

## Configurer l'application Promodag Reports dans Microsoft Entra ID

*Note : Cette procédure annule et remplace celle que nous avons publiée en novembre 2023. Si vous avez déjà publié votre application personnalisée dans Microsoft Entra ID (Azure AD) et qu'elle est toujours attribuée au rôle de lecteur général, passez directement à la page 3, **Si vous avez déjà créé l'application Promodag Reports et souhaitez lui accorder des autorisations minimales.***

Ce document décrit les étapes de la création et de la configuration de l'application "Promodag Reports RBAC Application" dans Microsoft Entra ID, ainsi que de son certificat, à l'aide du script PowerShell `CreateRepexRBACApp.ps1` pour activer l'authentification par certificat dans Office 365.


### Créer le certificat et l'application Promodag Reports

Veillez suivre ces étapes pour créer l'application Promodag Reports, certificat, les enregistrer dans Microsoft Entra ID et créer un groupe de rôles dédié dans le Centre d'administration Exchange :

#### Prérequis

La version du système d'exploitation de l'ordinateur doit être supérieure ou égale à Windows 10/Windows Server 2016. Microsoft PowerShell 7 ou supérieur est également requis.

Les modules PowerShell `ExchangeOnlineManagement` et `Microsoft.Graph` doivent être installés sur l'ordinateur. S'ils ne le sont pas, veuillez procéder comme suit :

1. Cliquez sur , recherchez PowerShell > Windows PowerShell 7 et exécutez-le en tant qu'administrateur.
2. Installez le module `ExchangeOnlineManagement` : [Install-Module ExchangeOnlineManagement -Scope AllUsers](#)
3. Installez le module `Microsoft.Graph` : [Install-Module Microsoft.Graph -Scope AllUsers](#)

### Créer le certificat et l'application avec le script fourni

Ces étapes vous permettront de créer un certificat auto-signé, une application dans Microsoft Entra ID pour accéder à votre tenant et un groupe de rôles dans le Centre d'administration Exchange.

1. Le script est livré par défaut dans le répertoire `C:\Users\Public\Documents\Promodag\Reports\`, mais vous pouvez l'utiliser à partir d'un autre emplacement.
2. Exécutez le script : `.\CreateRepexRBACApp.ps1`
3. Saisissez le mot de passe du certificat à l'invite et notez-le.
4. Le script se poursuit et vous êtes invité à vous connecter à Office 365 afin de créer le groupe de rôles et lui attribuer les autorisations idoines. Utilisez un compte d'administrateur général.
5. Un certificat valable 2 ans a été créé dans le répertoire de scripts sous le nom « `RepexRBACAppCertificate.pfx` ». L'application a été créée dans Microsoft Entra ID sous le nom de « Promodag Reports RBAC Application », un groupe de rôles nommé « Promodag Reports RBAC Role Group » a été créé dans Exchange Admin Center, un objet principal de service a été créé pour cette nouvelle application et il a été ajouté en tant que membre du nouveau groupe de rôles.
6. Le script affiche le résumé des informations à utiliser dans Promodag Reports : ID de l'application et chemin du certificat, ainsi qu'un lien (*Authorization URL*) permettant de se connecter à Microsoft Entra ID et d'autoriser l'application nouvellement créée. Ces informations sont ensuite enregistrées dans un fichier dans le répertoire actuel.

```
[INFO] Check Windows version: OK
[INFO] Check Microsoft Graph module: OK
[INFO] Check ExchangeOnlineManagement module: OK
Input certificate password, please: *****
[INFO] MS Graph connection established.
[INFO] Creating the client application (Promodag Reports RBAC Application)
[INFO] Creating the Service Principal for the client application (Promodag Reports RBAC Application)
[INFO] 'Administrator@promodagdev.onmicrosoft.com' added as an application owner to app 'Promodag Reports RBAC Application'
[INFO] Done creating the client application ()
[INFO] Getting API permissions for Microsoft Graph, Microsoft 365 Exchange Online, Microsoft 365 SharePoint Online
[INFO] Adding permissions.
[INFO] Please connect to Exchange Online.
[INFO] Exchange Online connection established.
[INFO] Role Group created.
[INFO] Service Principal created.
[INFO] Service Principal added to the Role Group.

-----
Your Promodag Reports application and certificate has been successfully generated.
-----

Tenant domain: promodag.dev
Tenant ID: 8b36c697-b53d-4f39-bea8-9b2b03000000
Application name: Promodag Reports RBAC Application
Application ID: 83b6c697-b53d-4f39-bea8-9b2b03000000
RoleGroup name: Promodag Reports RBAC Role Group
Service Principal name: SP for Promodag Reports RBAC Application
Certificate file: \ReperRBACAppCertificate.pfx
Certificate expiration: 06/06/2026 18:34:12

Copy the below URL and paste it into your browser to grant permission to the application:
URL: https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/CallAnAPI/appId/83b6c697-b53d-4f39-bea8-9b2b03000000/permissions/Exchange.ManageAsApp

A summary of these information has been saved in \ReperRBACAppCreation.log
```

