ELO Sync

Registrierung in Azure

Inhaltsverzeichnis

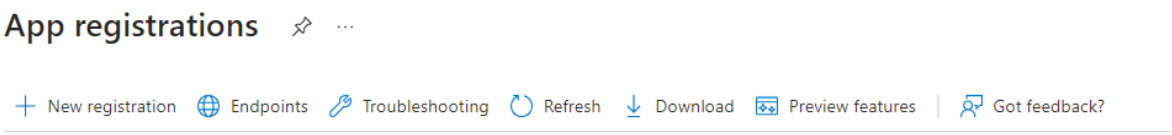
ELO Sync in Azure

Dieses Kapitel beschreibt die Registrierung von ELO Sync bei Azure. Diese Aktionen sind für die Authentifizierung mit Microsoft Entra und den Zugriff auf Microsoft 365-Ressourcen erforderlich.

In unserer Anleitung ist ELO Sync unter der URL *https://elo-sync.local/* zu erreichen und wird als *ELOSyncApp* registriert, ersetzen Sie diese nach Bedarf.

1. Erstellen Sie eine neue App-Registrierung im Azure Management Portal.

   Navigieren Sie zu App registrations, und klicken Sie dann auf *New registration*.

2. Geben Sie die erforderlichen Informationen über die neue Anwendung ein.

   1. Geben Sie den Name *EloSyncApp* als Namen für die Anwendung ein (oder wählen Sie einen eigenen Namen).
   2. Bei den supported account types müssen Sie in der Regel *Accounts in this organizational directory only (Single tenant)* auswählen, je nach Struktur Ihrer Organisation könnte es auch die zweite Option *Multitenant* sein.
   3. Wählen Sie unter Redirect URI die Plattform *Web* und geben Sie *https://elo-sync.local/signin-oidc-custom* ein.

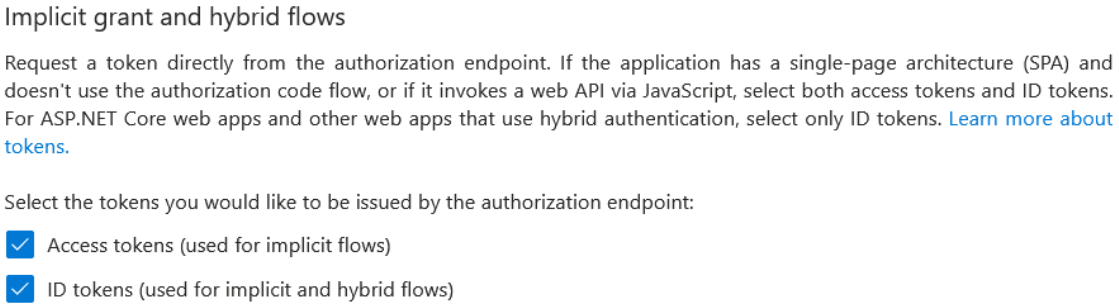
      > **Information**
      >
      > Der Pfad `/signin-oidc-custom`kann in der Datei *appsettings.json* geändert werden. Siehe Konfiguration für weitere Informationen.

   4. Bestätigen Sie die Informationen und erstellen Sie die App-Registrierung.

3. Wenn Sie gerade die Datei appsettings.json bearbeiten, gehen Sie zu *Overview* der Anwendung und kopieren Sie die Informationen `ClientId` und `TenantId` hinein.

4. Öffnen Sie die neu erstellte Anwendung *ELOSyncApp* und wählen Sie dann den Menüpunkt *Authentication*.

