

Ashby | Docs

Custom Name Andrei

CONTENTS

1. Test Mapping Ivanti	4
2. Test page	5
3. Calls Tab Enhancement	6
4. Detected API	13
4.1. Authentication	14
4.1.1. Create an access token	14
4.2. Alerts	16
4.2.1. List alerts	16
4.3. Analysis	19
4.3.1. List profile analyses	19
4.4. Audit Logs	21
4.4.1. List audit logs	21
4.5. Brands	24
4.5.1. List brands	24
4.6. Case Management Users	27
4.6.1. List case management users	27
4.6.2. Retrieve a case management user	30
4.7. Checklists	32
4.7.1. List profile checklists	32
4.7.2. Retrieve a profile checklist	36
4.8. Documents	38
4.8.1. List document library types	38
4.8.2. Upload documents to a profile	40
4.8.3. List documents	44
4.8.4. Retrieve a document	47
4.9. Forms	50
4.9.1. List forms	50
4.9.2. Retrieve a form	52
4.9.3. List representative forms	54
4.9.4. Retrieve a representative form	56
4.9.5. Submit answers to a profile form	58
4.9.6. List profile forms	60
4.9.7. Assign a form to a profile	62
4.9.8. Retrieve a profile form	64
4.10. Onboarding	66
4.10.1. Submit a profile for review	66
4.10.2. Retrieve onboarding status	68
4.11. Portal Configurations	70
4.11.1. List portal configurations	70
4.11.2. Retrieve a profile portal configuration	72
4.11.3. Update a profile portal configuration	79
4.12. Portal Users	85
4.12.1. List portal user activity	85
4.12.2. List portal users	88
4.12.3. Create a portal user	91
4.12.4. Create a portal user login link	93
4.12.5. Retrieve a portal user	95
4.13. Profiles	97
4.13.1. List profile custom fields	97
4.13.2. List profiles	99
4.13.3. Create a profile	103
4.13.4. Retrieve a profile	107
4.13.5. Delete a profile	109
4.13.6. Update a profile	111
4.13.7. Retrieve a profile domain	114
4.13.8. Create a profile domain	118
4.13.9. Stop profile monitoring	120
4.13.10. Assign a portal user to a profile	122
4.13.11. Retrieve profile type configuration	124

4.14. Representatives	126
4.14.1. Create a representative login link	127
4.14.2. Download the IDV report for a representative	129
4.14.3. Run a verification for a representative	131
4.14.4. List representative verifications	133
4.14.5. List representatives	135
4.14.6. Create a representative	139
4.14.7. Retrieve a representative	144
4.14.8. Delete a representative	148
4.14.9. Stop screening monitoring for a representative	150
4.14.10. Reset the verification flow for a representative	152
4.15. Search	154
4.15.1. Search for an entity	154
4.15.2. Retrieve search type configuration	157
4.15.3. List search types	166

1. Test Mapping Ivanti



Log in to Figma to view this file

Log in

No account? [Create one](#)



2. Test page

Andrei eeeeeeeee

3. Calls Tab Enhancement

{name_english}

/

Automated Clearing House (ACH)

A computer-based funds transfer system established by NACHA to process the exchange of transactions between participating financial institutions in the U.S.; uses batch processing and a store-and-forward system.

BACS Global ACH – Bankers' Automated Clearing System

BACS payments are electronic payments where money in GBP moves from one bank account to another within the United Kingdom. This is similar to ACH, however since these payments are processed in UK, they are transmitted by BACS Payment Schemes Limited.

Checkpoint

A check that is printed and cut by the bank instead of in-house of the business. The user submits check print files for the Bank to print and distribute to vendors.

FedWire Domestic Wire USD

An electronic funds transfer system that occurs in real time for central bank funds. It is used by Federal Reserve banks to transfer funds between participating member institutions. No physical money is transferred between banks or financial institutions when conducting a wire transfer. Instead, information is passed between banking institutions about the recipient, the recipient bank account number, and the amount transferred.

Global ACH / CPA Payments

Electronic payments where money moves from one bank account to another within Canada. This is similar to ACH, however since these payments are processed in Canada, they are transmitted with the help of the Canadian Payments Association (CPA) network.

International Wire USD

An electronic transfer of funds sent internationally across a payment network administered by hundreds of banks or transfer service agencies across the world. No physical money is transferred between banks or FIs when conducting a wire transfer. Instead, information is passed between banking institutions about the recipient, the recipient bank account number, and the amount transferred. Sent from an USD origin account, funds may be exchanged into the local currency once deposited into the payees bank account.

Positive Pay

An automated cash-management service offered by financial institutions for fraud prevention. Checks that a company presents for payment are matched against the checks that were issued by the company to detect check fraud.

FISPAN helps the client to digitally transmit a list of checks that it has issued physically via mail. The bank compares the list to the actual checks, flags any that do not match, and notifies the client. The client will then tell the bank whether or not to cash the check.

SEPA (Single Euro Payments Area)

A system that harmonizes the way cashless payments transact between European countries in euros, created by the European Union (EU). You can now use your debit card anywhere in this area and do easy cross-border bank transfers.

Single Use Account (SUA) aka Virtual Card Network (VCN)

A Single-Use Account is a card-based payment solution that acts like a check by providing a 16-digit virtual account number for each payment. The credit limit of each card is determined by the specific payment amount. SUA payments are issued by email to the Vendor.

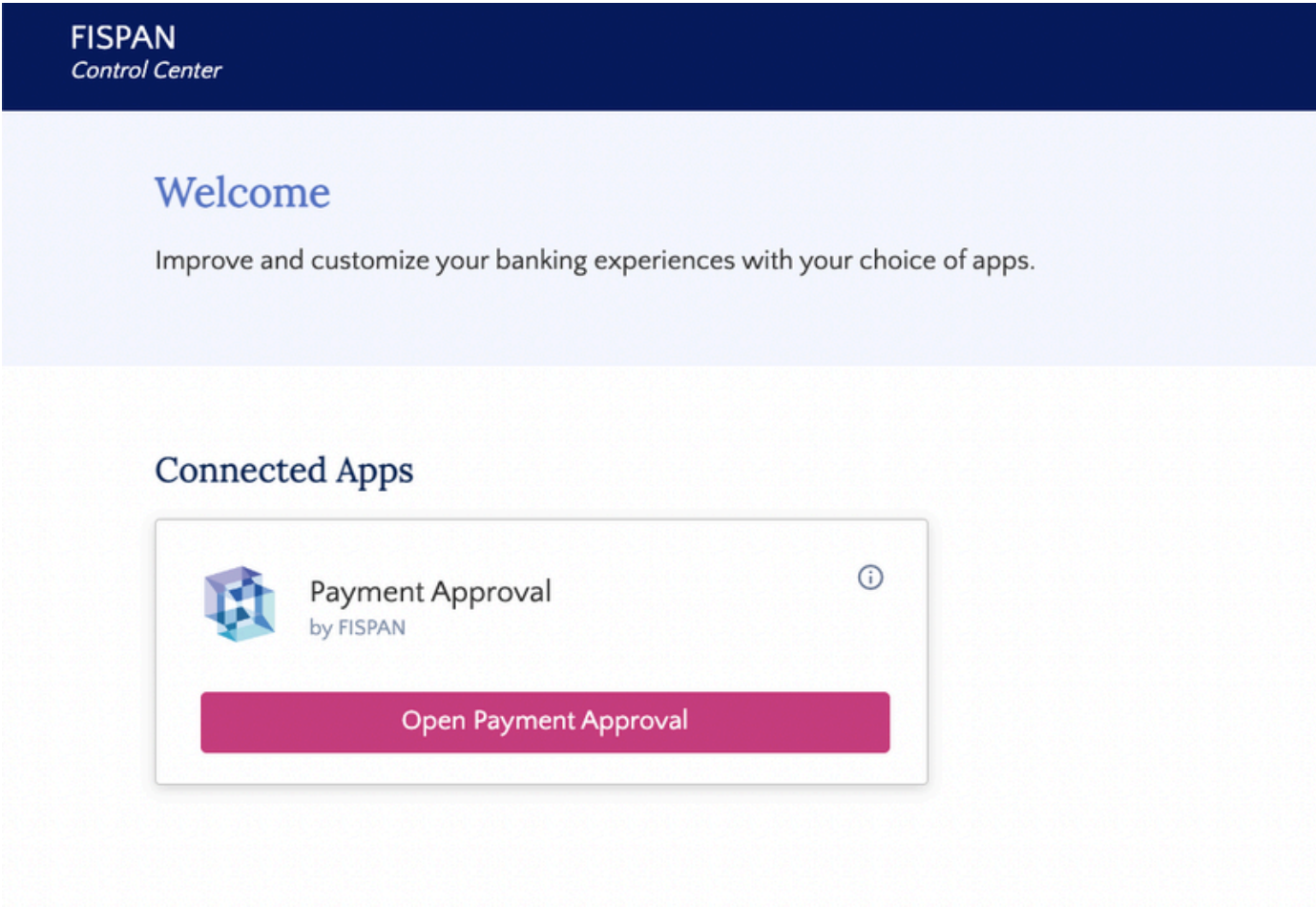
Access the Approval Portal Here

The FISPAN Approval Portal allows for a seamless experience from payment initiation in your ERP to the release of payments. If you are using the Approval Portal, all payments (including positive pay) will be held for approval.

