du cabinet

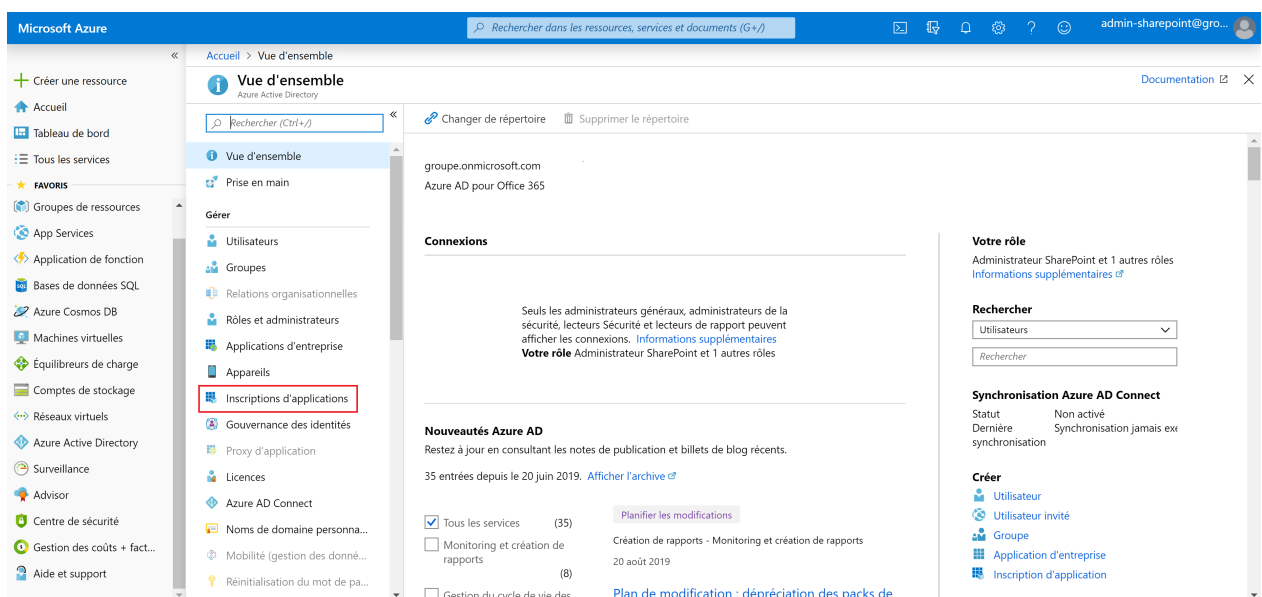
Cette action est à réaliser lors de la création du cabinet.

## Créer l'application RDD

1. Allez à l'adresse suivante : <https://portal.azure.com/>.
2. Au niveau de la barre de menu située à gauche de l'écran, cliquez sur **[Azure Active Directory]**.

