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

  > **Please note**
  >
  > When using SSL: Configure the root certificate entered in the ELO setup on the ELO server in the respective certificate store. Example for Windows: under *Trusted Root Certification Authorities*.
  >
  > Otherwise, ELO Azure Administration may not be able to be reached.

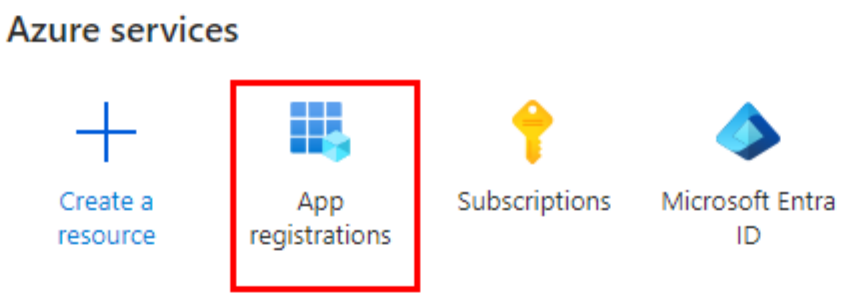
- You have access to a Microsoft Azure environment and the corresponding administrator account.
    - For more information, refer to the Microsoft documentation.
- An app for ELO Azure Administration is registered in Microsoft Azure.
    - Refer to the section Initial app registration in Microsoft Azure for more information.
- You are using an account with main administrator rights in ELO.

Initial app registration in Microsoft Azure

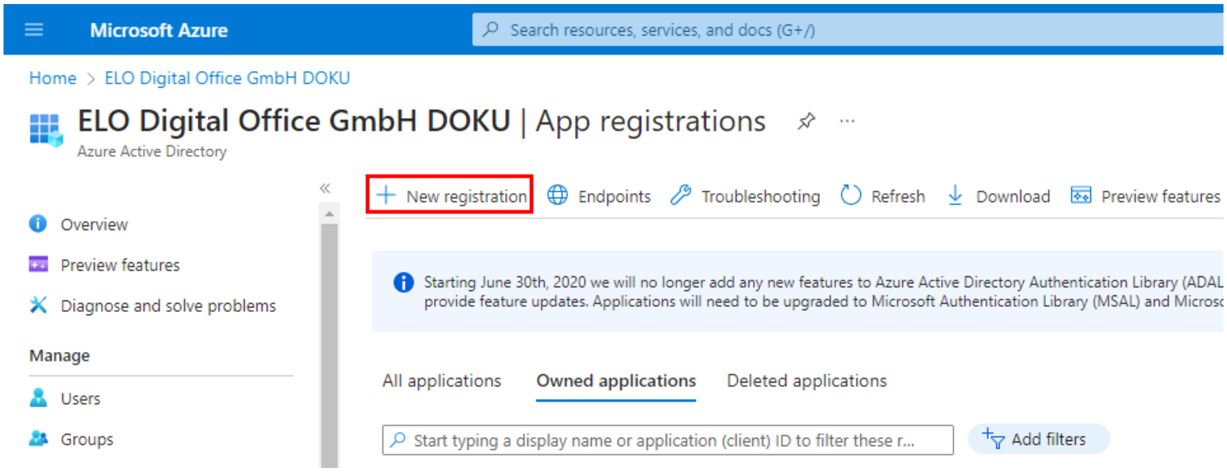
For ELO Azure Administration to connect to Microsoft Azure, you will have to register the app in Microsoft Azure first.

> **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. Go to *App registrations*.


Microsoft Azure
Search resources, services, and docs (G+/)
Home
ELO Digital Office GmbH DOKU
ELO Digital Office GmbH DOKU | App registrations
Azure Active Directory
New registration
Endpoints
Troubleshooting
Refresh
Download
Preview features
Overview
Preview features
Diagnose and solve problems
Manage
Users
Groups
All applications
Owned applications
Deleted applications
Start typing a display name or application (client) ID to filter these r...
Add filters

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsc

3. Select *New registration*.

   The *Register an application* page opens.

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

   Example: ELO Azure Administration

5.

Under *Supported account types*, select *Accounts in any organizational directory and personal Microsoft accounts (any Microsoft Entra ID tenant – multi-tenant capable) and personal Microsoft accounts (e.g. Skype, Xbox)*.