## Autoriser cette nouvelle application dans Microsoft Entra ID

### Accorder le consentement administratif

1. Collez le lien affiché dans un navigateur web pour vous connecter à Microsoft Entra ID. Connectez-vous en utilisant un compte d'administrateur général. La page Promodag Reports RBAC Application | API autorisées s'ouvre.
2. Cliquez sur **Accorder un consentement d'administrateur pour <nom de votre tenant Office 365>**.
3. Examinez les autorisations accordées à l'application.

Utilisation	Autorisations requises	Description de l'autorisation
Importer les licences Office 365.	Microsoft Graph User.Read.All	Permet à l'application de lire l'ensemble des propriétés du profil, l'appartenance à des groupes, les rapports et les managers d'autres utilisateurs de votre organisation, sans que l'utilisateur soit connecté.
Exécuter les rapports sur le contenu des boîtes aux lettres et des dossiers publics.	Office 365 Exchange Online full_access_as_app	Permet à l'application d'avoir un accès complet à toutes les boîtes aux lettres via Exchange Web Services sans qu'un utilisateur ne soit connecté.
Importer l'annuaire, créer les fichiers de suivi des messages Office 365, importer la taille de stockage, exécuter les rapports sur les autorisations des boîtes aux lettres et des dossiers de boîtes aux lettres.	Office 365 Exchange Online Exchange.ManageAsApp	Permet à l'application de gérer l'environnement Exchange de l'organisation sans aucune interaction avec un utilisateur. Cela inclut les boîtes aux lettres, les groupes et d'autres objets de configuration. Pour activer les actions de gestion, un administrateur doit attribuer les rôles appropriés directement à l'application.
Publier des rapports dans une bibliothèque SharePoint Online	SharePoint Sites.Selected	Permettre à l'application d'accéder à un sous-ensemble de collections de sites sans qu'un utilisateur soit connecté. Les collections de sites spécifiques et les autorisations accordées seront configurées dans SharePoint Online.

Facultatif : vous pouvez supprimer le certificat auto-signé et utiliser votre propre certificat si vous le préférez. Consultez le fichier d'aide pour voir comment procéder.

## Appliquer les paramètres de "Promodag Reports RBAC Application" à Promodag Reports

Assurez-vous d'avoir récupéré les informations suivantes lors de la première étape :

- ID de l'application,
  - Chemin du certificat,
  - Mot de passe du certificat.
1. Dans Promodag Reports, allez dans **Outils > Options, Configuration Office 365**.
  2. Sélectionnez Authentification par certificat.
  3. Saisissez l'ID de l'application, le chemin d'accès au fichier du certificat et le mot de passe du certificat dans les champs correspondants.
  4. Cliquez sur le lien [Vérifier la validité](#) pour vérifier la date d'expiration du certificat.
  5. Cliquez sur les liens [Vérifier la connexion](#) pour vérifier que Promodag Reports peut se connecter à votre tenant à l'aide de l'application Microsoft Entra ID et du certificat.