JS JS

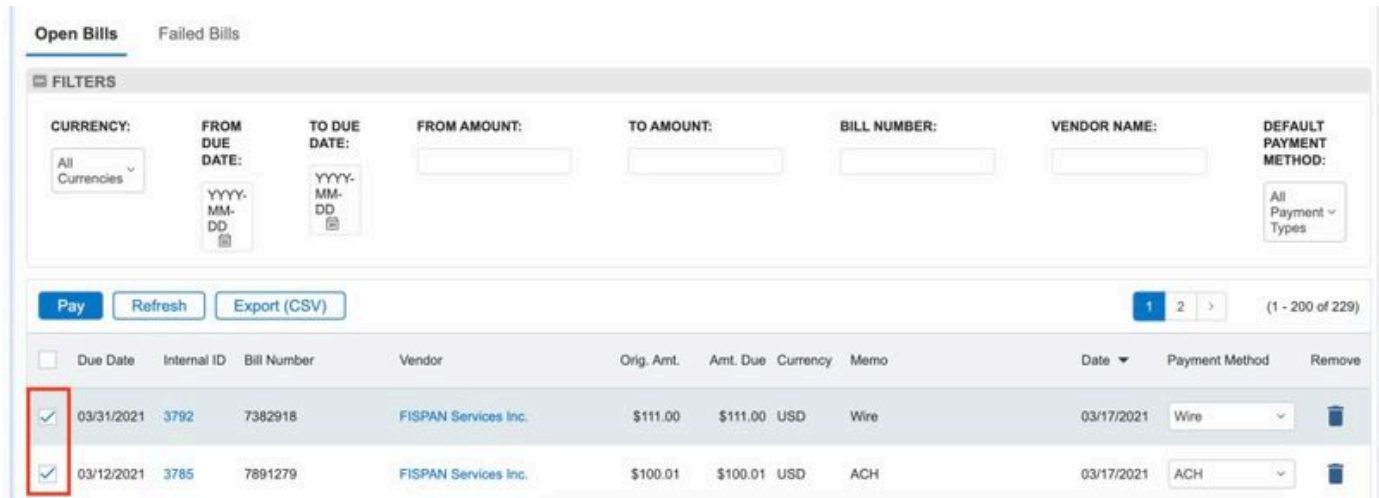
asda asda sd asdasdasdsa

Using the Approval Portal



Open Payment Approval

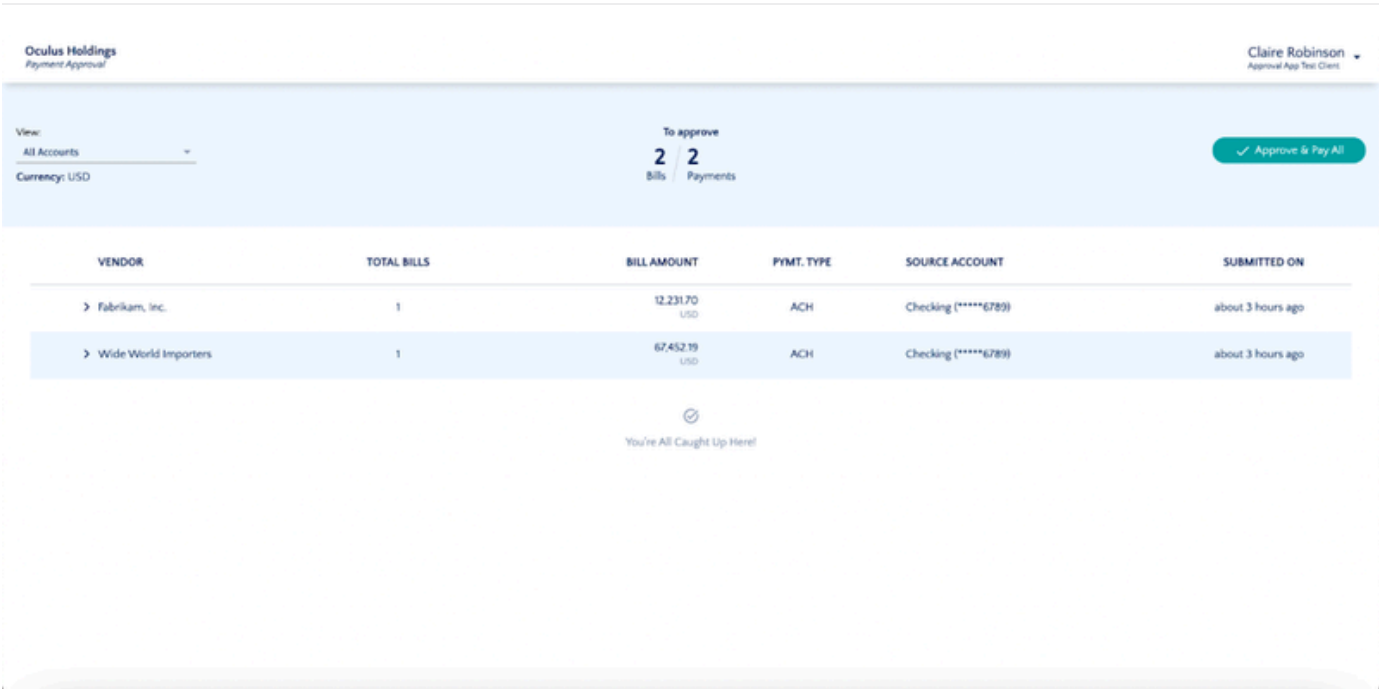
Once you log into after the Approval Portal has been activated, you can find a 'Open Payment Approval' button by hovering over the Payment Approval card in the Control Center.



Process a Payment in your ERP bank plugin

Process a payment through the Pay Bills page in the bank plugin of your ERP.

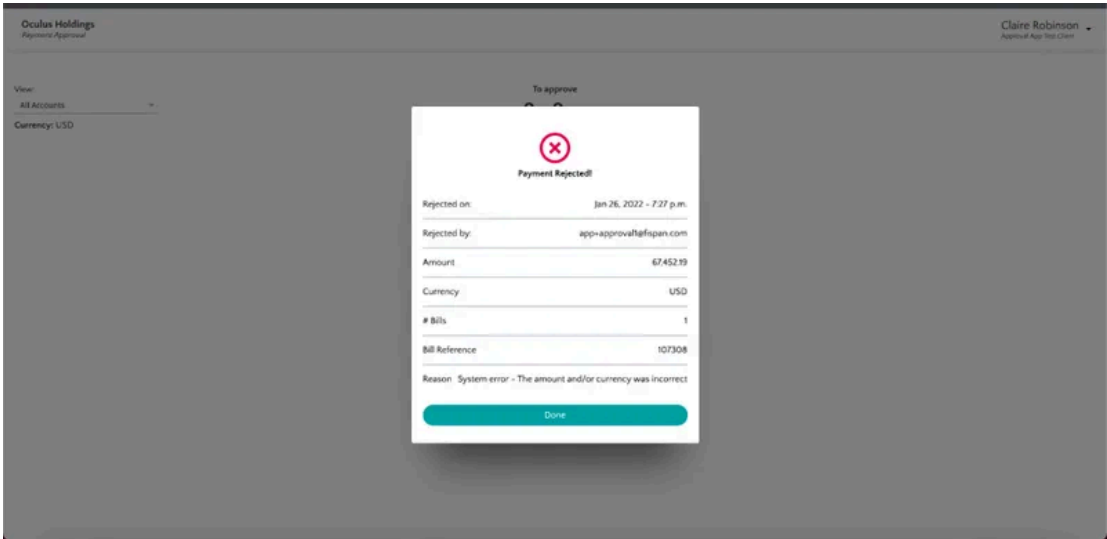
Please note that the example above depicts the Pay Bills page in the Sage Intacct bank plugin. This page may look different depending on which ERP you have installed the bank plugin in.



View the Pending Payments

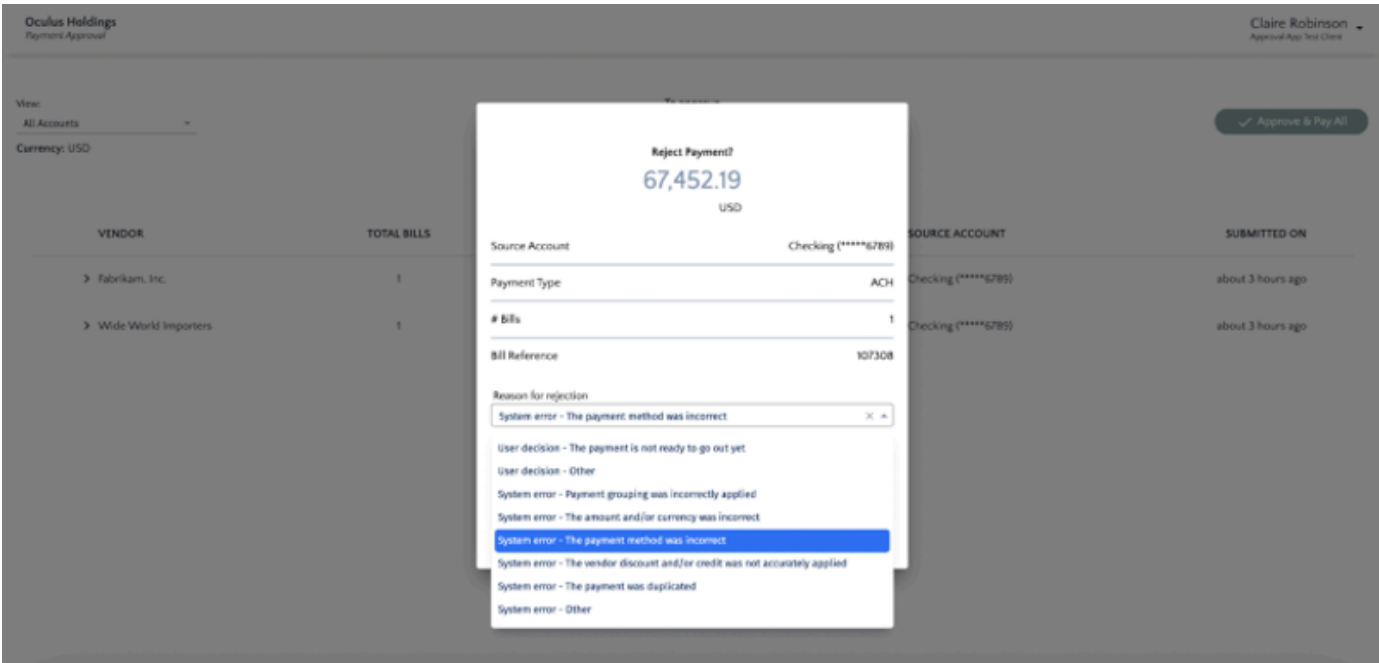
A permissioned user logs into the Payables Approval Portal to view payments sent from the plugin for **Rejection** or **Approval + Release**.

