ELO Sync

Postman



3

3

Table des matières

Postman

Accessing the ELOSync REST API with Postman

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.

Params Authorization •	Headers (7) Bod	ly Pre-request Script Tests Settings •		Cookies
Туре ОАш	ıth 2.0 🗸 🗸	Share token Sharing this token will allow anyone with access to the second s	his request to view and use it.	
The authorization data will be au generated when you send the re Learn more about authorization	utomatically equest.	Configure New Token Configuration Options Advanced Options		
Add authorization data Reg	uest Head 🗸 🗸	Token Name	Bearer	
		Grant Type	Authorization Code V	
		Callback URL ③	https://localhost registration in azure	
			Authorize using browser	
		Auth URL ^①	https://login.microsoftonline.com/Tenant-ID/oauth2/v2.0/authoriz	e
		Access Token URL ③	https://login.microsoftonline.com/Tenant-ID/oauth2/v2.0/token	
		lient ID () ELOSync Client ID / Other Azure App ID	ELOSync Client ID / Other Azure App ID	
		Client Secret ^①	Client Secret of selected Azure App	
		Scope ③	Client ID of ELOSync Azure App/.default	
		State ①		
		Client Authentication	Send as Basic Auth header \sim	
		🖏 Clear cookies 🚯		
		Get New Access Token		

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.

DELETE v https://localhost:44318/odata/approvals(200)						
MANAGE ACCESS TOKENS ×						
All Tokens Delete 🗸	Token Details	Use Token				
BearerClientApp						
Bearer	Token Name	Bearer 💉				
Bearer	Access Token	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NilsImtpZCl6li1LSTNROW5OU idiUm9meG1lWm9YcWJlWkdldvJ9.evJhdWQiOiJIMzMvMzZhYS1iN				
Bearer		WVILTQ1ZmUtOTMwYy03MjNIZjk0YTQ1NjEILCJpc3MiOiJodHRwcz				
Deeres		ovL2xvZ2luLm1pY3Jvc29mdG9ubGluZS5jb20vMzYxOGM40DgtNj				
bearer		djNS00ZjUyLWI0N2YtYjA2N2ZjOTFmNzE4L3YyLjAiLCJpYXQiOjE2				
BearerClientAppRunS		ODk4MTYwOTIsIm5iZil6MTY4OTgxNjA5MiwiZXhwljoxNjg5ODlwMz				
		UZ00vbmpzMFNTVnU1akVNNzVXbGFzNnIra1U2bTNXZE12YTRYZ				
Bearer		VJUODJJRHphQStWYUhUZXIHbGVidjirTGY5eisyMG9rMVhvZTd1ak				
Bearer		dBbE9ZUVRJV2hRd2pYdlZlQnFsTXRvcFN1VFRpcDhVVClsImF6cCl				
		6ImUzMzIzNmFhLWI1ZWItNDVmZS05MzBjLTcyM2VmOTRhNDU2				
Bearer		MSIsImF6cGFjcil6ljEiLCJuYW1lljoiRCBJliwib2lkljoiNGRmNzk5MmEt				
BearerClientApp		YmM1YS00YWM0LTljNWYtZmM3NDRhYjE1YjEzliwicHJIZmVycmVk	m/3			
		X3VZZXJUYW IIIJOIZGFYAW8ZMUBIDG9KYXJpbZMZLm9ubWijcm9Zb				

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.



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



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