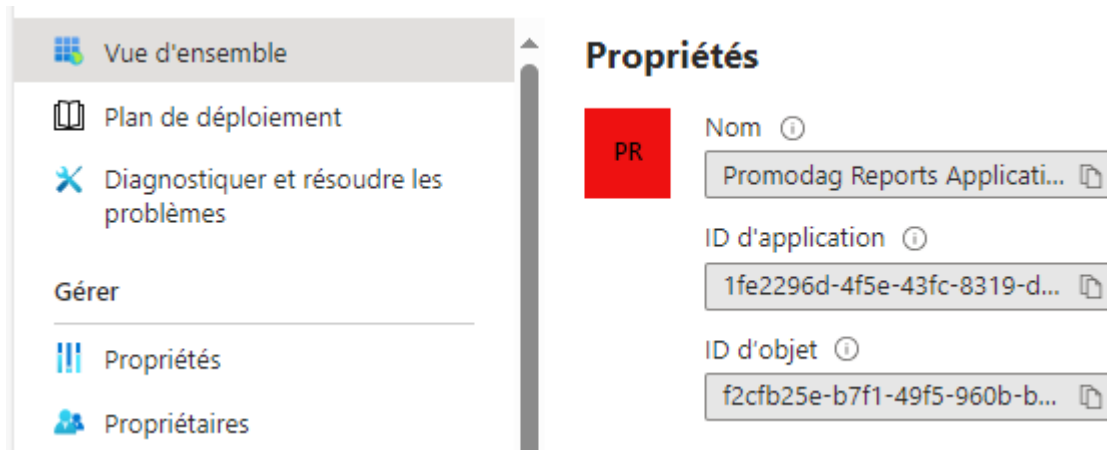
Si vous avez déjà créé l'application Promodag Reports et souhaitez lui accorder des autorisations minimales

### Étape 1 Supprimer le rôle de lecteur général

1. Ouvrez le portail Azure AD à l'adresse <https://portal.azure.com/>.
2. Sous Gérer Microsoft Entra ID, cliquez sur **Vue**.
3. Sur la page de vue d'ensemble qui s'ouvre, sous **Gérer**, sélectionnez Rôles et administrateurs.
4. Dans le champ de recherche, entrez le nom du rôle Lecteur général.
5. Sélectionnez le rôle Lecteur général.
6. Supprimer l'application Promodag Reports des affectations.

### Étape 2 : Récupérer les identifiants de l'application Promodag Reports Microsoft Entra ID

1. Ouvrez le portail Azure AD à l'adresse <https://portal.azure.com/>.
2. Sous Gérer Microsoft Entra ID, cliquez sur **Vue**.
3. Sur la page de vue d'ensemble qui s'ouvre, sous **Gérer**, sélectionnez Applications d'entreprise.
4. Décochez Type d'application ==**Applications d'entreprise** à côté du champ Rechercher par nom d'application.
5. Dans le champ de recherche, saisissez le nom de l'application Promodag Reports personnalisée existante (par défaut : « Promodag Reports Application »).
6. Dans Propriétés, notez l'ID de l'application et l'ID de l'objet. Ces informations seront utilisées ultérieurement.



### Étape 3 : Créer un groupe de rôles Exchange Admin pour Promodag Reports

1. Allez dans le Centre d'administration Microsoft 365, Centre d'administration Exchange.
2. Développez Rôles sur la gauche et cliquez sur Rôles d'administrateur.
3. Cliquez sur Ajouter un groupe de rôles.
4. Dans la fenêtre Nouveau groupe de rôles qui s'affiche, saisissez « Groupe de rôles Promodag Reports » comme nom du groupe de rôles ainsi qu'une description.
5. Cliquez sur **Suivant**.
6. Dans la fenêtre Ajouter des autorisations, sélectionnez Destinataires en visualisation seule et Destinataires du courrier.
7. Cliquez sur **Suivant**.
8. L'affectation des groupes de rôles sera effectuée à l'étape suivante. Cliquez donc à nouveau sur Suivant puis sur Ajouter un groupe de rôles pour créer le groupe de rôles.

### Étape 4 : Créer l'attribution d'un rôle de gestion

Dans une fenêtre PowerShell 7, connectez-vous à Exchange Online PowerShell.

*Créez un objet principal de service pour l'application Promodag Reports Microsoft Entra ID*  
`$SP = New-ServicePrincipal -AppId <appId de l'étape 6> -ObjectId <Object id de l'étape 6> -  
DisplayName « SP pour l'application Promodag Reports »`

*Ajouter le principal de service en tant que membre du groupe de rôles personnalisé :*  
`Add-RoleGroupMember -Identity «Groupe de rôles Promodag Reports» -Member $SP.Identity`

Suivez ensuite les instructions données ci-dessus dans **Appliquer les paramètres de « Promodag Reports RBAC Application » à Promodag Reports**.