API documentation

Version: November 18th, 2024

Summary

In a nutshell

The SPI Online API (Application Programming Interface) is organized around Representational State Transfer (REST). Our API is designed to use built-in HTTP features HTTP response codes. Regarding the responses, JSON is returned in responses from the API. The current version of the API provides data about your audits and can also return all the data for one given audit. Only users who have an API role can access the API. This can only be trigger by an SPI Online administrator (from Cerise-SPTF)

There currently are 3 end points a user can call: login_check, audits and {uuidAudit}.

- https://api.spi-online.org/api/login_check
- https://api.spi-online.org/api/v1/audits
- https://api.spi-online.org/api/v1/audits/{uuidAudit}

The audits list is limited to 30 items per page. And needs to be called as:
- https://api.spi-online.org/api/v1/audits?page=XX

API role

The API can only be called by users who have the API role. By default, they do not have this role, neither as an organization administrator or as a member. Only an SPI Online administrator can give this role to a user. They need to contact the SPI Online support directly for this type of request. Conditions may apply.

Errors

SPI Online API uses HTTP response codes to indicate success or failure of requests. Specifically, codes in the 2xx range indicate success, codes in the 4xx range indicate an error that resulted from the provided arguments (e.g. instead of an integer a string is supplied) and 500 error code indicate an internal SPI online error. Please be aware that for the time being users may access an endpoint with an non HTTPs connection yet we strongly recommend you use HTTPs.

Here are the most common errors:

- Response 401 (json) : {"message": "Invalid JWT Token"} // Wrong identifiers

- Response 401 (json) : {"message": "JWT Token not found"} // No Authorization header

- Response 403 (json) : {"hydra:description": "You do not have permission to access this resource"} // No API rights

- Response 404 (json): Not found // Check the url

Rate limits

There currently is no rate limit as to the number of requests per hour. We will probably limit the number of requests as the number of API users grow. We nonetheless expect users to be reasonable.

Authentication

Once a user has the API role he may call the login_check endpoint with the email and password as parameters. The email and password are the same ones the user needs to connect to SPI Online.
Please note the email and password must be passed as parameters and not as a Basic Auth.

Users: User with API role

Content:

→ EndPoint name: login_check

→ URL : {APIServerName}/api/{endPoint}

(ex : https://api.spi-online.org/api/login_check)

→ Method: POST

→ Parameters :

- Email (user authentication email)

- Password (user password)

→ Response: {"token": "jwtToken"}

Rules :

→ Authentication tokens are valid for 24 hours.

Example:
```
curl --request POST \
  --url https://api.spi-online.org/api/login_check \
  --header 'content-type: application/json' \
  --data '{"email": "user@example.com", "password":"password_here"}'
```

Audits list

Once the user has received the jwttoken he can call the audits endpoint in order to retrieve information on all the audits he has access to. This means audits visible within the “My audits” page for the user:

- Audits where the user’s organization is either auditor organization, audited organization or owner organization.

- Audits that were shared with his organization

- Audits that were shared with the user

Users: User with API role

Content:

→ Name endPoint: audits

→ URL: {APIServerName}/api/v{x}/{endPoint}

(ex : https://api.spi-online.org/api/v1/audits)

→ Method: GET

→ Parameters: n/a

→ Authentication performed by token obtained in login_check (Bearer jwtToken)

→ Response: {...} // List of audits

Example:

```
curl --request GET \
  --url https://api.spi-online.org/api/v1/audits \
  --header 'Authorization: Bearer jwt.....token'
```

Response example:


```
[
  {
    "auditedAccess": {
      "code": "can_edit",
      "label": "Can edit the settings and answers"
    },
    "auditedContact": {
      "familyName": "Example",
      "givenName": "User",
      "fullName": "User Example"
    },
    "auditedActivities": [
      {
        "code": "SVG",
        "label": "Savings"
      },
      {
        "code": "INS",
```

```
      "label": "Insurance"
    }
  ],
  "auditorAccess": {
    "code": "can_edit",
    "label": "Can edit the settings and answers"
  },
  "auditorContact": {
    "familyName": "Example",
    "givenName": "User",
    "fullName": "User Example"
  },
  "auditedOrganization": {
    "country": {
      "code": "FRA",
      "uuid": "8b86cb11-d5a9-4c33-9be3-951aecbb75df",
      "label": "France"
    },
    "name": "Example",
    "uuid": "db35b107-5583-44dc-b5e0-fe3195a63582"
  },
  "auditorOrganization": {
    "country": {
      "code": "FRA",
      "uuid": "8b86cb11-d5a9-4c33-9be3-951aecbb75df",
      "label": "France"
    },
    "name": "Example",
    "uuid": "db35b107-5583-44dc-b5e0-fe3195a63582"
  },
  "category": {
    "code": "espm_5",
    "name": "SEPM Pathway"
  },
  "fake": true,
  "methodology": {
    "code": "TEST",
    "label": "Test"
  },
  "name": "API audit",
  "owningAccess": {
    "code": "can_edit",
    "label": "Can edit the settings and answers"
  },
  "owningContact": {
    "familyName": "Example",
    "givenName": "User",
    "fullName": "User Example"
  },
  "owningOrganization": {
    "country": {
      "code": "FRA",
      "uuid": "8b86cb11-d5a9-4c33-9be3-951aecbb75df",
      "label": "France"
    },
    "name": "Example",
    "uuid": "db35b107-5583-44dc-b5e0-fe3195a63582"
```

```
  },
  "privacy": 2,
  "progression": 43.6,
  "qualificationAudit": false,
  "date": "2024-06-27",
  "status": {
    "code": "ongoing",
    "label": "In progress"
  },
  "tool": {
    "name": "ALINUS",
    "position": 2,
    "alias": "ALINUS"
  },
  "authorizedOrganizations": [],
  "score": {
    "spi5_esg": 0.22448979591836735,
    "spi5_full": 0.1382794784580499,
    "spi5_entry": 0.1537082560296846,
    "spi5_alinus": 0.2307142857142857
  },
  "author": {
    "familyName": "Example",
    "givenName": "User",
    "fullName": "User Example"
  },
  "periodicity": {
    "code": "annual",
    "label": "Annual"
  },
  "accesses": {
    "see": true,
    "edit_answer": true,
    "edit": true
  },
  "id": 4301,
  "uuid": "3fc924f3-edf8-4955-8061-714ff75cb62d",
  "globalScore": "0.23"
 }
]
```