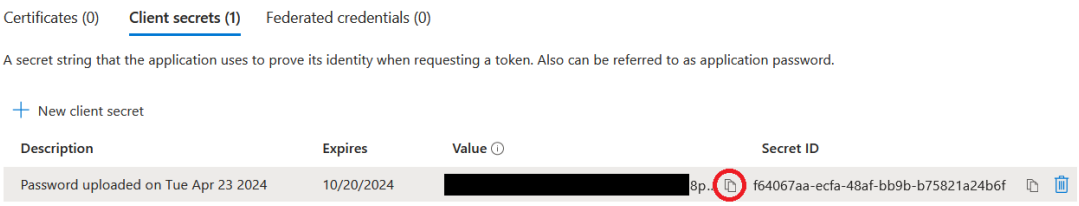
   Hier müssen Sie die Einstellungen unter *Implicit grant and hybrid flows* ändern und sowohl *Access tokens* als auch *ID tokens* aktivieren.



Nachdem Sie die Einstellungen geändert haben, klicken Sie auf Save.

5. Ein neues App Secret erstellen

    1. Wählen Sie den Menüpunkt *Certificates & secrets*.
    2. Aktivieren Sie den Tab *Client secrets*.
    3. Klicken Sie auf *New client secret*.
    4. Wählen Sie eine sinnvolle Beschreibung und die Dauer des neuen Secrets und bestätigen Sie mit Add.
    5. WICHTIG: Nach der Erstellung des Geheimnisses ist es nur jetzt möglich, das erstellte Secret zu kopieren. Wenn Sie die Datei appsettings.json bearbeiten, dann kopieren Sie diesen Wert jetzt nach `ClientSecret`, andernfalls kopieren Sie ihn an einen temporären, sicheren Ort, an dem Sie ihn abrufen können.



6. Fügen Sie die erforderlichen Berechtigungen für ELO Sync hinzu.

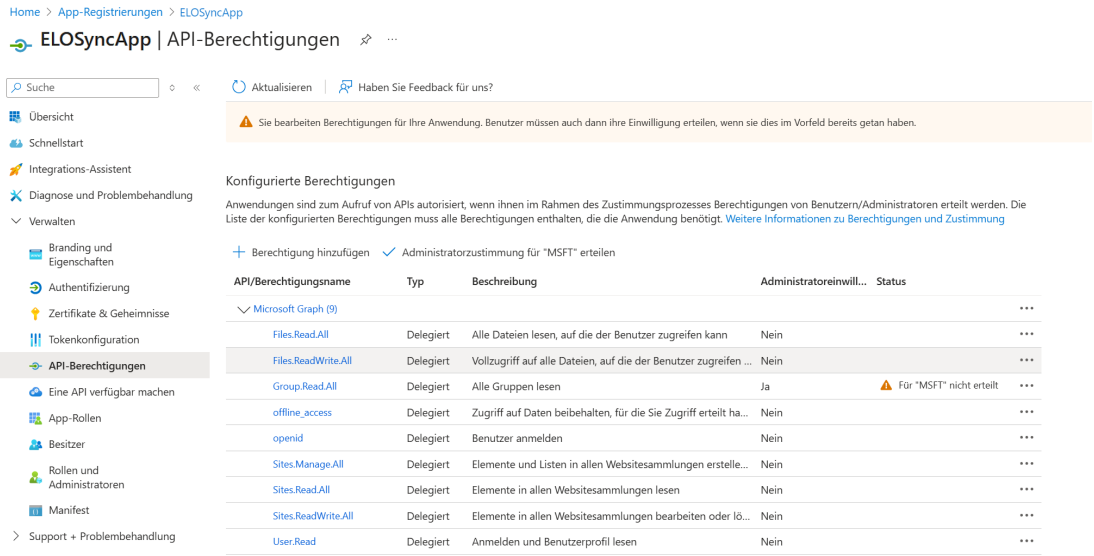
    ELO Sync selbst benötigt Berechtigungen für den Zugriff auf Daten über die Microsoft Graph API, entweder für sich selbst oder im Namen von Benutzern.