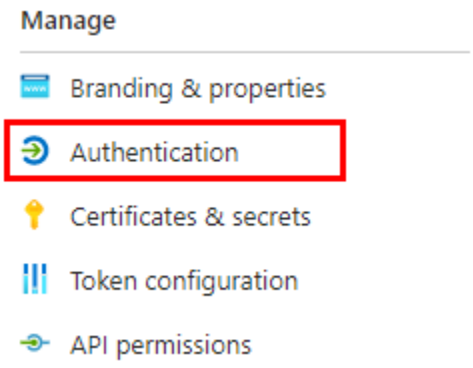
6. Select *Register*.

   The app is registered in Microsoft Azure.

Authentication settings

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

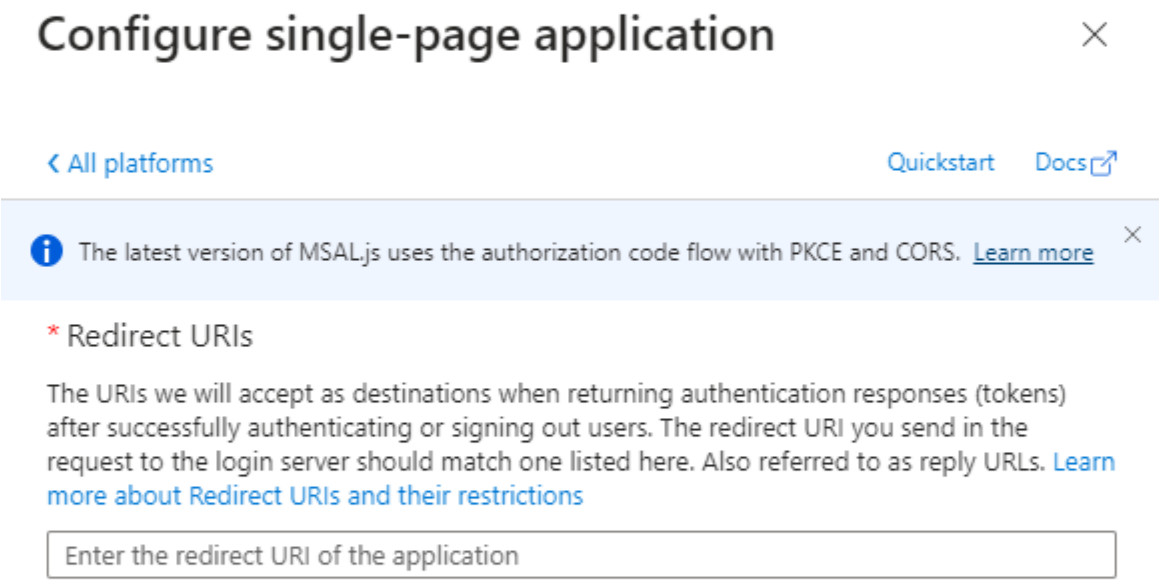
1. In Microsoft Azure, go to *Authentication*.



2. Select *Add a platform*.

   The *Configure platform* area appears.

3. Select *Single-page application*.


Configure single-page application
All platforms
Quickstart
Docs
Learn more
* Redirect URIs
Enter the redirect URI of the application

The latest version of MSAL.js uses the authorization code flow with PKCE and CORS. Learn more

