ELO Sync

Registration in Azure

Table of contents

ELO Sync in Azure 3
Required permissions for each application 8

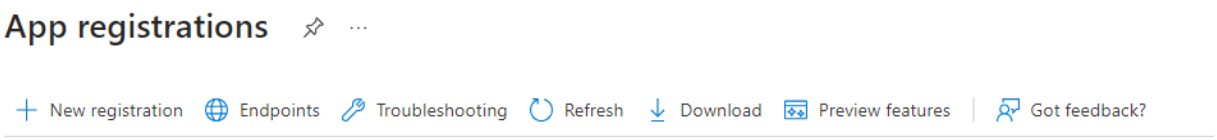
ELO Sync in Azure

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.

      > **Information**
      >
      > If *Single tenant* is selected and you want to access ELO Sync via REST API, the `Api.ForceSingleTenantLogin` setting has to be set to *true*. For more information, refer to the chapter Configuration.

   3. Under Redirect URI, select the *Web* platform and enter `https://<server name:port>/signin-oidc-custom`.

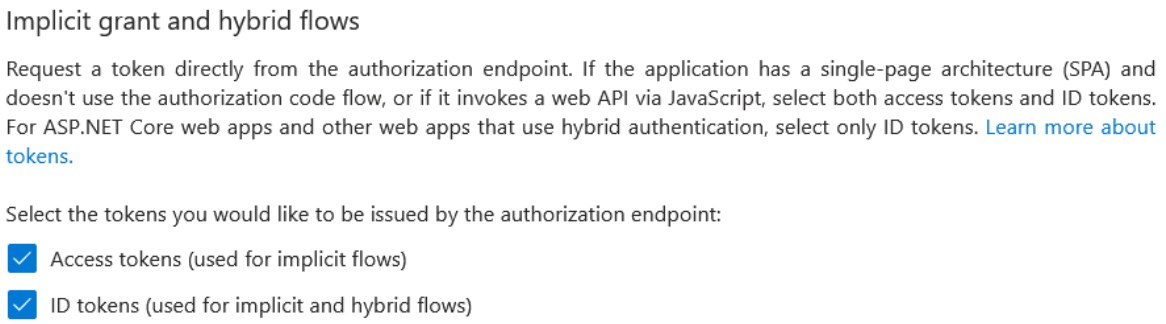
      > **Information**
      >
      > The path `/signin-oidc-custom` can be changed in the *appsettings.json* file. See Configuration for more information.

   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*.

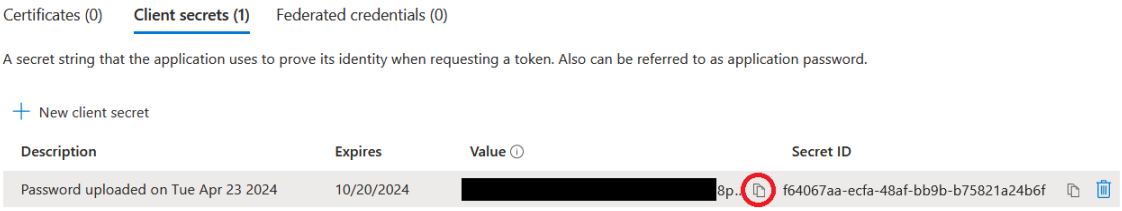
Here, you have to change the settings under *Implicit grant and hybrid flows* and enable both *Access tokens* and *ID tokens*.



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.



6. Add the required permissions for ELO Sync.

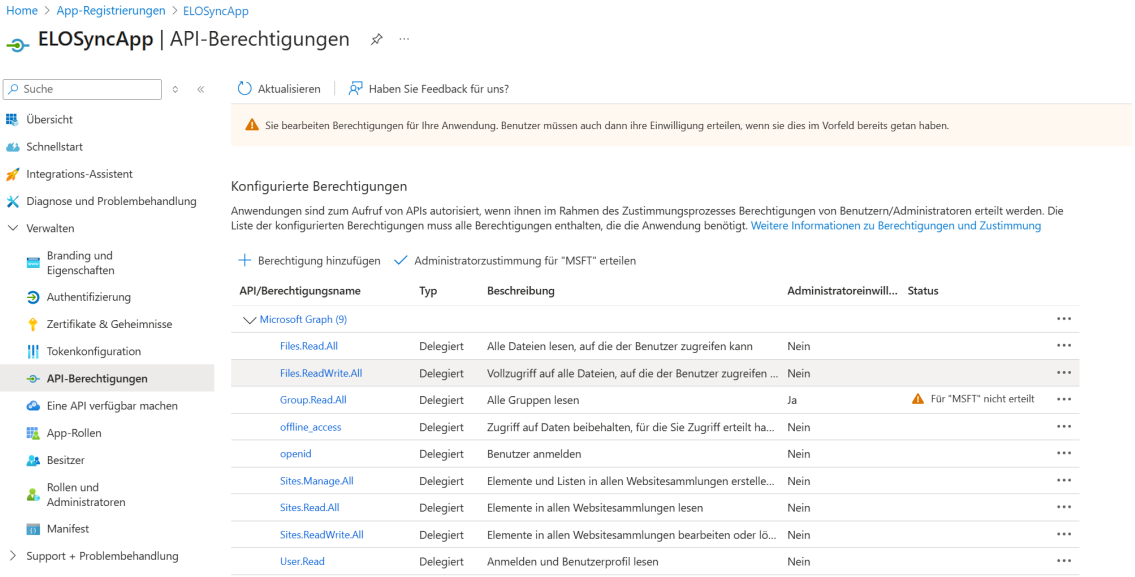
    ELO Sync itself requires permissions to access data via the Microsoft Graph API, either for itself or on behalf of users.

