

Einstellung der Promodag-Berichts-anwendung in Microsoft Entra ID

*Hinweis: Dieses Verfahren annulliert und ersetzt das im November 2023 veröffentlichte Verfahren. Wenn Sie Ihre benutzerdefinierte Anwendung bereits in Microsoft Entra ID (Azure AD) veröffentlicht haben und sie noch der Rolle Global Leser zugewiesen ist, gehen Sie direkt zu Seite 3, **Wenn Sie die Anwendung Promodag Reports bereits erstellt haben**.*

In diesem Dokument werden die Schritte beschrieben, die zum Erstellen und Konfigurieren der "Promodag Reports RBAC Application" in Azure sowie ihres Zertifikats mithilfe des PowerShell-Skripts CreateRepexRBACApp.ps1 erforderlich sind, um die zertifikatsbasierte Authentifizierung bei Office 365 zu aktivieren.

Das Zertifikat und die Promodag Reports-Anwendung erstellen

Bitte folgen Sie diesen Schritten, um die Promodag Reports Application und das Zertifikat zu erstellen und in Microsoft Entra ID zu registrieren:

Voraussetzungen

Die Mindestversion des Betriebssystems, die für diese Vorgänge erforderlich ist, ist Windows 10/Windows Server 2016. Microsoft PowerShell 7 oder höher ist erforderlich.

Die Module ExchangeOnlineManagement und Microsoft.Graph PowerShell sollten auf dem Computer installiert sein. Ist dies nicht der Fall, fahren Sie bitte mit diesen Schritten fort:

1. Klicken Sie auf  und suchen Sie nach PowerShell > Windows PowerShell 7 und führen Sie es als Administrator aus.
2. Installieren Sie das ExchangeOnlineManagement-Modul: [Install-Module ExchangeOnlineManagement -Scope AllUsers](#)
3. Installieren Sie das Microsoft.Graph-Modul: [Install-Module Microsoft.Graph -Scope AllUsers](#)

Das Zertifikat und die Anwendung mithilfe des mitgelieferten Skripts erstellen

Mit diesen Schritten können Sie ein selbstsigniertes Zertifikat sowie eine Anwendung namens "Promodag Reports RBAC Application" in Microsoft Entra ID erstellen, um auf Ihren Mandanten zuzugreifen. Auch im Exchange Admin Center wird eine Rollengruppe erstellt.

1. Das Skript wird standardmäßig im Verzeichnis C:\Users\Public\Documents\Promodag\Reports\ ausgeliefert, aber Sie können es auch an einem anderen Ort verwenden.
2. Führen Sie das Skript aus: `.\ CreateRepexRBACApp.ps1`
3. Geben Sie das Zertifikatspasswort an der Eingabeaufforderung ein und notieren Sie es.
4. Das Skript wird ausgeführt, und Sie werden aufgefordert, sich bei Office 365 anzumelden, um die Rollengruppe zu erstellen und ihr die entsprechenden Berechtigungen zu erteilen. Verwenden Sie ein globales Administratorkonto.
5. Im Skriptverzeichnis wurde nun ein für 2 Jahre gültiges Zertifikat mit dem Namen "RepexAppRBACCertificate.pfx" erstellt. Die Anwendung wurde in Microsoft Entra ID mit dem Namen „Promodag Reports RBAC Application“ erstellt, eine Rollengruppe mit dem Namen „Promodag Reports RBAC Role Group“ wurde im Exchange Admin Center erstellt, ein Dienstprinzipalobjekt wurde für diese neue Anwendung erstellt und sie wurde als Mitglied dieser neuen Rollengruppe hinzugefügt.
6. Das Skript zeigt die zusammenfassenden Informationen an, die in Promodag Reports verwendet werden sollen: Anwendungs-ID und Zertifikatsdateipfad, sowie einen Link