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

   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
```

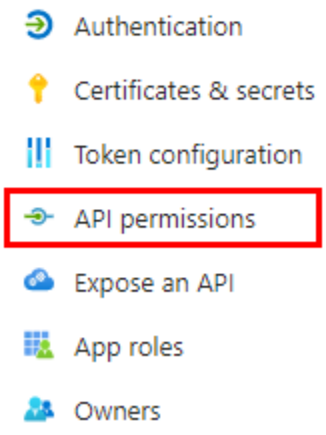
> **Information**
>
> The URL must match the path to ELO Azure Administration in the respective ELO environment.

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.

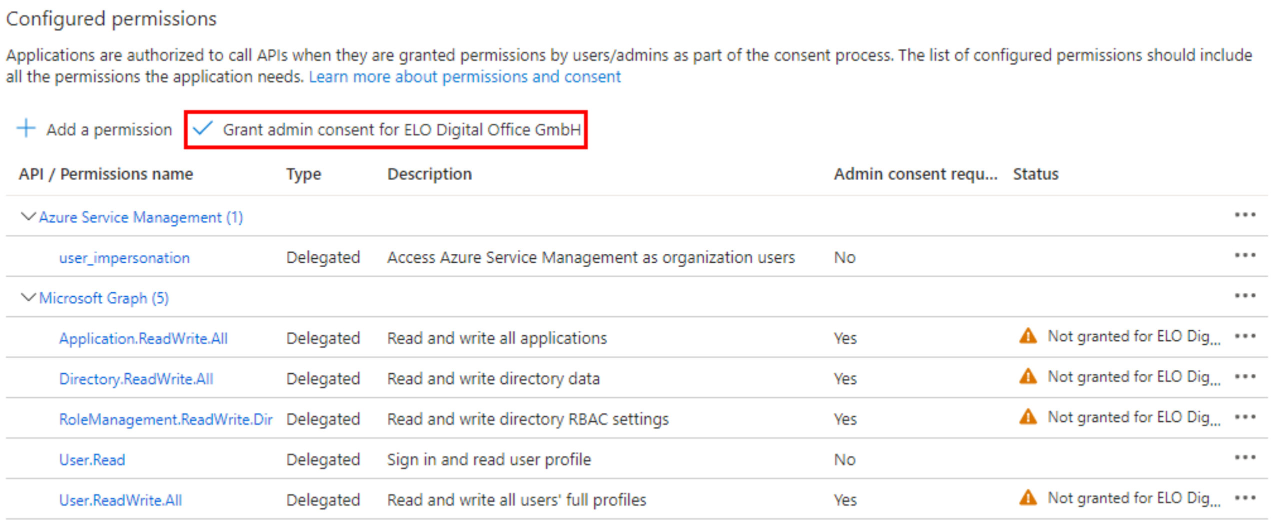


1. Open the *API permissions* area.
2. Select *Add permissions*.

   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



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	
Azure Service Management (1)					•••
user_impersonation	Delegated	Access Azure Service Management as organization users	No		•••
Microsoft Graph (5)					•••
Application.ReadWrite.All	Delegated	Read and write all applications	Yes	⚠ Not granted for ELO Dig...	•••
Directory.ReadWrite.All	Delegated	Read and write directory data	Yes	⚠ Not granted for ELO Dig...	•••