    1. Wählen Sie den Menüeintrag *API permissions* aus.
    2. Klicken Sie auf *Add a permission* für folgende:

Key	Ort	Benötigt für
openid	Microsoft Graph / Delegated / openid	Anmelden von Benutzern
offline_access	Microsoft Graph / Delegated / offline_access	Behalten Sie den Zugriff auf die Daten, auf die Sie ELO Sync Zugriff gegeben haben.
User.Read	Microsoft Graph / Delegated / User.Read	Anmelden und Benutzerprofil lesen.

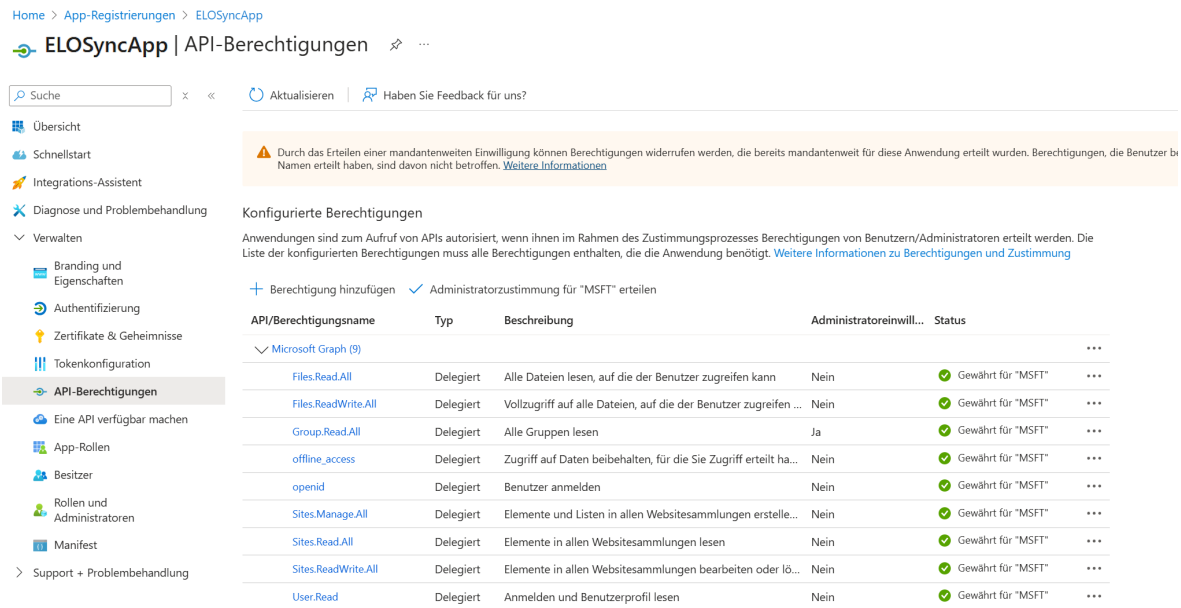
Beachten Sie

WICHTIG: Dies sind die einzigen grundlegenden Berechtigungen; je nach Anwendungsfall sind zusätzliche Berechtigungen erforderlich. Weitere Informationen finden Sie im Artikel Berechtigungen.



3. Falls gewünscht, können Sie jetzt die Zustimmung des Administrators für alle konfigurierten Berechtigungen erteilen, so dass die Benutzer den Zugriff auf ihre Daten nicht einzeln freigeben müssen.

7. Überprüfen Sie, ob alle Berechtigungen korrekt sind. Im folgenden Screenshot sehen Sie ein Beispiel für die Verwendung der Administratorzustimmung:



