ELO Sync

Registration in Azure

Table of contents

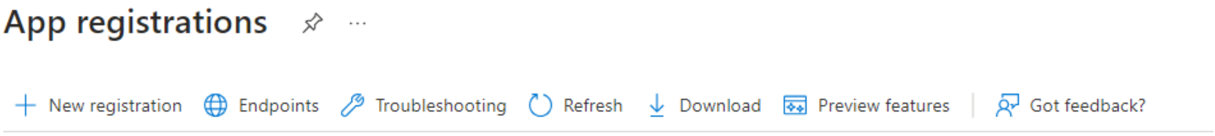
ELO Sync in Azure

This chapter describes how to register ELO Sync in Azure. These actions are required for authentication with Microsoft Entra and access to Microsoft 365 resources.

In our guide, ELO Sync is available under *https://elo-sync.local/* and registered as *ELOSyncApp* (replace as needed).

1. Create a new app registration in the Azure Management portal.

   Navigate to [App registrations](), then click *New registration*.

2. Enter the information required for the new application.

   1. Enter the name *EloSyncApp* as the name for the application (or a name of your choice).
   2. For supported account types, generally select *Accounts in this organizational directory only (Single tenant)*, though the second option *Multitenant* may apply depending on the structure of your organization.
   3. Under Redirect URI, select the *Web* platform and enter *https://elo-sync.local/signin-oidc-custom*.

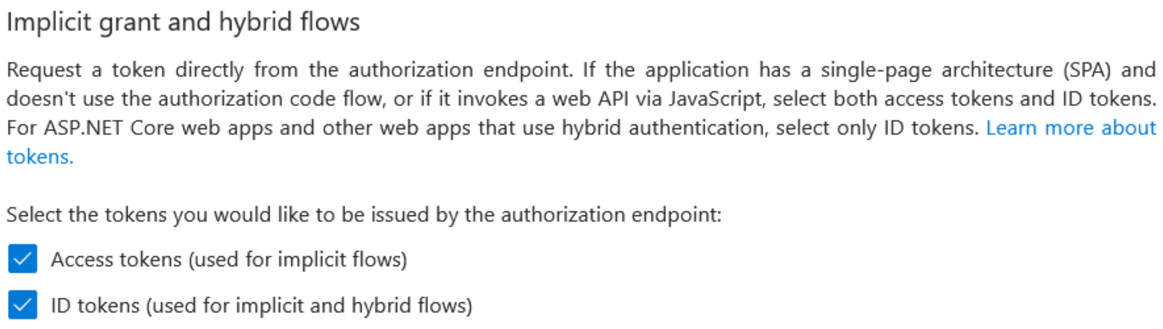
      > **Information**
      >
      > The path `/signin-oidc-custom` can be changed in the *appsettings.json* file. See Configuration for more information.

   4. Confirm the information and create the app registration.

3. While you are editing the appsettings.json file, go to the *Overview* for the application and copy the `ClientId` and `TenantId` information.

4. Open the newly created *ELOSyncApp* application and select the menu item *Authentication*.

   Here, you have to change the settings under *Implicit grant and hybrid flows* and enable both *Access tokens* and *ID tokens*.



Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more about tokens.

Select the tokens you would like to be issued by the authorization endpoint:

☑ Access tokens (used for implicit flows)

☑ ID tokens (used for implicit and hybrid flows)

Once you have changed the settings, click Save.

5. Create a new app secret

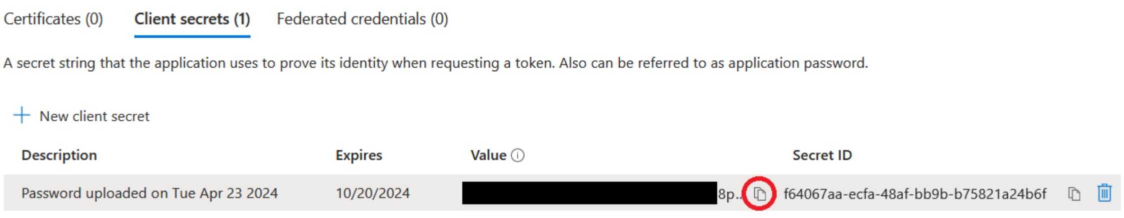
    1. Select the *Certificates & secrets* menu item.

