

BULK ACTIVATION TOOL FOR AZURE MFA OATH TOKENS V0.4

FOR INTERNAL USE AND BETA-TESTING ONLY. DO NOT DISTRIBUTE!

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

1. INTRODUCTION

The current process to activate an OATH token with Azure MFA is cumbersome, error-prone and needs Global Administrators (GA) valuable time. Token2 has developed a solution to automate the activation of imported hardware tokens with Azure MFA. This is a PowerShell based solution that uses the same CSV file used to import the OATH tokens to Azure MFA. Instead of manually entering the OTP code generated on the hardware token, the solution uses the CSV file to calculate the current OTP using the secret of each token and submits it directly to Azure MFA endpoint via an HTTPS request.

2. HOW THIS TOOL WORKS

Microsoft is using web endpoints API for OATH token activation process. Although it is not documented, by analyzing the API calls initiated by the Azure AD admin web interface, we found methods and parameters used, which allows to automatically apply the same operations to multiple tokens in an automated manner.

It is important to mention that as this is a non-documented feature, there is always a risk that Microsoft will change the APIs or methods used by this tool.

3. PRE-REQUISITES

Following is needed to bulk activate the tokens.

- A csv file with tokens associated with user UPNs. This is the same file used to import the tokens to Azure MFA. The tokens must have already been imported, but not activated, as shown on the example below:

Dashboard > **Multi-Factor Authentication | OATH tokens**

Getting started
 Diagnose and solve problems
 Settings

Account lockout
 Block/unblock users
 Fraud alert
 Notifications
OATH tokens
 Phone call settings
 Providers
 Manage MFA Server
 Server settings
 One-time bypass
 Caching rules
 Server status
 Reports
 Activity report
 Troubleshooting + Support
 New support request

Upload Download Delete Refresh Documentation Columns Got feedback?

To get started, select the Upload button above and choose a .csv file. This file should contain the secret keys for the OATH tokens you wish to use. The column should be: "upn, serial number, secret key, time interval, manufacturer, model".
 For more information on available authentication and verification methods, view the public documentation.

Name	Username	Serial Number	Model	Manufacturer	Activated
<input type="checkbox"/> user11	user11@versoix.onmicr...	1234623092672	C202	Token2	Activate
<input type="checkbox"/> User5	user5@versoix.onmicros...	1234623738430	C202	Token2	Activate
<input type="checkbox"/> user15	user15@versoix.onmicr...	1234623738477	C202	Token2	Activate
<input type="checkbox"/> user18	user18@versoix.onmicr...	1234623738480	C202	Token2	Activate
<input type="checkbox"/> user10	user10@versoix.onmicr...	1234623747686	C202	Token2	Activate
<input type="checkbox"/> User Three	User3@versoix.onmicro...	1234623321028	C202	Token2	Activate
<input type="checkbox"/> user12	user12@versoix.onmicr...	1234623092674	C202	Token2	Activate
<input type="checkbox"/> user8	user8@versoix.onmicros...	1234623497298	C202	Token2	Activate
<input type="checkbox"/> user20	user20@versoix.onmicr...	1234623092688	C202	Token2	Activate
<input type="checkbox"/> user14	user14@versoix.onmicr...	1234623738476	C202	Token2	Activate
<input type="checkbox"/> user19	user19@versoix.onmicr...	1234623738481	C202	Token2	Activate
<input type="checkbox"/> user7	user7@versoix.onmicros...	1234623836867	C202	Token2	Activate
<input type="checkbox"/> user9	user9@versoix.onmicros...	1234623305030	C202	Token2	Activate
<input type="checkbox"/> user6	user6@versoix.onmicros...	1234623474251	C202	Token2	Activate

[If you need to exclude some users from this process, simply remove corresponding lines in the CSV file]

