Configuration and administration

ELO Azure Administration

Table of contents

ELO Azure administration

Requirements

To start ELO Azure Administration, the following requirements must be met:

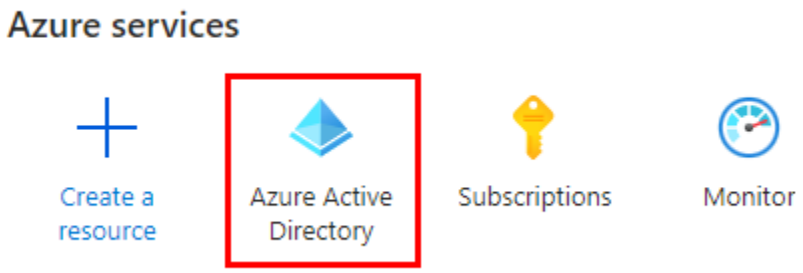
- The ELO Azure Administration service is installed and started. This module is installed using the ELO Server Setup.
    - You will find more information in the ELO server documentation under ELO server > Installation > ELO Server Setup
- You have access to a Microsoft Azure environment and the corresponding administrator account.
    - For more information, refer to the Microsoft documentation.
- An app for ELO Azure Administration is registered in Microsoft Azure.
    - Refer to the section Initial app registration in Microsoft Azure for more information.
- You are using an account with main administrator rights in ELO.

Initial app registration in Microsoft Azure

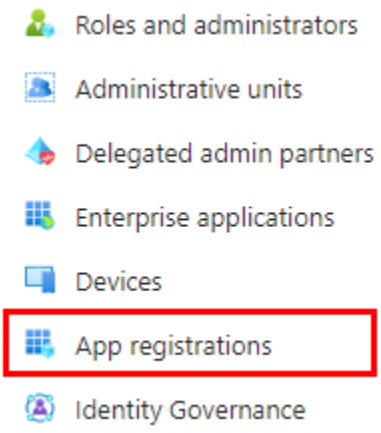
For ELO Azure Administration to connect to Microsoft Azure, you will have to register the app in Microsoft Azure first.

> **Please note**
>
> This documentation does not cover basic configuration of a Microsoft Azure environment or subscriptions, both of which are required for this.

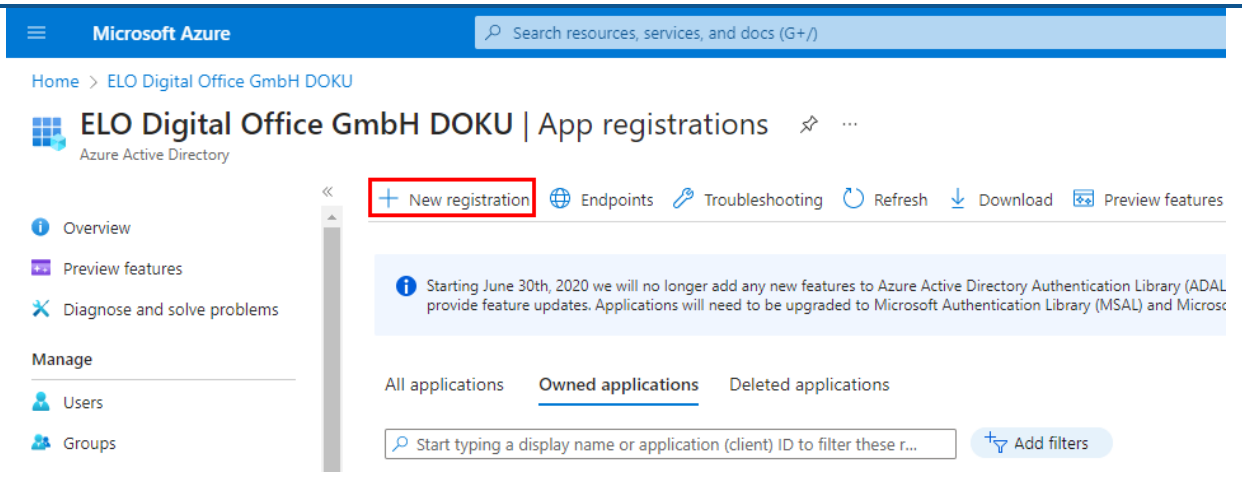
1. Log on to Microsoft Azure as an administrator.



