Configuring the Promodag Reports Application in Microsoft Entra ID

*Note: This procedure cancels and replaces the one we published in November 2023. If you have already published your custom application in Microsoft Entra ID (Azure AD) and it is still assigned to the Global Reader role, go directly to page 3, **If you have already created the Promodag Reports application**.*

This document describes the steps involved in creating and configuring the "Promodag Reports RBAC Application" in Microsoft Entra ID, along with its certificate, using the CreateRepexRBACApp.ps1 PowerShell script to enable certificate-based authentication to Office 365.

Create the certificate and the Promodag Reports Application

Please follow these steps to create the Promodag Reports Application, the certificate, register them in Microsoft Entra ID and create a dedicated role group in Exchange Admin Center:

Prerequisites

The computer's operating version must be greater than or equal to Windows 10/Windows Server 2016. Microsoft PowerShell 7 or higher is required.

The ExchangeOnlineManagement and Microsoft.Graph PowerShell modules should be installed on the computer. It they are not, please proceed with these steps:

1. Click ▦ and search for PowerShell > Windows PowerShell 7 and run it as administrator.
2. Install the ExchangeOnlineManagement module: Install-Module ExchangeOnlineManagement -Scope AllUsers
3. Install the Microsoft.Graph module: Install-Module Microsoft.Graph -Scope AllUsers

Create the certificate and application using the provided script

These steps will enable you to create a self-signed certificate, an application in Microsoft Entra ID to access your tenant, and a role group in Exchange Admin Center.

1. The script is delivered by default in the C:\Users\Public\Documents\Promodag\Reports\ directory but you can use it from a different location.
2. Run the script: .\CreateRepexRBACApp.ps1
3. Enter certificate password at prompt and write it down.
4. The script will proceed, and you will be prompted to sign-in to Office 365 to create the role group and grant it the relevant permissions. Use a Global Administrator account.
5. A certificate valid for two years has now been created in the script directory with the name " RepexRBACAppCertificate.pfx". The application has been created in Microsoft Entra ID with the name "Promodag Reports RBAC Application", a role group with the name "Promodag Reports RBAC Role Group" has been created in Exchange Admin Center, a service principal object has been created for this new application and it has been added as a member of this new role group.
6. The script displays the summary information to be used in Promodag Reports: Application ID and certificate path, plus a link (*Authorization URL*) to connect to Microsoft Entra ID and authorize the newly created application. This information is then saved into a file in the current directory.

Authorize this new application in Microsoft Entra ID

Grant admin consent

1. Paste the URL displayed in a web browser to connect to Microsoft Entra ID. Sign in using a Global Administrator account. The Promodag Reports RBAC Application | API permissions page opens.
2. Click **Grant admin consent for <name of your Office 365 tenant>**.
3. Review the permissions granted to the application.

What for?	Required permissions	Permission description
Import Office 365 licenses.	Microsoft Graph User.Read.All	Allows the application to read the full set of profile properties, group membership, reports and managers of other users in your organization, without a signed-in user.
Import group members faster than with PowerShell.	Microsoft Graph Group.Read.All	Allows the application to list groups, and to read their properties and all group memberships on behalf of the signed-in user. Also allows the app to read calendar, conversations, files, and other group content for all groups the signed-in user can access.
Run reports on mailbox and public folder content.	Office 365 Exchange Online full_access_as_app	Allows the application to have full access via Exchange Web Services to all mailboxes without a signed-in user.
Import the directory, create Office 365 message tracking files, import the storage size, Run reports on mailbox and mailbox folder permissions.	Office 365 Exchange Online Exchange.ManageAsApp	Allows the application to manage the organization's Exchange environment without any user interaction. This includes mailboxes, groups, and other configuration objects. To enable management actions, an admin must assign the appropriate roles directly to the app.
Publish reports onto a SharePoint Online library.	SharePoint Sites.Selected	Allows the application to access a subset of site collections without a signed in user. The specific site collections and the permissions granted will be configured in SharePoint Online.

Optional: You can delete the self-signed certificate and use your own if you prefer. See the help file, Replace or renew the certificate.

Apply "Promodag Reports RBAC Application" settings to Promodag Reports

Please make sure that you have retrieved the following information the first step:

- Application ID,
- Certificate path,
- Certificate password.