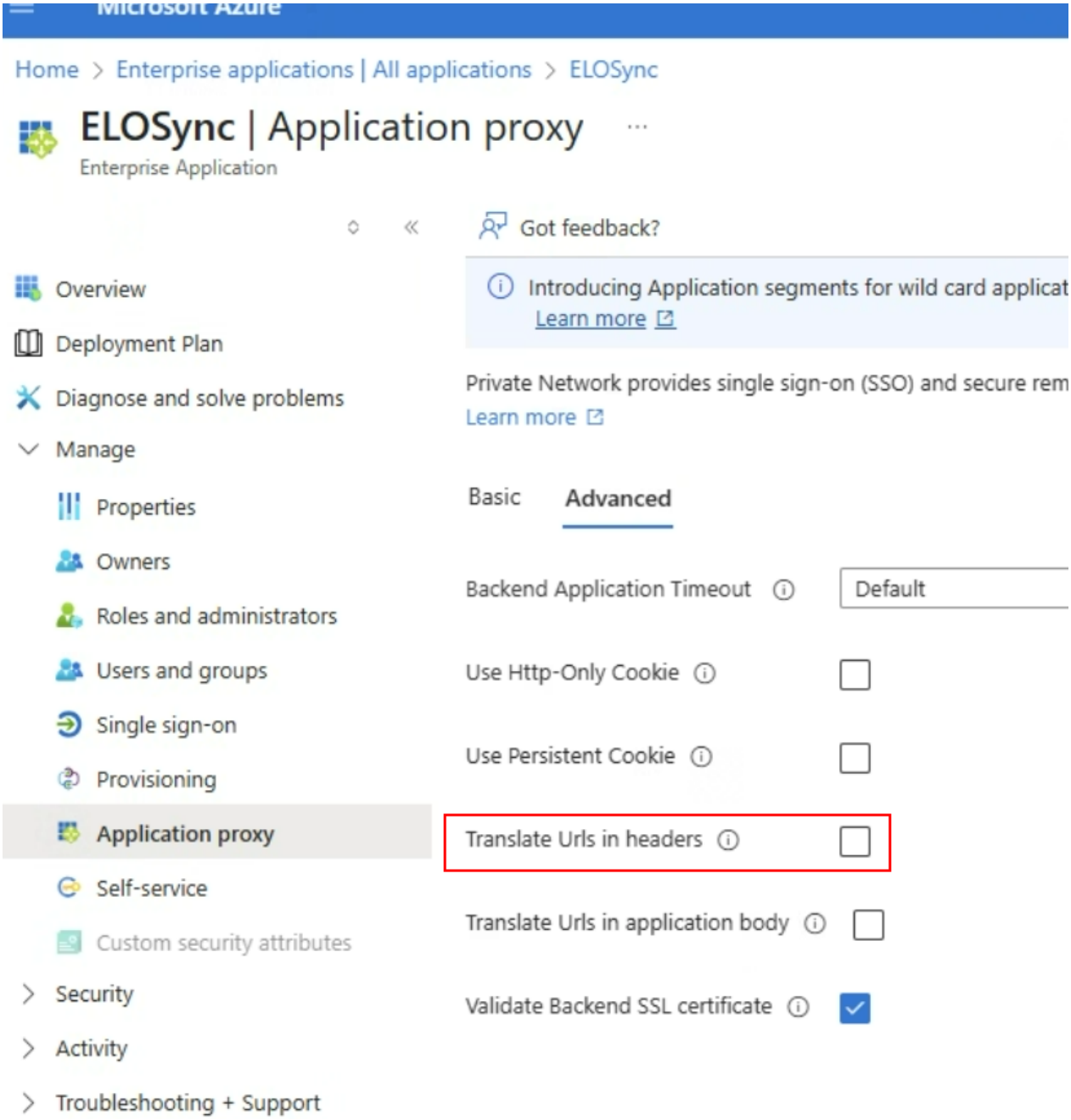
8. Stellen Sie sicher, dass in der AAD Graph App Manifest der korrekte Wert für `accessTokenAcceptedVersion` gesetzt ist. Dieser muss `accessTokenAcceptedVersion: 2` sein. Ist dieser nicht gesetzt, so funktioniert die Anmeldung über die REST-API nicht, und

Anfragen werden mit dem Fehlercode `IDX10214: Audience validation failed` abgebrochen.