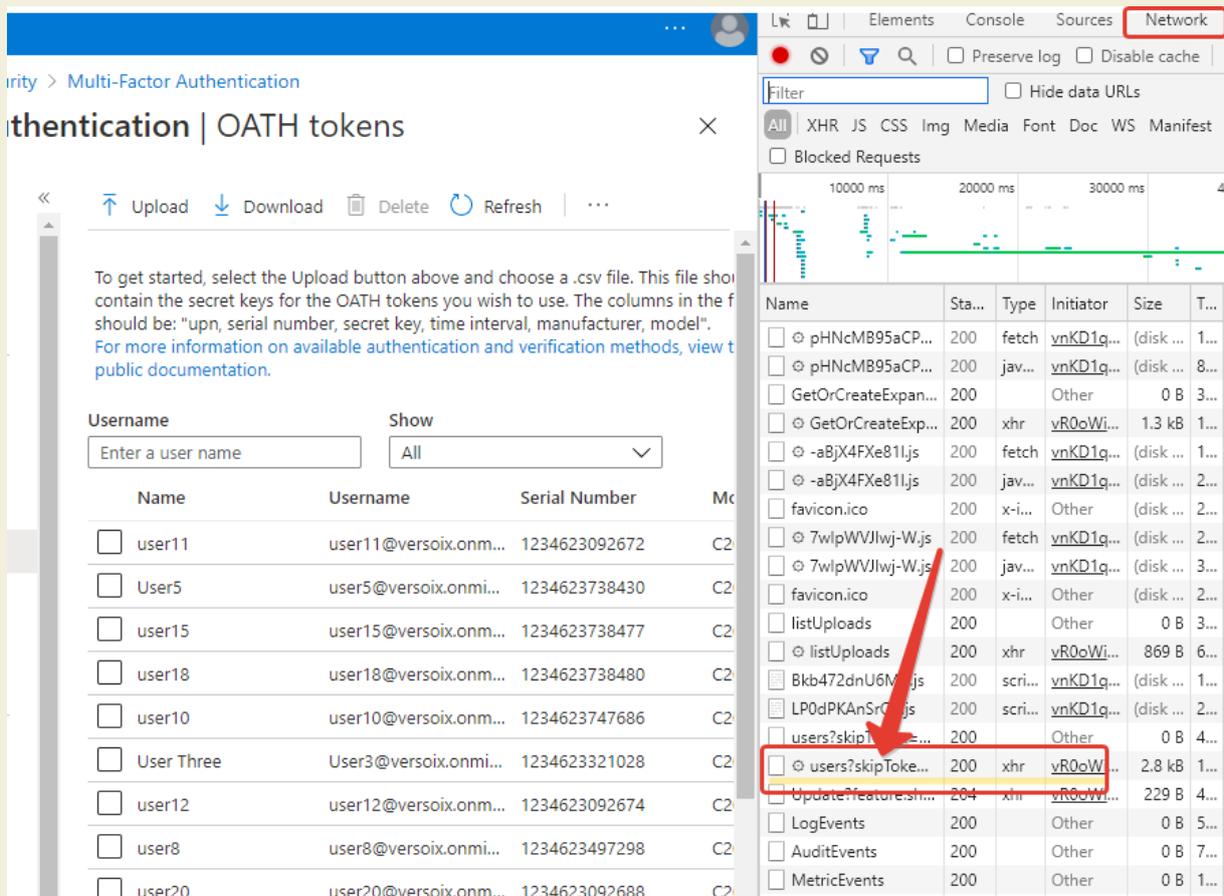
- **OATH-Bulk-Activate.exe** file – this is the main executable that will take care of the bulk activation
- Azure Web Endpoint Authorization key string – to be obtained from your Admin portal web session; see instructions in the next section

4. OBTAIN WEB ENDPOINT AUTHORIZATION KEY

Azure Web Endpoint Authorization key string is a web session value that will be sent to Azure MFA web endpoints to authorize the actions. Follow the steps below to obtain the Authorization key. The steps below are the same with any browser, but we will use Google Chrome as an example.

1. Open your browser (currently, **only Google Chrome** can be used) and login to your Azure Admin portal using a Global Tenant Administrator account. The direct URL is: <https://aad.portal.azure.com/>
2. Navigate to Azure Active Directory -> Security -> MFA -> OATH Tokens page