2. Open the *Azure Active Directory* service.



3. Go to *App registrations*.



4. Select *New registration*.

   The *Register an application* page opens.

5. Enter a name for the app. You can choose any name you like.

   Example: ELO Azure Administration

6. Under *Supported account types*, select *Accounts in any organizational directory and personal Microsoft accounts (Any Azure AD directory – Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)*.

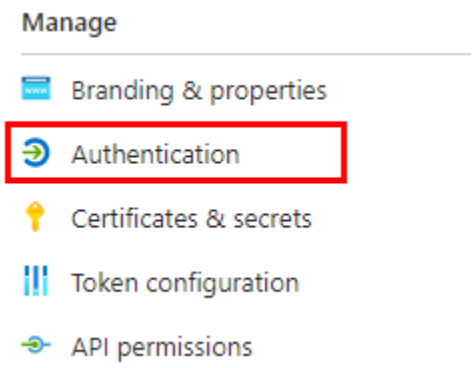
7. Select *Register*.

   The app is registered in Microsoft Azure.

Authentication settings

Once registration is complete, you have to configure some settings for app authentication.

1. In Microsoft Azure, go to *Authentication*.

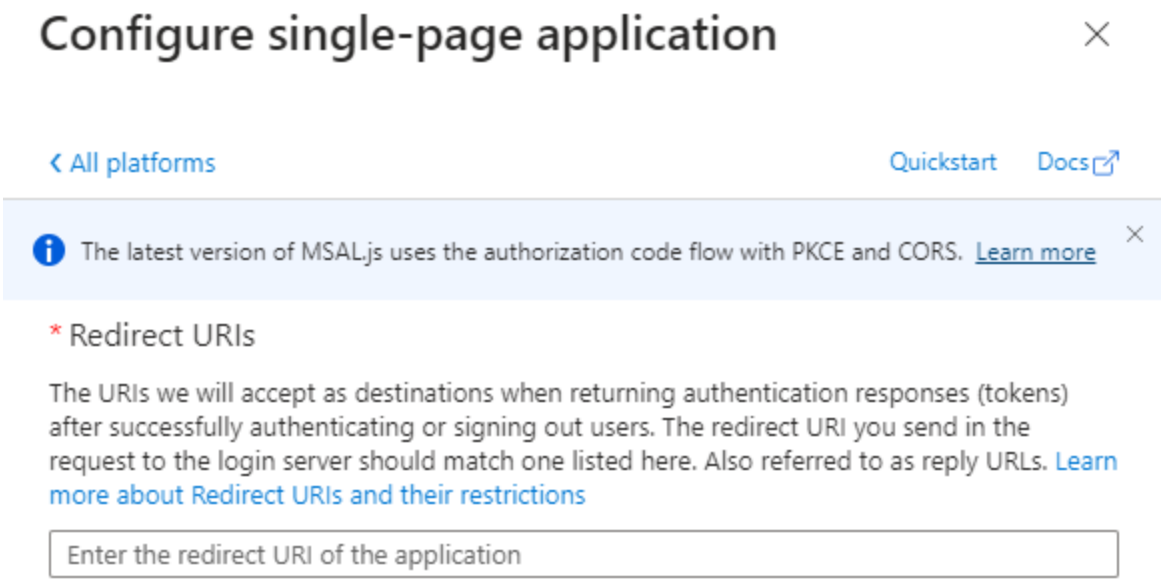


2. Select *Add a platform*.

   The *Configure platform* area appears.

3.

Select *Single-page application*.



The *Configure single-page application* area opens.