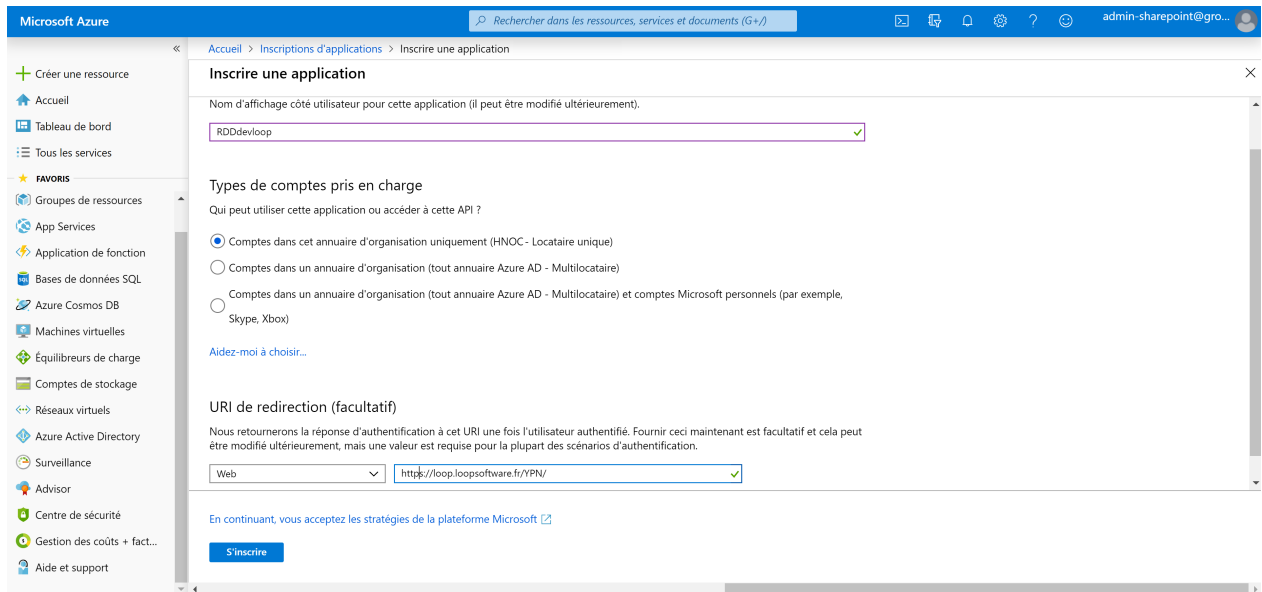


3. Cliquez sur **[Inscriptions d'applications]**.



4. Cliquez sur **[Nouvelle inscription]**.
5. Saisissez les champs comme indiqué dans ci-après :

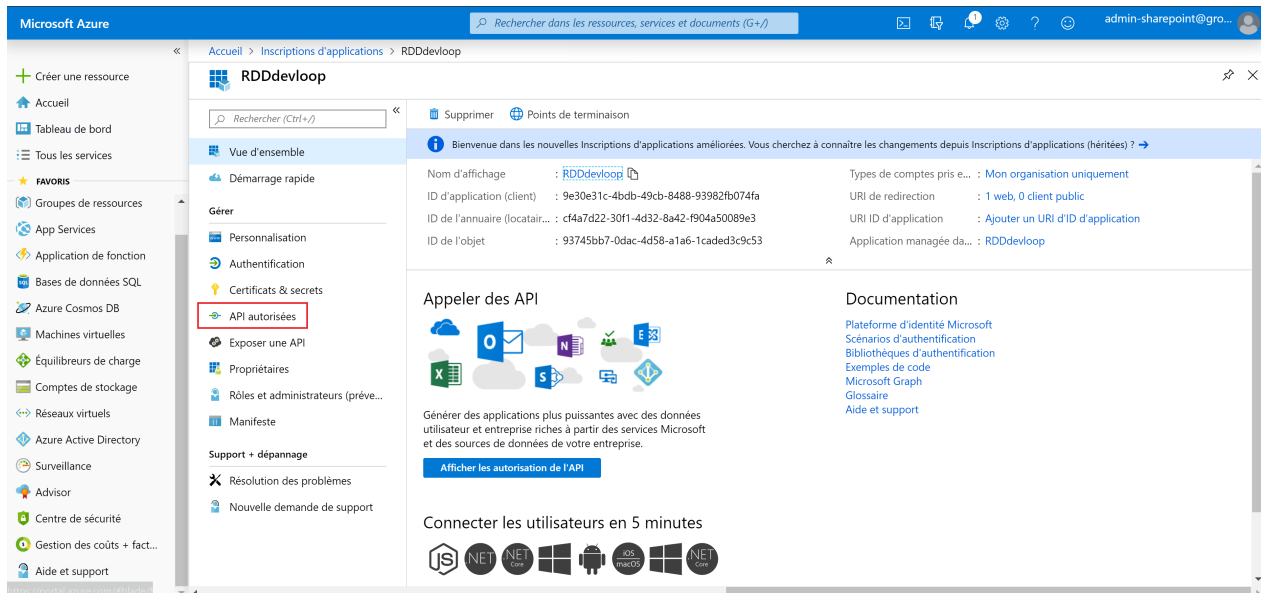
- **[Nom d'affichage côté utilisateur pour cette application]** : RDDdeveloop
- **[Type de compte pris en charge]** : Comptes dans cet annuaire d'organisation uniquement
- **[URI de redirection]** : <https://loop.loopsoftware.fr/YPN/>



6. Cliquez ensuite sur **<S'inscrire>**.

## Autoriser l'API Loop

1. Cliquez sur **[API autorisées]**.



2. Cliquez sur **<Ajouter une autorisation>**.

**API autorisées**

Les applications sont autorisées à appeler des API quand elles reçoivent des autorisations de la part des utilisateurs/administrateurs dans le cadre du processus de consentement. La liste des autorisations configurées doit comprendre toutes les autorisations dont l'application a besoin.

**+ Ajouter une autorisation**

API / NOMS DES AUTORISATIONS	TYPE	DESCRIPTION	CONSENTEMENT ADMINISTRAT...	STATUT
Microsoft Graph (1)				
User.Read	Déléguée	Sign in and read user profile	-	

Voici les autorisations que cette application requiert de manière statique. Vous pouvez également demander des autorisations avec consentement de manière dynamique par le biais du code. [Voir les meilleures pratiques pour la demande d'autorisations](#)

**Donner son consentement**

Ces autorisations ont été accordées pour HNOC mais ne figurent pas dans la liste des autorisations configurées. Si votre application requiert ces autorisations, vous devez envisager de les ajouter à la liste des autorisations configurées.

Accorder un consentement d'administrateur pour HNOC

3. Sélectionnez ensuite [API utilisées par mon organisation] puis recherchez Loop.

**Demander des autorisations d'API**

Sélectionner une API

API Microsoft Graph **API utilisées par mon organisation** Mes API

Les applications dans votre annuaire qui exposent les API sont indiquées ci-dessous

LOOP

NOM	ID D'APPLICATION (CLIENT)
Loop	ff28182b
LoopHub	410f64ab

4. Cliquez sur **Loop**.

5. Au niveau du bloc [Autorisations déléguées], cochez [user\_impersonation Access Loop] puis cliquer sur <Ajouter des autorisations>.

