Authentication API

Version 7.0.36, 2026-11-02

Authentication API

Introduction . . . 1
Authentication method . . . 1
1. The `/token` endpoint . . . 2
1.1. POST request example . . . 2
1.1.1. Explanation of parameters . . . 2
1.1.2. HTTP response . . . 2
2. The `/revoke` endpoint . . . 4
2.1. POST request example . . . 4
2.1.1. Explanation of parameters . . . 4
2.1.2. HTTP response . . . 4

Introduction

© 2024 LEKAB Communication Systems AB. Version 7.0.36, 2026-11-02.

This Web Service is used to handle 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=`

Alternatively, for the `/token` endpoint, username and password can be passed as `client_id` and `client_secret` form parameters in the `x-www-form-urlencoded` body of the HTTP POST request.

Chapter 1. The `/token` endpoint

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

1.1. POST request example

Using Basic authentication (username and password in a Base64 from UTF-8 encoded header)

```
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
```

Using username and password in body (client_id and client_secret url-encoded from UTF-8)

```
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&client_id=username&client_secret=password'
```

1.1.1. Explanation of parameters

POST param	query param value	Description
grant_type	client_credentials (string)	The requested grant type. Only `client_credentials` is supported.
client_id	user name (string)	User name if Basic authentication is not used. Url encoded from utf-8 if necessary
client_secret	user password (string)	Password if Basic authentication is not used. Url encoded from utf-8 if necessary

1.1.2. 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. If the user has the `DISALLOW_BASIC` role, that is disregarded for this purpose (for obvious reasons).

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 2. The `/revoke` endpoint

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

2.1. 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
```

2.1.1. Explanation of parameters

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

2.1.2. 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.