(*Authorization URL*), um sich mit Microsoft Entra ID zu verbinden und die neu erstellte Anwendung zu autorisieren. Diese Informationen werden dann in einer Datei im aktuellen Verzeichnis gespeichert.

```
[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: 71a1b11e-1a11-4a11-8a11-1a1111111111
Application name: Promodag Reports RBAC Application
Application Id: 038e097f-3b3d-4f29-baaa-1a1111111111
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 10:04:12

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/e786097f-3b3d-4f29-baaa-1a1111111111/tenantId/71a1b11e-1a11-4a11-8a11-1a1111111111/App/

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

Diese neue Anwendung in Microsoft Entra ID autorisieren

Administratorzustimmung erteilen

1. Fügen Sie den angezeigten Link in einen Webbrowser ein, um sich mit Microsoft Entra ID zu verbinden. Melden Sie sich mit einem globalen Administratorkonto an Die Seite Promodag Reports RBAC Application | API-Berechtigungen wird geöffnet.
2. Klicken Sie auf Admininstratorzustimmung für <Name Ihres Office 365-Mandanten> erteilen.
3. Überprüfen Sie die der Anwendung gewährten Berechtigungen.

Wozu?	Erforderliche Berechtigungen	Beschreibung der Berechtigung
Office 365-Lizenzen importieren.	Microsoft Graph User.Read.All	Ermöglicht es der Anwendung, alle Profileigenschaften, Gruppenmitgliedschaften, Berichte und Manager anderer Benutzer in Ihrer Organisation zu lesen, ohne dass ein angemeldeter Benutzer erforderlich ist.
Gruppenmitglieder schneller als mit PowerShell importieren.	Microsoft Graph Group.Read.All	Ermöglicht es der Anwendung, Gruppen aufzulisten und ihre Eigenschaften und alle Gruppenmitgliedschaften im Namen des angemeldeten Benutzers zu lesen. Außerdem kann die Anwendung Kalender, Unterhaltungen, Dateien und andere Gruppeninhalte für alle Gruppen lesen, auf die der angemeldete Benutzer zugreifen kann.
Berichte über den Inhalt von Postfächern und öffentlichen Ordnern erstellen.	Office 365 Exchange Online full_access_as_app	Ermöglicht der Anwendung den vollen Zugriff über Exchange Web Services auf alle Postfächer, ohne dass ein angemeldeter Benutzer erforderlich ist.

<p>Das Verzeichnis importieren, Office 365-Nachrichtenverfolgungsdateien erstellen, die Speichergröße importieren, Berichte über Postfach- und Postfachordnerberechtigungen ausführen.</p>	<p>Office 365 Exchange Online Exchange.ManageAsApp</p>	<p>Ermöglicht der Anwendung die Verwaltung der Exchange-Umgebung des Unternehmens ohne jegliche Benutzerinteraktion. Dazu gehören Postfächer, Gruppen und andere Konfigurationsobjekte. Um Verwaltungsaktionen zu aktivieren, muss ein Administrator der Anwendung die entsprechenden Rollen direkt zuweisen.</p>
<p>Berichte in einer SharePoint Online-Bibliothek veröffentlichen.</p>	<p>SharePoint Sites.Selected</p>	<p>Ermöglicht der Anwendung den Zugriff auf eine Untergruppe von Websitesammlungen ohne einen angemeldeten Benutzer. Die spezifischen Websitesammlungen und die gewährten Berechtigungen werden in SharePoint Online konfiguriert.</p>

Optional: Sie können das selbstsignierte Zertifikat löschen und Ihr eigenes verwenden, wenn Sie dies wünschen. Lesen Sie in der Hilfedatei nach, wie Sie das Zertifikat ersetzen oder erneuern können.

Die Einstellungen von "Promodag Reports RBAC Application" auf Promodag Reports anwenden

Bitte vergewissern Sie sich, dass Sie die folgenden Informationen im ersten Schritt abgerufen haben:

- Anwendungs-ID,
 - Pfad der Zertifikatsdatei,
 - Passwort für das Zertifikat.
1. Gehen Sie in Promodag Reports auf **Extras > Optionen**, Office 365 Konfiguration.
 2. Wählen Sie Zertifikatsbasierte Authentifizierung.
 3. Geben Sie die Anwendungs-ID, den Pfad der Zertifikatsdatei und das Zertifikatspasswort in die entsprechenden Felder ein.