    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.

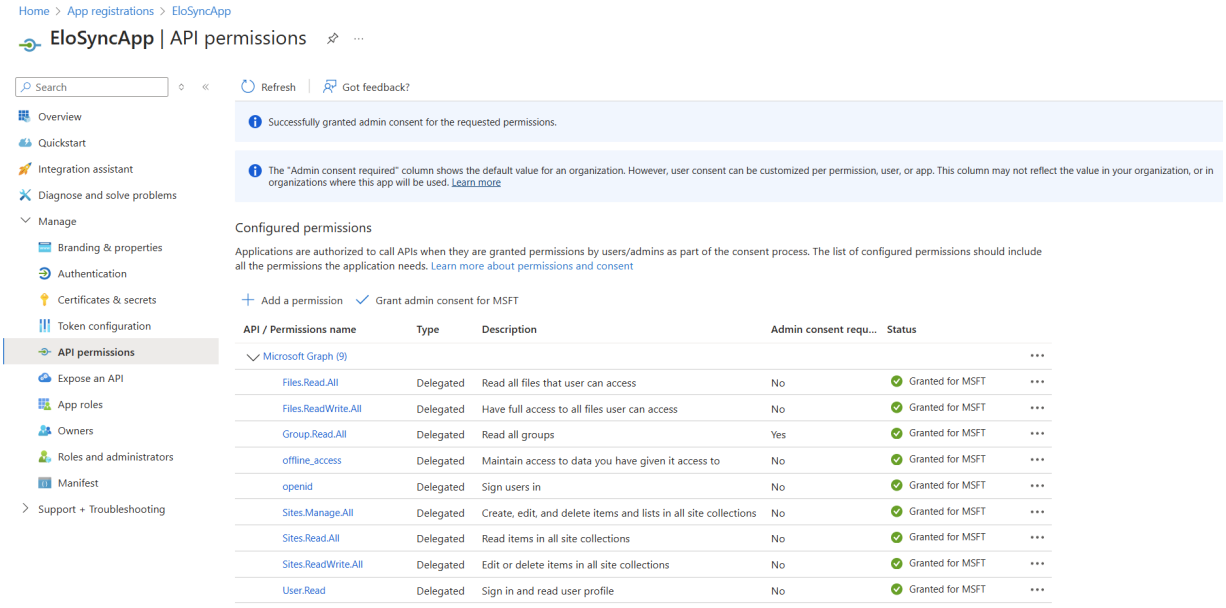
Key	Location	Required for
User.Read	Microsoft Graph/Delegated/ User.Read	Sign in and read user profile

> **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.



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:

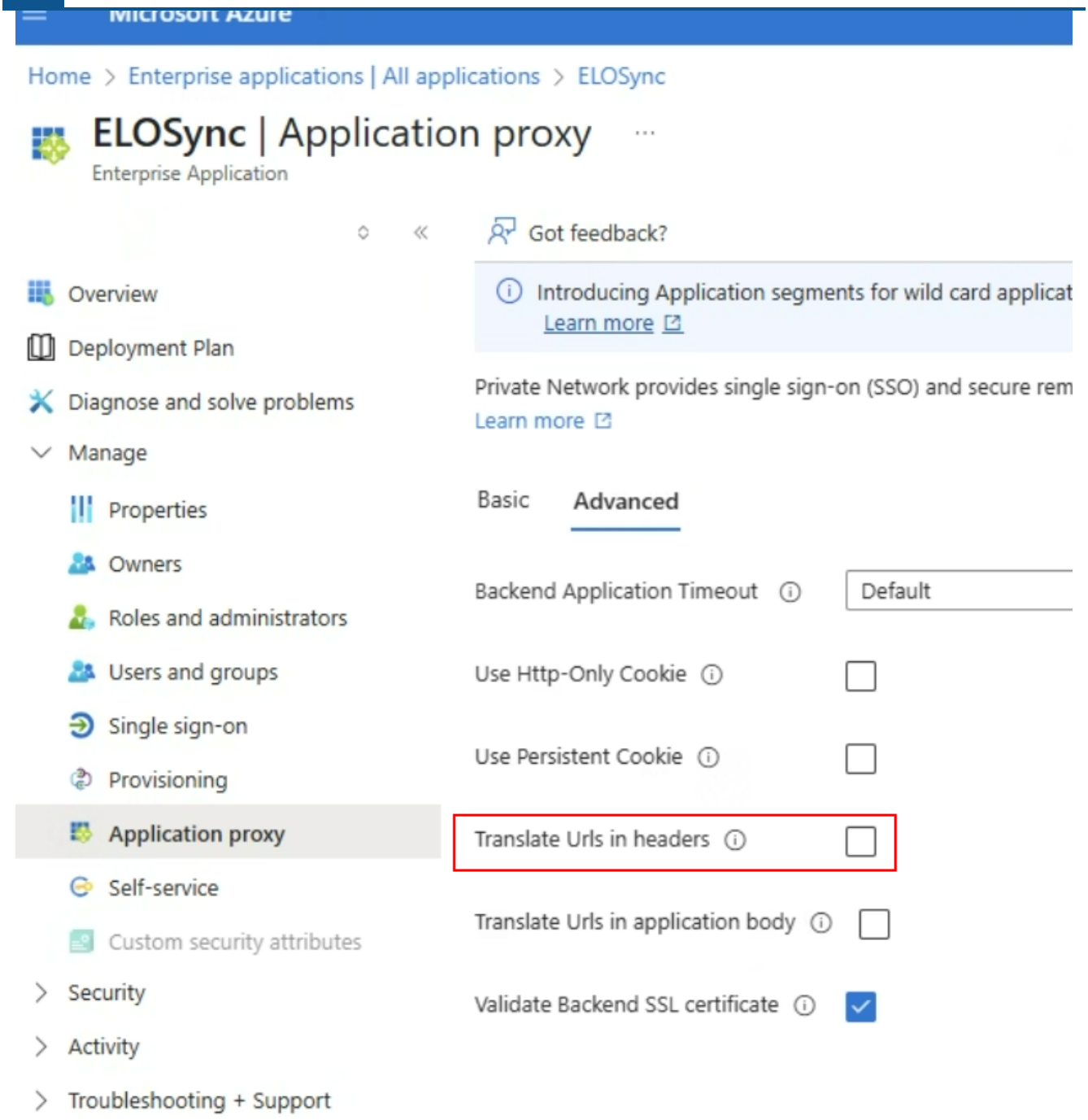


8. In the AAD Graph app manifest, make sure that the correct value is set for `accessTokenAcceptedVersion`. This must be `accessTokenAcceptedVersion: 2`. If this value is not set, authentication via the REST API will not work, and requests will be terminated with the error code `IDX10214: Audience validation 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:



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

Microsoft Graph → Delegated permissions:

		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	Mail.Read or Mail.ReadWrite or Mail.Read.Shared or Mail.ReadWrite.Shared
SharePoint Online	Folder → ELO	✓	✓	✓	✓		✓				
	List/DocLib → ELO	✓	✓	✓	✓		✓				
	Site → ELO	✓	✓	✓	✓		✓				
	Folder ← ELO	✓	✓	✓		✓	✓				
	List/DocLib ← ELO	✓	✓	✓		✓		✓			
	Site ← ELO	✓	✓	✓		✓		✓	✓		
	Folder ↔ ELO	✓	✓	✓		✓	✓				
	List/DocLib ↔ ELO	✓	✓	✓		✓		✓			
	Site ↔ ELO	✓	✓	✓		✓		✓	✓		
OneDrive	Folder → ELO	✓	✓	✓	✓					✓	
	Folder ← ELO	✓	✓	✓		✓				✓	
	Folder ↔ ELO	✓	✓	✓		✓				✓	
Exchange Online	Folder → ELO	✓	✓	✓							✓

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.

Exchange Online

Archiving e-mails or attachments

Archiving e-mails and attachments from e-mails requires the following permission: *Microsoft Graph → Delegated permissions → Mail.Read*.

Using shared mailboxes

Using shared mailboxes requires the additional permission *Microsoft Graph → Delegated permissions → Mail.Read.Shared* or *Microsoft Graph → Delegated permissions → Mail.ReadWrite.Shared*.

Executing operations in Exchange Online after archiving to ELO

Editing e-mails after archiving to ELO, e.g. adding a prefix to the subject, marking them as read, or deleting archived e-mails in Exchange Online requires the permission *Microsoft Graph → Delegated permissions → Mail.ReadWrite*. This permission is also required so that ELO XC properties can be automatically included in the e-mail after archiving.