1. In Promodag Reports, go to **Tools > Options**, *Office 365 configuration*.
2. Select Certificate-based authentication.
3. Enter the Application ID, Certificate file path and Certificate password in the corresponding fields.
4. Click the Check validity link to verify the certificate expiration date.
5. Click the Check connection links to verify that Promodag Reports can connect to your tenant using the Microsoft Entra ID application and the certificate.

If you have already created the Promodag Reports application and wish to grant it minimum permissions

Prerequisites

The computer's operating version must be greater than or equal to Windows 10/Windows Server 2016. Microsoft PowerShell 7 or higher is required.

The ExchangeOnlineManagement and Microsoft.Graph PowerShell modules should be installed on the computer. It if is not, please proceed with these steps:

1. Click ⊞ and search for PowerShell > Windows PowerShell 7 and run it as administrator.
2. Install the ExchangeOnlineManagement module: Install-Module ExchangeOnlineManagement -Scope AllUsers
3. Install the Microsoft.Graph module: Install-Module Microsoft.Graph -Scope AllUsers

Step 1 Remove the Global Reader role

1. Open the Azure AD portal at https://portal.azure.com/.
2. Under Manage Microsoft Entra ID, click **View**.
3. On the Overview page that opens, under Manage, select **Roles and administrators**.
4. In the search field, enter the name of the Global Reader role.
5. Select the Global Reader role.
6. Remove the Promodag Reports Application from the assignments.

Step 2: Retrieve the Promodag Reports Microsoft Entra ID application identifiers

1. Open the Azure AD portal at https://portal.azure.com/.
2. Under Manage Microsoft Entra ID, click **View**.
3. On the Overview page that opens, under Manage, select **Enterprise applications**.
4. Uncheck Application type ==**Enterprise Applications** next to the Search by application name field.
5. In the search field, enter the name of the existing custom Promodag Reports application (default: "Promodag Reports Application").
6. In Properties, write down the Application ID and Object ID. This will be used later.
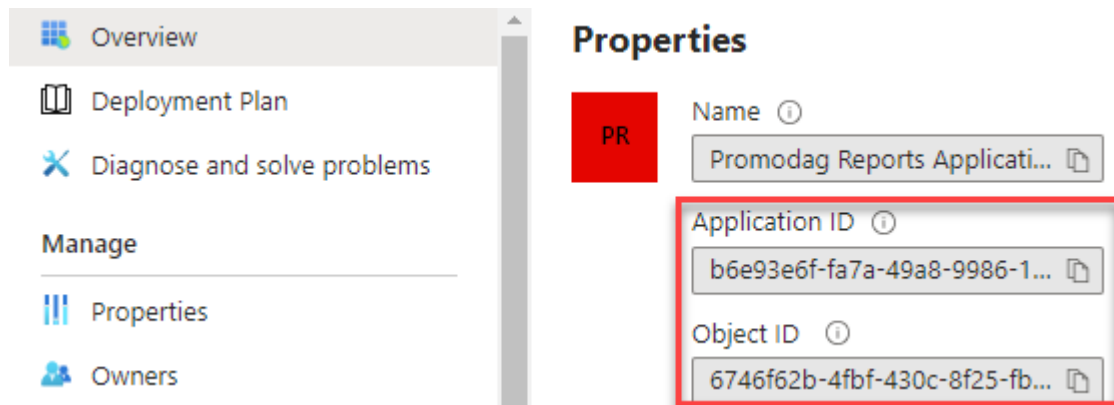
Step 3: Create an Exchange Admin role group for Promodag Reports

1. Go to Microsoft 365 admin center, Exchange admin center.
2. Expand Roles on the left and click Admin roles.
3. Click Add role group.
4. In the New role group window that appears, enter "Promodag Reports role group" as the name of the role group along with a description.
5. Click **Next**.
6. In the Add permissions window, select View-Only Recipients and Mail Recipients.
7. Click **Next**.
8. Role group assignment will be performed in the next step. So, click **Next** again then **Add role group** to create the Role group.

Step 4: Create Management Role Assignment

In a PowerShell 7 window, connect to Exchange Online PowerShell.

Create a service principal object for the Promodag Reports Microsoft Entra ID application
$SP = New-ServicePrincipal -AppId <appId from step 2> -ObjectId <Object id from step 2> -DisplayName "SP for Promodag Reports Application"

Add the service principal as a member of the custom role group:
Add-RoleGroupMember -Identity "Promodag Reports role group" -Member $SP.Identity

Then follow the instructions given above in *Apply "Promodag Reports RBAC Application" settings to Promodag Reports*.