TOKEN2 | CHE-218.895.438
chemin du Pré-Colomb 10
CH-1290 Versoix
office@token2.ch
+41 22 519 62 02

BULK ACTIVATION TOOL FOR AZURE MFA OATH TOKENS V0.4

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

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

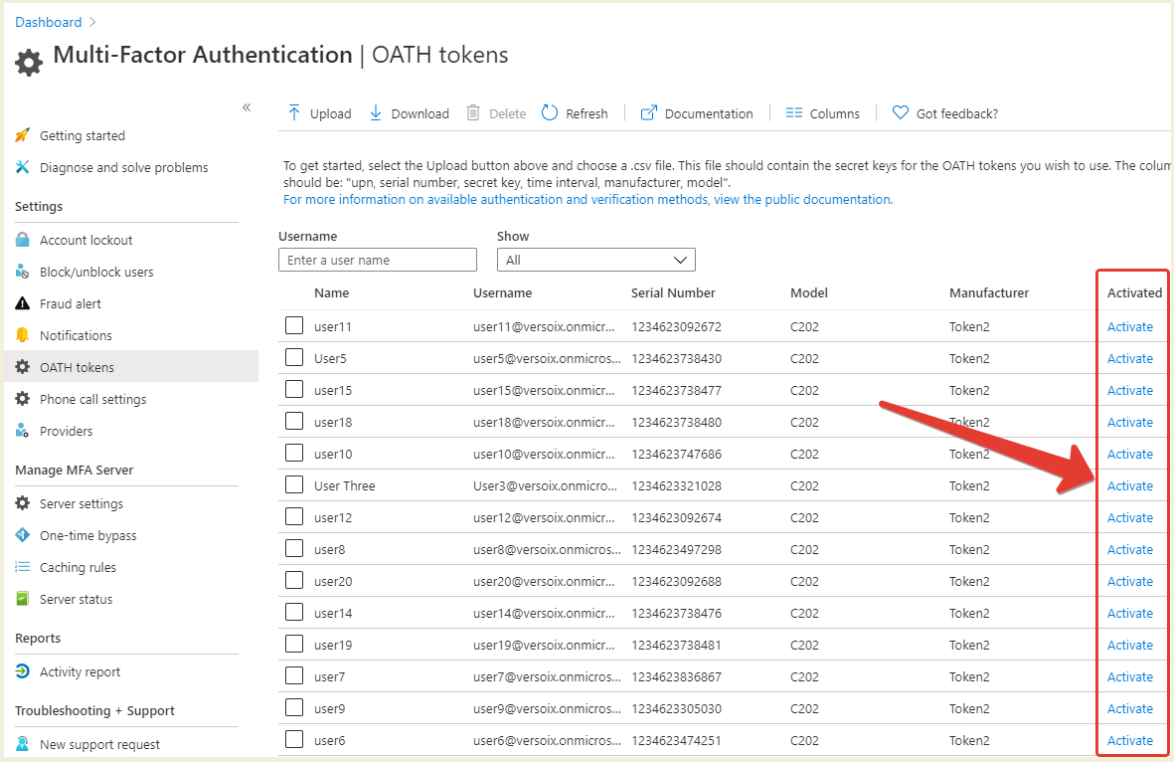
Microsoft is using web endpoints API for OATH token activation process. Although it is not documented, by analyzing the API calls initiated by the Azure AD admin web interface, we found methods and parameters used, which allows to automatically apply the same operations to multiple tokens in an automated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

TOKEN2 | CHE-218.895.438
chemin du Pré-Colomb 10
CH-1290 Versoix
office@token2.ch
+41 22 519 62 02



