**Authorization requirements**

The MCP should use the Device Code authorization setup using 3 different calls.

1. Get Device Code
2. Get Access Token
3. Get Refresh Access Token

It is crucial that all tokens, tenant id and client id are kept encrypted. This also goes for any device code and access / refresh tokens that are received in API calls and must be kept.

Authorization should include a validation of the computer id as well, so if the code is moved to another PC, it should require a new authorization.

**Authorization flow:**

When the MCP is started – it should validate if a valid Device Code, Access token exists.

1. If it does, do not run the Get Device Code.
2. If an expired Access Token exists, and the Refresh Token is available. Run Get Refresh Access Token.
3. If no device code exists, run Get Device Code, and once the user has signed in, run the Get Access Token.

When a tool is called, if an expired Access Token exists, trigger the Get Refresh Access Token.

**Get Device Code**

URL: <https://login.microsoftonline.com/{{Tenant}}/oauth2/v2.0/devicecode>

Type: GET

{{tenant}} 🡪 Tenant GUID, must be configured.

Body:

client\_id – string

scope – string

Response:

{

    "user\_code": "USER CODE",

    "device\_code": "DEVICE CODE",

    "verification\_uri": "https://microsoft.com/devicelogin",

    "expires\_in": 900,

    "interval": 5,

    "message": "To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code L7JVEBF5A to authenticate."

}

The device code should be kept.

User code is needed for the user to login using the verification URL.

**Get Access Token**

URL: [https://login.microsoftonline.com/{{Tenant}}/oauth2/v2.0/token](https://login.microsoftonline.com/%7b%7bTenant%7d%7d/oauth2/v2.0/token)

Type: GET

{{tenant}} 🡪 Same GUID as Get Device Code

Body:

client\_id – same as Get Device Code

grant\_type – predefined to “urn:ietf:params:oauth:grant-type:device\_code”

device\_code – the value received before.

Response:

{

"token\_type": "Bearer",

"scope": "Calendars.Read Calendars.ReadWrite Contacts.Read Mail.Read Mail.ReadWrite Mail.Send openid profile User.Read email",

"expires\_in": 3790,

"ext\_expires\_in": 3790,

"access\_token": "ACCESS TOKEN",

"refresh\_token": "REFRESH TOKEN,

"id\_token": "ID TOKEN"

}

Access\_token must be kept.

Refresh\_Token must be kept.

**Get Refresh Access Token**

URL: <https://login.microsoftonline.com/{{Tenant}}/oauth2/v2.0/token>

Type: GET

{{tenant}} 🡪 Same GUID as Get Device Code

Body:

grant\_type - refresh\_token

client\_id

refresh\_token – from Get Access Token call.

scope – from Get Device Code.

Reponse:

{

"token\_type": "Bearer",

"scope": "Calendars.Read Calendars.ReadWrite Contacts.Read Mail.Read Mail.ReadWrite Mail.Send openid profile User.Read email",

"expires\_in": 3948,

"ext\_expires\_in": 3948,

"access\_token": "ACCESS TOKEN",

"refresh\_token": "REFRESH TOKEN",

"id\_token": "ID TOKEN"

}

The response must update the values from the Get Access Token call.