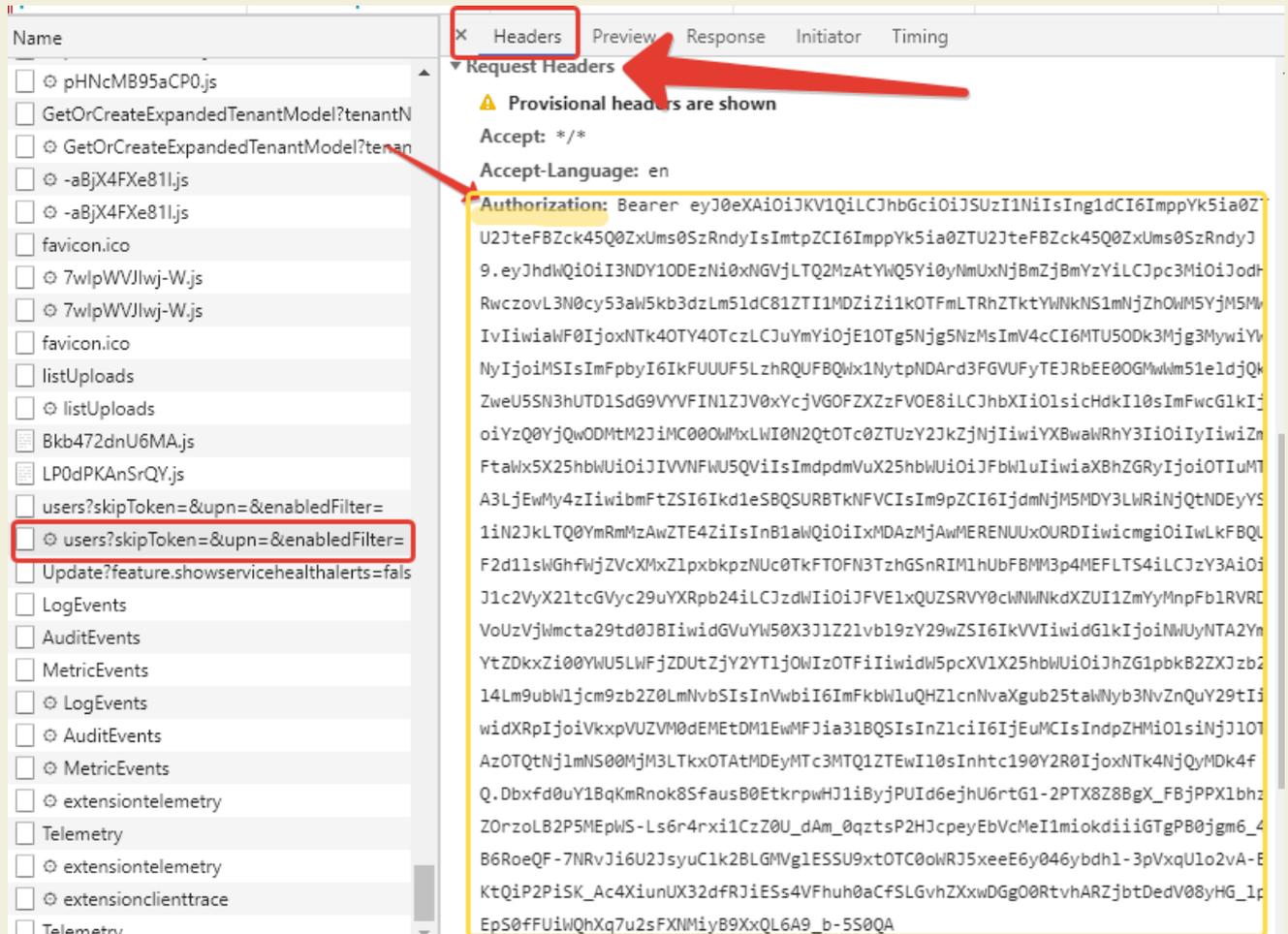
3. Open Developer tools of your browser (Menu -> More Tools -> Developer Tools of F12 key on your keyboard)
4. Select Network tab on the Developer Tools
5. Refresh the current page (OATH Tokens list) and wait for the page to fully reload
6. In the Developer Tools > Network, look for an XHR response named “users?skipToken...”



Click on “users?skipToken...” line. This will open a list of headers sent by the resource

7. Scroll down to “Request Headers” section, find the “Authorization” header value, and copy it to clipboard. The string should start with “Bearer” text. Copying the text is a bit non-trivial (due to colors used in that area of the window). See the video below to have a look at the whole procedure:

<https://youtu.be/VyVuRLTNAAtM>



- Save the key to a text file named “AuthKey.txt” in the same folder with the exe file or keep it in the clipboard – this will be requested when you launch the tool.

