ELO Sync

Postman

Inhaltsverzeichnis

Postman

Accessing the ELOSync REST API with Postman

This chapter will explain how to use Postman to access and test the ELO Sync REST API.

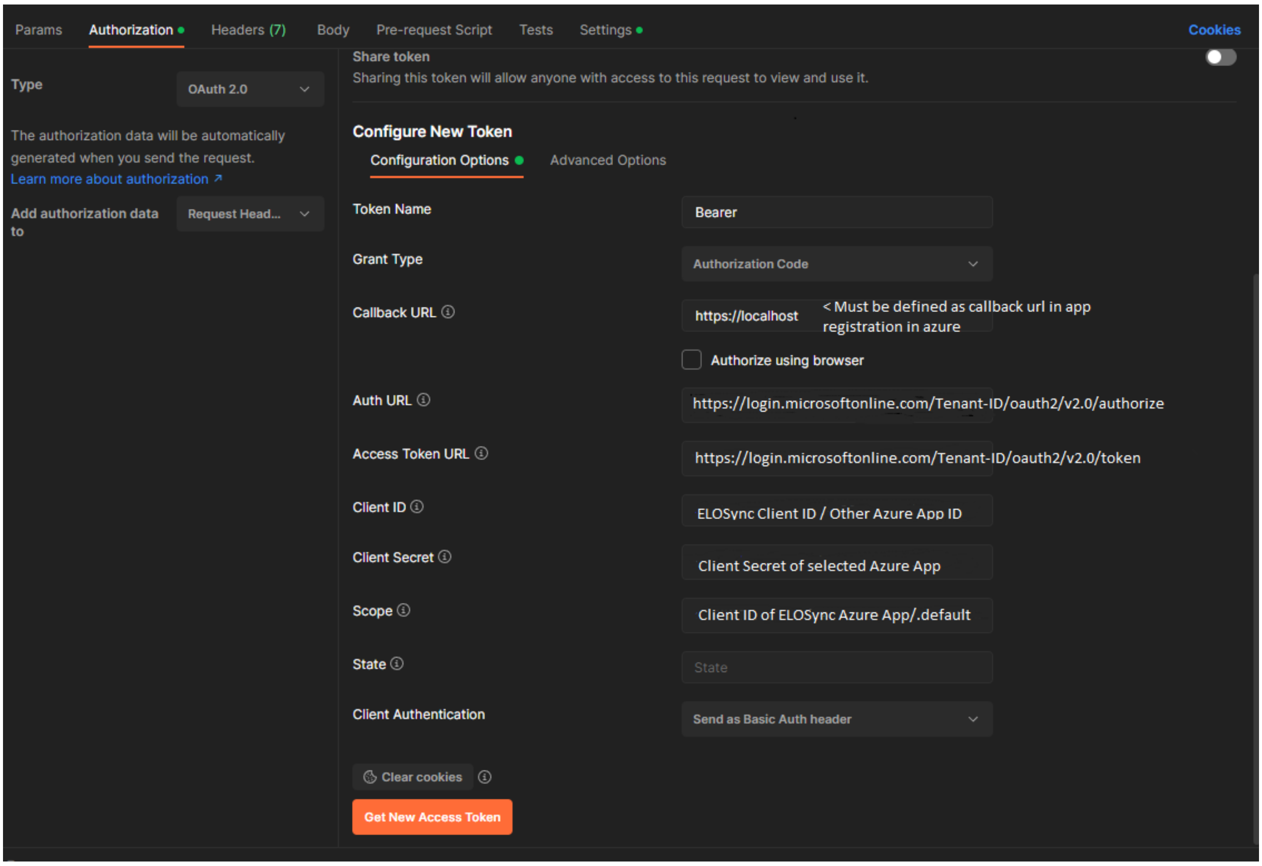
Since a user's access token is required to access ELO Sync, you must specify an Azure application in Postman against which authentication should take place.

There are two choices:

1. You use the Azure app that also uses ELOSync for user authentication

2. You use a different Azure app, but define Syncjobs.ReadWrite.All from the application created in chapter Create ELO Sync Azure App as the required right.

To obtain the access token in Postman, switch to the Authorization tab and select Oauth 2.0. You can select any name for the bearer token name. Select Authorization Code as Grant Type and proceed as shown in the picture below.