[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

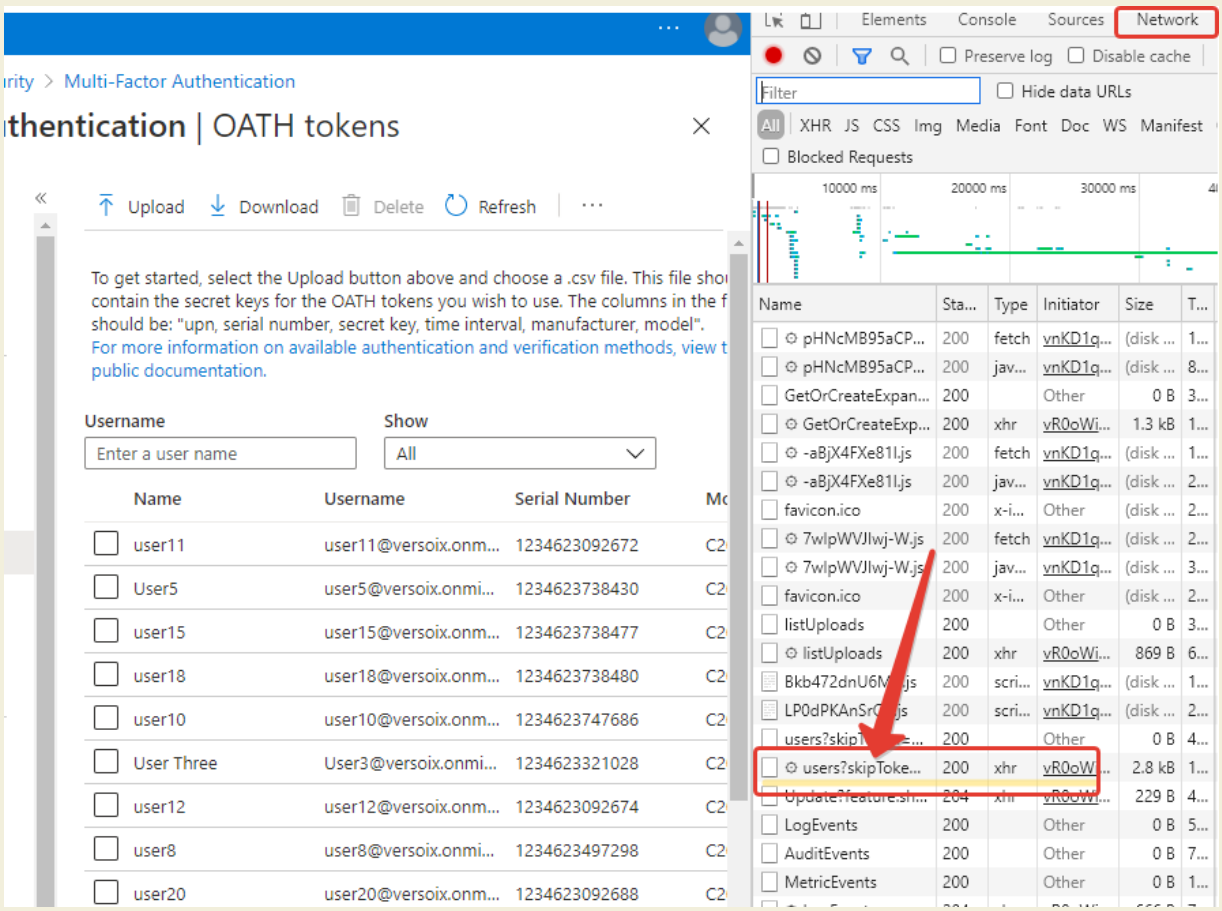
Azure Web Endpoint Authorization key string is a web session value that will be sent to Azure MFA web endpoints to authorize the actions. Follow the steps below to obtain the Authorization key. The steps below are the same with any browser, but we will use Google Chrome as an example.

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

TOKEN2 | CHE-218.895.438
chemin du Pré-Colomb 10
CH-1290 Versoix
office@token2.ch
+41 22 519 62 02

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…"