    2. Select the *Client secrets* tab.

    3. Click *New client secret*.

    4. Select a meaningful description and duration for the new secret and confirm with Add.

    5. IMPORTANT: After you create the secret, it is only possible to copy the created secret. While you are editing the appsettings.json file, copy this value to `ClientSecret`, otherwise copy it to a temporary, secure location where you can access it.



A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
Password uploaded on Tue Apr 23 2024	10/20/2024	[redacted]8p...	f64067aa-ecfa-48af-bb9b-b75821a24b6f

6. Add the required permissions for ELO Sync.

   ELO Sync itself requires permissions to access data via the Microsoft Graph API, either for itself or on behalf of users.

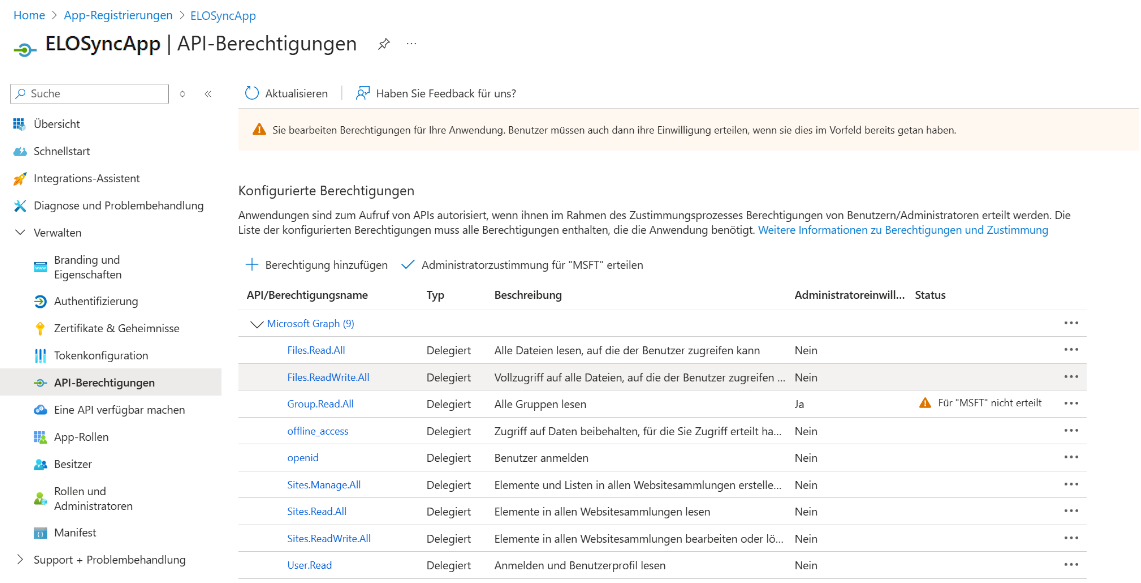
    1. Select the *API permissions* menu item.

    2. Click *Add a permission* for the following:

Key	**Location**	**Required for**
openid	Microsoft Graph/Delegated/openid	User authentication
offline_access	Microsoft Graph/Delegated/offline_access	Retain access to the data you gave ELO Sync access to.
User.Read	Microsoft Graph/Delegated/User.Read	Sign in and read user profile

Please note

IMPORTANT: These are the only basic permissions. Additional permissions may be required depending on the application. You will find more information under Permissions.



Home > App-Registrierungen > ELOSyncApp

ELOSyncApp | API-Berechtigungen

Suche
Übersicht
Schnellstart
Integrations-Assistent
Diagnose und Problembehandlung
Verwalten
Branding und Eigenschaften
Authentifizierung
Zertifikate & Geheimnisse
Tokenkonfiguration
API-Berechtigungen
Eine API verfügbar machen
App-Rollen
Besitzer
Rollen und Administratoren
Manifest
Support + Problembehandlung
Aktualisieren
Haben Sie Feedback für uns?

⚠ Sie bearbeiten Berechtigungen für Ihre Anwendung. Benutzer müssen auch dann ihre Einwilligung erteilen, wenn sie dies im Vorfeld bereits getan haben.