Audit list pagination

The audit list is limited to 30 items per page. If you have more than 30 audits you will need to check the total number of items you have access to. This information can be found in the raw response in the "hydra:totalItems" element.

For example:

{"@context":"\/api\/contexts\/Audit","@id":"\/api\/v1\/audits","@type":"hydra:Collection",**"hydra:totalItems":81**,"hydra:member":[{"@id":"\/api\/v1\/audits\/.....}

In this case the users will need to call 3 pages in order to retrieve all audits. This can be done with a page query parameters or by modifying the url structure in order to have:

→ Name endPoint: audits

→ URL: {APIServerName}/api/v{x}/{endPoint}?oage=XX

(ex : https://api.spi-online.org/api/v1/audits?page=3)

→ Method: GET

→ Parameters: n/a

→ Authentication performed by token obtained in login_check (Bearer jwtToken)

→ Response: {...} // List of audits
Example:

```
curl --request GET \
  --url https://api.spi-online.org/api/v1/audits \
  --header 'Authorization: Bearer jwt.....token'
```

Audit data

Once the user has received the jwttoken and/or has the uuid of an audit he has access to he can call the audits endpoint in order to retrieve the audit data. T

Users: User with API role

Content:

→ Name endPoint: audits/{uuidAudit}

→ URL: {APIServerName}/api/v{x}/{endPoint}

(ex : https://api.spi-online.org/api/v1/audits/3fc924f3-edf8-4955-8061-714ff75cb62d)

→ Method: GET

→ Parameters: UUID of audit

→ Authentication performed by token obtained in login_check (Bearer jwtToken)

→ Response: {...} // audit answers

Example:

```
curl --request GET \
  --url https://api.spi-online.org/api/v1/audits/ 3fc924f3-edf8-4955-8061-714ff75cb62d \
  --header 'Authorization: Bearer jwt...token' \
  --header 'content-type: application/json' \
  --data '{3fc924f3-edf8-4955-8061-714ff75cb62d}'
```

Example response:


```
[
  {
    "id": 4301,
    "uuid": "3fc924f3-edf8-4955-8061-714ff75cb62d",
    "name": "API audit",
    "author": "User Example",
    "category": "ESPM 5 pathway",
    "tool": "ALINUS",
    "methodology": "TEST",
    "auditorOrganization": {
      "id": 1806,
      "name": "Example",
      "access": "can_edit",
      "mixId": "87421114"
    },
    "auditedOrganization": {
      "id": 1806,
      "name": "Example",
      "access": "can_edit",
      "mixId": "87421114"
    },
```

```
    "owningOrganization": {
      "id": 1806,
      "name": "Example",
      "access": "can_edit",
      "mixId": "87421114"
    },
    "status": "ongoing",
    "score": {
      "spi5_esg": 0.22448979591836735,
      "spi5_full": 0.1382794784580499,
      "spi5_entry": 0.1537082560296846,
      "spi5_alinus": 0.2307142857142857
    },
    "createdAt": "2024-06-27T08:22:20+00:00",
    "updatedAt": "2024-06-27T08:33:03+00:00",
    "answers": [
      {
        "code": "1",
        "value": null,
        "score": {
          "spi5_esg": 0.5,
          "spi5_full": 0.21875,
          "spi5_entry": 0.2723214285714286,
          "spi5_alinus": 0.625
        }
      },
      {
        "code": "1.A",
        "value": null,
        "score": {
          "spi5_esg": 0.5,
          "spi5_full": 0.3125,
          "spi5_entry": 0.35714285714285715,
          "spi5_alinus": 0.5
        }
      },
      [...]
      {
        "code": "ORG_485",
        "value": null,
        "score": {
          "spi5_esg": null,
          "spi5_full": null,
          "spi5_entry": null,
          "spi5_alinus": null
        }
      }
    ],
    "activities": [
      "SVG",
      "INS"
    ],
    "privacy": 2,
    "periodicity": "annual"
  }
]
```