RoleManagement.ReadWrite.Dir	Delegated	Read and write directory RBAC settings	Yes	⚠ Not granted for ELO Dig...	•••
User.Read	Delegated	Sign in and read user profile	No		•••
User.ReadWrite.All	Delegated	Read and write all users' full profiles	Yes	⚠ Not granted for ELO Dig...	•••

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

   The *Confirm admin consent* dialog box opens.

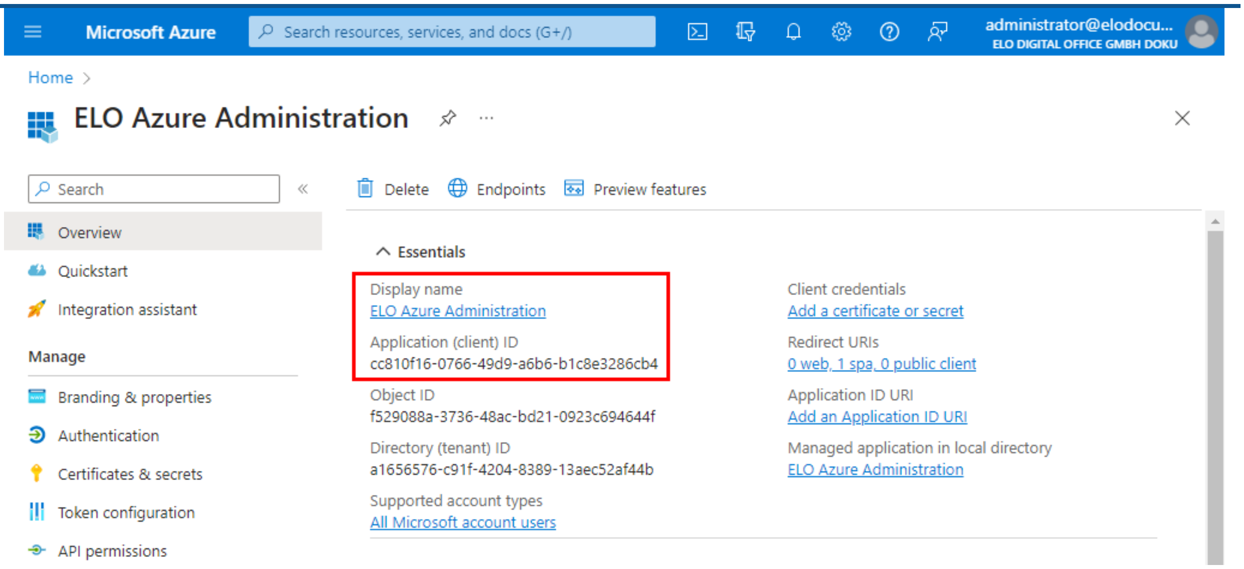
2. Click *Yes* to confirm.

   The permissions are added.

Configuring the service

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

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



Display name
ELO Azure Administration

Application (client) ID
cc810f16-0766-49d9-a6b6-b1c8e3286cb4

Object ID
f529088a-3736-48ac-bd21-0923c694644f

Directory (tenant) ID
a1656576-c91f-4204-8389-13aec52af44b

Supported account types
All Microsoft account users

Client credentials
Add a certificate or secret

Redirect URIs
