

LeadU Webservice API Documentation

Version: 1.2.1
Date: 2020/01/24

Table of Content

1. General	3
2. Authentication	3
2.1. Requesting a JWT (JSON Web Token)	3
2.1.1. Form data	3
2.1.2. Return data	3
2.1.3. Example call	3
2.1.4. Example output	4
3. Getting Person Information	4
3.1. Person Data Request	4
3.1.1. Header	4
3.1.2. Return data	4
3.1.3. Error conditions	5
3.1.4. Example call	6
3.1.5. Example output	6
4. Rate Limit	6
4.1. Access Log	6
5. Test Integration	6

1. General

The LeadU Integrators REST API is really simple and straightforward for fast & easy integration into your custom applications.

It basically boils down to just one method giving you contact details of a person.

The root API URL can be found on the FAQ of the leadu portal for your congress and is congress specific as well. It usually can be derived from the portal url by appending “-api” to the subdomain like this:

`https://<congress-code>-api.leadu.at`

2. Authentication

The API is secured via OpenID Connect client credentials grant (<http://openid.net/connect/>). The OpenID Connect 1.0 (OID) protocol is a simple identity layer on top of the OAuth 2.0 protocol. After ordering the webservice product you will get a client id and a secret key that allows you to request a JSON Web Token (<https://jwt.io/>). This token has to be placed in the header of every call to the API.

2.1. Requesting a JWT (JSON Web Token)

To request an authorization token you have to issue a POST request in x-www-form-urlencoded format to the following URL:

`https://<api-domain>/connect/token`

2.1.1. Form data

- **client_id=<client id>**
this is the client id you get after purchasing the webservice product.
- **grant_type=client_credentials**
This specifies the authentication method (grant flow) and has to be hardcoded
- **scope=IntegratorsAPI**
This specifies what the client wants to have access for and has to be hardcoded

This request has to contain your client id as well as your password using basic authentication.

2.1.2. Return data

Given that the request contains the correct parameters the API will return a JWT in JSON format containing the following fields:

- **access_token:** This is the token you have to store and use in the header of every subsequent call
- **expires_in:** Contains an int value specifying the expiration of this token in seconds. Before expiration you have to request another token to continue successfully retrieving person data.
- **token_type: Bearer**
this will never change

2.1.3. Example call

```
set url=https://<api-domain>/connect/token
set clientId=<username>
set password=<password>
curl "%url%" -H "content-type: application/x-www-form-urlencoded" --data
"client_id=%clientId%&grant_type=client_credentials&scope=IntegratorsAPI" --cacert
cacert.pem --basic --user %clientId%:%password%
```

If you don't have curl, you can get it from here: <https://curl.haxx.se/download.html>

Please note that some fields may be empty if not filled in by the participant, or if the person has declined propagation of some of his/her data.

3.1.3. Error conditions

If the requested person cannot be found in the database a **404** error code is returned.

If the authentication failed a **401** error code is returned.