Konfigurierte Berechtigungen

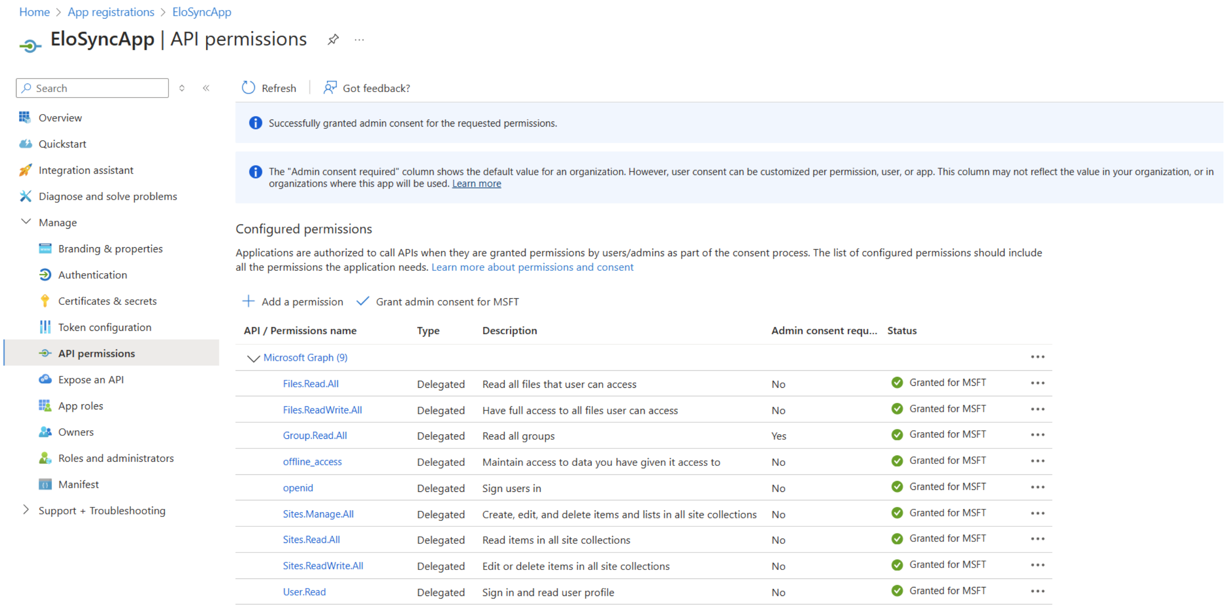
Anwendungen sind zum Aufruf von APIs autorisiert, wenn ihnen im Rahmen des Zustimmungsprozesses Berechtigungen von Benutzern/Administratoren erteilt werden. Die Liste der konfigurierten Berechtigungen muss alle Berechtigungen enthalten, die die Anwendung benötigt. Weitere Informationen zu Berechtigungen und Zustimmung

+ Berechtigung hinzufügen
✓ Administratorzustimmung für "MSFT" erteilen

API/Berechtigungsname	Typ	Beschreibung	Administratoreinwill...	Status	
Microsoft Graph (9)					•••
Files.Read.All	Delegiert	Alle Dateien lesen, auf die der Benutzer zugreifen kann	Nein		•••
Files.ReadWrite.All	Delegiert	Vollzugriff auf alle Dateien, auf die der Benutzer zugreifen ...	Nein		•••
Group.Read.All	Delegiert	Alle Gruppen lesen	Ja	⚠ Für "MSFT" nicht erteilt	•••
offline_access	Delegiert	Zugriff auf Daten beibehalten, für die Sie Zugriff erteilt ha...	Nein		•••
openid	Delegiert	Benutzer anmelden	Nein		•••
Sites.Manage.All	Delegiert	Elemente und Listen in allen Websitesammlungen erstelle...	Nein		•••
Sites.Read.All	Delegiert	Elemente in allen Websitesammlungen lesen	Nein		•••
Sites.ReadWrite.All	Delegiert	Elemente in allen Websitesammlungen bearbeiten oder lö...	Nein		•••
User.Read	Delegiert	Anmelden und Benutzerprofil lesen	Nein		•••

3. If required, you can grant admin consent for all configured permissions so that users do not have to grant individual access to their data.

