empower suite

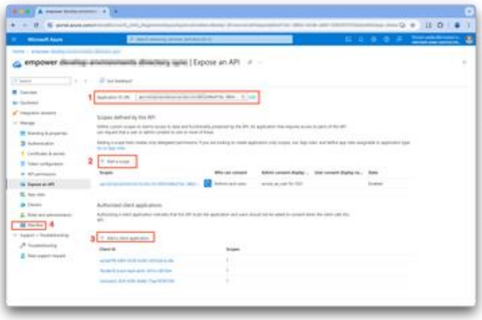
Version: August 2024

Contents

App Registration Settings for SSO

Adjust Existing App Registration

In production, it is not necessary to create a new app registration as there’s already an existing empower® app registration, which is also used by the empower® Sync or the empower® backend (e.g. for the directory sync), that can be adapted.



In total, 4 settings need to be changed in order to configure SSO in the existing app registration:

- Add and configure an Application ID URI
- Add and configure scopes
- Add and configure authorized client applications
- Set the required access token version

1.1.1 Add and configure an Application ID URI

Select the designated Microsoft Entra ID App Registration

- Navigate to *Expose an API*
- Click on **Add** right next to *Application ID URI*
- By default, it is generated in the form of **api://<applicationId>**
- Change the API URI to reflect the following schema **api://<fullyQualifiedDomainName>/<applicationId>**

<applicationId> is the unique identifier of the app registration (aka client ID).

<fullyQualifiedDomainName> is the endpoint from which the backend (and specifically our web sync) is hosted.

If that contains a port number, include it as well.

Example:

If your empower® Web App is accessible at

https://empower.empowersuite.cloud/empower/websync/app

and your existing app registration has application ID

bfed17dc-380d-42d8-a90f-f2802f2152b4

then your *application ID URI* would be:

api://empower.empowersuite.cloud/bfed17dc-380d-42d8-a90f-f2802f2152b4

Please note:
Find additional information on that topic here: https://learn.microsoft.com/en-us/office/dev/add-ins/develop/register-sso-add-in-aad-v2#expose-a-web-ap

Make sure the *<fully-qualified-domain-name>* matches the host name of the instance of your empower® installation.

Note the *api:// prefix*.

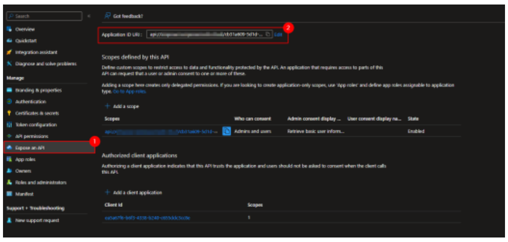
Note down the *application ID* and *application ID URI* as they will be used for configuring SSO when installing the empower® Web Sync.

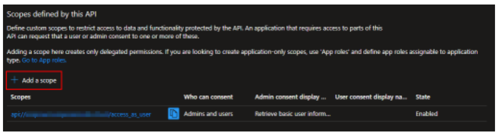
> **Please note:**
> Provide us with the *application ID* and *application ID URI* if you are hosting empower® in your own corporate cloud.

1.1.2 Add and configure scopes

Click on *Add a scope*.

1. Set the *Scope name* to **access_as_user**.
2. Set the *Admin consent display name* to **Retrieve basic user information**
3. Set the *Admin consent description* to **Allow empower® to access basic information on behalf of the Office user** to identify them in add-ins that support Single Sign-On.

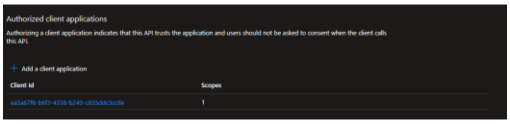




> **Please note:**
> Find additional information here: https://learn.microsoft.com/en-us/office/dev/add-ins/develop/register-sso-add-in-aad-v2#add-a-scope

1.1.3 Add and configure authorized client applications

Add the following 3 client IDs to the list of authorized client applications.



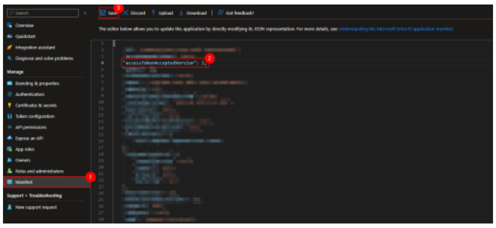
These GUIDs are **predefined clients from Microsoft that bundle a selection of Microsoft Office** applications:

- ea5a67f6-b6f3-4338-b240-c655ddc3cc8e (All Office Applications)
- 1fec8e78-bce4-4aaf-ab1b-5451cc387264 (Teams Desktop + Mobile)
- 5e3ce6c0-2b1f-4285-8d4b-75ee78787346 (Teams Web)

> **Please note:**
> Find additional information as well as the id ↔ product mapping here: https://learn.microsoft.com/en-us/office/dev/add-ins/develop/register-sso-add-in-aad-v2#add-a-scope (Section 5).

1.1.4 Set the required access token version

This setting cannot be set via the UI and has to be set directly via the *manifest*.



1. Click on **Manifest**.
2. Change the value of *accessTokenAcceptedVersion*.
3. By default, it is set to *null* and must be set to *2*: **"accessTokenAcceptedVersion": 2,**
4. Click **save**.

> **Please note:**
> Find additional information here: https://learn.microsoft.com/en-us/entra/identity-platform/reference-app-manifest#accesstokenacceptedversion-attribute.