**Demander des autorisations d'API**

< Toutes les API

Loop  
https://loop.loopssoftware.fr

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

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

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

Sélectionner des autorisations développer tout

Entrer le texte à rechercher

AUTORISATION	CONSENTEMENT ADMINISTRATEUR REQUIS
<input checked="" type="checkbox"/> user_impersonation Access Loop	-

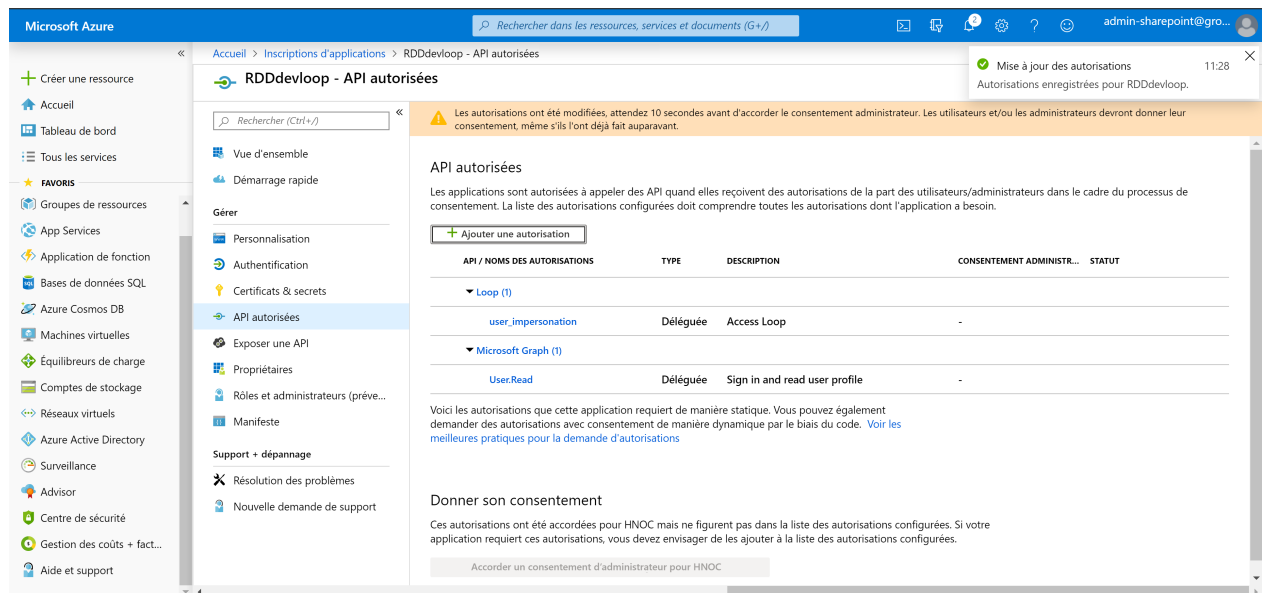
Donner son consentement

Ces autorisations ont été accordées pour HNOC mais ne figurent pas dans la liste des autorisations configurées. Si votre application requiert ces autorisations, vous devez envisager de les ajouter à la liste des autorisations configurées.

Accorder un consentement d'administrateur pour HNOC

**Ajouter des autorisations** Abandonner

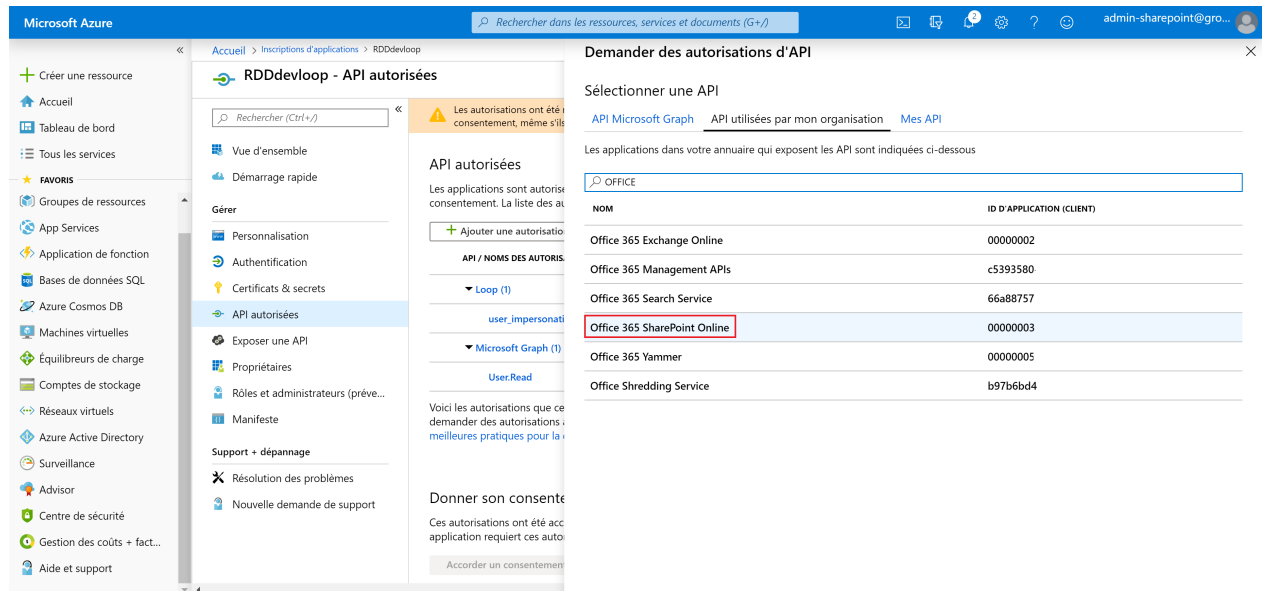
L'écran suivant apparaît :