Rejecting a Payment



Reject the Payment

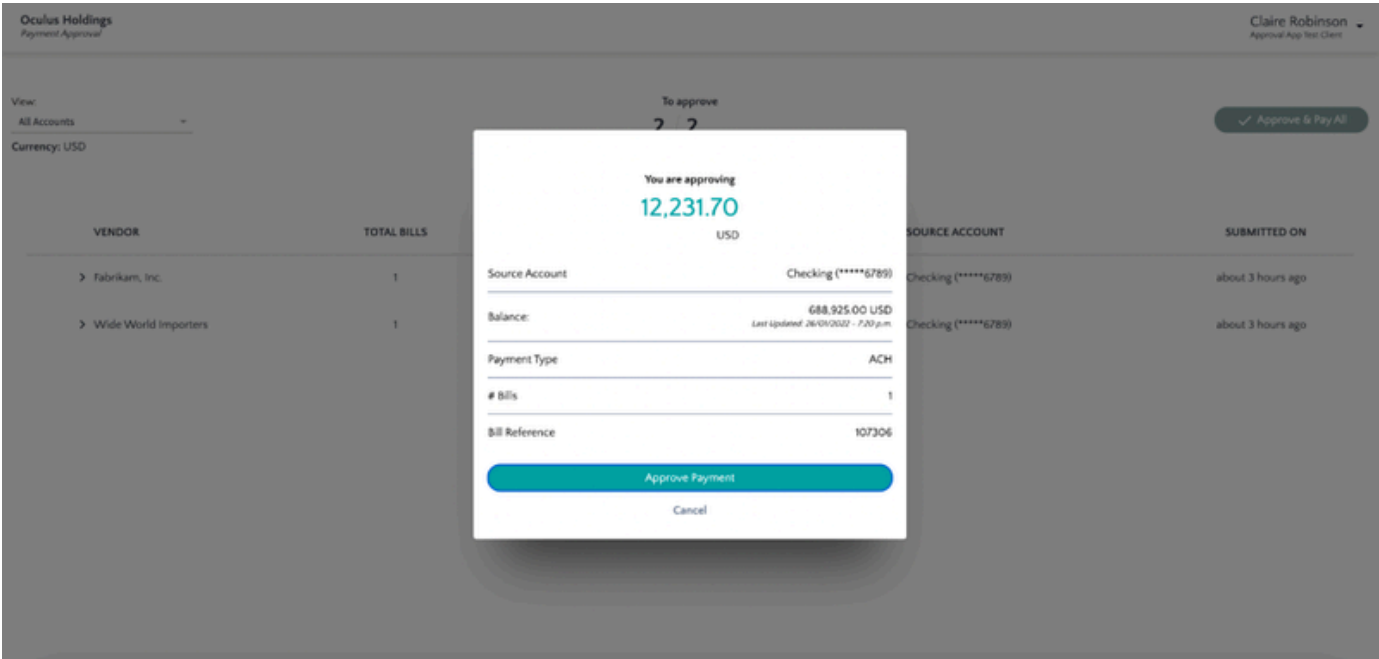
Reject the payment within Approval Portal.



Select Rejection Reason

Select a reason for rejection. Once rejected, the payment is sent back to the ERP and is reopened, thus becoming available to be repaid.

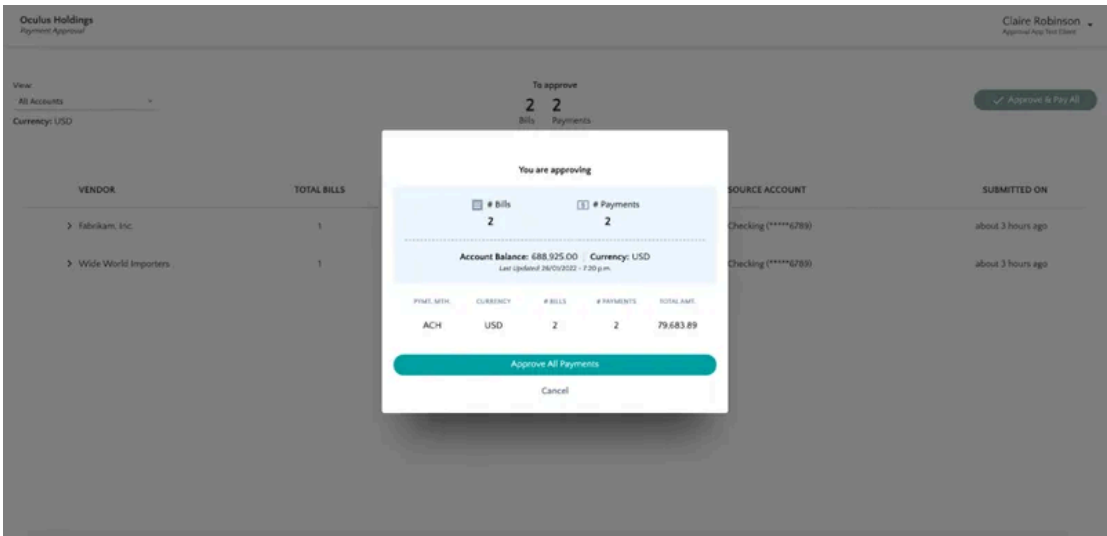
Approving Payments (one-by-one)



Approve Single Payment

Approve the payment one by one.

Approving Payments (multiple payments)



Approve Multiple Payments

Approve multiple payments in one click.

Litmus Unify (Unify) is a high-performance, secure, and highly available data hub that is designed for scalability. It is built upon an enterprise-class MQTT engine for better functionality and reliability.

You can access Unify using any of the following:

- Web UI (User Interface)
- APIs
- time.bsn.cloud

/emb

Security

Unify is designed with security integrated at every stage to meet the specific demands of Industrial IoT.

It offers:

- **Deployment Security:** Supports offline first and air-gapped installation.
- **Authentication and Authorization:** Enterprise-ready authentication, authorization, and RBAC (Role-Based Access Control) policies. The Unify user interface is only accessible with a login and password.
- **Platform Access Security:** Protected and modern HTTPS web interfaces.
- **Certificate Management:** Includes a default self-signed certificate, and therefore, all communications are secure by default.
- **Encryption:** All communication between a Unify device and user's browser is protected by transport layer encryption.
- **Software Update:** Over-the-air update systems implement detailed hash and other verifications.
- **Token-Based Security:** Provides token-based security for app authentication.

- **Data Access Security:** Secure and isolated message broker for real-time data subscription.

Features

Unify offers a set of features that allows you to implement your UNS designs and achieve strategic data goals.

1. Executing and monitoring corporate Unified Namespace
 2. Serves as a single source of truth for all data consumers
 3. Fulfill data governance requirements
- **time.bsn.cloud**

Next: Test ddd document

Ivanti

4. Detected API

4.1. Authentication

4.1.1. Create an access token

POST

`https://api.detected.app/api/v2/public/oauth/token`

Try it ▶

Production

Requests an OAuth 2.0 access token for your integration client, using the `app_credentials` grant type. Send the client ID and client secret of the integration client, and your account slug.

Send the returned `access_token` in the `Authorization` header of your requests, in the format `Bearer <access_token>`. The token expires after `expires_in` seconds. Request a new one when it does.