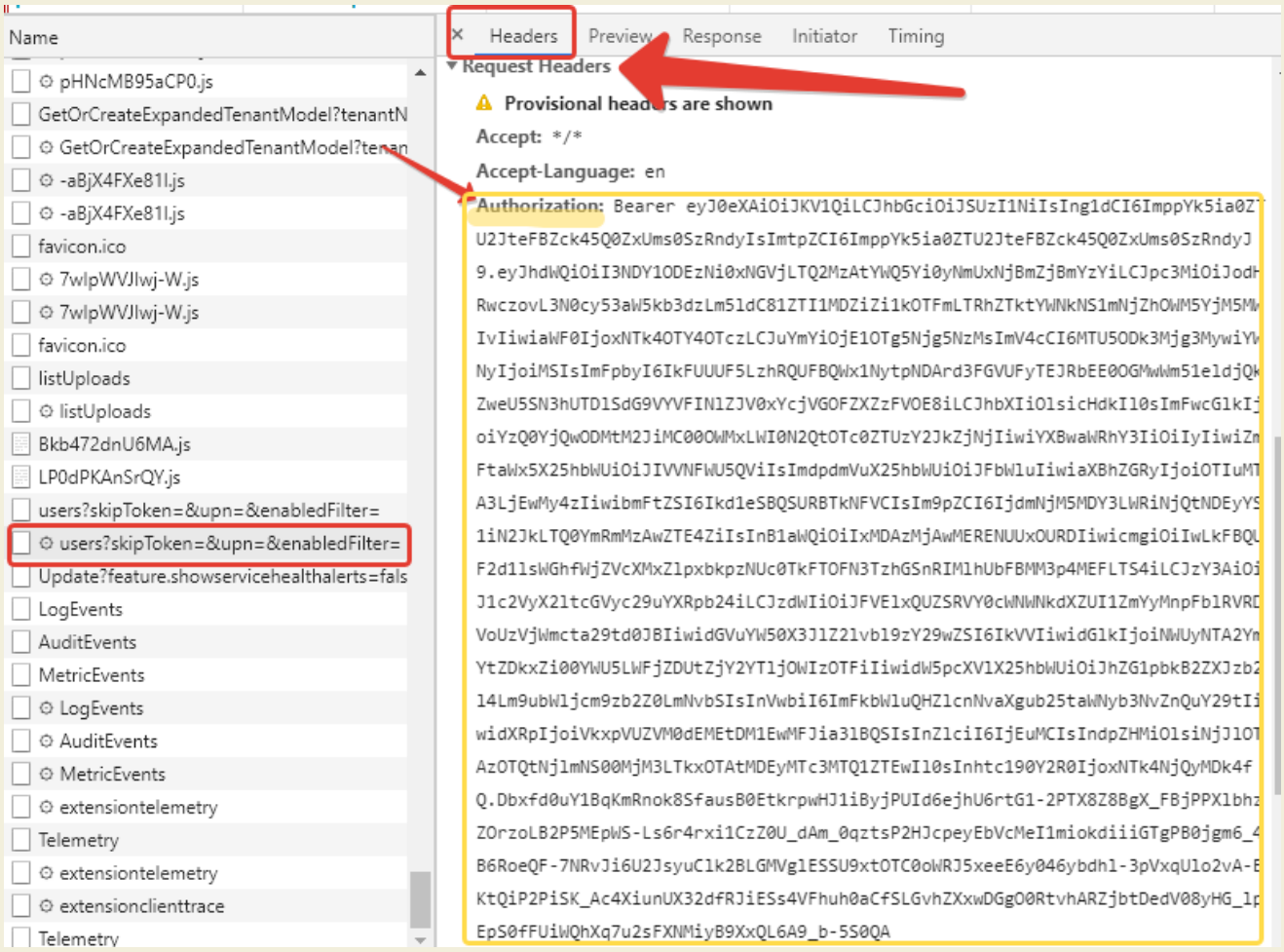


Click on "users?skipToken…" line. This will open a list of headers sent by the resource

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/VyVuRLTNAtM

TOKEN2 | CHE-218.895.438
chemin du Pré-Colomb 10
CH-1290 Versoix
office@token2.ch
+41 22 519 62 02



8. 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.