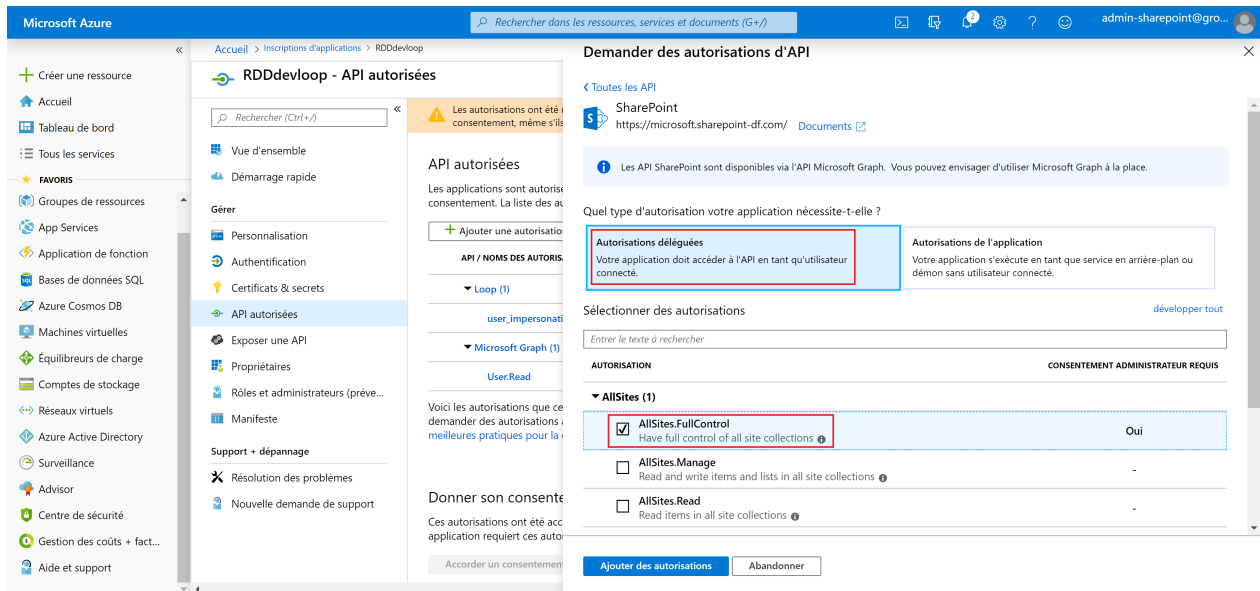
## Autoriser l'API SharePoint

De la façon que pour autoriser l'API Loop, ajoutez une nouvelle autorisation.

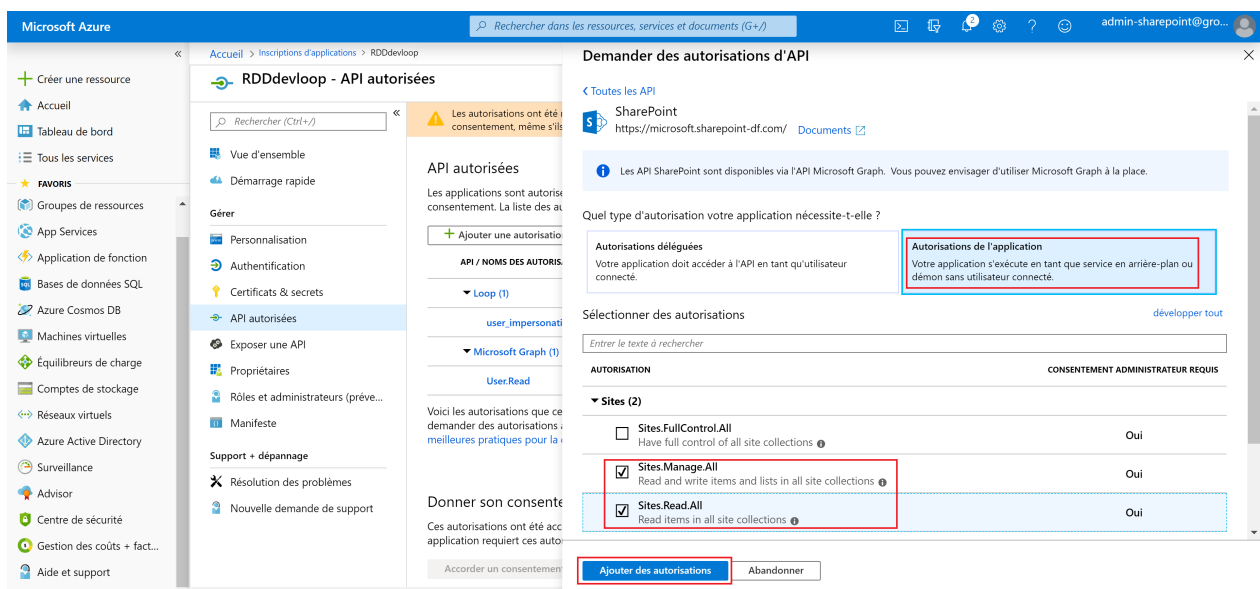
1. Cliquez sur **[API autorisées]**.
2. Cliquez sur **<Ajouter une autorisation>**.
3. Sélectionnez ensuite **[API utilisées par mon organisation]** puis recherchez Office 365 SharePoint Online.