Body Parameters

▼ **body** `CreateTokenRequest`

- > **grant_type** `string<app_credentials>` *
- > **client_id** `string` *
- > **client_secret** `string` *
- > **slug** `string` *

Select... ▼

Responses

▼ ● 200 OK

▼ **object**

- > **data** `TokenResourceResponse`

Response Headers

X-RateLimit-Limit**X-RateLimit-Remaining****x-ratelimit-reset****retry-after**▼ ● 400 Bad Request. The request could not be processed because it is invalid. The `message` field explains why.▼ **object**

- > **message** `string`

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> message string

- ▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request POST \
  --url https://api.detected.app/api/v2/public/oauth/token \
  --header 'accept: application/json' \
  --header 'content-type: application/json' \
  --data '{
    "grant_type": "",
    "client_id": "",
    "client_secret": "",
    "slug": ""
  }'
```

Responses

● 200

```
// OK
{
  "data": {
    "token_type": "",
    "expires_in": 0,
    "access_token": ""
  }
}
```

4.2. Alerts

4.2.1. List alerts

GET

https://api.detected.app/api/v2/public/alerts

Try it ▶

Production

Returns the alerts raised for profiles in your account, most recent first. An alert is raised when monitored information about a profile changes. Use the query parameters to filter the results.

This endpoint is paginated. Use the `page` parameter to request further pages. The `meta` and `links` objects in the response describe the current page and link to the others.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Query Parameters

> `page` string

> `acknowledged` string

> `profile_id` string<uuid>

Select... ▼

Format: uuid

Responses

▼ ● 200 OK

▼ object

> `data` ProfileNotificationAlertsResourceResponse[]

> `links` LinksResource

> `meta` MetaResource

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

16 / 169

Created at Oct 06, 2026

▼ object

> message string

- ▼ ● **422** Unprocessable Content. The request was understood but failed validation. The response lists the fields that failed and why.

▼ object

> message string

> example_field string[]

- ▼ ● **429** Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/alerts \  
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "data": [
    {
      "id": 0,
      "profile_id": "",
      "attribute": "",
      "change": {
        "current": "",
        "previous": ""
      },
      "acknowledged": "",
      "acknowledged_by": "",
      "acknowledged_at": "",
      "created_at": ""
    }
  ],
  "links": {
    "first": "",
    "last": "",
    "prev": "",
    "next": ""
  },
  "meta": {
    "current_page": 0,
    "from": 0,
    "last_page": 0,
    "links": [
      {
        "url": "",
        "label": "",
        "active": false
      }
    ],
    "path": "",
    "per_page": 0,
    "to": 0,
    "total": 0
  }
}
```

4.3. Analysis

4.3.1. List profile analyses

GET

`https://api.detected.app/api/v2/public/profiles/{uuid}/analysis`

Try it ▶

Production

Returns the analyses for a profile. Each analysis includes the overall score and risk level and a detailed report grouped by rule group.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> **uuid** string *

Responses

✓ ● 200 OK

▼ object

> **data** AnalysisResource

Response Headers

X-RateLimit-Limit**X-RateLimit-Remaining****x-ratelimit-reset****retry-after**

✓ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> **message** string✓ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> **message** string

Request



```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/profiles/{uuid}/analysis \  
  --header 'accept: application/json'
```

Responses

● 200

```
// OK  
{  
  "data": {  
    "id": "",  
    "status": "",  
    "score": 0,  
    "workflow": [  
      {  
        "id": "",  
        "name": ""  
      }  
    ],  
    "risk": "",  
    "report": [  
      {  
        "name": "",  
        "total_rules": 0,  
        "total_completed_rules": 0,  
        "result": [  
          {  
            "id": "",  
            "analysis_id": "",  
            "score": 0,  
            "state": "",  
            "label": "",  
            "description": "",  
            "result": ""  
          }  
        ]  
      }  
    ],  
    "created_at": ""  
  }  
}
```

4.4. Audit Logs

4.4.1. List audit logs

GET

https://api.detected.app/api/v2/public/audit-logs

Try it ▶

Production

Returns audit log entries across all profiles in your account. Use `profile_id` to see the entries for a single profile, and the other query parameters to filter the results.

This endpoint is paginated. Use the `page` parameter to request further pages. The `meta` and `links` objects in the response describe the current page and link to the others.

Credentials

`HTTP Bearer` `AccessToken`

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Query Parameters

> `order_by` string

> `sort_by` string

> `page` string

> `profile_id` string

> `action` string

> `performed_by` string

Select... ▼

Responses

▼ ● 200 OK

▼ object

> `data` AuditLogResource[]

> `links` LinksResource

> `meta` MetaResource

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

x-ratelimit-reset

retry-after

✓ ● **401** Unauthorized. The access token is missing, invalid or has expired.

▼ object

> message string

✓ ● **403** Forbidden. Your access token is valid, but you do not have permission to access this resource.

▼ object

> message string

✓ ● **429** Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/audit-logs \  
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "data": [
    {
      "id": 0,
      "profile_id": "",
      "profile_name": "",
      "actioned_at": "",
      "performed_by": "",
      "auth_type": "",
      "application": "",
      "resource": "",
      "action": "",
      "reason": ""
    }
  ],
  "links": {
    "first": "",
    "last": "",
    "prev": "",
    "next": ""
  },
  "meta": {
    "current_page": 0,
    "from": 0,
    "last_page": 0,
    "links": [
      {
        "url": "",
        "label": "",
        "active": false
      }
    ],
    "path": "",
    "per_page": 0,
    "to": 0,
    "total": 0
  }
}
```

4.5. Brands

4.5.1. List brands

GET

`https://api.detected.app/api/v2/public/brands`

Try it ▶

Production

Returns the brands configured for your account, including their logos, fonts and the styling of buttons and inputs.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Responses

▼ ● 200 OK

▼ object

> data BrandResource[]

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

x-ratelimit-reset

retry-after

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> message string

▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request



```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/brands \  
  --header 'accept: application/json'
```

Responses

● 200

```
// OK  
{  
  "data": [  
    {  
      "id": "",  
      "name": "",  
      "slug": "",  
      "is_default": false,  
      "configuration": {  
        "logo": {  
          "url": "",  
          "size": ""  
        },  
        "inputs": {  
          "text": {  
            "corners": "",  
            "border-color": "",  
            "background-color": "",  
            "border-color-focus": ""  
          },  
          "checkboxes": {  
            "icon-color": "",  
            "background-color-focus": ""  
          }  
        },  
        "buttons": {  
          "primary_button": {  
            "glow": false,  
            "color": "",  
            "corners": "",  
            "border-color": "",  
            "background-color": ""  
          },  
          "secondry_button": {  
            "glow": false,  
            "corners": "",  
            "border-color": "",  
            "background-color": ""  
          }  
        }  
      },  
      "created_at": "",  
      "updated_at": ""  
    }  
  ]  
}
```


4.6. Case Management Users

4.6.1. List case management users

GET

https://api.detected.app/api/v2/public/users

Try it ▶

Production

Returns the case management users in your account. Use the query parameters to filter the results.

This endpoint is paginated. Use the `page` parameter to request further pages. The `meta` and `links` objects in the response describe the current page and link to the others.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Query Parameters

> order_by string

> sort_by string

> page string

> id string

> blocked string

> name string

> email string

Select... ▼

Select... ▼

Responses

▼ ● 200 OK

▼ object

> data UserListResource[]

> links LinksResource

> meta MetaResource

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

x-ratelimit-reset

retry-after

✓ ● **401** Unauthorized. The access token is missing, invalid or has expired.

▼ object

> message string

✓ ● **429** Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the **Retry-After** header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/users \  
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "data": [
    {
      "id": "",
      "name": "",
      "email": "",
      "blocked": false,
      "updated_at": "",
      "created_at": ""
    }
  ],
  "links": {
    "first": "",
    "last": "",
    "prev": "",
    "next": ""
  },
  "meta": {
    "current_page": 0,
    "from": 0,
    "last_page": 0,
    "links": [
      {
        "url": "",
        "label": "",
        "active": false
      }
    ],
    "path": "",
    "per_page": 0,
    "to": 0,
    "total": 0
  }
}
```

4.6.2. Retrieve a case management user

GET

`https://api.detected.app/api/v2/public/users/{userId}`

Try it ▶

Production

Returns a single case management user, including the teams and profiles they are assigned to.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> `userId` `string` *

Responses

▼ ● 200 OK

▼ `object`> `data` `UserViewResource`

Response Headers

`X-RateLimit-Limit``X-RateLimit-Remaining``x-ratelimit-reset``retry-after`

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ `object`> `message` `string`

▼ ● 404 Not Found. The requested resource does not exist, or is not available to your account.

▼ `object`> `message` `string`▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

- > message string

Request

 Curl

```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/users/{userId} \  
  --header 'accept: application/json'
```

Responses

 200

```
// OK  
{  
  "data": {  
    "id": "",  
    "name": "",  
    "email": "",  
    "blocked": false,  
    "teams": [  
      {  
        "id": 0,  
        "name": "",  
        "updated_at": "",  
        "created_at": ""  
      }  
    ],  
    "profiles": [  
      {  
        "id": "",  
        "review_status": "",  
        "updated_at": "",  
        "created_at": ""  
      }  
    ],  
    "updated_at": "",  
    "created_at": ""  
  }  
}
```

4.7. Checklists

4.7.1. List profile checklists

GET

https://api.detected.app/api/v2/public/profiles/{uuid}/checklists

Try it ▶

Production

Returns the checklists for a profile. Each checklist is made up of sections, and each section of tasks. Use the query parameters to filter the results.

This endpoint is paginated. Use the `page` parameter to request further pages. The `meta` and `links` objects in the response describe the current page and link to the others.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Path Parameters

> `uuid` *string* *

Query Parameters

> `order_by` *string*

Select... ▼

> `sort_by` *string*

> `page` *string*

> `id` *string*

> `name` *string*

Responses

▼ ● 200 OK

▼ object

> `data` ChecklistResource[]

> `links` LinksResource

> `meta` MetaResource

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

x-ratelimit-reset

retry-after

✓ ● **401** Unauthorized. The access token is missing, invalid or has expired.