0 web, 1 spa, 0 public client

Application ID URI
Add an Application ID URI

Managed application in local directory
ELO Azure Administration

2. Copy the values of the following fields:
   - Display name
   - Application ID (client)
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.

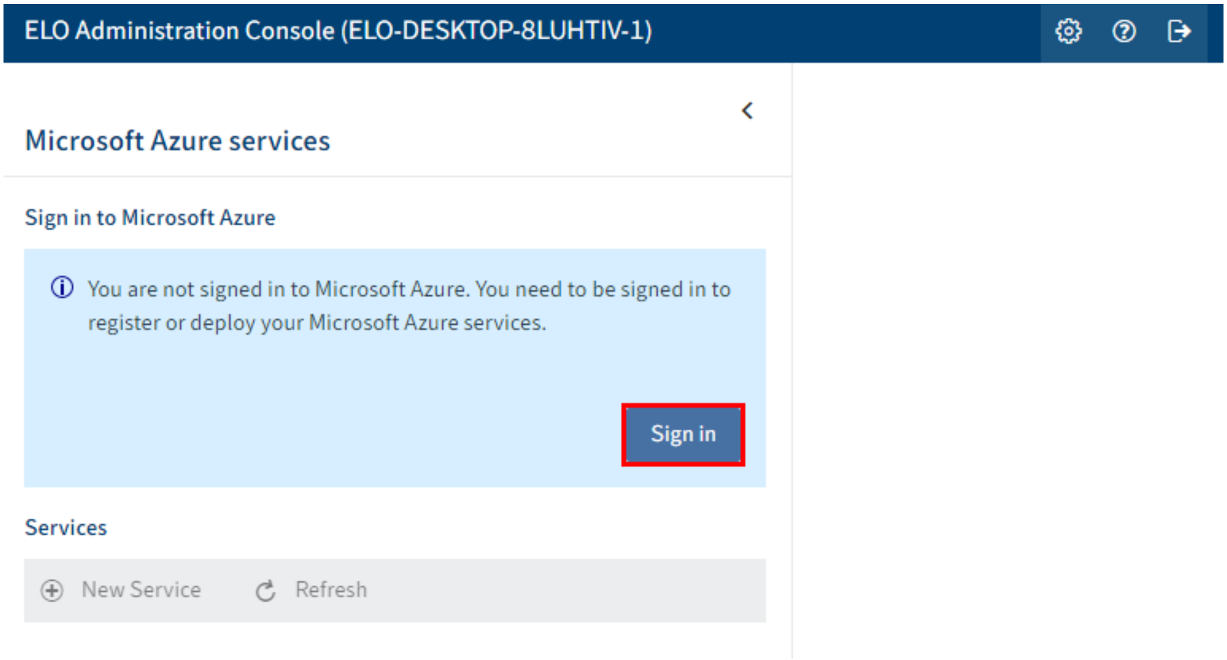
7. Restart the *ELO Azure Administration* service.

   Service configuration is now complete. 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.



ELO Administration Console (ELO-DESKTOP-8LUHTIV-1)

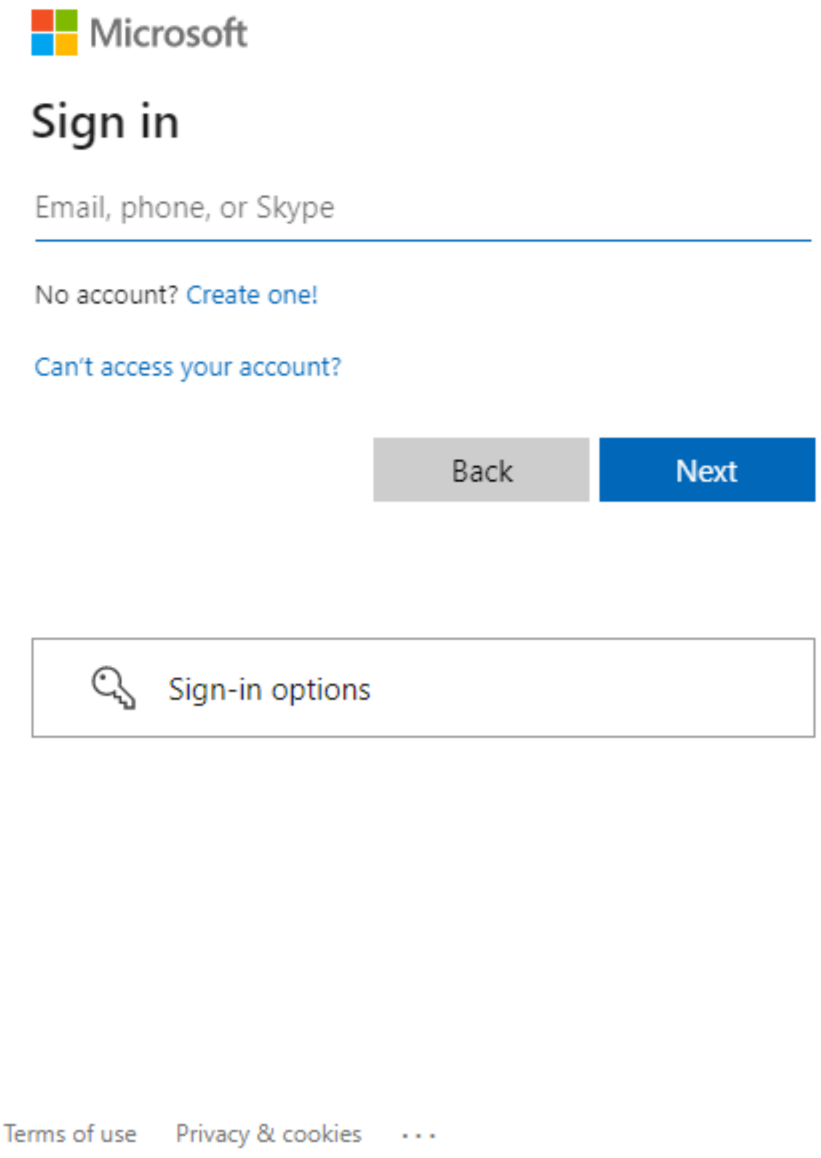
Microsoft Azure services

Sign in to Microsoft Azure

You are not signed in to Microsoft Azure. You need to be signed in to register or deploy your Microsoft Azure services.

Services

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).

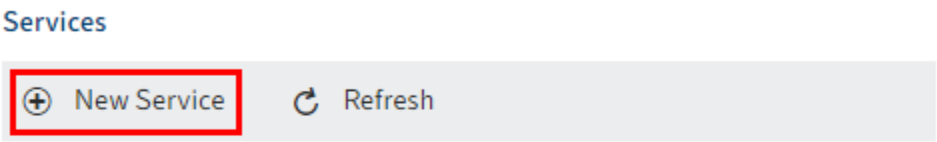
   ELO Azure Administration is now connected to Microsoft Azure. You can now create services.