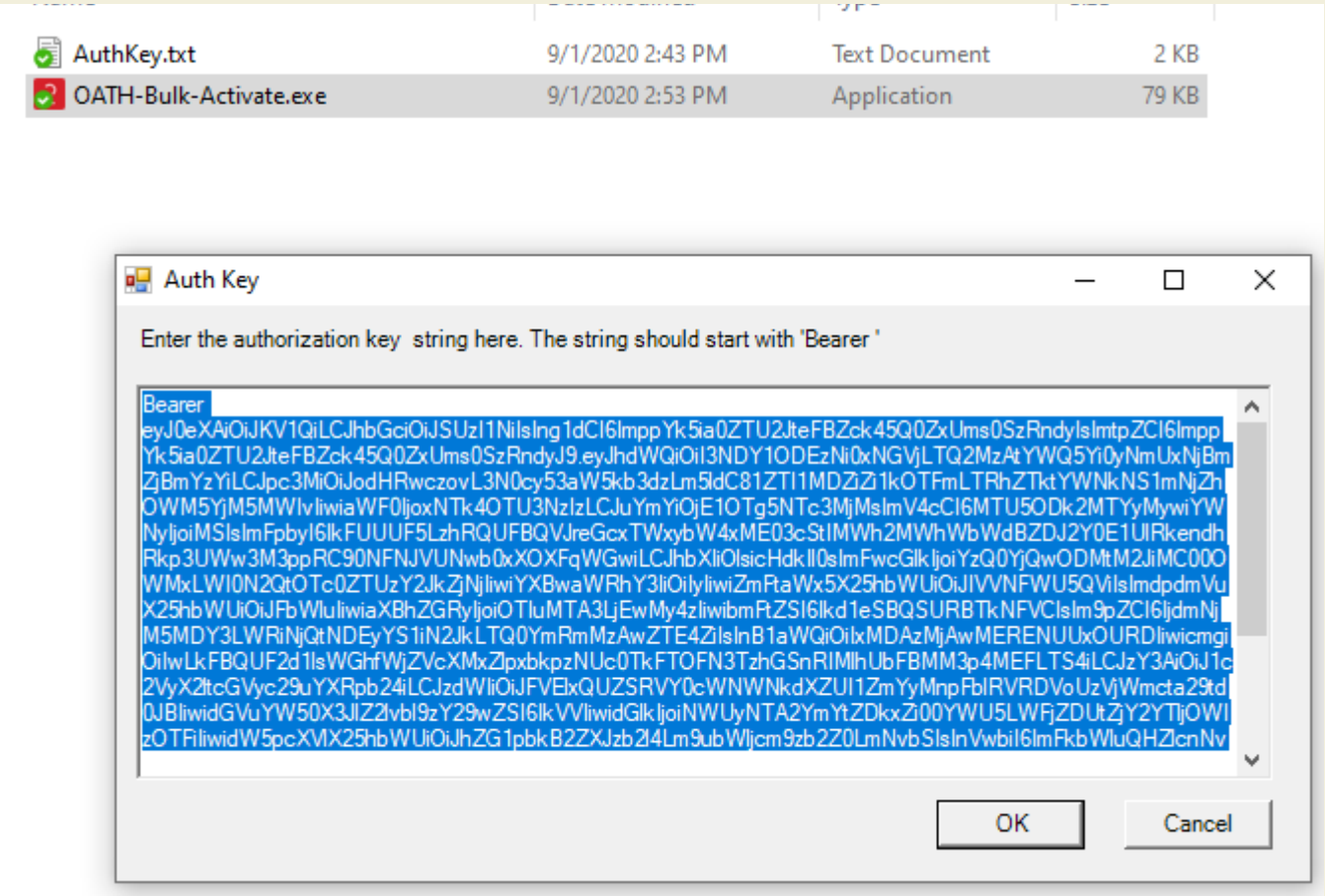
5. BULK ACTIVATE OATH TOKENS

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

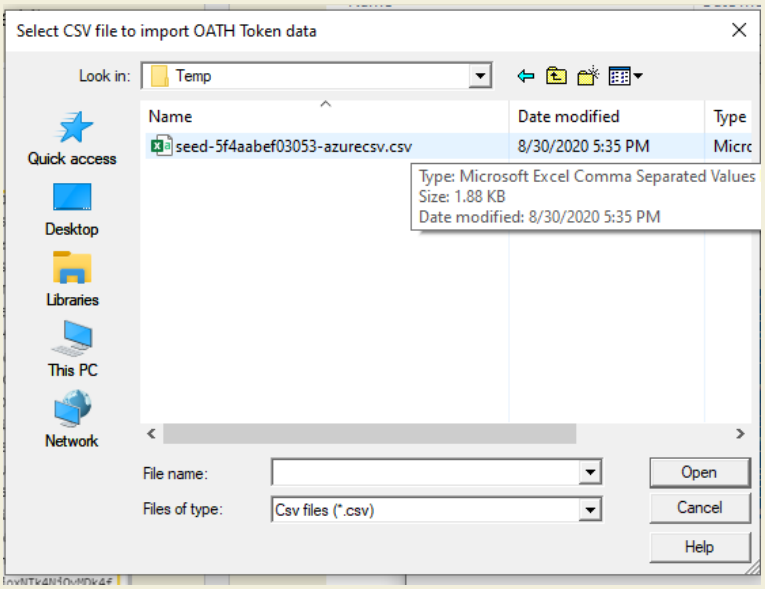
When launched, the application will ask for the Authorization key (or will read it from

TOKEN2 | CHE-218.895.438
chemin du Pré-Colomb 10
CH-1290 Versoix
office@token2.ch
+41 22 519 62 02