▼ object

> message string

✓ ● **429** Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the **Retry-After** header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/profiles/{uuid}/checklists \  
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "data": [
    {
      "id": 0,
      "name": "",
      "sections": [
        {
          "id": 0,
          "name": "",
          "tasks": [
            {
              "id": 0,
              "name": "",
              "team": {
                "id": 0,
                "name": "",
                "members_count": 0
              }
            }
          ]
        }
      ],
      "status": "",
      "total_comments": 0,
      "member_belongs_to_team": false
    }
  ],
  "uncompleted_tasks": 0,
  "completed_tasks": 0
},
{
  "links": {
    "first": "",
    "last": "",
    "prev": "",
    "next": ""
  },
  "meta": {
    "current_page": 0,
    "from": 0,
    "last_page": 0,
    "links": [
      {
        "url": "",
        "label": "",
        "active": false
      }
    ]
  },
  "path": "",
  "per_page": 0,
  "to": 0,
  "total": 0
}
```


4.7.2. Retrieve a profile checklist

GET

https://api.detected.app/api/v2/public/profiles/{uuid}/checklists/{id}

Try it ▶

Production

Returns a single checklist for a profile, including its sections, tasks and progress.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Path Parameters

> **uuid** string *

> **id** string *

Responses

▼ ● 200 OK

▼ object

> **data** ChecklistResource

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

x-ratelimit-reset

retry-after

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> **message** string

▼ ● 404 Not Found. The requested resource does not exist, or is not available to your account.

▼ object

> **message** string

▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

- > message string

Request

 Curl

```
curl --request GET \
  --url https://api.detected.app/api/v2/public/profiles/{uuid}/checklists/{id} \
  --header 'accept: application/json'
```

Responses

 200

```
// OK
{
  "data": {
    "id": 0,
    "name": "",
    "sections": [
      {
        "id": 0,
        "name": "",
        "tasks": [
          {
            "id": 0,
            "name": "",
            "team": {
              "id": 0,
              "name": "",
              "members_count": 0
            }
          }
        ],
        "status": "",
        "total_comments": 0,
        "member_belongs_to_team": false
      }
    ],
    "uncompleted_tasks": 0,
    "completed_tasks": 0
  }
}
```

4.8. Documents

4.8.1. List document library types

GET

`https://api.detected.app/api/v2/public/documents/libraries`

Try it ▶

Production

Returns the document library types available in your account. Use a library's ID as the `libraryId` when you upload documents to a profile.

This endpoint is paginated. Use the `page` parameter to request further pages. The `meta` and `links` objects in the response describe the current page and link to the others.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Query Parameters

> `page` string

Responses

✓ • 200 OK

✓ object

> `data` `DocumentLibraryListResponse[]`

Response Headers

`X-RateLimit-Limit``X-RateLimit-Remaining``x-ratelimit-reset``retry-after`

✓ • 401 Unauthorized. The access token is missing, invalid or has expired.

✓ object

> `message` string✓ • 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object
 > message string

Request

 Curl

```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/documents/libraries \  
  --header 'accept: application/json'
```

Responses

 200

```
// OK  
{  
  "data": [  
    {  
      "id": 0,  
      "name": "",  
      "type": "",  
      "label": ""  
    }  
  ]  
}
```

4.8.2. Upload documents to a profile

POST

https://api.detected.app/api/v2/public/profiles/{uuid}/documents/{libraryId}

Try it ▶

Production

Uploads one or more documents to a profile, into the document library given by `libraryId` . Send the files as `multipart/form-data` , with each file under a key of the form `document_1` , `document_2` and so on. The response lists the uploaded documents.

Credentials

HTTP Bearer

AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>` . The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Path Parameters

> `uuid` `string` *

> `libraryId` `integer` *

Form Parameters

> `documents` `map<string, BinaryFile>` *

Responses

▼

● 200

OK. The documents were uploaded, and the response lists them.

▼ `DocumentViewResponse[]`

- > `id` `number` *
- > `profile_id` `string` *
- > `document_id` `string` *
- > `category` `string` *
- > `name` `string` *
- > `link` `string` *
- > `file_type` `string` *
- > `link_expires_at` `string` *
- > `fraud_check` `object`
- > `translation` `object`
- > `ocr` `object`
- > `updated_at` `string` *
- > `created_at` `string` *

▼ ● **400** Bad Request. The request could not be processed because it is invalid. The `message` field explains why.

▼ `object`

- > `message` `string`

▼ ● **401** Unauthorized. The access token is missing, invalid or has expired.

▼ `object`

- > `message` `string`

▼ ● **422** Unprocessable Content. The request was understood but failed validation. The response lists the fields that failed and why.

▼ `object`

- > `message` `string`
- > `example_field` `string[]`

▼ ● **429** Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ `object`

- > `message` `string`

Request



```
curl --request POST \  
  --url https://api.detected.app/api/v2/public/profiles/{uuid}/documents/{libraryId} \  
  --header 'accept: application/json' \  
  --header 'content-type: multipart/form-data' \  
  --form 'documents="map"'
```

Responses

● 200

```
// OK. The documents were uploaded, and the response lists them.
```

```
[
  {
    "id": 0,
    "profile_id": "",
    "document_id": "",
    "category": "",
    "name": "",
    "link": "",
    "file_type": "",
    "link_expires_at": "",
    "fraud_check": {
      "processed_at": "",
      "analysis": {
        "score": "",
        "document_type": "",
        "meta_data": {
          "producer": "",
          "creator": "",
          "creation_date": "",
          "mod_date": "",
          "author": "",
          "keywords": "",
          "subject": "",
          "title": ""
        }
      },
      "indicators": [
        {
          "type": "",
          "category": "",
          "title": "",
          "description": ""
        }
      ]
    },
    "translation": {
      "status": "",
      "link": "",
      "file_type": "",
      "link_expires_at": "",
      "extracted": ""
    },
    "ocr": {
      "extracted": ""
    },
    "updated_at": "",
    "created_at": ""
  }
]
```

4.8.3. List documents

GET

https://api.detected.app/api/v2/public/documents

Try it ▶

Production

Returns a list of documents uploaded to profiles in your account. Use the query parameters to filter the results.

This endpoint is paginated. Use the `page` parameter to request further pages. The `meta` and `links` objects in the response describe the current page and link to the others.

Credentials

`HTTP Bearer` `AccessToken`

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Query Parameters

> id number

> order_by string

> sort_by string

> page string

> profile_id string

> document_id string

> category string

> name string

Select... ▼

Responses

▼ ● 200 OK

▼ object

> data DocumentListResponse[]

> links LinksResource

> meta MetaResource

Response Headers

- X-RateLimit-Limit
- X-RateLimit-Remaining
- x-ratelimit-reset

retry-after

✓ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> message string

✓ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/documents \  
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "data": [
    {
      "id": 0,
      "profile_id": "",
      "library_id": "",
      "category": "",
      "name": "",
      "updated_at": "",
      "created_at": ""
    }
  ],
  "links": {
    "first": "",
    "last": "",
    "prev": "",
    "next": ""
  },
  "meta": {
    "current_page": 0,
    "from": 0,
    "last_page": 0,
    "links": [
      {
        "url": "",
        "label": "",
        "active": false
      }
    ],
    "path": "",
    "per_page": 0,
    "to": 0,
    "total": 0
  }
}
```

4.8.4. Retrieve a document

GET

`https://api.detected.app/api/v2/public/documents/{id}`

Try it ▶

Production

Returns a single document, including a temporary link to download it and the results of processing, such as OCR, translation and fraud analysis.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> `id string *`

Responses

✓ • 200 OK

▼ object

> `data DocumentViewResponse`

Response Headers

`X-RateLimit-Limit``X-RateLimit-Remaining``x-ratelimit-reset``retry-after`

✓ • 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> `message string`

✓ • 404 Not Found. The requested resource does not exist, or is not available to your account.

▼ object

> `message string`✓ • 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object
 > message string

Request



```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/documents/{id} \  
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "data": {
    "id": 0,
    "profile_id": "",
    "document_id": "",
    "category": "",
    "name": "",
    "link": "",
    "file_type": "",
    "link_expires_at": "",
    "fraud_check": {
      "processed_at": "",
      "analysis": {
        "score": "",
        "document_type": "",
        "meta_data": {
          "producer": "",
          "creator": "",
          "creation_date": "",
          "mod_date": "",
          "author": "",
          "keywords": "",
          "subject": "",
          "title": ""
        }
      }
    },
    "indicators": [
      {
        "type": "",
        "category": "",
        "title": "",
        "description": ""
      }
    ]
  },
  "translation": {
    "status": "",
    "link": "",
    "file_type": "",
    "link_expires_at": "",
    "extracted": ""
  },
  "ocr": {
    "extracted": ""
  },
  "updated_at": "",
  "created_at": ""
}
```

4.9. Forms

4.9.1. List forms

GET

`https://api.detected.app/api/v2/public/forms`

Try it ▶

Production

Returns the forms available in your account.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Responses

▼ ● 200 OK

▼ object

> data ShortFormResource[]

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

x-ratelimit-reset

retry-after

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> message string

▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/forms \  
  --header 'accept: application/json'
```

Responses

 200

```
// OK  
{  
  "data": [  
    {  
      "id": 0,  
      "label": "",  
      "reference": "",  
      "version": 0,  
      "provider": "",  
      "archived": false,  
      "updated_at": "",  
      "created_at": ""  
    }  
  ]  
}
```

4.9.2. Retrieve a form

GET

`https://api.detected.app/api/v2/public/forms/{id}`

Try it ▶

Production

Returns a single form, including its schema and sections.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> `id string *`

Responses

▼ ● 200 OK

▼ object

> `data FormResource[]`

Response Headers

`X-RateLimit-Limit``X-RateLimit-Remaining``x-ratelimit-reset``retry-after`

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> `message string`▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> `message string`

Request

 Curl