Services

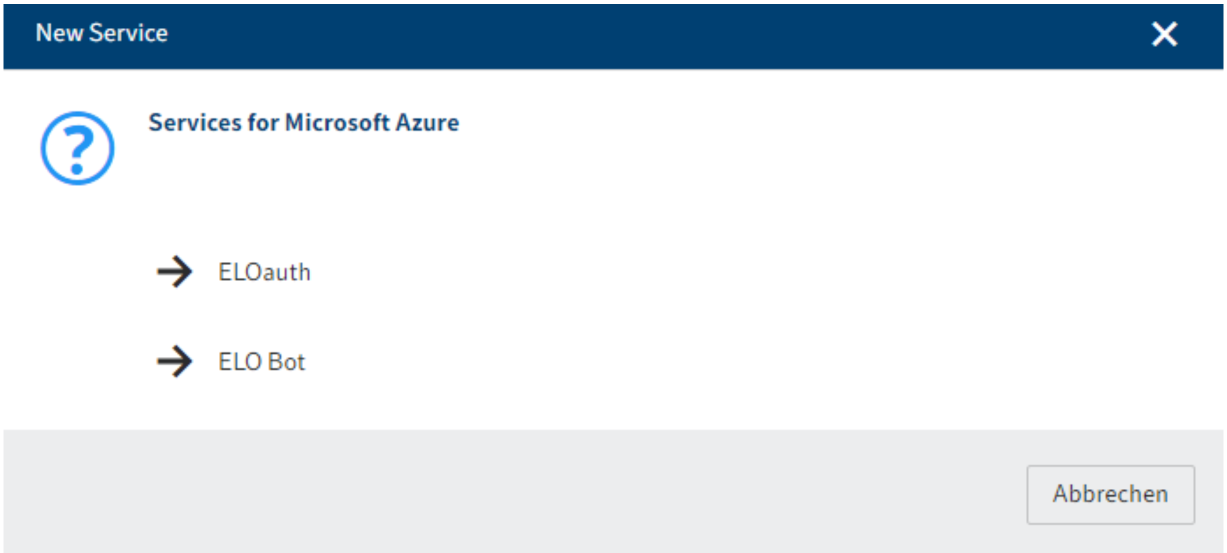
After successful logon, you can create services for Microsoft Azure apps via ELO Azure Administration.

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.

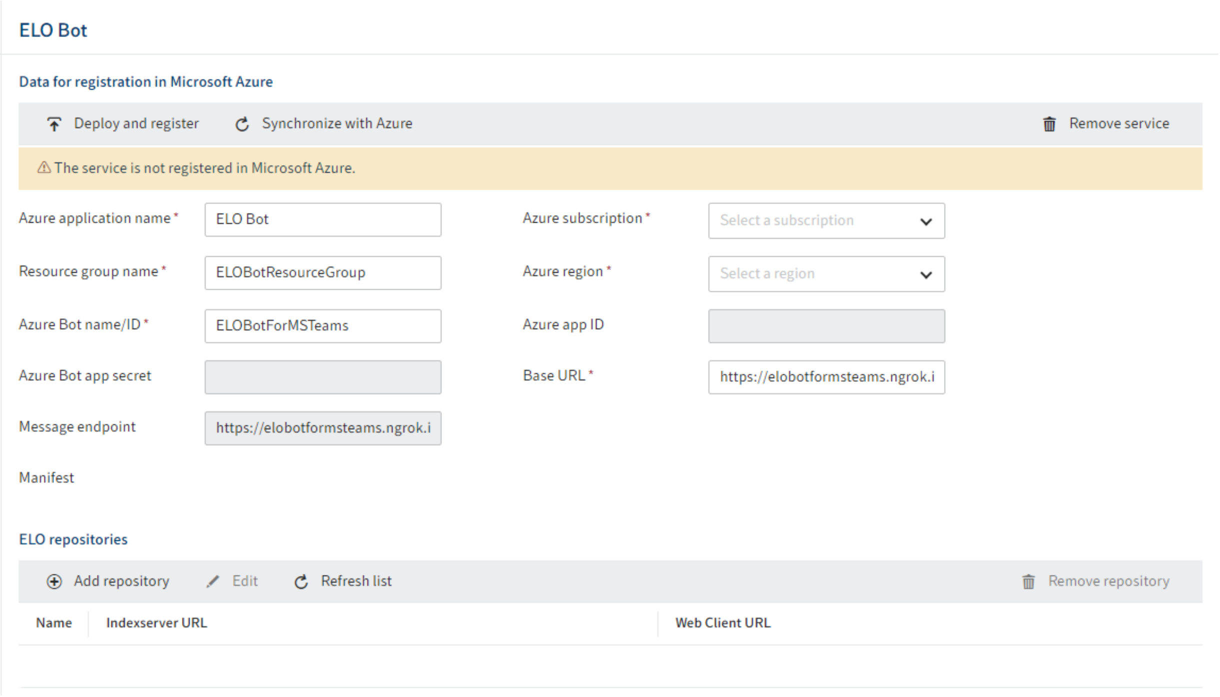
3. Select a service.

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.



ELO Bot

Data for registration in Microsoft Azure

⚠ The service is not registered in Microsoft Azure.

Azure application name *	ELO Bot	Azure subscription *	Select a subscription
Resource group name *	ELOBotResourceGroup	Azure region *	Select a region
Azure Bot name/ID *	ELOBotForMSTeams	Azure app ID	
Azure Bot app secret		Base URL *	https://elobotformsteams.ngrok.i
Message endpoint	https://elobotformsteams.ngrok.i		
Manifest			

ELO repositories

Name	Indexserver URL	Web Client URL

The configuration interface for the service opens.

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