AuthKey.txt file located in the same directory)

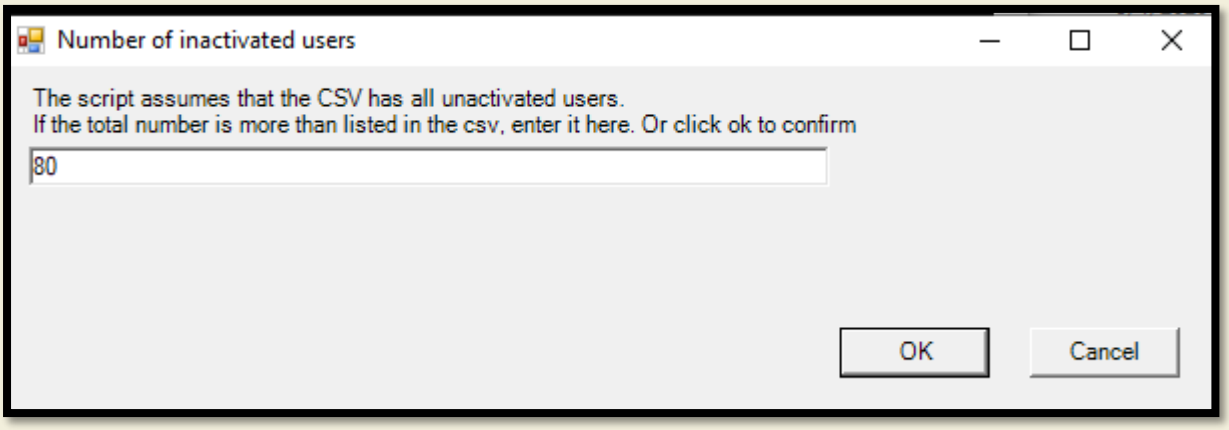


On the text step, it will ask to select the CSV file



TOKEN2 | CHE-218.895.438
chemin du Pré-Colomb 10
CH-1290 Versoix
office@token2.ch
+41 22 519 62 02

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.

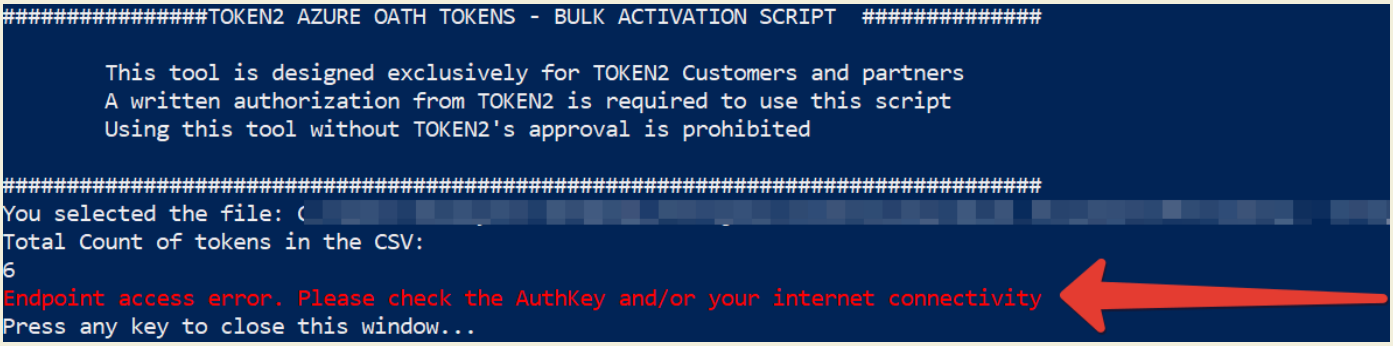
```
################TOKEN2 AZURE OATH TOKENS - BULK ACTIVATION SCRIPT  ##############

        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:\                                    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.
```

TOKEN2 | CHE-218.895.438
chemin du Pré-Colomb 10
CH-1290 Versoix
office@token2.ch
+41 22 519 62 02