Alternativ kann auch `"requestedAccessTokenVersion": 2` im Microsoft Graph App Manifest gesetzt werden.

Verwendung des Azure Application Proxy

Wird für ELO Sync ein Azure Application Proxy verwendet, dann muss in der Einstellung des Proxies die Eigenschaft 'Translate Urls in headers' deaktiviert werden:



Wenn diese Einstellung nicht deaktiviert wird, dann funktioniert die Anmeldung nicht korrekt und bricht mit "Correlation failed" ab.

Der Grund dafür ist, dass bei aktivierter Option ELO Sync nicht mitgeteilt wird, dass ein Proxy sich davor befindet. Damit wird bei der Anmeldung der `redirect_uri` Parameter fälschlicherweise auf die interne URL gesetzt und nicht die korrekte AppProxy-URL.

ELO Sync ist darauf ausgelegt mit Proxies zusammenzuarbeiten, die `Forwarded-*` Header setzen, was vom Azure AppProxy unterstützt wird.

Erforderliche Berechtigungen für jeden Anwendungsfall

Permission-Matrix Microsoft Graph

- Delegated
- Application

	openid	offline_access	User.Read	Files.Read or Files.Read.All	Files.ReadWrite or Files.ReadWrite.All	Sites.Read.All	Sites.ReadWrite.All	Sites.Manage.All	Group.Read.All
SPO-Folder->ELO	X	X	X	X		X			
SPO-List/DocLib->ELO	X	X	X	X		X			
SPO-Site->ELO	X	X	X	X		X			
SPO-Folder<-ELO	X	X	X		X	X			
SPO-List/DocLib<-ELO	X	X	X		X		X		
SPO-Site<-ELO	X	X	X		X		X	X	
SPO-Folder<->ELO	X	X	X		X	X			
SPO-List/DocLib<->ELO	X	X	X		X		X		
SPO-Site<->ELO	X	X	X		X		X	X	
OD-Folder->ELO	X	X	X	X					X
OD-Folder<-ELO	X	X	X		X				X
OD-Folder<->ELO	X	X	X		X				X

OpenID/Entra ID

Für die Authentifizierung von Benutzern sind die folgenden Berechtigungen erforderlich:

Microsoft Graph → Delegated permissions → openid: Erforderlich für die Anmeldung von Benutzern.

Microsoft Graph → Delegated permissions → offline_access: Erforderlich für die Aufrechterhaltung des Zugriffs auf Daten, auf die der Benutzer ELO Sync Zugriff erteilt hat. Dies ermöglicht die fortlaufende Synchronisierung von Daten ohne Benutzereingriff.

Microsoft Graph → Delegated permissions → User.Read: Erforderlich für die Anmeldung und das Lesen des Benutzerprofils. Dies ist für die Authentifizierung mit dem ELO Repository erforderlich.

SharePoint Online

Archivierung von Ordnern

Microsoft Graph → Delegated permissions → Sites.Read.All: Erforderlich, um den Inhalt der ausgewählten SharePoint-Sites, -Listen und -Dokumentenbibliotheken zu lesen. Nur die Elemente, die der Auftragsersteller sehen kann, werden archiviert.

Zusätzlich werden die gleichen Dateirechte benötigt wie in Archivierung von Dateien.

Zwei-Wege-Synchronisation von Ordnern

Erfordert die gleichen Berechtigungen wie Archivierung von Ordnern.

Zusätzlich werden die gleichen Dateirechte benötigt wie in Zwei-Wege-Synchronisation von Dateien.

Veröffentlichung in einen Ordner

Erfordert die gleichen Berechtigungen wie Archivierung von Ordnern.

Zusätzlich werden die gleichen Dateirechte benötigt wie bei Veröffentlichung auf ein Drive.

