OAUTH2 Guide for consumers

2022-03-15T10:55:24Z

Table of Contents

1. Introduction . . . 1
2. Getting credentials . . . 2
3. Getting a token . . . 3
4. Using the token to make an authorized request . . . 4
5. Troubleshooting . . . 5
   5.1. Using a token you got from one environment when communicating to another . . . 5
   5.2. Using an outdated token . . . 5
   5.3. Using my.email@mail.com as token . . . 5
   5.4. Using a non-existing path . . . 5
   5.5. Using invalid credentials . . . 6
   5.6. Using an invalid json body (when filtering elasticsearch for example) . . . 7
   5.7. Using an older/wrong contenttype version (accept/v3 for example) . . . 7
   5.8. Using a non-encoded authorization header (Authorization: Basic user:password) . . . 7
   5.9. Using the wrong token URL . . . 8
6. Azure AD Endpoints . . . 9
   6.1. DEV . . . 9
   6.2. UAT . . . 9
   6.3. PROD . . . 9
7. A2D-API Environments . . . 10

1. Introduction

This document contains all OAUTH2 related documentation for the A2D-API and A2D2.

2. Getting credentials

To be able to read from the A2D-API, you will need credentials (clientId/clientSecret), and the necessary roles.

Please fill out the following form: https://forms.office.com/r/JKq5WkcfgK

When we receive the data from the form, we will request the credentials for you.

More information on the A2D-API can be found here: https://a2d-api.toyota-europe.com/docs/

3. Getting a token

1. Fill in your clientId and clientSecret (for DEV!) in the following command.
2. Execute the following command:

```
curl -X POST --location "https://login.microsoftonline.com/41cb5478-1f8a-4a8e-a2b7-
58bbc1198c52/oauth2/v2.0/token" \
    -H "Content-Type: application/x-www-form-urlencoded" \
    -d "grant_type=client_credentials&scope=api://<yourClientID>/.default" \
    --basic --user <yourClientID>:<yourClientSecret>
```

This call will result in something like this:

```
{
  "token_type": "Bearer",
  "expires_in": 3599,
  "ext_expires_in": 3599,
  "access_token":
"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Im5PbzNaRHJPRFhFSzFqS1doWHNs..."
}
```

The `access_token` field contains the token you must use to make authenticated calls.

4. Using the token to make an authorized request

1. Fill in the token you received from the previous step in the `Authorization` header value
2. Execute the following command:

```
curl -X GET --location "https://a2d-api.toyota-europe.com/v2/de/_search" \
    -H "Authorization: Bearer <the received token>"
```

If everything went well, you should receive a 200 http response code.

5. Troubleshooting

Here we list all the things that "can go wrong", and how to fix them. We list the http responses, so that you can match those with the problem you might be experiencing.

5.1. Using a token you got from one environment when communicating to another

```
{
  "message": "Unauthorized (invalid issuer (https:\/\/sts.windows.net\/33690b94-3f16-
4d1a-9205-84421d2501e4\/) was specified for access token,
https:\/\/login.microsoftonline.com\/41cb5478-1f8a-4a8e-a2b7-
58bbc1198c52\/oauth2\/v2.0 was expected)"
}
```

Fix it by using the token of the correct/expected environment.

You can find the IDP you need to use in the message: `https:\/\/login.microsoftonline.com\/41cb5478-1f8a-4a8e-a2b7-58bbc1198c52\/oauth2\/v2.0 was expected`

5.2. Using an outdated token

```
{
  "message": "Unauthorized (invalid exp claim (1617101165) was specified for access
token)"
}
```

Fix it by getting a new token before making a call.

5.3. Using my.email@mail.com as token

```
{
  "message": "Unauthorized (invalid or inactive token)"
}
```

Fix it by getting an actual token (looks like "eyJ0eXAiOiJKV1QiLCJhbGci....ey.....).

5.4. Using a non-existing path

```
{
  "message": "no Route matched with those values"
}
```

Check for typo's, double trailing slashes, ... in the url you're using.

5.5. Using invalid credentials

You'll get the following if you entered an incorrect or non-existing client-id.


```
{
  "error": "unauthorized_client",
  "error_description": "AADSTS700016: Application with identifier 'snarf' was not
found in the directory '41cb5478-1f8a-4a8e-a2b7-58bbc1198c52'. This can happen if the
application has not been installed by the administrator of the tenant or consented to
by any user in the tenant. You may have sent your authentication request to the wrong
tenant.\r\nTrace ID: 3f8b8c6b-4468-4a94-a920-4dc8a7f3b800\r\nCorrelation ID: be0cee6a-
46c1-407b-bee8-09debba78ed5\r\nTimestamp: 2021-03-30 12:04:22Z",
  "error_codes": [
    700016
  ],
  "timestamp": "2021-03-30 12:04:22Z",
  "trace_id": "3f8b8c6b-4468-4a94-a920-4dc8a7f3b800",
  "correlation_id": "be0cee6a-46c1-407b-bee8-09debba78ed5",
  "error_uri": "https://login.microsoftonline.com/error?code=700016"
}
```