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

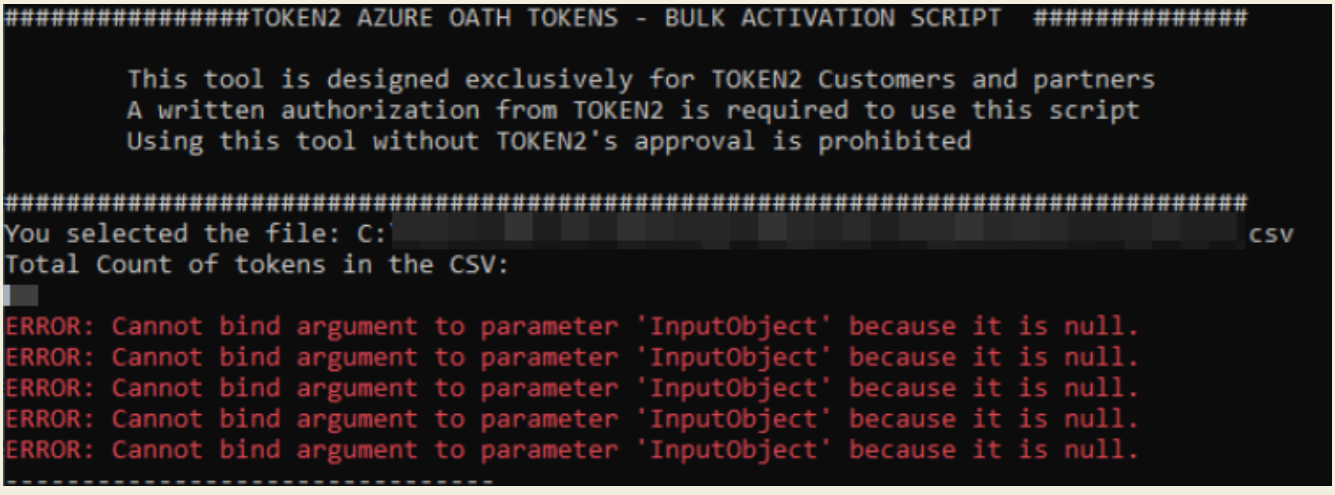
Endpoint access error



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

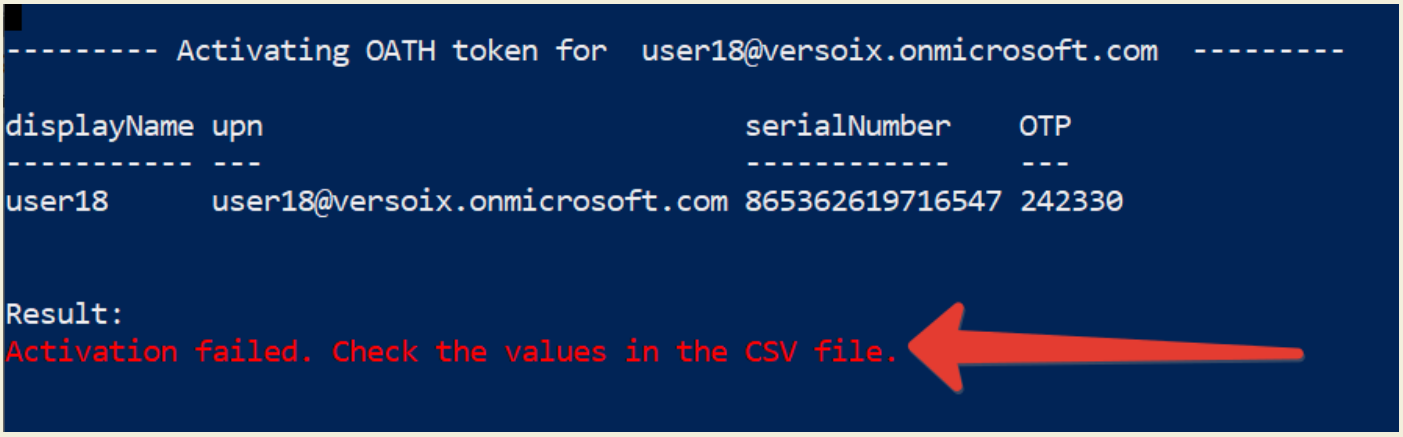
Although the tool is using standard ports (80 and 443) some “smart” firewall solutions (i.e Symantec or Cisco) may be limiting internet access per application. The symptoms are similar to the error shown below, but there may be other messages shown as well:
“Cannot bind argument to parameter 'InputObject' because it is null”



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

TOKEN2 | CHE-218.895.438
chemin du Pré-Colomb 10
CH-1290 Versoix
office@token2.ch
+41 22 519 62 02

Activation failed



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.