IMPORTANT:

This key is valid for a limited amount of time, you may need to redo this operation if your session times out

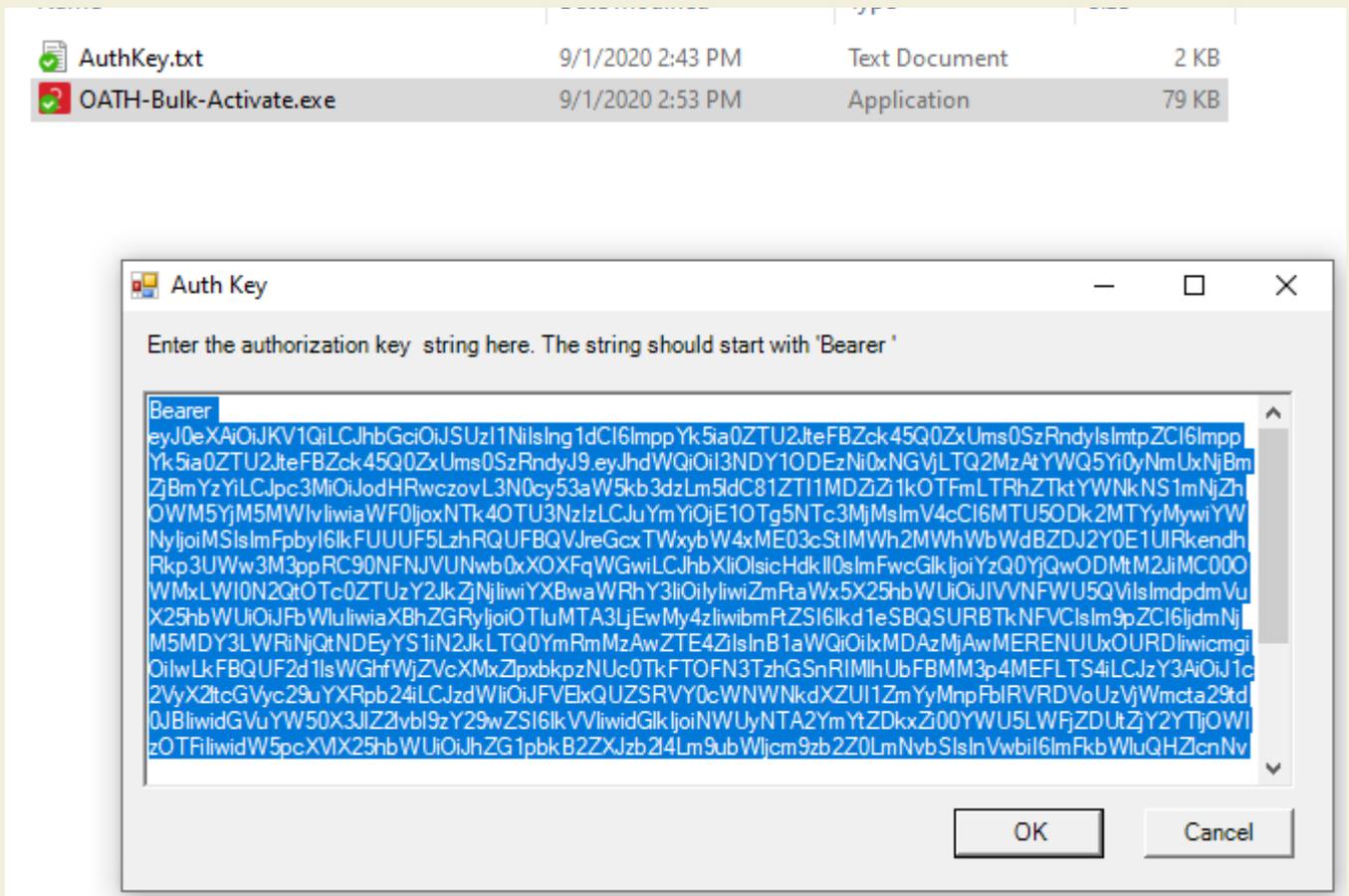
Handle this key with care, this is of a same importance as your admin password.

