



Configuration and administration

ELO Azure Administration



Table of contents

ELO Azure administration	3
Requirements	3
Initial app registration in Microsoft Azure	4
Authentication	10
Services	13

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

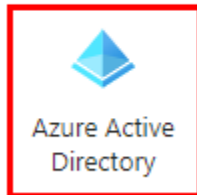
For ELO Azure Administration to connect to Microsoft Azure, you will have to register the app in Microsoft Azure first.

Please note

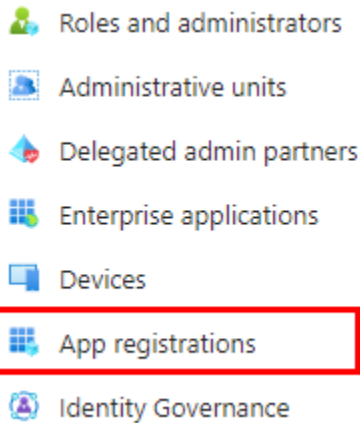
This documentation does not cover basic configuration of a Microsoft Azure environment or subscriptions, both of which are required for this.

1. Log on to Microsoft Azure as an administrator.

Azure services



2. Open the *Azure Active Directory* service.



3. Go to *App registrations*.

The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar and the text 'Microsoft Azure'. Below that, the breadcrumb 'Home > ELO Digital Office GmbH DOKU' is visible. The main heading is 'ELO Digital Office GmbH DOKU | App registrations'. A navigation menu on the left includes 'Overview', 'Preview features', 'Diagnose and solve problems', 'Manage', 'Users', and 'Groups'. The main content area has a '+ New registration' button highlighted with a red box, along with 'Endpoints', 'Troubleshooting', 'Refresh', 'Download', and 'Preview features' options. A notification banner states: '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 Micros...'. Below the notification, there are tabs for 'All applications', 'Owned applications', and 'Deleted applications'. A search bar for filtering applications is present, with the text 'Start typing a display name or application (client) ID to filter these r...' and an 'Add filters' button.

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*.

The screenshot shows the 'Manage' section of the Microsoft Azure portal. It includes a horizontal line and several options: 'Branding & properties', 'Authentication' (highlighted with a red box), 'Certificates & secrets', 'Token configuration', and 'API permissions'.

2. Select *Add a platform*.

The *Configure platform* area appears.

3.

Select *Single-page application*.

Configure single-page application ×

[< All platforms](#) [Quickstart](#) [Docs](#)

i The latest version of MSAL.js uses the authorization code flow with PKCE and CORS. [Learn more](#) ×

*** Redirect URIs**

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](#)

Enter the redirect URI of the application

The *Configure single-page application* area opens.

- 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.

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

The authentication settings are now configured.

API permissions

The app for ELO Azure Administration requires several permissions.

-  Authentication
-  Certificates & secrets
-  Token configuration
-  API permissions
-  Expose an API
-  App roles
-  Owners

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](#)

+ Add a permission ✔ Grant admin consent for ELO Digital Office GmbH

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 the *ELO Azure Administration* service in the ELO system.

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

The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar and navigation icons. The main content area is titled 'ELO Azure Administration'. On the left, there's a sidebar with navigation options like 'Overview', 'Quickstart', 'Integration assistant', 'Manage', 'Branding & properties', 'Authentication', 'Certificates & secrets', 'Token configuration', and 'API permissions'. The 'Overview' page is active, displaying a table of 'Essentials' for the application. A red box highlights the 'Display name' (ELO Azure Administration) and the 'Application (client) ID' (cc810f16-0766-49d9-a6b6-b1c8e3286cb4). Other fields include Object ID (f529088a-3736-48ac-bd21-0923c694644f), Directory (tenant) ID (a1656576-c91f-4204-8389-13aec52af44b), and Supported account types (All Microsoft account users). On the right, there are links for 'Client credentials', 'Redirect URIs', and 'Application ID URI'.