```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/forms/{id} \  
  --header 'accept: application/json'
```

Responses

 200

```
// OK  
{  
  "data": [  
    {  
      "id": 0,  
      "label": "",  
      "reference": "",  
      "version": 0,  
      "provider": "",  
      "schema": [  
        {}  
      ],  
      "sections": [  
        {}  
      ],  
      "archived": false,  
      "updated_at": "",  
      "created_at": ""  
    }  
  ]  
}
```

4.9.3. List representative forms

GET

https://api.detected.app/api/v2/public/representatives/{uuid}/forms

Try it ▶

Production

Returns the forms assigned to a representative, with the answers given. Use the query parameters to filter the results.

Credentials

HTTP Bearer

AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Path Parameters

> uuid string *

Query Parameters

> id string

> label string

> reference string

> applies_to string

Responses

▼

● 200 OK

▼

object

>

data EntityFormResource[]

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

x-ratelimit-reset

retry-after

▼

● 401 Unauthorized. The access token is missing, invalid or has expired.

▼

object

>

message string

- ▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/representatives/{uuid}/forms \  
  --header 'accept: application/json'
```

Responses

● 200

```
// OK  
{  
  "data": [  
    {  
      "id": 0,  
      "label": "",  
      "reference": "",  
      "answers": [  
        {  
          "label": "",  
          "answer": ""  
        }  
      ],  
      "updated_at": "",  
      "created_at": ""  
    }  
  ]  
}
```

4.9.4. Retrieve a representative form

GET

`https://api.detected.app/api/v2/public/representatives/{uuid}/forms/{id}`

Try it ▶

Production

Returns a single form assigned to a representative, with the answers given.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> `uuid string *`> `id string *`

Responses

▼ ● 200 OK

▼ object

> `data EntityFormResource`

Response Headers

`X-RateLimit-Limit``X-RateLimit-Remaining``x-ratelimit-reset``retry-after`

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> `message string`

▼ ● 404 Not Found. The requested resource does not exist, or is not available to your account.

▼ object

> `message string`▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/representatives/{uuid}/forms/{id} \  
  --header 'accept: application/json'
```

Responses

 200

```
// OK  
{  
  "data": {  
    "id": 0,  
    "label": "",  
    "reference": "",  
    "answers": [  
      {  
        "label": "",  
        "answer": ""  
      }  
    ],  
    "updated_at": "",  
    "created_at": ""  
  }  
}
```

4.9.5. Submit answers to a profile form

POST`https://api.detected.app/api/v2/public/profiles/{uuid}/forms/{id}/answers`

Try it ▶

Production

Submits answers to a form that has been assigned to a profile.

The request body is a JSON object that matches the form's schema, so its structure is different for each form. Retrieve a form's schema with `GET /forms/{id}` to find the exact field names and data types. Answers are validated against the schema.

Submitting answers again replaces the previous answers. Previously uploaded file answers are kept unless you send a new file for that field.

The form must be assigned to the profile before you submit answers.

Example payload

```
{
  "field_name_1": "answer value",
  "field_name_2": true,
  "field_name_3": ["option1", "option2"]
}
```

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> **uuid** string *> **id** string *

Responses

▼ ● 201 Created

▼ object

> **data** EntityFormResource

Response Headers

X-RateLimit-Limit**X-RateLimit-Remaining****x-ratelimit-reset**

retry-after

▼ ● **401** Unauthorized. The access token is missing, invalid or has expired.

▼ object

> **message** string

▼ ● **404** Not Found. The requested resource does not exist, or is not available to your account.

▼ object

> **message** string

▼ ● **429** Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the **Retry-After** header before trying again.

▼ object

> **message** string

Request

 Curl

```
curl --request POST \
  --url https://api.detected.app/api/v2/public/profiles/{uuid}/forms/{id}/answers \
  --header 'accept: application/json'
```

Responses

● 201

```
// Created
{
  "data": {
    "id": 0,
    "label": "",
    "reference": "",
    "answers": [
      {
        "label": "",
        "answer": ""
      }
    ],
    "updated_at": "",
    "created_at": ""
  }
}
```

4.9.6. List profile forms

GET

https://api.detected.app/api/v2/public/profiles/{uuid}/forms

Try it ▶

Production

Returns the forms assigned to a profile, with the answers given. Use the query parameters to filter the results.

Credentials

HTTP Bearer

AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Path Parameters

>

uuid

string

*

Query Parameters

>

id

string

>

label

string

>

reference

string

>

applies_to

string

Responses

▼

● 200

OK

▼

object

>

data

EntityFormResource[]

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

x-ratelimit-reset

retry-after

▼

● 401

Unauthorized. The access token is missing, invalid or has expired.

▼

object

>

message

string

- ▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/profiles/{uuid}/forms \  
  --header 'accept: application/json'
```

Responses

● 200

```
// OK  
{  
  "data": [  
    {  
      "id": 0,  
      "label": "",  
      "reference": "",  
      "answers": [  
        {  
          "label": "",  
          "answer": ""  
        }  
      ],  
      "updated_at": "",  
      "created_at": ""  
    }  
  ]  
}
```

4.9.7. Assign a form to a profile

PUT

https://api.detected.app/api/v2/public/profiles/{uuid}/forms

Try it ▶

Production

Assigns a form to a profile. Send a single form ID in the request body. The latest version of the form is assigned. If that version is already assigned to the profile, it is skipped, so there are no duplicates.

The response lists all the forms currently assigned to the profile, including the one you just assigned.

Restrictions

- Only forms of type `internal_forms` can be assigned.
- The form must belong to the same list as the profile.
- If the form does not exist or is not an allowed type, a validation error is returned.

Credentials

`HTTP Bearer` `AccessToken`

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Path Parameters

> `uuid` `string` *

Body Parameters

▼ `body` `AssignFormToProfileRequest`

> `id` `number` *

Responses

▼ ● 200 OK

▼ `object`

> `data` `ShortFormResource[]`

Response Headers

`X-RateLimit-Limit`

`X-RateLimit-Remaining`

`x-ratelimit-reset`

`retry-after`

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> message string

- ▼ ● 422 Unprocessable Content. The request was understood but failed validation. The response lists the fields that failed and why.

▼ object

> message string

> example_field string[]

- ▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request PUT \
  --url https://api.detected.app/api/v2/public/profiles/{uuid}/forms \
  --header 'accept: application/json' \
  --header 'content-type: application/json' \
  --data '{
    "id": ""
  }'
```

Responses

● 200

```
// OK
{
  "data": [
    {
      "id": 0,
      "label": "",
      "reference": "",
      "version": 0,
      "provider": "",
      "archived": false,
      "updated_at": "",
      "created_at": ""
    }
  ]
}
```

4.9.8. Retrieve a profile form

GET

https://api.detected.app/api/v2/public/profiles/{uuid}/forms/{id}

Try it ▶

Production

Returns a single form assigned to a profile, with the answers given.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Path Parameters

> uuid string *

> id string *

Responses

▼ ● 200 OK

▼ object

> data EntityFormResource

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

x-ratelimit-reset

retry-after

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> message string

▼ ● 404 Not Found. The requested resource does not exist, or is not available to your account.

▼ object

> message string

▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/profiles/{uuid}/forms/{id} \  
  --header 'accept: application/json'
```

Responses

 200

```
// OK  
{  
  "data": {  
    "id": 0,  
    "label": "",  
    "reference": "",  
    "answers": [  
      {  
        "label": "",  
        "answer": ""  
      }  
    ],  
    "updated_at": "",  
    "created_at": ""  
  }  
}
```

4.10. Onboarding

4.10.1. Submit a profile for review

POST

`https://api.detected.app/api/v2/public/onboardings/{uuid}/submissions`

Try it ▶

Production

Submits a profile for review. This is the API equivalent of the "Review and submit" step in the portal. It checks again that every required onboarding step is complete, then records a new submission declared by the representative you specify. The representative must already exist on the profile with the `declaratory` type.

Submitting moves the profile into `Needs Review`.

Credentials

`HTTP Bearer` `AccessToken`

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> `uuid` `string` *

Body Parameters

▼ `body` `OnboardingSubmissionCreateRequest`> `representative_id` `string<uuid>` *

Format: uuid

Responses

▼ ● 201 Created

▼ `OnboardingSubmissionResource`> `data` `object`

Response Headers

`X-RateLimit-Limit``X-RateLimit-Remaining`▼ ● 400 Bad Request. The request could not be processed because it is invalid. The `message` field explains why.▼ `object`> `message` `string`

✓ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object
> message string

✓ ● 404 Not Found. The requested resource does not exist, or is not available to your account.

▼ object
> message string

✓ ● 422 Unprocessable Content. The request was understood but failed validation. The response lists the fields that failed and why.

▼ object
> message string
> example_field string[]

✓ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object
> message string

Request

[Curl](#)

```
curl --request POST \
  --url https://api.detected.app/api/v2/public/onboardings/{uuid}/submissions \
  --header 'accept: application/json' \
  --header 'content-type: application/json' \
  --data '{
    "representative_id": ""
  }'
```

Responses

[201](#)

```
// Created
{
  "data": {
    "declared_at": "",
    "representative_id": ""
  }
}
```

4.10.2. Retrieve onboarding status

GET

`https://api.detected.app/api/v2/public/onboardings/{uuid}`

Try it ▶

Production

Returns the onboarding checklist for a profile: each step the profile must complete, and whether it is `pending`, `in-progress`, `in-complete` or `completed`. Use it to check whether a profile is ready to be submitted with `POST /onboardings/{uuid}/submissions`.