Please note

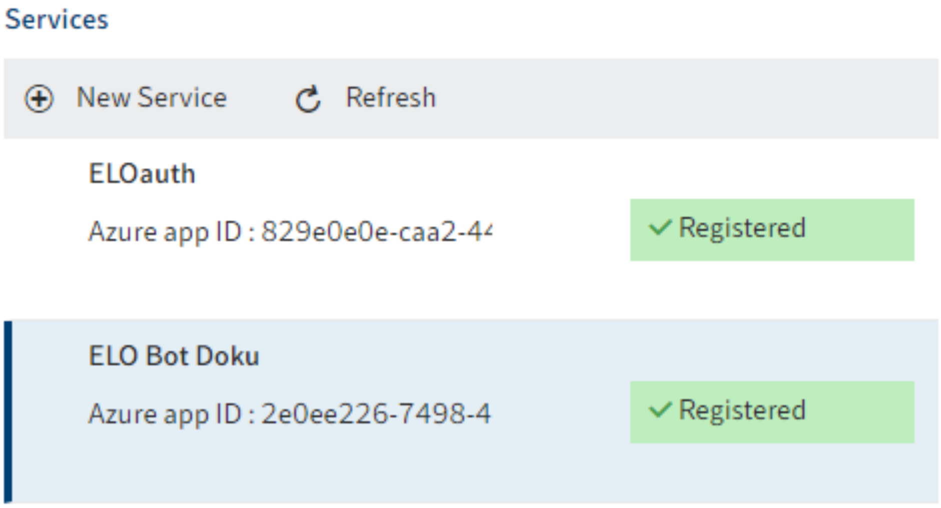
The base URL entered for the ELO Bot must be able to forward queries from the Internet to the internal ELO Bot for MS Teams service and must be available online.

You will find general information on the *ELO Bot* and *ELOauth* 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

> **Please note**
>
> If you use both the ELO Bot and ELOauth, you will have to register them via the same Azure app to enable communication between the services.

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



Services

ELOauth

Azure app ID : 829e0e0e-caa2-44

✓ Registered

ELO Bot Doku

Azure app ID : 2e0ee226-7498-4

✓ Registered

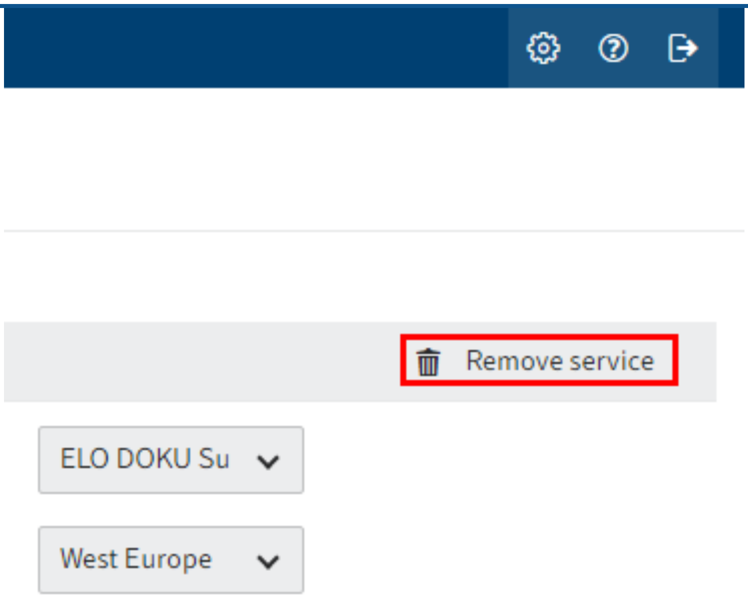
The service is registered as an app in Microsoft Azure. In ELO Azure Administration, the services are shown as *Registered*. You can now use the services.

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.