silverleads Webservice API Documentation

Version: 1.3.0
Date: 2026/09/14

Table of Content

Es wurden keine Einträge für das Inhaltsverzeichnis gefunden.

1. General

The silverleads 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 is specific to your congress. You will find it in the FAQ of the silverleads portal for your congress, in the section about the Webservice product. It is not derivable from the portal address, so please take it from there rather than constructing it:

https://<api-domain>

2. Authentication

The API is secured via OpenID Connect client credentials grant (https://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.se/download.html

2.1.4. Example output


```
{
        "access_token":
"eyJhbGciOiJSUzI1NiIsImtpZCI6IkE3ODNBRkVERTY3REQxQjVDODA5NTYxRTgxMjY4QTdBIiwidHlwIjoiYXQra
nd0In0.eyJpc3MiOiJodHRwczovLzxhcGktZG9tYWluPiIsIm5iZiI6MTc4OTMzOTg4NSwiaWF0IjoxNzg5MzM5ODg
1LCJleHAiOjE3ODkzNDM0ODUsImF1ZCI6ImNvbmdyZXNzLmFwaSIsImNsaWVudF9pZCI6IlRlc3RDbGllbnQiLCJzY
29wZSI6WyJJbnRlZ3JhdG9yc0FQSSJdfQ.CzBVep_E6Q4zWH2ix-
wRNluApcrvFDleg6jN8hc8YYar0PUaP2SJrtP4HUJnjLHW-yBFao-
02f4jSG2St9wBJktwlbrfBClOc5i94gcsUXabwOUKL1R5nsPoDTJXfKHG6xA1Wn-kye4TOF2Cp8zxFjtgharP9Bk-
Y4it0vccQWaLsNX6H0RpjrPY_SJHbJG22wAlSm-
Uud4DKE1yl7zhBitQdZq_5AkuU3idwucMMVZ7oMXqDzRZfqPI7RI3XIGm",
        "expires_in": 3600,
        "token_type": "Bearer"
}
```


3. Getting Person Information

To get person information you have to issue a GET request to the following URL:

https://<api-domain>/api/person/{badge-id}

- **badge-id: This is the alphanumeric id of the visitor that is scanned from the visitor badge. Pass it exactly as it is scanned - leading zeros are ignored, so 000532 and 532 address the same person. The test data uses ids prefixed with TEST- (see Test Integration below).**

3.1. Person Data Request

3.1.1. Header

The header at least has to contain the authorization header in the following form:

- Authorization: Bearer <access_token>

3.1.2. Return data

Person data is returned in JSON format and contains the following fields:

- firstName
- lastName
- email
- profession
- companyName
- companyStreet
- companyCity
- companyZip
- countryCode - in ISO 3166-1 alpha-2 format
- country – the readable country name of the visitor
- salutation
- academicTitle
- sex
- placeOfWork
- institution
- department
- state
- extKey – the scanned badge-id

Please note that a field without a value is omitted from the response rather than returned as null - the participant may not have filled it in, or may have declined propagation of that part of his/her data. Please do not rely on a field being present, and treat an absent field the same as an empty one. The response may also contain additional fields beyond the ones listed above, for example data supplied by the congress' registration system. Please ignore fields you do not know rather than rejecting the response.

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.

3.1.4. Example call

This sample is using the curl tool and is using windows notation. You will have to adapt slightly if you are running it on Linux.

```
set
token=eyJhbGciOiJSUzI1NiIsImtpZCI6IkE3ODNBRkVERTY3REQxQjVDODA5NTYxRTgxMjY4QTdBIiwidHlwIjoi
YXQrand0In0.eyJpc3MiOiJodHRwczovLzxhcGktZG9tYWluPiIsIm5iZiI6MTc4OTMzOTg4NSwiaWF0IjoxNzg5Mz
M5ODg1LCJleHAiOjE3ODkzNDM0ODUsImF1ZCI6ImNvbmdyZXNzLmFwaSIsImNsaWVudF9pZCI6IlRlc3RDbGllbnQi
LCJzY29wZSI6WyJJbnRlZ3JhdG9yc0FQSSJdfQ.CzBVep_E6Q4zWH2ix-
wRNluApcrvFDleg6jN8hc8YYar0PUaP2SJrtP4HUJnjLHW-yBFao-
02f4jSG2St9wBJktwlbrfBClOc5i94gcsUXabwOUKL1R5nsPoDTJXfKHG6xA1Wn-kye4TOF2Cp8zxFjtgharP9Bk-
Y4it0vccQWaLsNX6H0RpjrPY_SJHbJG22wAlSm-
Uud4DKE1yl7zhBitQdZq_5AkuU3idwucMMVZ7oMXqDzRZfqPI7RI3XIGm

set url=https://<api-domain>/api/person/TEST-1

curl "%url%" -H "content-type: text/plain" -H "Authorization: Bearer %token%" -H
"Connection: keep-alive" --cacert cacert.pem
```

3.1.5. Example output

```
{
        "extKey": "TEST-1",
        "firstName": "Lucas",
        "lastName": "Sebastian",
        "email": "lucas.sebastian@example.org",
        "salutation": "Mr.",
        "academicTitle": "Dr.",
        "profession": "Radiologist",
        "companyName": "Vitae Posuere Associates",
        "companyStreet": "Musterstrasse 3",
        "companyZip": "1130",
        "companyCity": "Vienna",
        "country": "AUSTRIA",
        "countryCode": "AT"
}
```

4. Rate Limit

Every call to the API is logged and counted against your client. Excessive or abusive use leads to your client being suspended. Please also note that the API may apply a rate limit: design your integration to handle an HTTP 429 response by waiting for the period given in the Retry-After header and then retrying.

4.1. Access Log

Apart from rate-limiting API access each access is also logged for analytical purpose.

5. Test Integration

We have prepared a test client for you to facilitate integration. It is served from a separate set of test persons, so you will never see real visitor data while integrating.
The test persons are keyed with the prefix TEST-, numbered from TEST-1 upwards, for example TEST-1 or TEST-42.

Client ID: TestClient
Password: MyClientSecret