5. BULK ACTIVATE OATH TOKENS

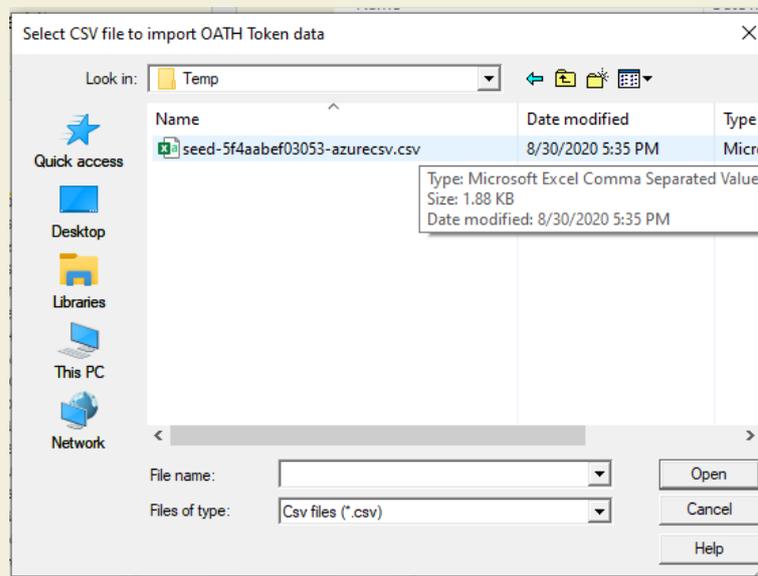
Have the CSV file and the Authorization key ready. Then, run **OATH-Bulk-Activate.exe** file and follow the steps below.

When launched, the application will ask for the Authorization key (or will read it from

AuthKey.txt file located in the same directory)



On the text step, it will ask to select the CSV file



On the next step, the tool will ask you to confirm the number of tokens to be activated.



*This step is new in Rel.4 – previously the script was assuming that the tokens imported are to be activated immediately. The reason for asking for this value is because the endpoint API used by this tool are not returning the total number of users. You don't have to put exact number here, just approximate would be fine – important to put a number that is definitely **higher than the number of imported tokens**.*

After you confirm the number, the bulk activation process starts immediately. The progress will be shown similar to below.

```
#####TOKEN2 AZURE OATH TOKENS - BULK ACTIVATION SCRIPT #####

This tool is designed exclusively for TOKEN2 Customers and partners
A written authorization from TOKEN2 is required to use this script
Using this tool without TOKEN2's approval is prohibited

#####
You selected the file: C:\[redacted] token2\tools\Bulk Activator\MFA-tokens2.csv
Total Count of tokens in the CSV:
80
----- Activating OATH token for user11@versoix.onmicrosoft.com -----

displayName upn                serialNumber    OTP
-----
user11      user11@versoix.onmicrosoft.com 865362618848581 546326

Result:
Activation successful.
```



Successfully activated OATH token should show “Activation successful” as a result. If an error is thrown, check the next section to identify the reason

6. LIST OF ERRORS

Endpoint access error

```
#####TOKEN2 AZURE OATH TOKENS - BULK ACTIVATION SCRIPT #####  
  
This tool is designed exclusively for TOKEN2 Customers and partners  
A written authorization from TOKEN2 is required to use this script  
Using this tool without TOKEN2's approval is prohibited  
  
#####  
You selected the file: C:\[redacted]  
Total Count of tokens in the CSV:  
6  
Endpoint access error. Please check the AuthKey and/or your internet connectivity  
Press any key to close this window..
```



This error means the Authorization Key is wrong or has already expired. Follow the instructions in Section 4 and obtain a new key.

Firewall-related issues

Although the tool is using standard ports (80 and 443) some “smart” firewall solutions (i.e Symantec or Cisco) may be limiting internet access per application. The symptoms are similar to the error shown below, but there may be other messages shown as well:

“Cannot bind argument to parameter 'InputObject' because it is null”

```
#####TOKEN2 AZURE OATH TOKENS - BULK ACTIVATION SCRIPT #####  
  
This tool is designed exclusively for TOKEN2 Customers and partners  
A written authorization from TOKEN2 is required to use this script  
Using this tool without TOKEN2's approval is prohibited  
  
#####  
You selected the file: C:\[redacted] CSV  
Total Count of tokens in the CSV:  
[redacted]  
ERROR: Cannot bind argument to parameter 'InputObject' because it is null.  
ERROR: Cannot bind argument to parameter 'InputObject' because it is null.  
ERROR: Cannot bind argument to parameter 'InputObject' because it is null.  
ERROR: Cannot bind argument to parameter 'InputObject' because it is null.  
ERROR: Cannot bind argument to parameter 'InputObject' because it is null.
```

The solution to this is to white-list the application (“OATH-Bulk-Activate-Rel4.exe”) in the firewall settings.