You'll get the following if you entered an incorrect client-secret.


```
{
  "error": "invalid_client",
  "error_description": "AADSTS7000215: Invalid client secret is provided.\r\nTrace ID:
0fb6934b-0edd-4a40-9f1d-fa58d0aa7a00\r\nCorrelation ID: c33e0e16-b5bc-4b17-b1c5-
f5e4c4f40b6e\r\nTimestamp: 2021-03-30 12:05:13Z",
  "error_codes": [
    7000215
  ],
  "timestamp": "2021-03-30 12:05:13Z",
  "trace_id": "0fb6934b-0edd-4a40-9f1d-fa58d0aa7a00",
  "correlation_id": "c33e0e16-b5bc-4b17-b1c5-f5e4c4f40b6e",
  "error_uri": "https://login.microsoftonline.com/error?code=7000215"
}
```


It might be that you don't have a client-id yet, so you'll have to set one up.

If you've entered a wrong password, check for typo's. If you used cURL, you might want to check if your password contains "!" (exclamation points), these might be interpreted by your shell. In that case you'll want to escape them, or pipe stdin to your curl command.

5.6. Using an invalid json body (when filtering elasticsearch for example)

Here Elastic Search is responding with the bad request because `auery` is not a valid query json object.

```
{
  "error": {
    "root_cause": [
      {
        "type": "parsing_exception",
        "reason": "Unknown key for a START_OBJECT in [auery].",
        "line": 2,
        "col": 12
      }
    ],
    "type": "parsing_exception",
    "reason": "Unknown key for a START_OBJECT in [auery].",
    "line": 2,
    "col": 12
  },
  "status": 400
}
```

5.7. Using an older/wrong contenttype version (accept/v3 for example)

```
Your requested version of the API (application/vnd.toyota-europe.a2d.v3+json) is not
supported.

Response code: 406 (Not Acceptable); Time: 395ms; Content length: 95 bytes
```

Your `Accept` header must be `application/vnd.toyota-europe.a2d.v4+json`

5.8. Using a non-encoded authorization header (Authorization: Basic user:password)

```
{
  "error": "invalid_request",
  "error_description": "AADSTS90023: Invalid authorization header. Decoding
failed.\r\nTrace ID: 218a6437-4ebd-4a1f-97b7-982c3225b000\r\nCorrelation ID: 60676ca2-
8a21-4952-9858-9dd7ca175449\r\nTimestamp: 2021-03-30 13:10:45Z",
  "error_codes": [
    90023
  ],
  "timestamp": "2021-03-30 13:10:45Z",
  "trace_id": "218a6437-4ebd-4a1f-97b7-982c3225b000",
  "correlation_id": "60676ca2-8a21-4952-9858-9dd7ca175449"
}
```

Authorization Basic expects a Base64 encoded string of clientid:password, and not plain text.

5.9. Using the wrong token URL

If you receive the following error, you're probably using the wrong token url. See Azure AD Endpoints fore correct URL's.

```
{
"message": "Forbidden (scopes required but no scopes found)"
}
```

6. Azure AD Endpoints

6.1. DEV

token_endpoint	https://login.microsoftonline.com/41cb5478-1f8a-4a8e-a2b7-58bbc1198c52/oauth2/v2.0/token
well-known	https://login.microsoftonline.com/41cb5478-1f8a-4a8e-a2b7-58bbc1198c52/v2.0/.well-known/openid-configuration
jwks_uri	https://login.microsoftonline.com/41cb5478-1f8a-4a8e-a2b7-58bbc1198c52/discovery/v2.0/keys

6.2. UAT

token_endpoint	https://login.microsoftonline.com/33690b94-3f16-4d1a-9205-84421d2501e4/oauth2/v2.0/token
well-known	https://login.microsoftonline.com/33690b94-3f16-4d1a-9205-84421d2501e4/v2.0/.well-known/openid-configuration
jwks_uri	https://login.microsoftonline.com/33690b94-3f16-4d1a-9205-84421d2501e4/discovery/v2.0/keys

6.3. PROD

token_endpoint	https://login.microsoftonline.com/52b742d1-3dc2-47ac-bf03-609c83d9df9f/oauth2/v2.0/token
well-known	https://login.microsoftonline.com/52b742d1-3dc2-47ac-bf03-609c83d9df9f/v2.0/.well-known/openid-configuration
jwks_uri	https://login.microsoftonline.com/52b742d1-3dc2-47ac-bf03-609c83d9df9f/discovery/v2.0/keys

7. A2D-API Environments

Table 1. A2D-API Environments

Environment	URL
DEV	https://a2d-api-dev.toyota-europe.com
UAT	https://a2d-api-acc.toyota-europe.com
PROD	https://a2d-api.toyota-europe.com