4. In the *Enter the redirect URI* field, enter a URL as follows:

   `https://<Server>:<Port>/ix-<Repository>/plugin/de.elo.ix.plugin.proxy/azadministrations/auth-end/blank.html`

   Example:

   `https://desktop-8luhtiv:9093/ix-EXTEN/plugin/de.elo.ix.plugin.proxy/azadministrations/auth-end/blank.html`

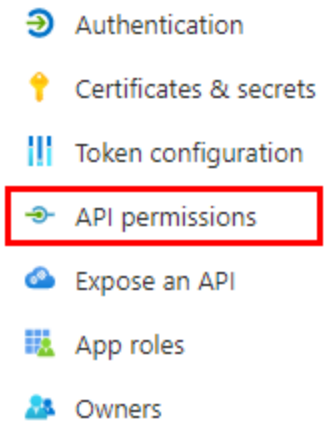
   > **Information**
   >
   > The URL must match the path to ELO Azure Administration in the respective ELO environment.

5. Enable the following settings:
   - Access tokens (used for implicit flows)
   - ID tokens (used for implicit and hybrid flows)
6. Save the settings with *Configure*.

   The authentication settings are now configured.

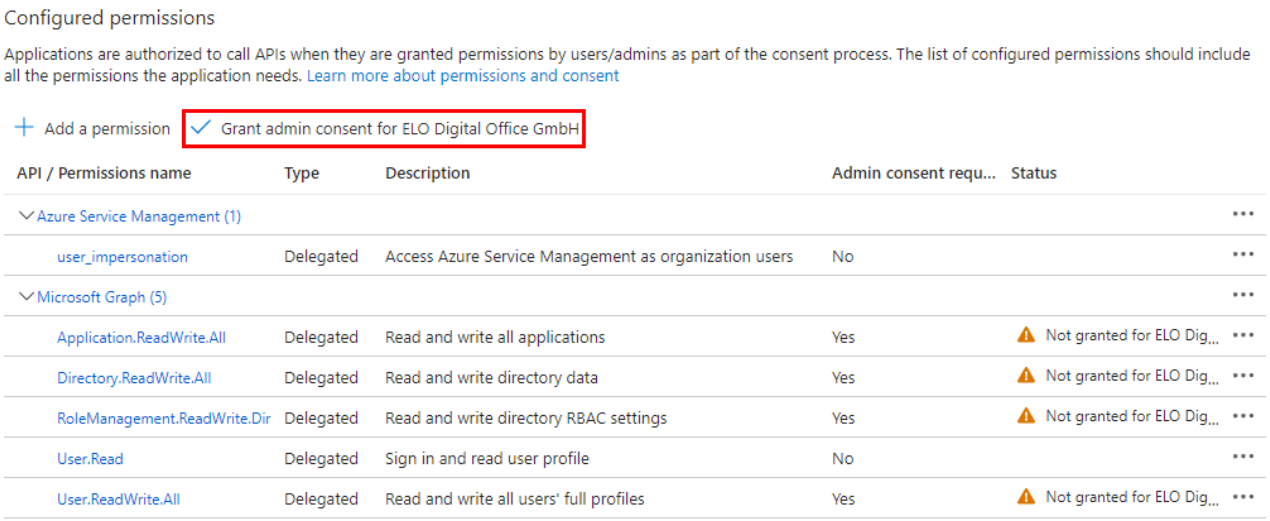
API permissions

The app for ELO Azure Administration requires several permissions.



1. Open the *API permissions* area.
2. Select *Add permissions*.

   The *Request API permissions* area opens.
3. Add the following delegated permissions:
   - Azure Service Management:
     - user_impersonation
   - Microsoft Graph:
     - Application.ReadWrite.All
     - Directory.ReadWrite.All
     - RoleManagement.ReadWrite.Directory
     - User.Read
     - User.ReadWrite.All



1. Select *Grant admin consent for <tenant>*.

   The *Confirm admin consent* dialog box opens.
2.