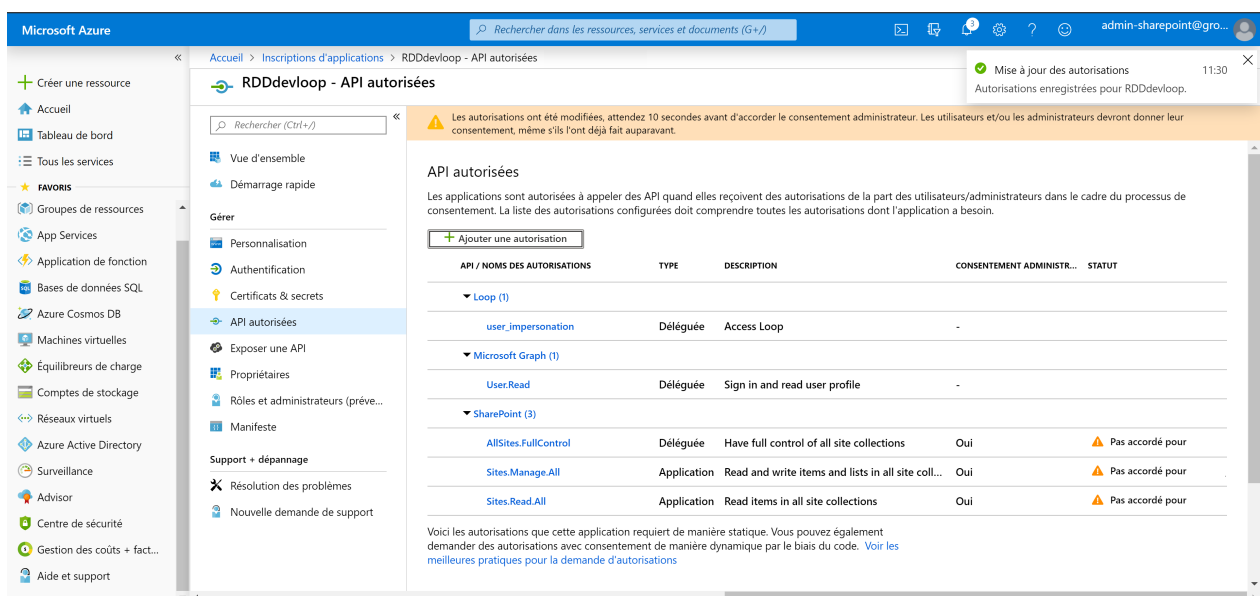
4. Cliquez sur **Office 365 SharePoint Online**.
5. Au niveau du bloc **[Autorisations déléguées]**, déroulez **[AllSites]** puis cochez **[AllSites.Fullcontrol]**.



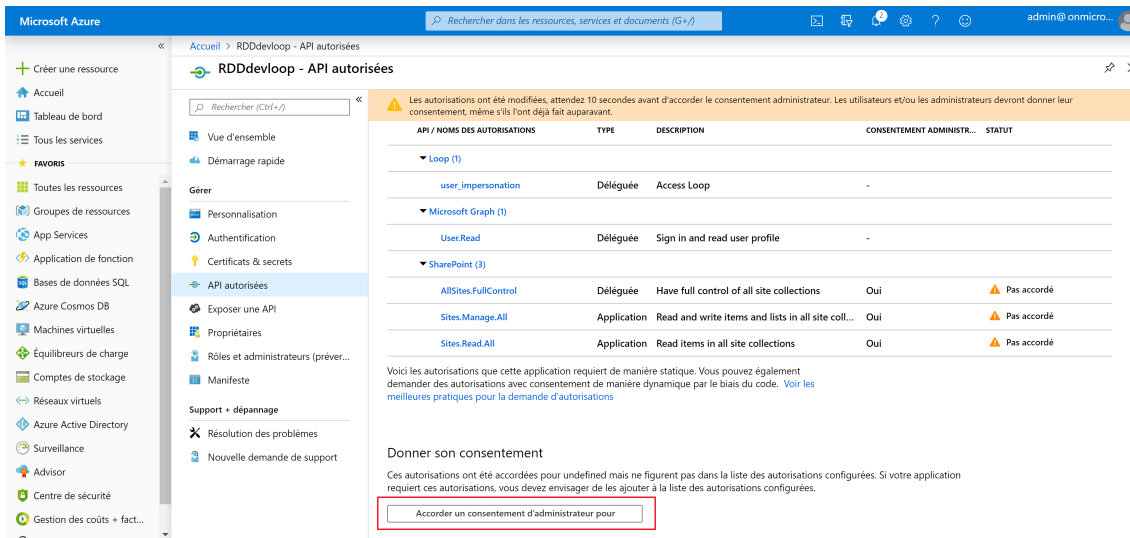
6. Au niveau du bloc [Autorisations de l'application], dérouler [Sites] puis cochez [Sites.Manage.All] et [Sites.Read.All].



