ELO Sync

Registration in Azure

Table des matières

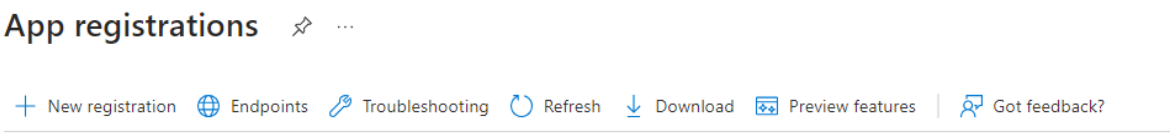
ELO Sync in Azure

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*.

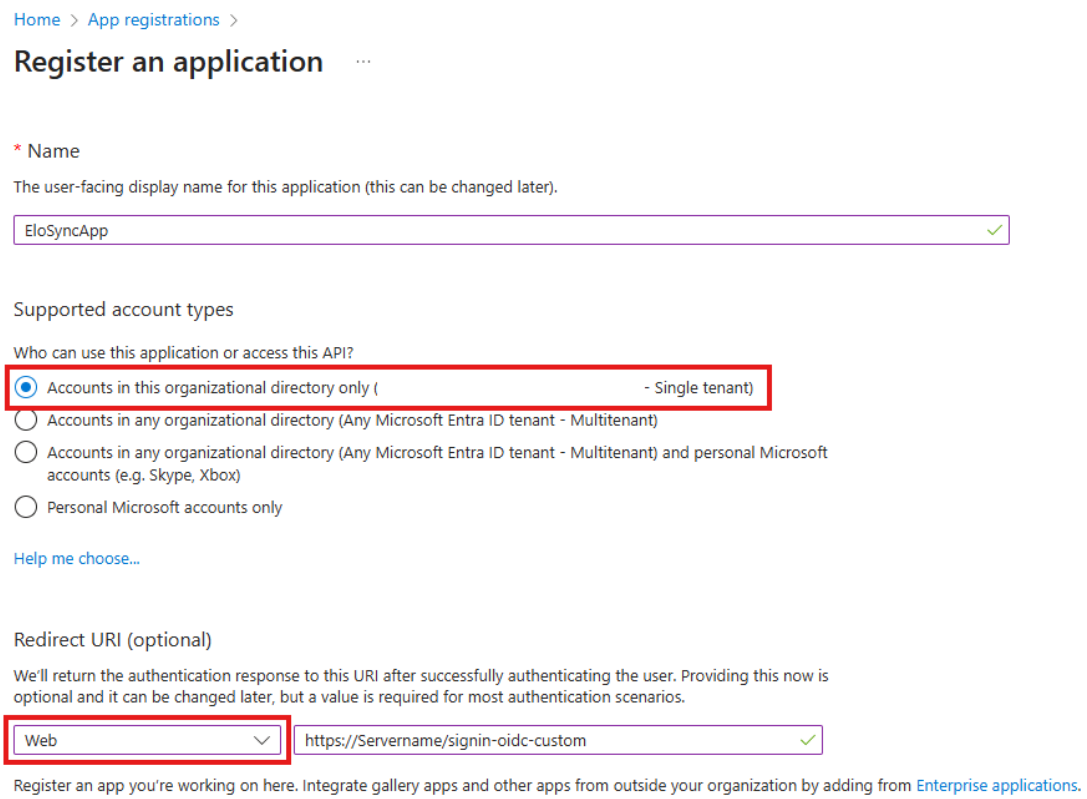


2. Enter the information required for the new application.

   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://<server name:port>/signin-oidc-custom`.



There are two options:

- The ‘PublicUrl’ node in the 'appsetings.json' file is empty: enter the following values: `https://myserver:5063/signin-oidc-custom`

```
37  "Kestrel": {
38    "Endpoints": {
39      "HttpsInlineCertFile": {
40        "Url": "https://myserver:5063",
```

- The 'PublicUrl' node in the 'appsetings.json' file was set: enter the following value in the Redirect URI: `https://mydomain.com/signin-oidc-custom`

```
11  "PublicUrl": "https://mydomain.com",
```

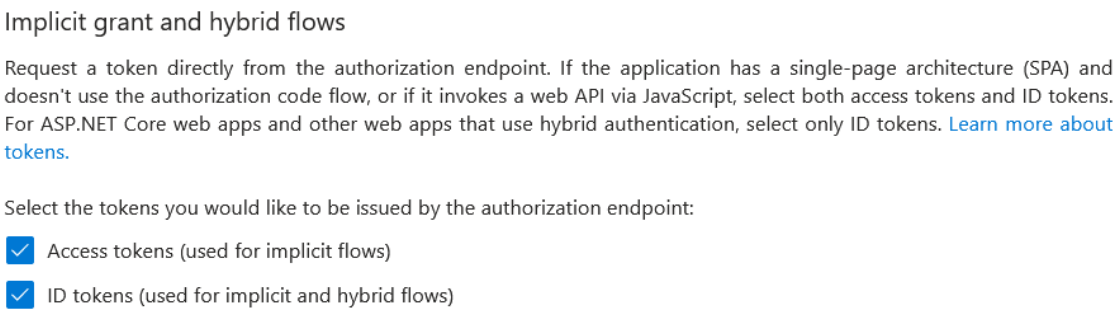
> **Information**
>
> The path `/signin-oidc-custom` can be changed in the *appsettings.json* file. See Configuration for more information.

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*.