Credentials

HTTP Bearer `AccessToken`

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> `uuid string *`

Responses

✓ ● 200 OK

▼ `OnboardingStatusResource`> `data object[]`

Response Headers

`X-RateLimit-Limit``X-RateLimit-Remaining`

✓ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ `object`> `message string`

✓ ● 404 Not Found. The requested resource does not exist, or is not available to your account.

▼ `object`> `message string`✓ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.▼ `object`> `message string`

Request



```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/onboardings/{uuid} \  
  --header 'accept: application/json'
```

Responses



```
// OK  
{  
  "data": [  
    {  
      "code": "",  
      "title": "",  
      "status": ""  
    }  
  ]  
}
```

4.11. Portal Configurations

4.11.1. List portal configurations

GET

https://api.detected.app/api/v2/public/portal-configurations

Try it ▶

Production

Returns the portal configurations for your account. A portal configuration defines what a profile's onboarding portal asks for.

This endpoint is paginated. Use the `page` parameter to request further pages. The `meta` and `links` objects in the response describe the current page and link to the others.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Query Parameters

> page string

> id string

> name string

Responses

▼

● 200 OK

▼

object

>

data PortalConfigurationResponse

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

x-ratelimit-reset

retry-after

▼

● 401 Unauthorized. The access token is missing, invalid or has expired.

▼

object

>

message string

- ✓ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object
 > message string

Request

 Curl

```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/portal-configurations \  
  --header 'accept: application/json'
```

Responses

● 200

```
// OK  
{  
  "data": {  
    "id": 0,  
    "name": "",  
    "updated_at": "",  
    "created_at": ""  
  }  
}
```

4.11.2. Retrieve a profile portal configuration

GET

`https://api.detected.app/api/v2/public/profiles/{uuid}/portal-configuration`

Try it ▶

Production

Returns the portal configuration currently assigned to a profile, with the detail of every setting. `GET /portal-configurations` lists the available configurations. This endpoint shows the settings applied to one profile.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> **uuid** `string` *

Responses

✓ • **200** OK▼ `object`> **data** `ProfilePortalConfigurationResourceResponse`

Response Headers

X-RateLimit-Limit**X-RateLimit-Remaining****x-ratelimit-reset****retry-after**✓ • **401** Unauthorized. The access token is missing, invalid or has expired.▼ `object`> **message** `string`✓ • **404** Not Found. The requested resource does not exist, or is not available to your account.▼ `object`> **message** `string`✓ • **429** Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object
 > message string

Request

 Curl

```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/profiles/{uuid}/portal-configuration \  
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "data": {
    "declaratory": {
      "enabled": false,
      "text": ""
    },
    "document": {
      "enabled": false,
      "documents": [
        {
          "uuid": "",
          "name": "",
          "description": "",
          "required": false,
          "example_document": [
            {
              "options": [
                ""
              ],
              "document": ""
            }
          ]
        }
      ]
    },
    "advanced_documents": {
      "enabled": false,
      "config_ids": [
        0
      ]
    },
    "identity": {
      "enabled": false
    },
    "director": {
      "enabled": false,
      "enable_director_country_of_birth": false,
      "people_model": {
        "id": 0
      },
      "max_number": 0,
      "auto_screening": false,
      "director_company": {
        "max_number": 0,
        "people_model": {
          "id": 0
        }
      }
    },
    "submitter": {
      "enabled": false,
      "people_model": {
        "id": 0
      },
      "auto_screening": false
    }
  }
}
```

```
,
"ownership": {
  "enabled": false,
  "enable_ownership_percentage": false,
  "enable_owner_country_of_birth": false,
  "ownership_percentage": "",
  "max_number": 0,
  "people_model": {
    "id": 0
  },
},
"auto_screening": false
},
"company_principals": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
},
"auto_screening": false,
"max_number": 0
},
"authorised_representative": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
},
"auto_screening": false,
"max_number": 0
},
"authorised_signatory": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
},
"auto_screening": false,
"max_number": 0
},
"treasurer": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
},
"auto_screening": false,
"max_number": 0
},
"secretary": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
},
"auto_screening": false,
"max_number": 0
},
"syndicator": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
},
"auto_screening": false,
"max_number": 0
```

```
},
"member": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
  "auto_screening": false,
  "max_number": 0
},
"agent": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
  "auto_screening": false,
  "max_number": 0
},
"designated_member": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
  "auto_screening": false,
  "max_number": 0
},
"club_manager": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
  "auto_screening": false,
  "max_number": 0
},
"trustee": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
  "max_number": 0,
```


4.11.3. Update a profile portal configuration

PATCH`https://api.detected.app/api/v2/public/profiles/{uuid}/portal-configuration`

Try it ▶

Production

Updates the portal configuration assigned to a profile. Currently you can only update the forms assigned to the configuration. More options will be added over time.

To remove all forms from the configuration, set `forms.form_ids` to `null`. See the examples.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> `uuid string *`

Body Parameters

▼ **body** `ProfilePortalConfigurationUpdateRequest`

> **forms** `object`

Responses

▼ ● **200** OK

▼ `object`

> **data** `ProfilePortalConfigurationResourceResponse`

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

x-ratelimit-reset

retry-after

▼ ● **401** Unauthorized. The access token is missing, invalid or has expired.

▼ `object`

> **message** `string`

▼ ● **404** Not Found. The requested resource does not exist, or is not available to your account.

▼ object

> message string

- ▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request PATCH \  
  --url https://api.detected.app/api/v2/public/profiles/{uuid}/portal-configuration \  
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "data": {
    "declaratory": {
      "enabled": false,
      "text": ""
    },
    "document": {
      "enabled": false,
      "documents": [
        {
          "uuid": "",
          "name": "",
          "description": "",
          "required": false,
          "example_document": [
            {
              "options": [
                ""
              ],
              "document": ""
            }
          ]
        }
      ]
    },
    "advanced_documents": {
      "enabled": false,
      "config_ids": [
        0
      ]
    },
    "identity": {
      "enabled": false
    },
    "director": {
      "enabled": false,
      "enable_director_country_of_birth": false,
      "people_model": {
        "id": 0
      },
      "max_number": 0,
      "auto_screening": false,
      "director_company": {
        "max_number": 0,
        "people_model": {
          "id": 0
        }
      }
    },
    "submitter": {
      "enabled": false,
      "people_model": {
        "id": 0
      },
      "auto_screening": false
    }
  }
}
```

```
,
"ownership": {
  "enabled": false,
  "enable_ownership_percentage": false,
  "enable_owner_country_of_birth": false,
  "ownership_percentage": "",
  "max_number": 0,
  "people_model": {
    "id": 0
  },
  "auto_screening": false
},
"company_principals": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
  "auto_screening": false,
  "max_number": 0
},
"authorised_representative": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
  "auto_screening": false,
  "max_number": 0
},
"authorised_signatory": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
  "auto_screening": false,
  "max_number": 0
},
"treasurer": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
  "auto_screening": false,
  "max_number": 0
},
"secretary": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
  "auto_screening": false,
  "max_number": 0
},
"syndicator": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
  "auto_screening": false,
  "max_number": 0
}
```

```
},
"member": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
  "auto_screening": false,
  "max_number": 0
},
"agent": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
  "auto_screening": false,
  "max_number": 0
},
"designated_member": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
  "auto_screening": false,
  "max_number": 0
},
"club_manager": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
  "auto_screening": false,
  "max_number": 0
},
"trustee": {
  "enabled": false,
  "people_model": {
    "id": 0
  },
  "max_number": 0,
```

4.12. Portal Users

4.12.1. List portal user activity

GET

https://api.detected.app/api/v2/public/portal-users/activity

Try it ▶

Production

Returns activity recorded for portal users, such as login events. By default it returns all activity for all portal users in your account. Narrow the results with filters such as `profile_id`.

The supported activity types (`types`) are:

- `access_log` : login events, including IP address, location, browser and session information
- More activity types may be added in future.

This endpoint is paginated. Use the `page` parameter to request further pages. The `meta` and `links` objects in the response describe the current page and link to the others.

Credentials

HTTP Bearer

AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Query Parameters

> id string

> user_id string

> profile_id string

> email string

> ip string

> types string

> name string

> order_by string

> sort_by string

> page string

Select... ▼

Responses

▼

● 200 OK

▼ object

> data ProfilePortalUserActivityResponse

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> message string

▼ ● 404 Not Found. The requested resource does not exist, or is not available to your account.

▼ object

> message string

▼ ● 422 Unprocessable Content. The request was understood but failed validation. The response lists the fields that failed and why.

▼ object

> message string

> example_field string[]

▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request