7. Cliquez sur <Ajouter des autorisations>.

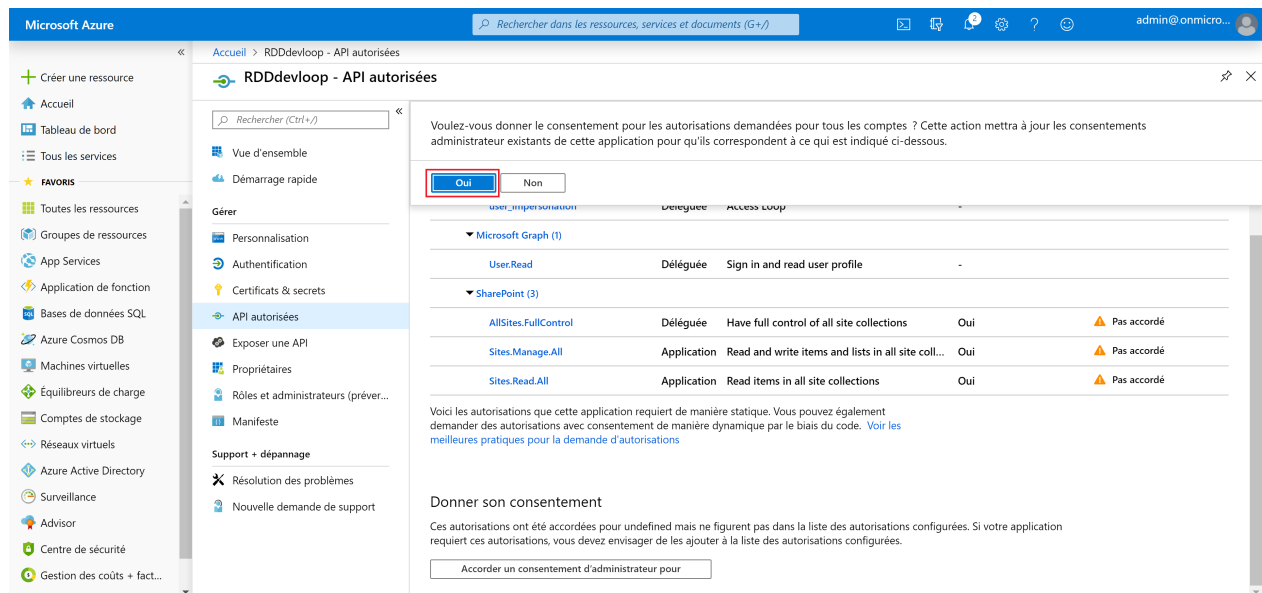


Accorder les autorisations



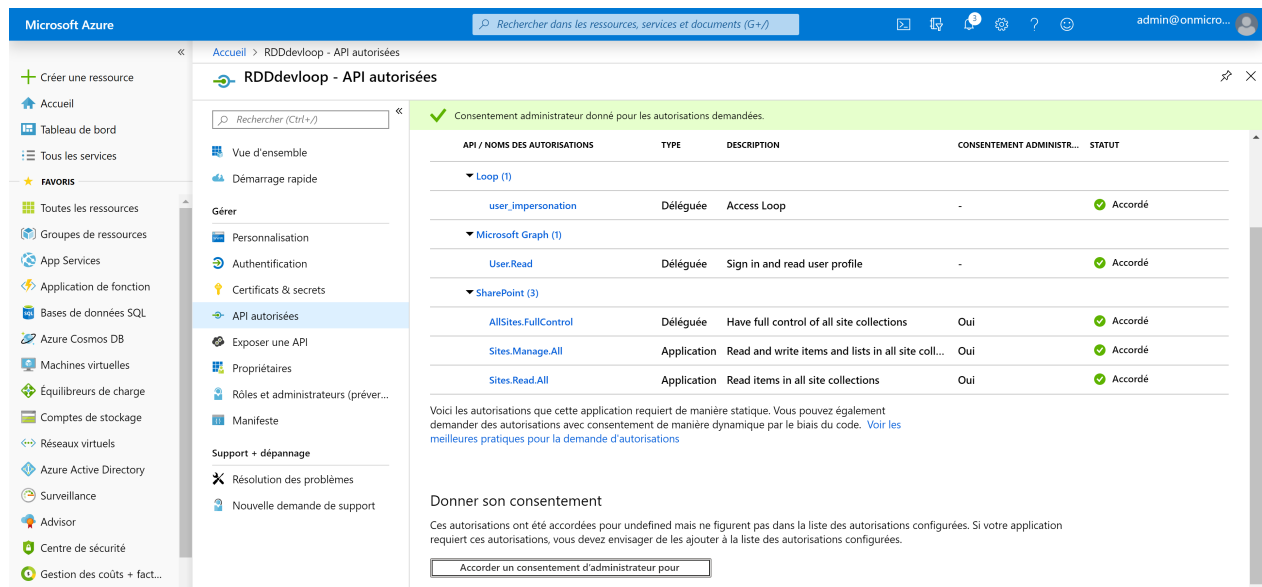
1. Cliquez ensuite sur **[Accorder le consentement administrateur pour...]**.

Le message suivant apparaît :



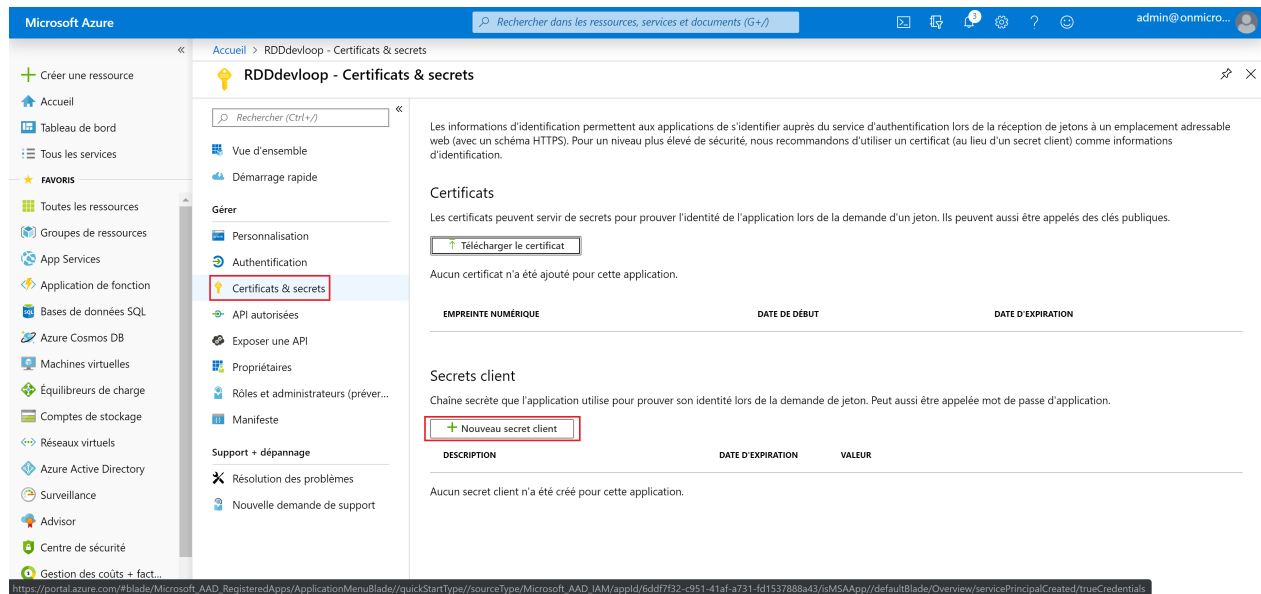
2. Cliquez sur **<Oui>**.