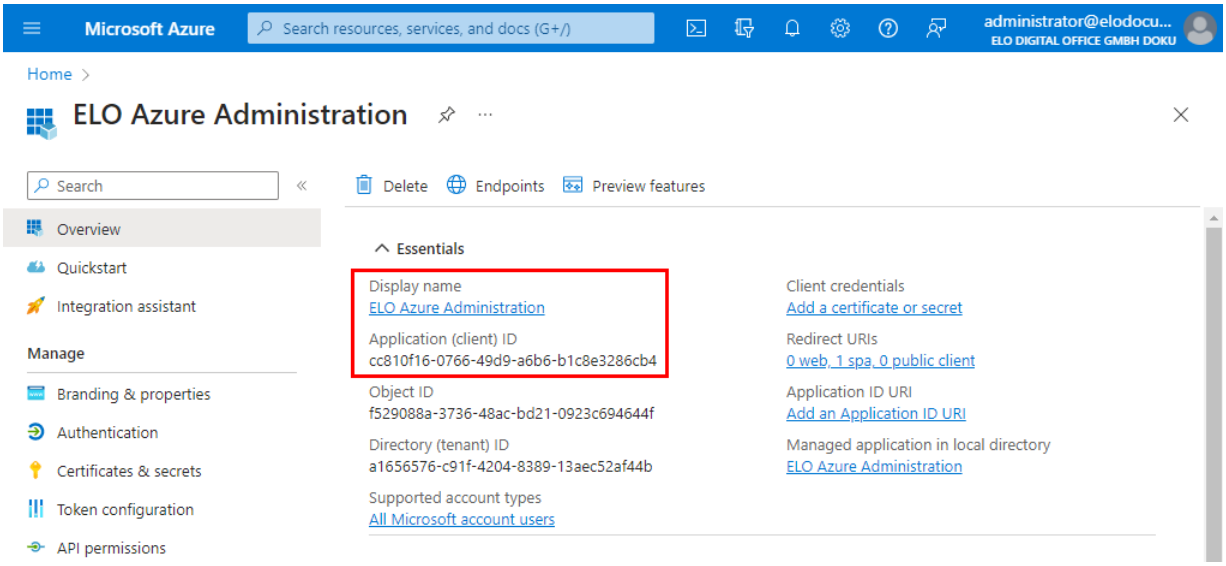
Click *Yes* to confirm.

The permissions are added.

Configuring the service

Once the app has been set up in Azure, you now have to update the configuration of the *ELO Azure Administration* service in the ELO system.

1. In Microsoft Azure, open the overview for the app you created above.



2. Copy the values of the following fields:
   - Display name
   - Application (client) ID
3. On the server machine running ELO, open the following directory:

   `<ELO>\servers\ELO-Azure-Administration`

   > **Information**
   >
   > The placeholder <ELO> stands for the ELO installation directory.

4. Open the *appsettings.json* file in a suitable editor.

   You will find the following entries in the header area of the file:

```
"AppsManagementDashboard": {
  "MicrosoftAppId": "",
  "MicrosoftAppName": ""
},
```

5.

Insert the copied values into the JSON file.

Example:

```
"AppsManagementDashboard": {
  "MicrosoftAppId": "cc810f16-0766-49d9-a6b6-b1c8e3286cb4",
  "MicrosoftAppName": "ELO Azure Administration"
},
```

