ELO Sync

Authentication and authorization

Table of contents

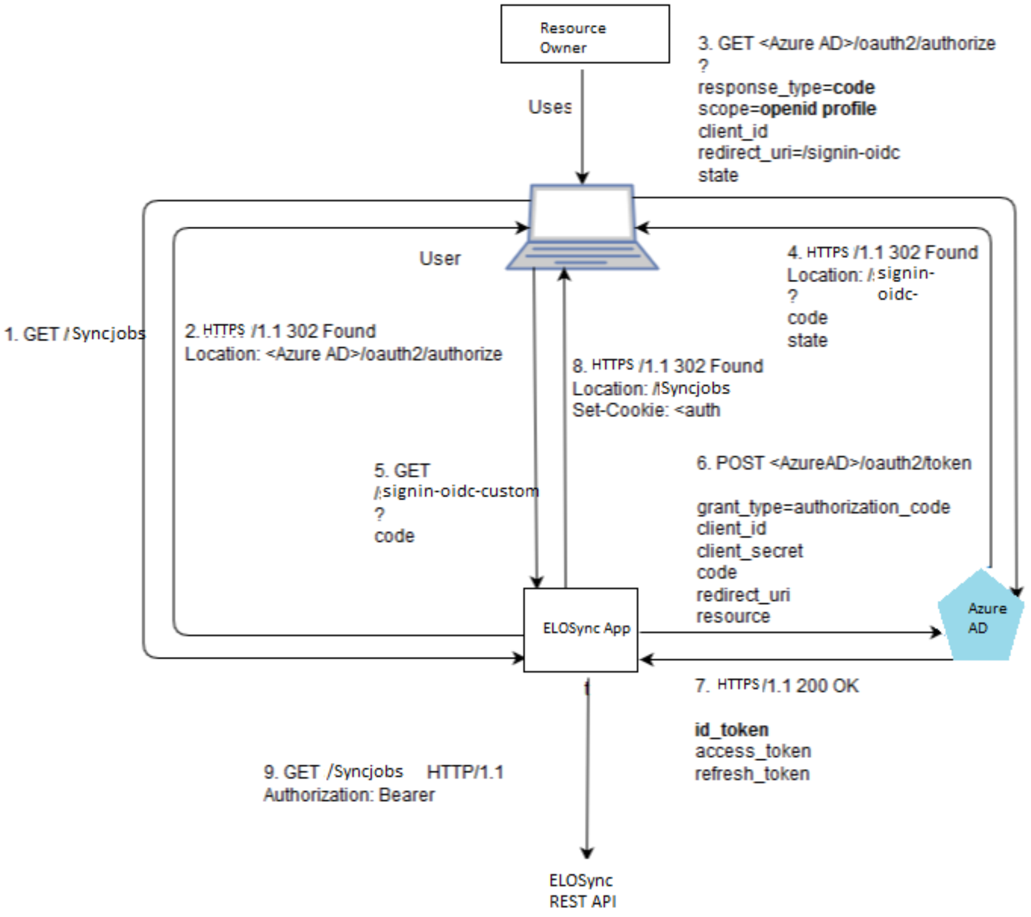
Authentication and authorization in ELO Sync

ELO Sync uses OpenID authentication for users via the ELO Sync web UI. An app registration has to be created in Azure for this purpose. The required steps are described in the chapter Azure.

> **Information**
>
> From Azure's point of view, ELO Sync is a confidential client app, meaning authentication data must be managed on the server side.
>
> For this reason, all received access data is stored in a distributed cache in the database used by ELO Sync.

Code Flow in ELO Sync

The following figure shows the OpenID Authentication Code Flow and the OAuth 2.0 Authorization Flow used by ELO Sync.



Entra user access data

After successful authentication in Microsoft Entra ID, ELO Sync receives the user access data for the current user.

This includes the access token and the refresh token. This data is used to enable background synchronization for the user.

The received user access data is stored in a *distributed cache/database* for later use. The table used for storage is called *elosync_msal*.

You can find more information in the table overview in the chapter on the database.

Each logged on user has an entry in the *elosync_msal* table with a unique key. The unique key currently has the following structure: `{User Object ID}.{Tenant ID}`.

The ELO Sync Service user also has an entry in this table, but because the Service User isn't a real user, its key has the structure: `{Client ID}_{Tenant ID}`.

User authentication in ELO

After the access token is received from Entra ID, the individual users must also access the ELO repository.

The ELOauth plug-in for the ELO Indexserver is required for this reason and must be configured with a profile that uses the same tenant as ELO Sync.

See the chapter OAuth section in the configuration for more details on configuring the ELO Sync site and the ELO Indexserver documentation for the ELOauth plug-in.

Permission for applications

This article describes the steps required for a third-party application to access the ELO Sync REST API.

This requires the third-party application to be registered in Azure with the permission to access the ELO Sync API.

Authentication with Azure

The third-party application should authenticate with Azure with the following parameters:

```
**TODO**
```

After this, authentication returns an access token for the application that has to be used for every request to ELO Sync (sent in the HTTP header `Authorization`).