Authentication API

Version 5.1.161, 2024-06-10

Authentication API

Introduction

 Version 5.1.161, 2024-06-10.

This Web Service is used to handle API Keys and OAuth 2.0 Bearer Tokens.

Authentication method

Username and password shall be given as Basic authentication, i.e, the header `Authorization` should have the value `Basic token`, where the token is the `Base64` encoding of (a `UTF-8` byte array representation of) `username:password`. Here `testuser:testpass` will be encoded as `dGVzdHVzZXI6dGVzdHBhc3M=` and the `Authorization` header will have the value `Basic dGVzdHVzZXI6dGVzdHBhc3M=`

Chapter 1. The `/apikey` endpoint

1.1. GET request example e.g. from web browser

```
curl https://secure.lekab.com/auth/api/v1/apikey?name=MyApiKey \
    --basic --user username:password
```

1.1.1. Explanation of parameters

GET query param	query param value	Description
name	string	The name of the API key

1.1.2. HTTP response

A successful request will return `200` OK and a String with the API Key e.g. `bGlNOmRHVnpkR2xrOkxKUjRJekw5WEY2MVA0bnY`. If the user does not present proper login credentials a `401` Unauthorized will be returned.

Chapter 2. The /token endpoint

The /token endpoint is used to request an OAuth 2.0 Bearer Token.

2.1. POST request example

```
curl -X POST --location "https://secure.lekab.com/auth/api/v1/token" \
    -H "Content-Type: application/x-www-form-urlencoded" \
    -d 'grant_type=client_credentials' \
    --basic --user username:password
```

2.1.1. Explanation of parameters

POST param	query param value	Description
grant_type	client_credentials (string)	The requested grant type. Only client_credentials is supported.

2.1.2. HTTP response

A successful request will return 200 OK and a JSON object containing the Bearer token. If the user does not present proper login credentials a 401 Unauthorized will be returned.

Successful Response HTTP response code 200 OK

```
{
  "access_token" : "e45c538d-a416-4489-9d5f-a78d3c4fc69a",
  "token_type" : "bearer",
  "expires_in" : 599
}
```

ERROR Response HTTP response code 400 Bad Request

If any other grant_type than client_credentials is requested the following error message will be sent.

```
{
  "error" : "unsupported_grant_type"
}
```

Any other request error will have the following error message.

```
{
  "error" : "bad_request"
```

```
}
```

Chapter 3. The `/revoke` endpoint

The `/revoke` endpoint is used to revoke an OAuth 2.0 Bearer Token.

3.1. POST request example

```
curl -X POST --location "https://secure.lekab.com/auth/api/v1/revoke" \
    -H "Content-Type: application/x-www-form-urlencoded" \
    -d 'token=e45c538d-a416-4489-9d5f-a78d3c4fc69a' \
    --basic --user username:password
```

3.1.1. Explanation of parameters

POST param	query param value	Description
token	string	The bearer token. e.g. `e45c538d-a416-4489-9d5f-a78d3c4fc69a`

3.1.2. HTTP response

A successful or unsuccessful request will return `200` OK regardless of the outcome. If the user does not present proper login credentials a `401` Unauthorized will be returned.