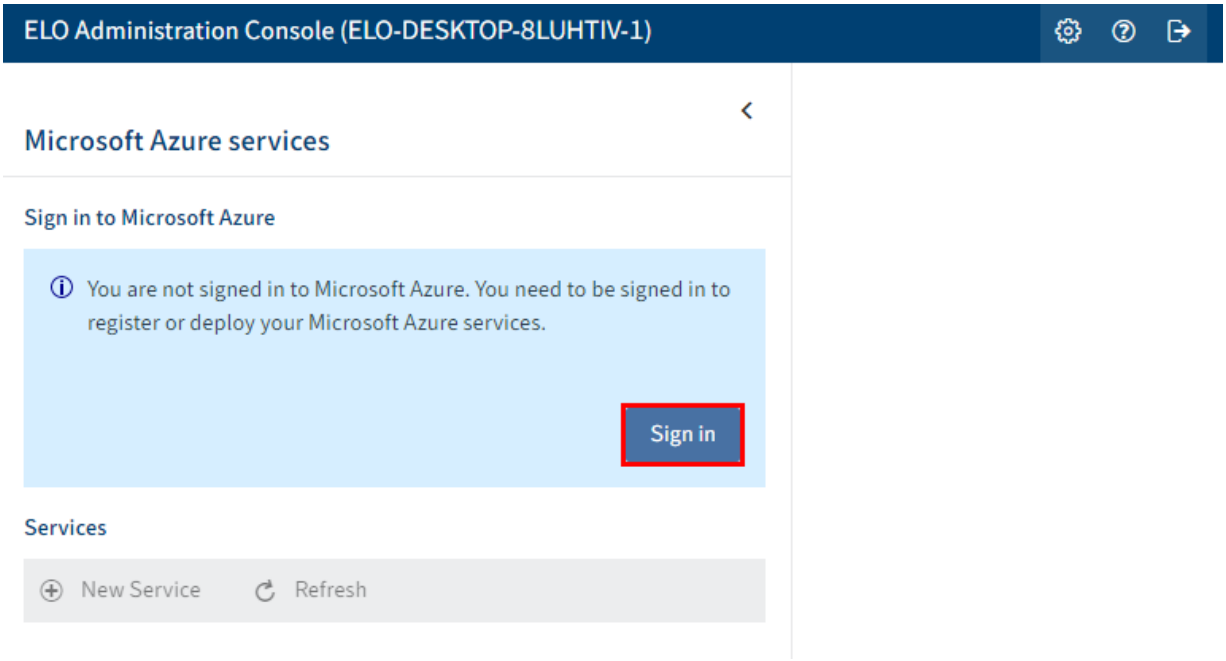
6. Save the file.
7. Restart the *ELO Azure Administration* service.

   You have finished configuring the service. You can now authenticate with Microsoft Azure via ELO Azure Administration.