Type: OAuth 2.0

The authorization data will be automatically generated when you send the request.

Add authorization data to: Request Head...

Share token

Sharing this token will allow anyone with access to this request to view and use it.

Configure New Token

Token Name: Bearer

Grant Type: Authorization Code

Callback URL: https://localhost < Must be defined as callback url in app registration in azure

□ Authorize using browser

Auth URL: https://login.microsoftonline.com/Tenant-ID/oauth2/v2.0/authorize

Access Token URL: https://login.microsoftonline.com/Tenant-ID/oauth2/v2.0/token

Client ID: ELOSync Client ID / Other Azure App ID

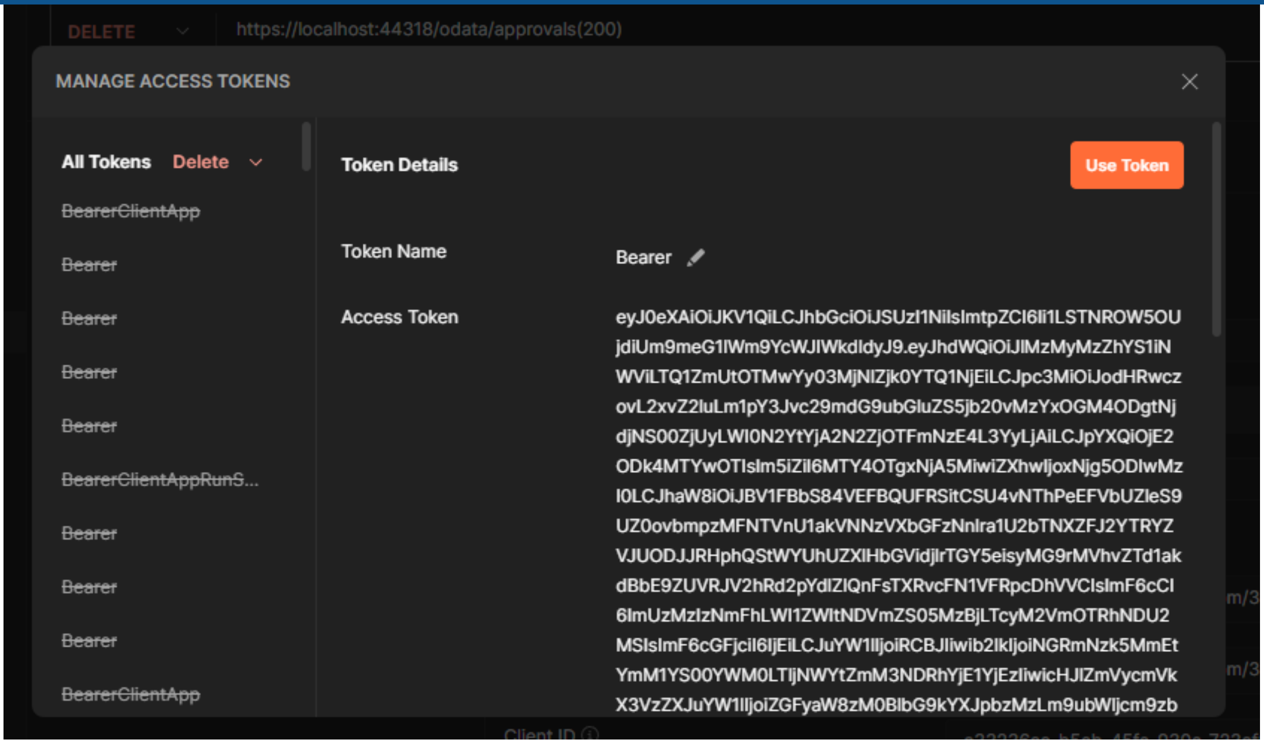
Client Secret: Client Secret of selected Azure App

Scope: Client ID of ELOSync Azure App/.default

State: State

Client Authentication: Send as Basic Auth header

Once you have entered all the data, click the Get New Access Token button to receive the Access Token. If the login to Azure was successful, you will receive the access token in the image below.