7. Check that all permissions are correct. In the screenshot below you can see an example for using admin consent:



Home > App registrations > EloSyncApp

EloSyncApp | API permissions

ⓘ Successfully granted admin consent for the requested permissions.

ⓘ The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status	
Microsoft Graph (9)					•••
Files.Read.All	Delegated	Read all files that user can access	No	✓ Granted for MSFT	•••
Files.ReadWrite.All	Delegated	Have full access to all files user can access	No	✓ Granted for MSFT	•••
Group.Read.All	Delegated	Read all groups	Yes	✓ Granted for MSFT	•••
offline_access	Delegated	Maintain access to data you have given it access to	No	✓ Granted for MSFT	•••
openid	Delegated	Sign users in	No	✓ Granted for MSFT	•••
Sites.Manage.All	Delegated	Create, edit, and delete items and lists in all site collections	No	✓ Granted for MSFT	•••
Sites.Read.All	Delegated	Read items in all site collections	No	✓ Granted for MSFT	•••
Sites.ReadWrite.All	Delegated	Edit or delete items in all site collections	No	✓ Granted for MSFT	•••
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for MSFT	•••

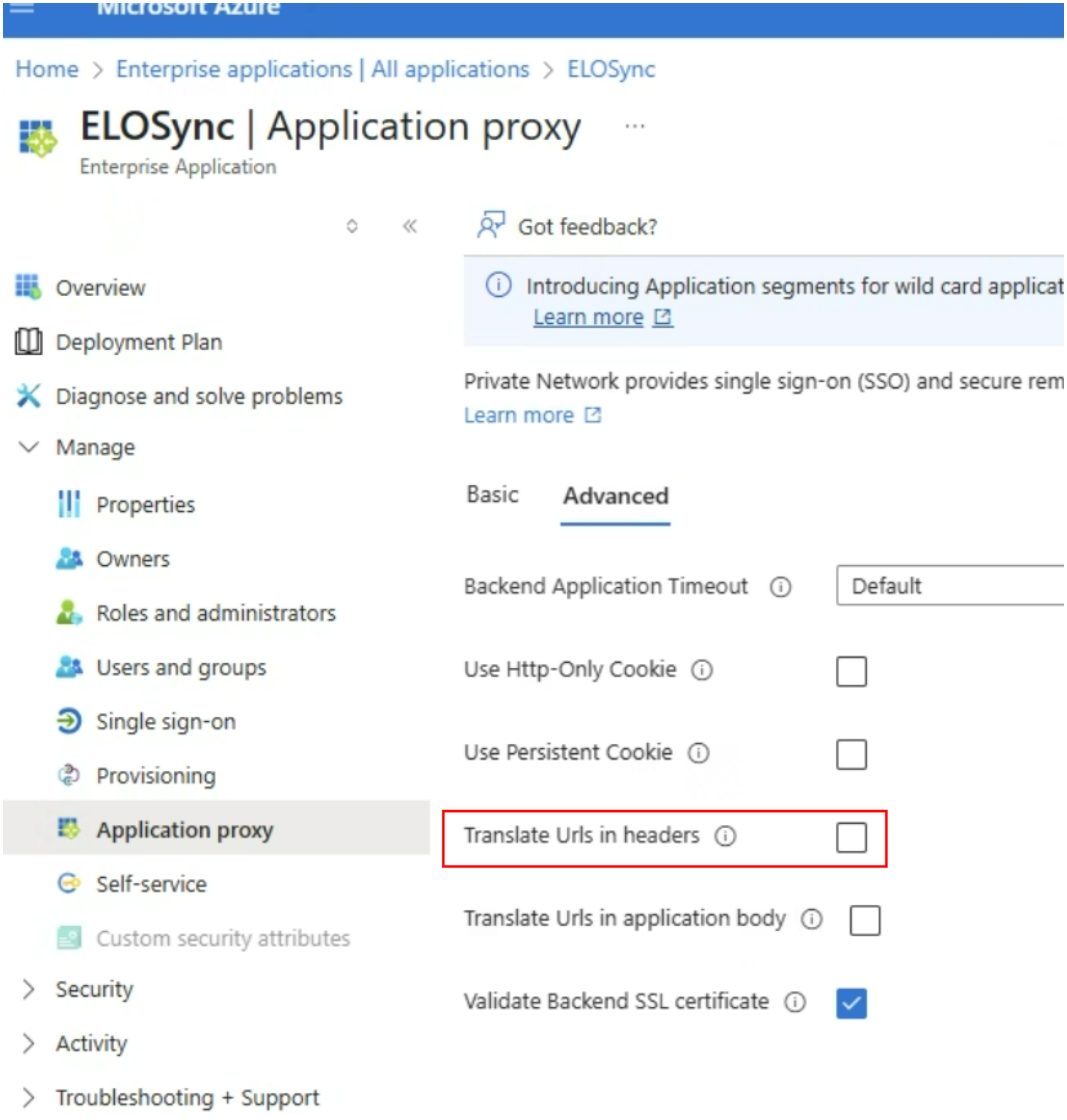
8. In the AAD Graph app manifest, make sure that the correct value is set for `accessTokenAcceptedVersion`. This must be `accessTokenAcceptedVersion: 2`. If this value is