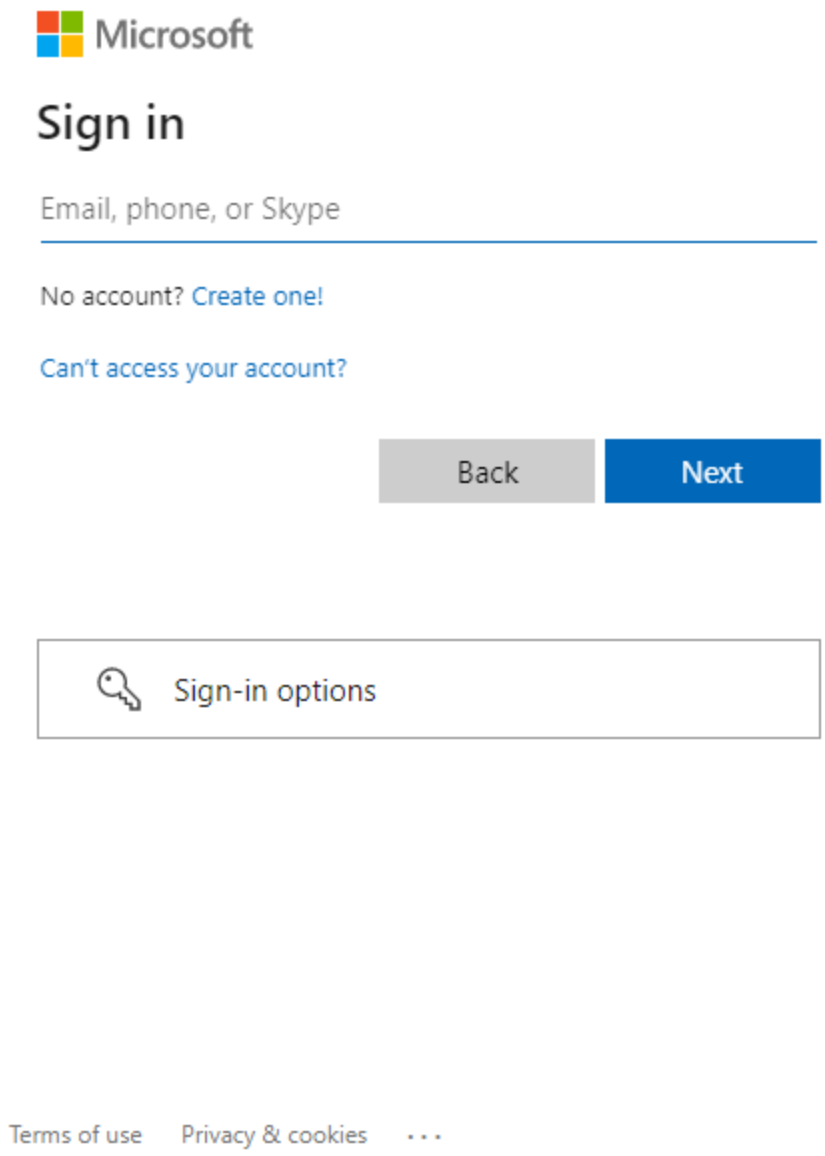
Authentication

When starting ELO Azure Administration for the first time, you will have to log on with the Azure administrator account.

1. Open the ELO Administration Console.
2. Log on with an account with main administrator rights.
3. Open the *ELO Azure Administration* area.



4. Select *Sign in*.



The *Sign in* dialog box opens.

> **Please note**
>
> This pop-up dialog box may be blocked by your browser. If this is the case, disable your pop-up blocker for the sign-in URL.

5. Enter the e-mail address for the administrator account in Microsoft Azure.
6. Select *Next*.

   The *Enter password* dialog box appears.
7. Enter the password for the administrator account in Microsoft Azure.
8.

Select *Sign in*.

The system attempts to sign in.

9. Verify sign-in via a method of your choice (Microsoft Authenticator app or by phone).

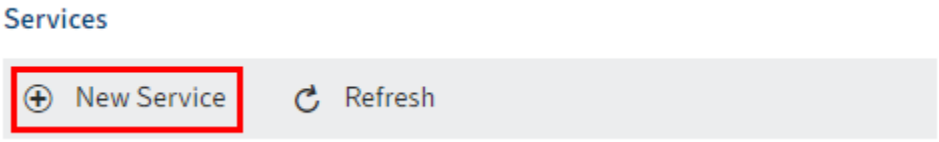
   ELO Azure Administration is now connected to Microsoft Azure. You can now create services.

Services

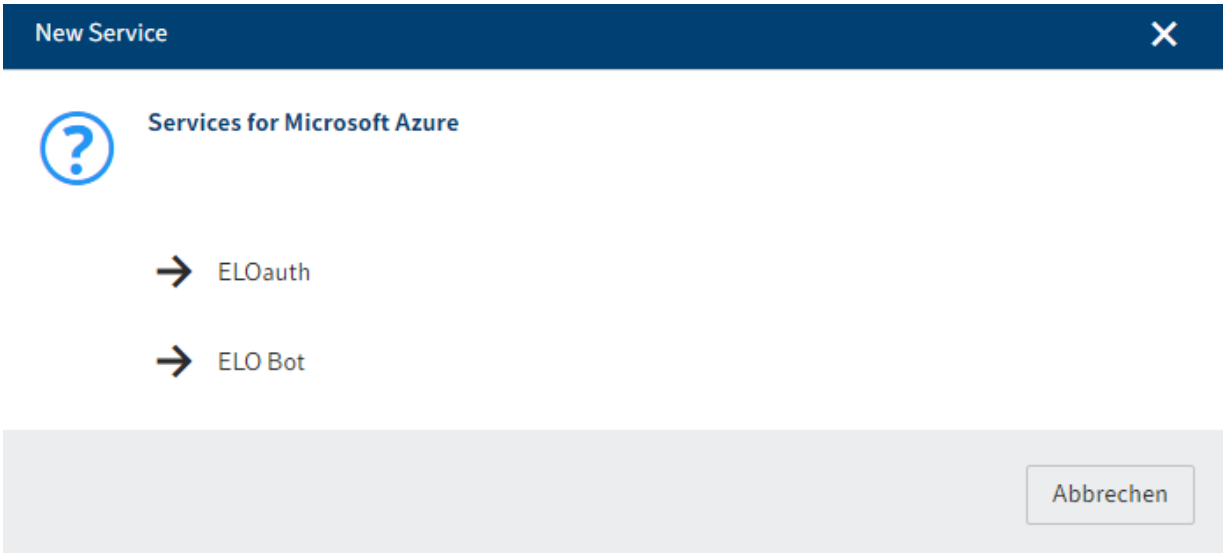
After successful logon, you can create services for Microsoft Azure apps via ELO Azure Administration.