Le message de confirmation suivant apparaît :

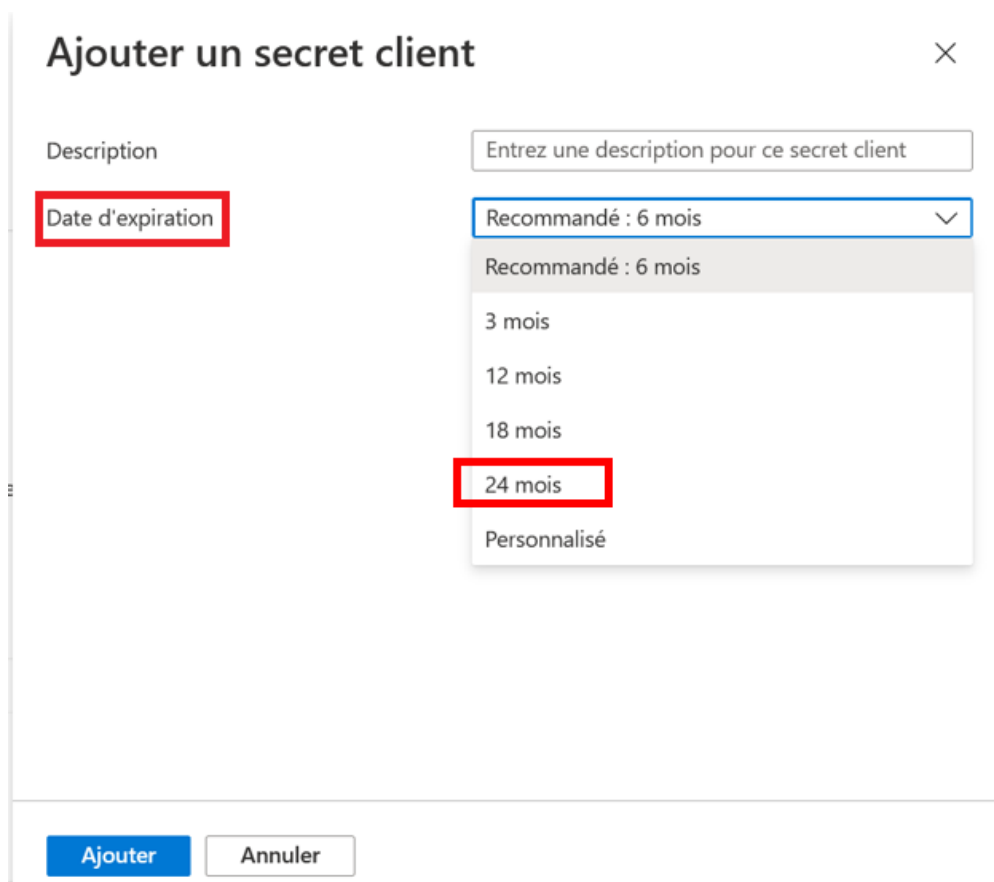


# Ajouter la clé "clientSecret"

1. Cliquez sur **[Certificats et secrets]** puis sur **[Nouveau secret client]**.



2. Nommez la clé en saisissant **RDDKEY** dans le champ **[Description]**.
3. Au niveau du champ **[Date d'expiration]**, sélectionnez **[ 24 mois]**.



4. Cliquez sur **<Ajouter>**.

La clé "clientSecret" est alors générée :

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

admin@onmicro...

Accueil > RDDdeveloop - Certificats & secrets

RDDdeveloop - Certificats & secrets

Rechercher (Ctrl+J)

Copiez la valeur du nouveau secret client. Vous ne pourrez plus la récupérer après avoir effectué une autre opération ou quitté ce panneau.

Les informations d'identification permettent aux applications de s'identifier auprès du service d'authentification lors de la réception de jetons à un emplacement adressable web (avec un schéma HTTPS). Pour un niveau plus élevé de sécurité, nous recommandons d'utiliser un certificat (au lieu d'un secret client) comme informations d'identification.

**Certificats**

Les certificats peuvent servir de secrets pour prouver l'identité de l'application lors de la demande d'un jeton. Ils peuvent aussi être appelés des clés publiques.

Télécharger le certificat

Aucun certificat n'a été ajouté pour cette application.