Activation failed

```
----- Activating OATH token for user18@versoix.onmicrosoft.com -----  
  
displayName upn                serialNumber    OTP  
-----  
user18      user18@versoix.onmicrosoft.com 865362619716547 242330  
  
Result:  
Activation failed. Check the values in the CSV file.
```

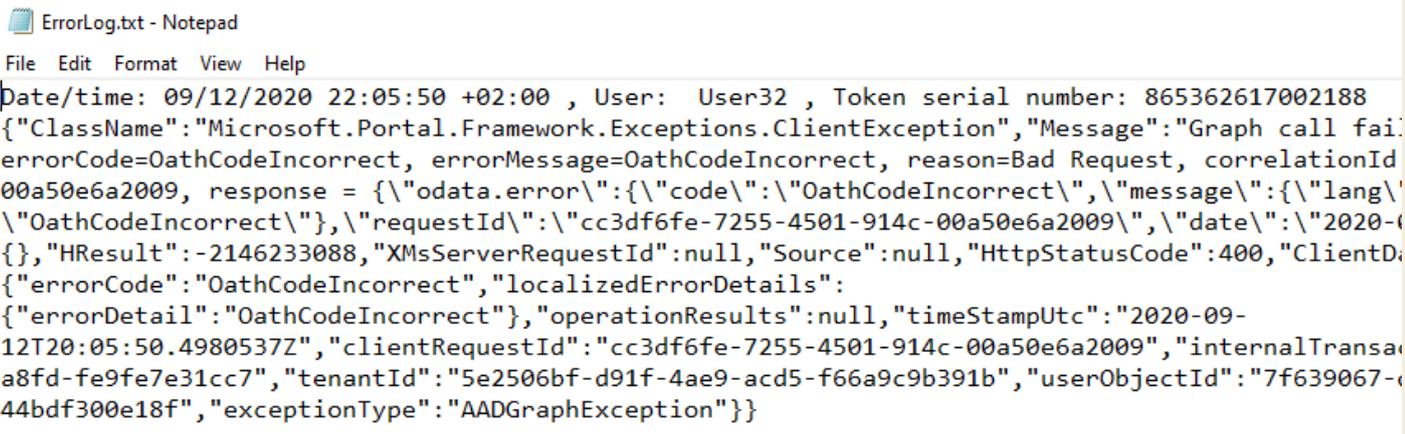


This error is shown when the OTP sent for activation is wrong, this can happen in following cases:

- The secret value in the CSV file is wrong or incomplete
- The line for the token is missing in the CSV file (this is normal if you removed a user from the file to skip the activation, the error will still be shown)
- The time or time zone on your machine is wrong (OTP calculation relies on local system time, so this is important)

Log file

The tool creates a log file with more details for deeper troubleshooting. The file is created in the same folder as *ErrorLog.txt*. Please make sure the user running the tool is able to create files in the current directory. Log history is not kept, the will gets truncated when the tool is (re)launched.



```
ErrorLog.txt - Notepad  
File Edit Format View Help  
Date/time: 09/12/2020 22:05:50 +02:00 , User: User32 , Token serial number: 865362617002188  
{ "ClassName": "Microsoft.Portal.Framework.Exceptions.ClientException", "Message": "Graph call fai:  
errorCode=OathCodeIncorrect, errorMessage=OathCodeIncorrect, reason=Bad Request, correlationId  
00a50e6a2009, response = { \"odata.error\": { \"code\": \"OathCodeIncorrect\", \"message\": { \"lang\  
\"OathCodeIncorrect\", \"requestId\": \"cc3df6fe-7255-4501-914c-00a50e6a2009\", \"date\": \"2020-0  
{, \"HResult\": -2146233088, \"XMsServerRequestId\": null, \"Source\": null, \"HttpStatusCode\": 400, \"ClientD  
{ \"errorCode\": \"OathCodeIncorrect\", \"localizedErrorDetails\":  
{ \"errorDetail\": \"OathCodeIncorrect\", \"operationResults\": null, \"timestampUtc\": \"2020-09-  
12T20:05:50.4980537Z\", \"clientRequestId\": \"cc3df6fe-7255-4501-914c-00a50e6a2009\", \"internalTransac  
a8fd-fe9fe7e31cc7\", \"tenantId\": \"5e2506bf-d91f-4ae9-acd5-f66a9c9b391b\", \"userObjectId\": \"7f639067-c  
44bdf300e18f\", \"exceptionType\": \"AADGraphException\" } }
```