not set, authentication via the REST API will not work, and requests will be terminated with the error code `IDX10214: Audience validation failed`.

Alternatively, `"requestedAccessTokenVersion": 2` can also be set in the Microsoft Graph app manifest.

Use of the Azure application proxy

If an Azure application proxy is used for ELO Sync, the property 'Translate Urls in headers' must be disabled in the proxy settings:



Introducing Application segments for wild card applicat
Learn more

Private Network provides single sign-on (SSO) and secure rem
Learn more

Backend Application Timeout: Default

Use Http-Only Cookie □

Use Persistent Cookie □

Translate Urls in headers □

Translate Urls in application body □

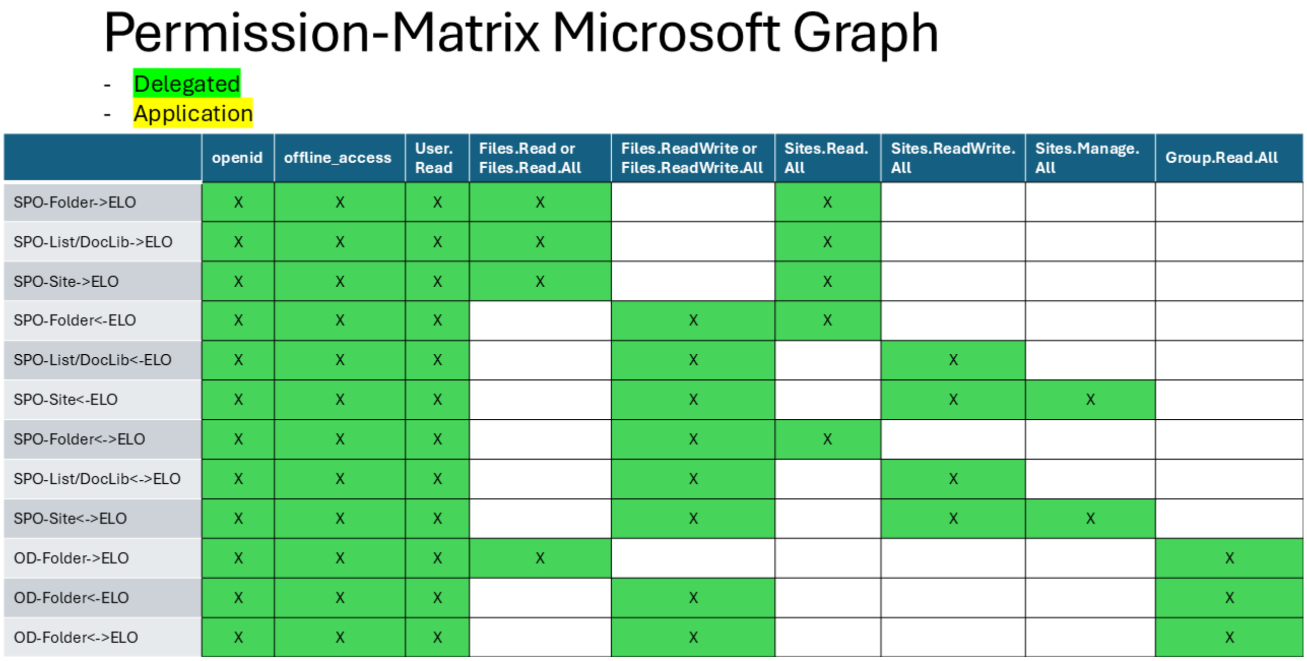
Validate Backend SSL certificate ☑

If this setting is not disabled, authentication does not work correctly and aborts with "Correlation failed".