~~BearerClientApp~~

~~Bearer~~

~~Bearer~~

~~Bearer~~

~~Bearer~~

~~BearerClientAppRunS...~~

~~Bearer~~

~~Bearer~~

~~Bearer~~

~~BearerClientApp~~

Token Details

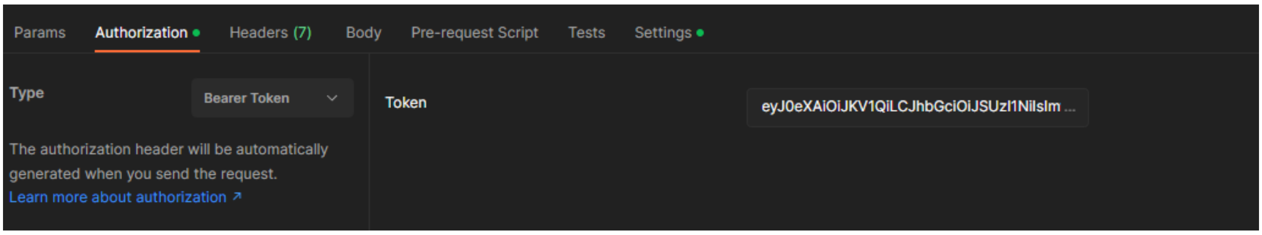
Token Name: Bearer

Access Token:

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Ii1LSTNROW5OU
jdiUm9meG1lWm9YcWJIWkdldyJ9.eyJhdWQiOiJlMzMyMzZhYS1iN
WViLTQ1ZmUtOTMwYy03MjNlZjk0YTQ1NjEiLCJpc3MiOiJodHRwcz
ovL2xvZ2luLm1pY3Jvc29mdG9ubGluZS5jb20vMzYxOGM4ODgtNj
djNS00ZjUyLWI0N2YtYjA2N2ZjOTFmNzE4L3YyLjAiLCJpYXQiOjE2
ODk4MTYwOTIsIm5iZiI6MTY4OTgxNjA5MiwiZXhwIjoxNjg5ODIwMz
I0LCJhaW8iOiJBV1FBbS84VEFBQUFRSitCSU4vNThPeEFVbUZleS9
UZ0ovbmpzMFNTVnU1akVNNzVXbGFzNnlra1U2bTNXZFJ2YTRYZ
VJUODJJRHphQStWYUhUZXlHbGVidjlrTGY5eisyMG9rMVhvZTd1ak
dBbE9ZUVRJV2hRd2pYdlZlQnFsTXRvcFN1VFRpcDhVVCIsImF6cCI
6ImUzMzIzNmFhLWI1ZWItNDVmZS05MzBjLTcyM2VmOTRhNDU2
MSIsImF6cGFjciI6IjEiLCJuYW1lIjoiRCBJIiwib2lkIjoiNGRmNzk5MmEt
YmM1YS00YWM0LTljNWYtZmM3NDRhYjE1YjEzIiwicHJlZmVycmVk
X3VzZXJuYW1lIjoiZGFyaW8zM0BlbG9kYXJpbzMzLm9ubWljcm9zb
```

First copy the token to the clipboard, as it will be needed elsewhere, and then click on the Use Token button.

In the Authorization tab, navigate to the Bearer authorization type and enter the access token from the clipboard.

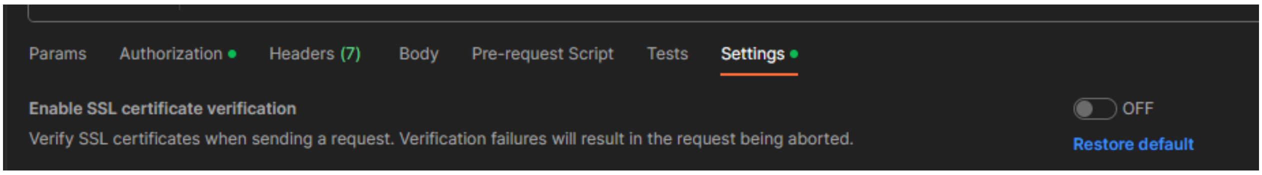


Type: Bearer Token

The authorization header will be automatically generated when you send the request.

Token: eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIm ...

Next, switch to the Settings tab and deactivate the verification of the SSL certificate.



Enable SSL certificate verification: OFF

Verify SSL certificates when sending a request. Verification failures will result in the request being aborted.

Now you can define the desired URL and the parameters and send the request.