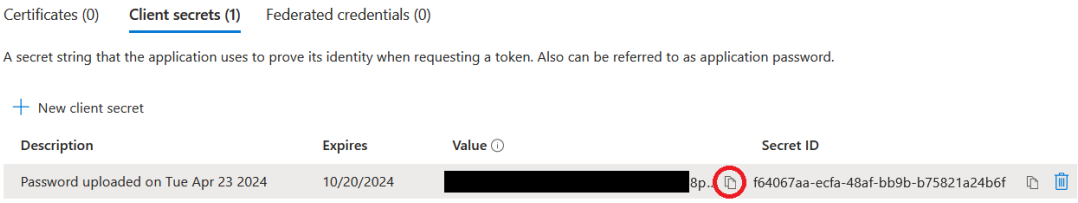


   Once you have changed the settings, click Save.

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.



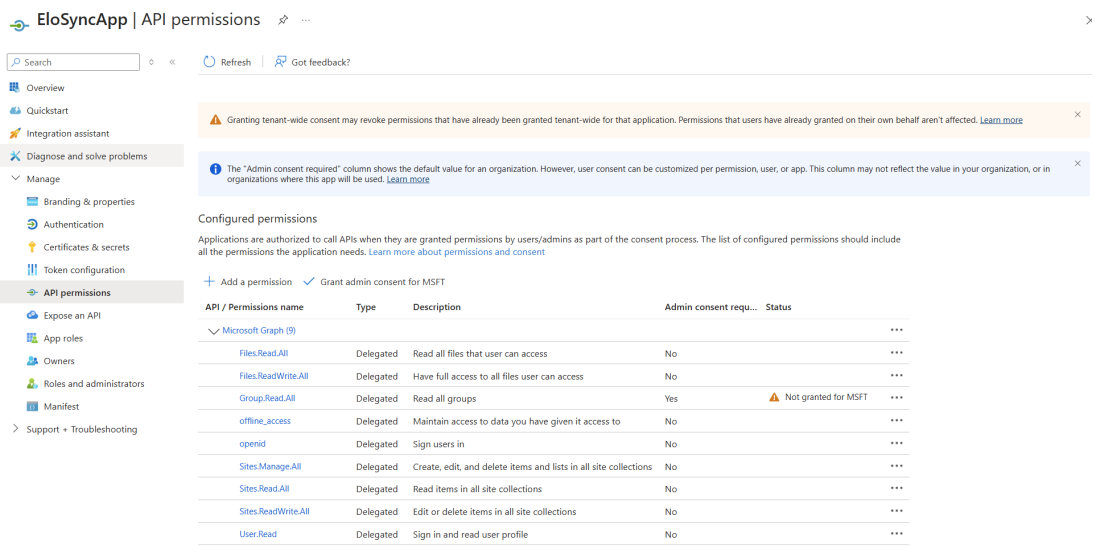
6. Add the required permissions for ELO Sync.

   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.
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.

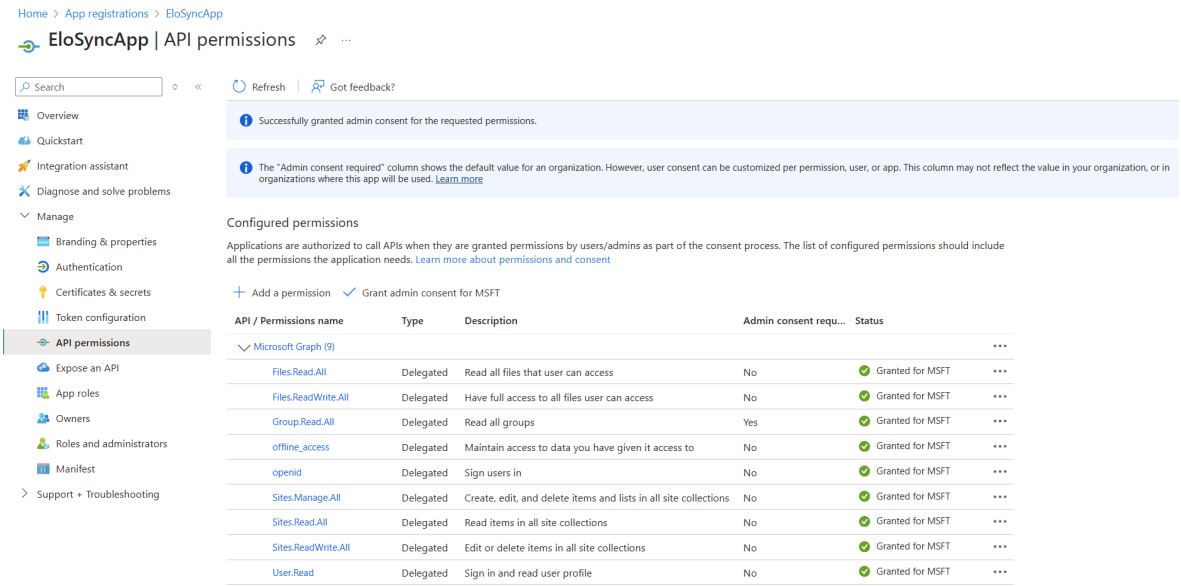
Click *Add a permission*, then select *APIs my organization uses*

4. Search for and select *ELOSyncApp*. Add the newly created permission *SyncJobs.ReadWrite.All*.

> **Information**
>
> The permission may not be listed yet. This can take a few minutes for the changes to be synchronized across all systems in Azure. If this is the case, try again later.

5. 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:



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.