Create service

1. Open ELO Azure Administration.



2. Select *New Service*.



The *New Service* dialog box appears. The following services are available:

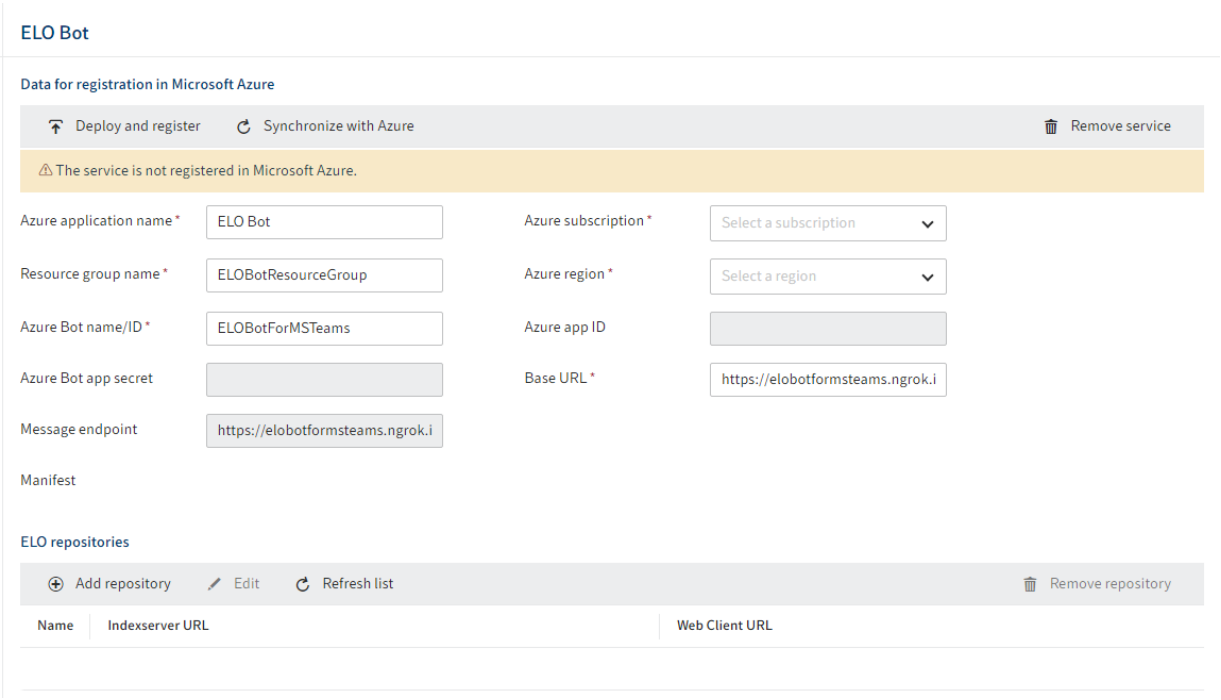
   - ELOauth: The ELOauth ELO Indexserver plug-in authenticates against an external system. You will find more information in the *ELO Indexserver* documentation under Plug-ins > ELOauth.
   - ELO Bot: The ELO Bot for Microsoft Teams connects Microsoft Teams to the ELO repository. Refer to the ELO Bot for Microsoft Teams documentation for more information.

3. Select a service.

> **Information**
>
> This documentation uses the *ELO Bot* service as an example. The configuration interface may vary depending on which service is selected.

In ELO Azure Administration, the service is shown as *Not registered*.