EMPREINTE NUMÉRIQUE	DATE DE DÉBUT	DATE D'EXPIRATION

**Secrets client**

Chaîne secrète que l'application utilise pour prouver son identité lors de la demande de jeton. Peut aussi être appelée mot de passe d'application.

Nouveau secret client

DESCRIPTION	DATE D'EXPIRATION	VALEUR
RDDKEY	31/12/2299	[Redacted]

Copier dans le Presse-papiers



Une fois cette étape passée la clé ne sera plus jamais consultable. Il est donc impératif de la récupérer (via l'outil **[Copier dans le Presse-papiers]** disponible à la droite de la clé) et de la conserver.

A noter qu'une nouvelle clé pourra être générée mais la première restera active.

## Ajouter l'URL de réponse de Loop

### 1. Cliquer sur **[Authentification]**.

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

admin@onmicro...

Accueil > RDDdeveloop - Authentification

RDDdeveloop - Authentification

Rechercher (Ctrl+J)

Enregistrer Abandonner Essayer la nouvelle expérience Des commentaires ?

**Authentification**

**URI de redirection**

URI que nous acceptons comme destinations lors du renvoi des réponses d'authentification (jetons) après l'authentification des utilisateurs. Ils sont aussi parfois appelés URL de réponse.

En savoir plus sur l'ajout de la prise en charge pour les clients web, mobiles et de bureau

TYPE	URI DE REDIRECTION
Web	https://loop.loopsoftware.fr/YPN/
Web	exemple : https://myapp.com/oauth

URI de redirection suggérées pour les clients publics (mobile, bureau)

Si vous utilisez la bibliothèque d'authentification Microsoft (MSAL) ou la bibliothèque d'authentification Active Directory (ADAL) afin de générer des applications pour des appareils mobiles ou de bureau, vous pouvez effectuer votre sélection parmi les URI de redirection suggérés ci-dessous ou entrer un URI de redirection personnalisé ci-dessus. Pour plus d'informations, consultez la documentation sur la bibliothèque.

msal6ddf7b32-c951-41af-a731-fd1537888a43://auth (MSAL uniquement)

https://login.microsoftonline.com/common/oauth2/nativeclient

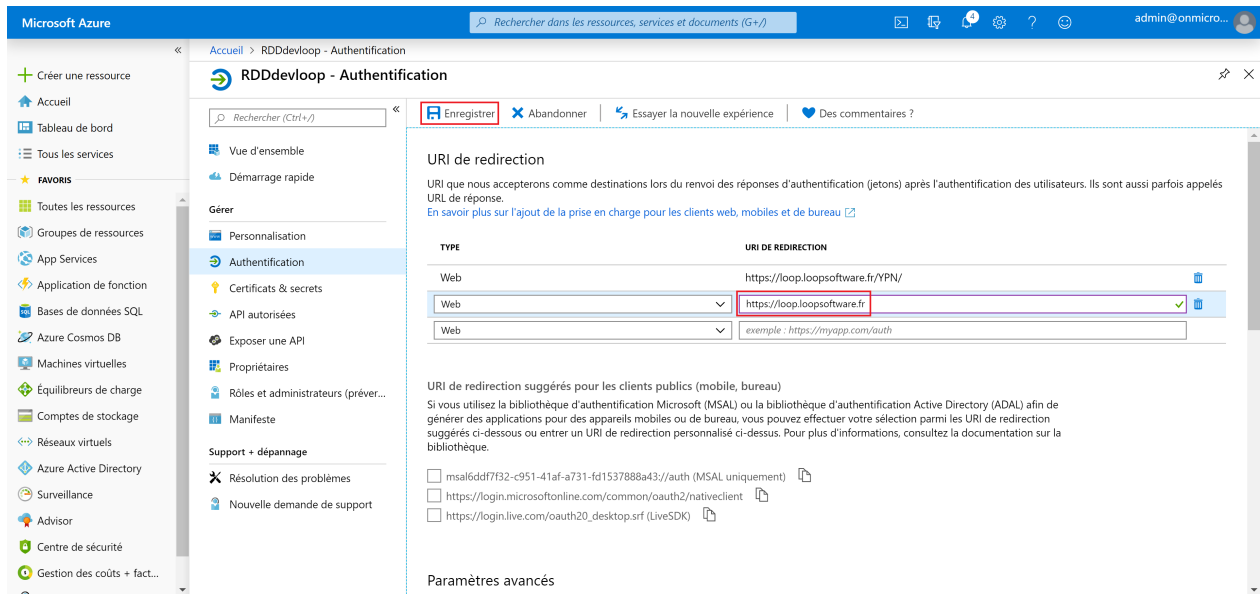
https://login.live.com/oauth20\_desktop.srf (LiveSDK)

Paramètres avancés

https://portal.azure.com/#blade/Microsoft\_AAD\_RegisteredApps/ApplicationMenuBlade/quickStartType/resourceType/Microsoft\_AAD\_IAM/appId/6ddf7b32-c951-41af-a731-fd1537888a43/overview/servicePrincipalCreated/true/Authentication

### 2. Ajouter une autre **[URL de redirection]** : `https://loop.loopsoftware.fr` puis cliquer sur **<Enregistrer>**.





### 3. Cliquer enfin sur [Vue d'ensemble].

Depuis cet écran, récupérer [ID d'application (client)]. Cet ID ainsi que la clé clientSecret générée précédemment seront utilisés lors d'une RDD, afin que les documents GED soient déposés dans les SharePoint correspondant à chaque dossier.