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"  
},
```

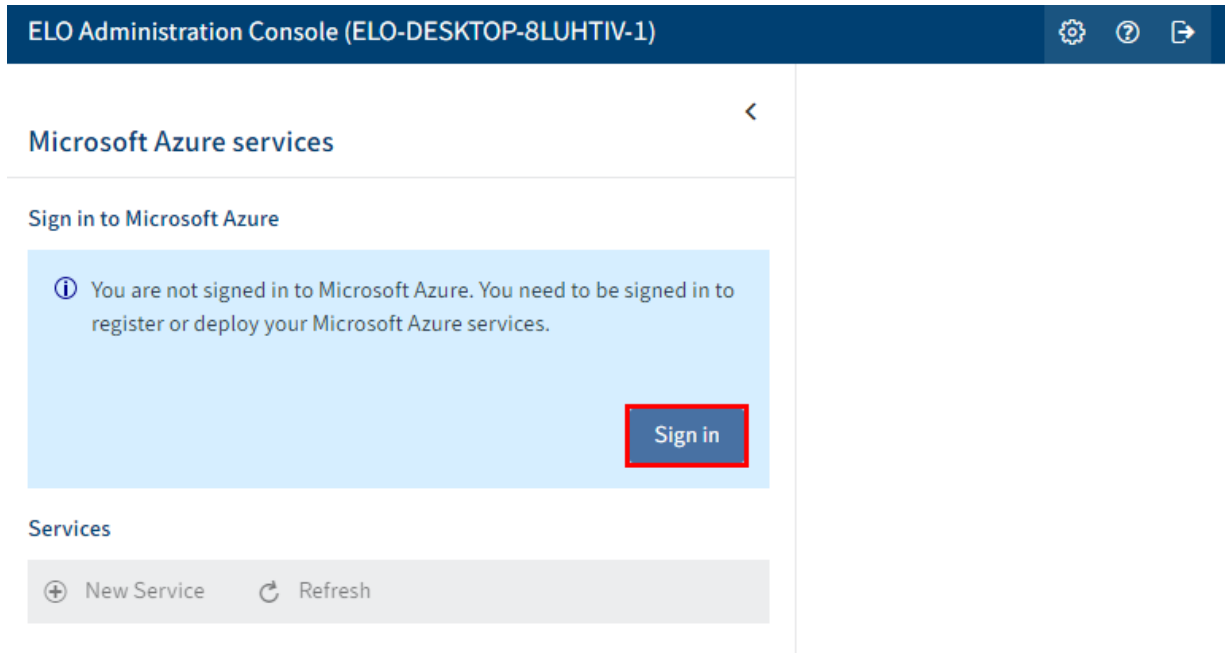
6. Save the file.
7. Restart the *ELO Azure Administration* service.

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*.



Sign in

Email, phone, or Skype

No account? [Create one!](#)

[Can't access your account?](#)

Back

Next



Sign-in options

[Terms of use](#) [Privacy & cookies](#) ...

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.

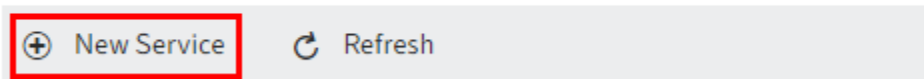
Services

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

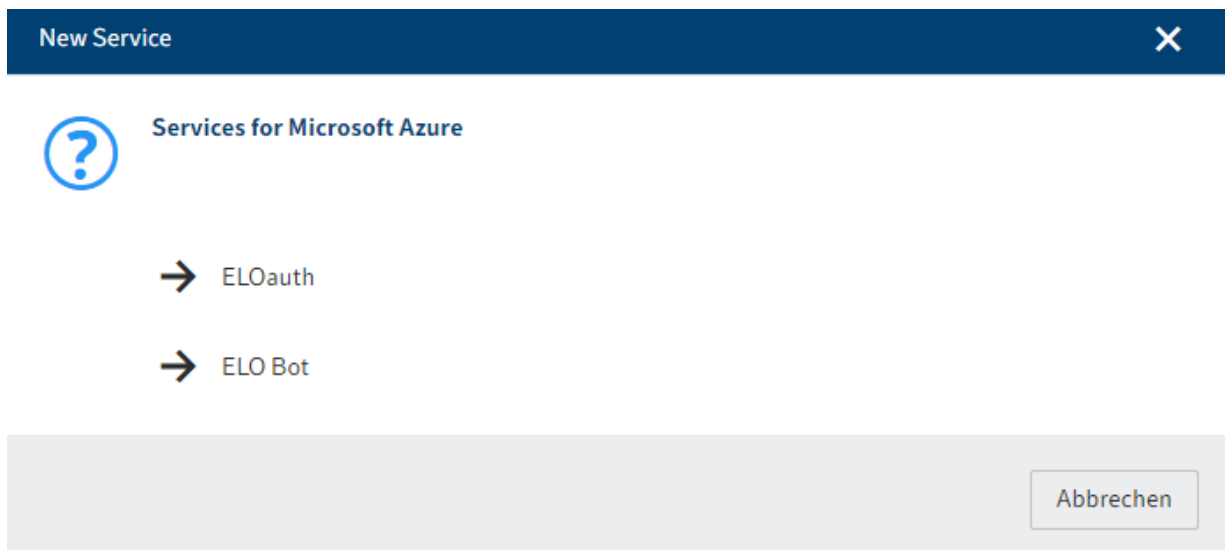
Create service

1. Open ELO Azure Administration.

Services



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

Deploy and register Synchronize with Azure Remove service

⚠ 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

Add repository Edit Refresh list Remove repository

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.

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*.

Services

Services

+ New Service Refresh

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.

Settings Help Share

Remove service

ELO DOKU Su

West Europe

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.