Archivierung von Listen/Bibliotheken

Microsoft Graph → Delegated permissions → Sites.Read.All: Erforderlich, um den Inhalt der ausgewählten SharePoint-Sites, -Listen und -Dokumentenbibliotheken zu lesen. Nur die Elemente, die der Auftragsersteller sehen kann, werden archiviert.

Zwei-Wege-Synchronisation von Listen oder Bibliotheken

Microsoft Graph → Delegated permissions → Sites.ReadWrite.All: Erforderlich zum Erstellen, Bearbeiten oder Löschen von Elementen in den ausgewählten SharePoint-Listen und -Dokumentenbibliotheken. Der Auftragsersteller muss Lese-/Schreibzugriff auf die Liste/Bibliothek haben.

Veröffentlichung in eine Liste/Bibliothek

Erfordert die gleichen Berechtigungen wie Zwei-Wege-Synchronisation von Listen oder Bibliotheken.

Archivierung einer Seite

Microsoft Graph → Delegated permissions → Sites.Read.All: Erforderlich, um den Inhalt der ausgewählten SharePoint-Site zu lesen.

Zwei-Wege-Synchronisation einer Seite

Alle Berechtigungen sind für die volle Funktionalität erforderlich.

Microsoft Graph → Delegated permissions → Sites.ReadWrite.All: Erforderlich zum Erstellen, Bearbeiten oder Löschen von Elementen in den Listen/Bibliotheken der ausgewählten SharePoint-Seite.

Microsoft Graph → Delegated permissions → Sites.Manage.All: Erforderlich für die Erstellung von Dokumentenbibliotheken in der ausgewählten SharePoint-Seite. Neue Dokumentenbibliotheken werden automatisch für jeden entsprechenden Unterordner im ELO-Zielordner erstellt.

Veröffentlichung auf eine Seite

Erfordert die gleichen Berechtigungen wie Zwei-Wege-Synchronisation einer Seite.

OneDrive

Allgemein

Microsoft Graph → Delegated permissions → Group.Read.All: Wird benötigt, um die verfügbaren OneDrive-Gruppen auszulesen, sodass der Benutzer die Laufwerke dieser Gruppen in der Job-Konfiguration auswählen kann.

Archivierung von Dateien

Eine der folgenden Berechtigungen ist erforderlich, beide zu setzen ist nicht notwendig und bietet keine zusätzlichen Funktionen.

Microsoft Graph → Delegated permissions → Files.Read: Erforderlich, um den Inhalt der ausgewählten OneDrive-Laufwerke zu lesen. Nur Dateien des Auftragserstellers werden archiviert, freigegebene Dateien anderer Benutzer werden nicht archiviert.

Microsoft Graph → Delegated permissions → Files.Read.All: Erforderlich, um den Inhalt der ausgewählten OneDrive-Laufwerke zu lesen. Alle Dateien, die dem Auftragsersteller gehören oder für ihn freigegeben wurden, werden archiviert.

Zwei-Wege-Synchronisation von Dateien

Eine der folgenden Berechtigungen ist erforderlich, beide zu setzen ist nicht notwendig und bietet keine zusätzlichen Funktionen.

Microsoft Graph → Delegated permissions → Files.ReadWrite: Erforderlich zum Erstellen, Bearbeiten oder Löschen von Dateien in den ausgewählten OneDrive-Laufwerken. Nur Dateien, die dem Auftragsersteller gehören, werden synchronisiert, freigegebene Dateien anderer Benutzer werden nicht synchronisiert.

Microsoft Graph → Delegated permissions → Files.ReadWrite.All: Erforderlich zum Erstellen, Bearbeiten oder Löschen von Dateien in den ausgewählten OneDrive-Laufwerken. Alle Dateien, die der Auftragsersteller besitzt oder für die er eine Freigabe erhalten hat, werden synchronisiert.

Veröffentlichung auf ein Drive

Erfordert die gleichen Berechtigungen wie Zwei-Wege-Synchronisation von Dateien.