4. Select the service.



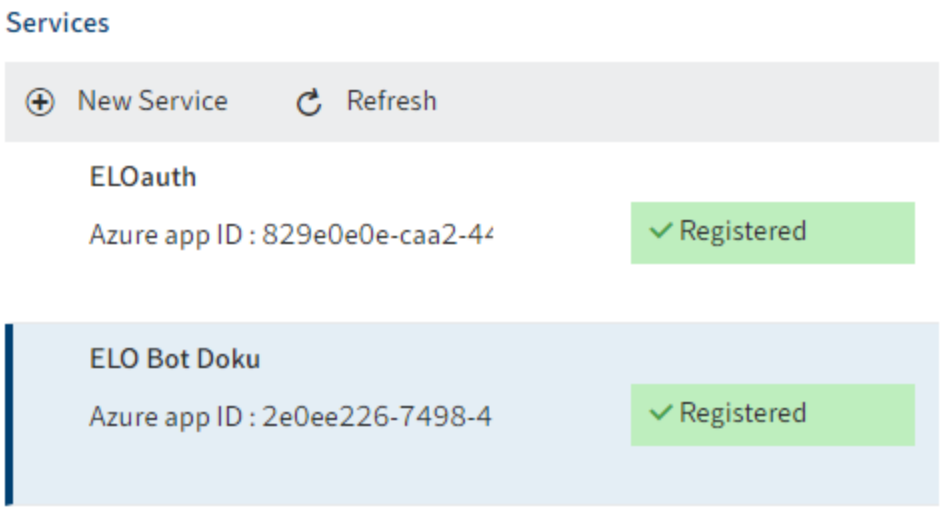
The configuration interface for the service opens.

5. Enter the data required to register the service. Grayed out fields are completed automatically.

   You will find more information in the following documents:

   - For ELO Bot: *ELO Bot for Microsoft Teams* documentation under ELO for Microsoft > ELO Bot for Microsoft Teams
   - For ELOauth: *ELO Indexserver* documentation under Plug-ins > ELOauth

6. Once you have entered the required data, select *Deploy and register*.



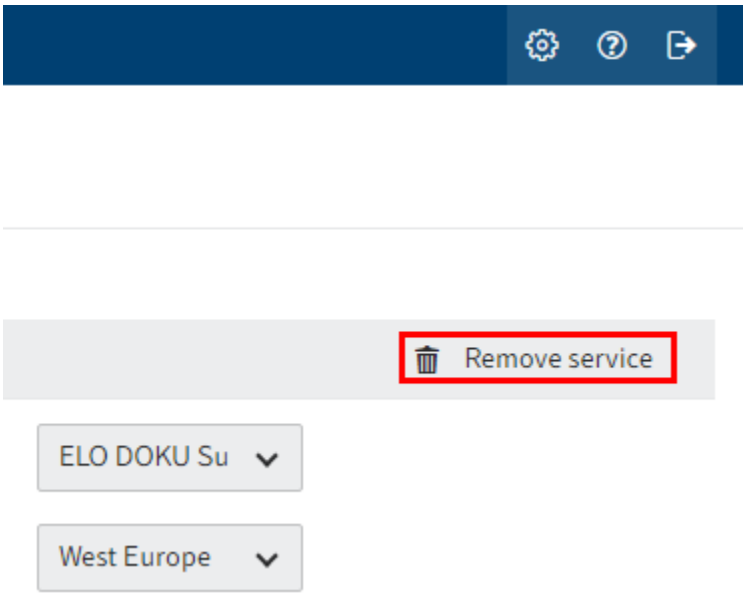
The service is registered as an app in Microsoft Azure. In ELO Azure Administration, the services are shown as *Registered*. You can now use the services.

Remove service

You can remove services via ELO Azure Administration and unregister them in ELO as well as Microsoft Azure.

1. Select the service you want to remove.

   The configuration interface for the service opens.



2. Select *Remove service*.

> **Please note**

> The service is deleted without any further confirmation.

The service is removed. ELO Azure Administration also automatically removes the service in Microsoft Azure.