 4. Klicken Sie auf den Link [Gültigkeit prüfen](#), um das Ablaufdatum des Zertifikats zu überprüfen.
 5. Klicken Sie auf die Links [Verbindung überprüfen](#), um zu bestätigen, ob Promodag Reports eine Verbindung zu Ihrem Tenant mit der Azure-Anwendung und dem Zertifikat herstellen kann.

Wenn Sie die Anwendung Promodag Reports bereits erstellt haben und ihr minimale Berechtigungen erteilen möchten

Voraussetzungen

Die Mindestversion des Betriebssystems, die für diese Vorgänge erforderlich ist, ist Windows 10/Windows Server 2016. Microsoft PowerShell 7 oder höher ist erforderlich.

Die Module ExchangeOnlineManagement und Microsoft.Graph PowerShell sollten auf dem Computer installiert sein. Ist dies nicht der Fall, fahren Sie bitte mit diesen Schritten fort:Klicken Sie auf [PowerShell](#) und suchen Sie nach PowerShell > Windows PowerShell und führen Sie es als Administrator aus.

1. Klicken Sie auf  und suchen Sie nach PowerShell > Windows PowerShell 7 und führen Sie es als Administrator aus.
2. Installieren Sie das ExchangeOnlineManagement-Modul: [Install-Module ExchangeOnlineManagement -Scope AllUsers](#)
3. Installieren Sie das Microsoft.Graph-Modul: [Install-Module Microsoft.Graph -Scope AllUsers](#)

Schritt 1 Entfernen Sie die Rolle Globaler Leser

1. Öffnen Sie das Azure AD-Portal unter <https://portal.azure.com/>.
2. Klicken Sie unter Verwalten von Microsoft Entra ID auf **Sicht**.
3. Wählen Sie auf der sich öffnenden Übersichtsseite unter **Verwalten** die Option Rollen und Administratoren.
4. Geben Sie in das Suchfeld den Namen der Rolle Globaler Leser ein.
5. Wählen Sie die Rolle Globaler Leser aus.
6. Entfernen Sie die Anwendung Promodag Reports aus den aktiven Zuweisungen.

Schritt 2: Abrufen der Promodag Reports Microsoft Entra ID Anwendungskennungen

1. Öffnen Sie das Azure AD Portal unter <https://portal.azure.com/>.
2. Klicken Sie unter Manage Microsoft Entra ID auf **Sicht**.
3. Wählen Sie auf der sich öffnenden Übersichtsseite unter **Verwalten** die Option Unternehmensanwendungen.
4. Deaktivieren Sie das Kontrollkästchen Anwendungstyp ==Unternehmensanwendungen neben dem Feld Nach Anwendungsname oder Object-ID suchen.
5. Geben Sie in das Suchfeld den Namen der vorhandenen benutzerdefinierten Promodag Reports-Anwendung ein (Standard: „Promodag Reports Application“).
6. Notieren Sie unter Eigenschaften die Anwendungs- und Objekt-ID. Diese werden später verwendet.



Schritt 3: Erstellen Sie eine Exchange-Admin-Rollengruppe für Promodag Reports

1. Gehen Sie zu Microsoft 365 Admin Center, Exchange Admin Center.
2. Erweitern Sie **Rollen** auf der linken Seite und klicken Sie auf Admin-Rollen.
3. Klicken Sie auf Rollengruppe hinzufügen.
4. Geben Sie im erscheinenden Fenster Neue Rollengruppe den Namen der Rollengruppe „Promodag Reports Rollengruppe“ und eine Beschreibung ein.
5. Klicken Sie auf **Weiter**.

6. Wählen Sie im Fenster Berechtigungen hinzufügen die Optionen Nur-Ansicht-Empfänger und Mail-Empfänger.
7. Klicken Sie auf **Weiter**.
8. Die Zuweisung der Rollengruppe wird im nächsten Schritt durchgeführt. Klicken Sie also erneut auf **Weiter** und dann auf **Rollengruppe hinzufügen**, um die Rollengruppe zu erstellen.

Schritt 4: Verwaltungsrollenzuweisung erstellen

Erstellen Sie ein Dienstprinzipalobjekt für die Promodag Reports Microsoft Entra ID- Anwendung
\$SP = New-ServicePrincipal -AppId <appId aus Schritt 2> -ObjectId <Object id aus Schritt 2> -
DisplayName „SP for Promodag Reports Application“

Fügen Sie den Dienstprinzipal als Mitglied der benutzerdefinierten Rollengruppe hinzu
Add-RoleGroupMember -Identity „Promodag Reports role group“ -Member \$SP.Identity

Folgen Sie dann den Anweisungen, die oben unter **Die Einstellungen von "Promodag Reports RBAC Application auf Promodag Reports anwenden** angegeben sind.