The reason for this is that when this option is enabled, ELO Sync is not informed that there is a proxy in place. During authentication, the `redirect_uri` parameter is incorrectly set to the internal URL, and not the correct app proxy URL.

ELO Sync is designed to work with proxies that set `Forwarded-*` headers, supported by the Azure app proxy.

Required permissions for each application



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

The following permissions are required for user authentication:

Microsoft Graph → Delegated permissions → openid: Required for user authentication.

Microsoft Graph → Delegated permissions → offline_access: Required to retain access to data the user gave ELO Sync access to. This enables the continuous synchronization of data without user intervention.

Microsoft Graph → Delegated permissions → User.Read: Required for authentication and to read the user profile. This is required for authentication with the ELO repository.

SharePoint Online

Archiving folders

Microsoft Graph → Delegated permissions → Sites.Read.All: Required to read the content of the selected SharePoint sites, lists, and document libraries. Only the elements that the user who created the job can see are archived.

In addition, the same file rights are required as with archiving files.

Bidirectional synchronization of folders

Requires the same permissions as archiving folders.

In addition, the same file rights are required as with bidirectional synchronization of files.

Publishing in a folder

Requires the same permissions as archiving folders.

In addition, the same file rights are required as with publishing on a drive.

Archiving lists/libraries

Microsoft Graph → Delegated permissions → Sites.Read.All: Required to read the content of the selected SharePoint sites, lists, and document libraries. Only the elements that the user who created the job can see are archived.

Bidirectional synchronization of lists or libraries

Microsoft Graph → Delegated permissions → Sites.ReadWrite.All: Required to create, edit, or delete elements in the selected SharePoint lists and document libraries. The user creating the job must have read/write access to the list/library.

Publishing in a list/library

Requires the same permissions as bidirectional synchronization of lists or libraries.

Archiving a site

Microsoft Graph → Delegated permissions → Sites.Read.All: Required to read the content of the selected SharePoint site.

Bidirectional synchronization of a site

All permissions are required for full functionality.

Microsoft Graph → Delegated permissions → Sites.ReadWrite.All: Required to create, edit, or delete elements in the lists/libraries of the selected SharePoint site.

Microsoft Graph → Delegated permissions → Sites.Manage.All: Required to create document libraries in the selected SharePoint site. New document libraries are created automatically for each of the corresponding child folders in the ELO target folder.

Publishing on a site

Requires the same permissions as bidirectional synchronization of a site.

OneDrive

General

Microsoft Graph → Delegated permissions → Group.Read.All: Required to read the available OneDrive groups so that the user can select the drives of this group in the job configuration.

Archiving files

One of the following permissions is required. Setting both is not necessary and does not offer any additional functions.

Microsoft Graph → Delegated permissions → Files.Read: Required to read the content of the selected OneDrive drives. Only files of the user creating the job are archived. Shared files of other users are not archived.

Microsoft Graph → Delegated permissions → Files.Read.All: Required to read the content of the selected OneDrive drives. All files belonging to the user who created the job or that were shared with them are archived.

Bidirectional synchronization of files

One of the following permissions is required. Setting both is not necessary and does not offer any additional functions.

Microsoft Graph → Delegated permissions → Files.ReadWrite: Required to create, edit, or delete files in the selected OneDrive drives. Only files belonging to the user who created the job are synchronized. Shared files of other users are not synchronized.

Microsoft Graph → Delegated permissions → Files.ReadWrite.All: Required to create, edit, or delete files in the selected OneDrive drives. All files that the user who created the job owns that have been shared with them are synchronized.

Publishing on a drive

Requires the same permissions as bidirectional synchronization of files.