```
curl --request GET \
  --url https://api.detected.app/api/v2/public/portal-users/activity \
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "data": {
    "id": 0,
    "type": "",
    "user": {
      "id": 0,
      "name": "",
      "email": ""
    },
    "ip": "",
    "browser_agent": "",
    "session_information": {
      "city": "",
      "region": "",
      "country_code": "",
      "latitude": "",
      "longitude": "",
      "time_zone": "",
      "privacy_node": {
        "tor": false,
        "vpn": false,
        "proxy": false,
        "relay": false,
        "hosting": false,
        "service": ""
      }
    },
    "updated_at": "",
    "created_at": ""
  }
}
```

4.12.2. List portal users

GET

https://api.detected.app/api/v2/public/portal-users

Try it ▶

Production

Returns the portal users in your account. Use the query parameters to filter the results.

This endpoint is paginated. Use the `page` parameter to request further pages. The `meta` and `links` objects in the response describe the current page and link to the others.

Credentials

`HTTP Bearer` `AccessToken`

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Query Parameters

> `order_by` `string`

> `sort_by` `string`

> `page` `string`

> `id` `string`

> `name` `string`

> `email` `string`

> `profile_id` `string`

Select... ▼

Responses

▼ ● 200 OK

▼ `object`

> `data` `PortalUserViewResource[]`

> `links` `LinksResource`

> `meta` `MetaResource`

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

88 / 169

Created at Oct 06, 2026

▼ object

> message string

- ▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request GET \
  --url https://api.detected.app/api/v2/public/portal-users \
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "data": [
    {
      "id": 0,
      "name": "",
      "email": "",
      "profiles": [
        {
          "id": "",
          "name": "",
          "role": ""
        }
      ],
      "updated_at": "",
      "created_at": ""
    }
  ],
  "links": {
    "first": "",
    "last": "",
    "prev": "",
    "next": ""
  },
  "meta": {
    "current_page": 0,
    "from": 0,
    "last_page": 0,
    "links": [
      {
        "url": "",
        "label": "",
        "active": false
      }
    ],
    "path": "",
    "per_page": 0,
    "to": 0,
    "total": 0
  }
}
```

4.12.3. Create a portal user

POST`https://api.detected.app/api/v2/public/portal-users`

Try it ▶

Production

Creates a portal user with the given email address. You can then assign the user to a profile with `PUT /profiles/{uuid}/portal-users`.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Body Parameters

▼ **body** PortalUserCreateRequest> **email** string *

Responses

▼ ● **201** Created

▼ object

> **data** PortalUserViewResource

Response Headers

X-RateLimit-Limit**X-RateLimit-Remaining**▼ ● **401** Unauthorized. The access token is missing, invalid or has expired.

▼ object

> **message** string▼ ● **422** Unprocessable Content. The request was understood but failed validation. The response lists the fields that failed and why.

▼ object

> **message** string> **example_field** string[]▼ ● **429** Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request POST \  
  --url https://api.detected.app/api/v2/public/portal-users \  
  --header 'accept: application/json' \  
  --header 'content-type: application/json' \  
  --data '{  
    "email": ""  
  }'
```

Responses

● 201

```
// Created  
{  
  "data": {  
    "id": 0,  
    "name": "",  
    "email": "",  
    "profiles": [  
      {  
        "id": "",  
        "name": "",  
        "role": ""  
      }  
    ],  
    "updated_at": "",  
    "created_at": ""  
  }  
}
```

4.12.4. Create a portal user login link

POST`https://api.detected.app/api/v2/public/portal-users/{userId}/login-links`

Try it ▶

Production

Creates a login link for a portal user, for a specific profile. The portal user uses the link to sign in to the portal. Currently the only supported purpose is `onboarding`.

The response includes the time at which the link expires (`expires_at`).

Credentials

HTTP Bearer `AccessToken`

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> `userId string *`

Body Parameters

▼ `body PortalUserLoginLinkCreateRequest`> `profile_id string *`> `purpose string<onboarding> *`

Responses

▼ ● **201** Created▼ `object`> `data PortalUserLinkLoginResourceResponse`

Response Headers

`X-RateLimit-Limit``X-RateLimit-Remaining``x-ratelimit-reset``retry-after`▼ ● **401** Unauthorized. The access token is missing, invalid or has expired.▼ `object`> `message string`

▼ ● 404 Not Found. The requested resource does not exist, or is not available to your account.

▼ object
> message string

▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object
> message string

Request

 Curl

```
curl --request POST \
  --url https://api.detected.app/api/v2/public/portal-users/{userId}/login-links \
  --header 'accept: application/json' \
  --header 'content-type: application/json' \
  --data '{
    "profile_id": "",
    "purpose": ""
  }'
```

Responses

 201

```
// Created
{
  "data": {
    "purpose": "",
    "link": "",
    "expires_at": ""
  }
}
```

4.12.5. Retrieve a portal user

GET

`https://api.detected.app/api/v2/public/portal-users/{userId}`

Try it ▶

Production

Returns a single portal user, including the profiles they are assigned to and their role on each.

Credentials

HTTP Bearer `AccessToken`

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> `userId string *`

Responses

▼ ● 200 OK

▼ object

> `data PortalUserViewResource`

Response Headers

`X-RateLimit-Limit``X-RateLimit-Remaining`

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> `message string`▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> `message string`

Request

 Curl

```
curl --request GET \
  --url https://api.detected.app/api/v2/public/portal-users/{userId} \
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "data": {
    "id": 0,
    "name": "",
    "email": "",
    "profiles": [
      {
        "id": "",
        "name": "",
        "role": ""
      }
    ],
    "updated_at": "",
    "created_at": ""
  }
}
```

4.13. Profiles

4.13.1. List profile custom fields

GET

https://api.detected.app/api/v2/public/profiles/{uuid}/custom-fields

Try it ▶

Production

Returns the custom fields defined for a profile, with the label and current value of each.

This endpoint is paginated. Use the `page` parameter to request further pages. The `meta` and `links` objects in the response describe the current page and link to the others.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Path Parameters

> `uuid` *string* *

Query Parameters

> `page` *string*

Responses

▼

● 200 OK

▼

object

> `data` *ProfileCustomFieldResource[]*

> `links` *LinksResource*

> `meta` *MetaResource*

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

x-ratelimit-reset

retry-after

▼

● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> message string

- ▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request GET \
  --url https://api.detected.app/api/v2/public/profiles/{uuid}/custom-fields \
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "data": [
    {
      "label": "",
      "type": "",
      "is_required": false,
      "value": {}
    }
  ],
  "links": {
    "first": "",
    "last": "",
    "prev": "",
    "next": ""
  },
  "meta": {
    "current_page": 0,
    "from": 0,
    "last_page": 0,
    "links": [
      {
        "url": "",
        "label": "",
        "active": false
      }
    ],
    "path": "",
    "per_page": 0,
    "to": 0,
    "total": 0
  }
}
```

4.13.2. List profiles

GET

https://api.detected.app/api/v2/public/profiles

Try it ▶

Production

Returns a list of profiles for your account. Use the query parameters to filter the results.

This endpoint is paginated. Use the `page` parameter to request further pages. The `meta` and `links` objects in the response describe the current page and link to the others.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Query Parameters

> order_by string

> sort_by string

> page string

> id string

> entity_type string

> review_status string

> team_id string

> assignee_id string

> risk_id string

> customer_reference string

> configuration_id string

Select... ▼

Select... ▼

Select... ▼

Responses

▼ ● 200 OK

▼ object

> data ProfileListResource[]

> links LinksResource

> meta MetaResource

Response Headers

X-RateLimit-Limit**X-RateLimit-Remaining****x-ratelimit-reset****retry-after**

▼ ● **401** Unauthorized. The access token is missing, invalid or has expired.

▼ object

> message string

▼ ● **422** Unprocessable Content. The request was understood but failed validation. The response lists the fields that failed and why.

▼ object

> message string

> example_field string[]

▼ ● **429** Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/profiles \  
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "data": [
    {
      "id": "",
```

4.13.3. Create a profile

POST`https://api.detected.app/api/v2/public/profiles`

Try it ▶

Production

Creates a profile. There are two ways to do it, both using this endpoint with different fields.

Option 1: create from a search result

Use this after you have searched for the company with `POST /search`. Send the `lookup_id` from the search response and the `response_id` of the result you want. The company details come from the search result, so do not send them yourself.

- Required: `customer_reference`, `lookup_id`, `response_id`
- Optional: `type`, `domain`, `brand_id`

Option 2: create manually

Use this when the company cannot be found by search, or when you want to supply the details yourself. Send the company details.

- Required: `customer_reference`, `name`, `address` (with `country_code` and `city`)
- Optional: `type`, `company_number`, `vat_number`, `domain`, `brand_id`, and the rest of the address

If you do not send `type`, `company_number` is also required. If you send `type`, the exact company details that are required depend on the entity type.

You cannot mix the two options: a request that contains `lookup_id` or `response_id` together with any of the company details (`name`, `company_number`, `vat_number` or `address`) is rejected with a `422` error.

Credentials

`HTTP Bearer` `AccessToken`

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Body Parameters

body CreateProfileRequest

Description
Send either the search result fields (Option 1) or the company details (Option 2). See the description of this endpoint.

One Of
CreateProfileFro... ▾

Select... ▾

Format: uuid

- > type string<company | sole_trader | partnership | charity | government_ent...
- > lookup_id number *
- > response_id number *
- > customer_reference string *
- > brand_id string<uuid>
- > domain string

Responses

201 Created. The profile was created.

- object
 - > data ProfileListResource

Response Headers

- X-RateLimit-Limit
- X-RateLimit-Remaining
- x-ratelimit-reset
- retry-after

401 Unauthorized. The access token is missing, invalid or has expired.

- object
 - > message string

422 Unprocessable Content. The request was understood but failed validation. The response lists the fields that failed and why.

- object
 - > message string
 - > example_field string[]

429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the **Retry-After** header before trying again.

▼ object
 > message string

Request

 Curl

```
curl --request POST \  
  --url https://api.detected.app/api/v2/public/profiles \  
  --header 'accept: application/json' \  
  --header 'content-type: application/json' \  
  --data '{  
    "lookup_id": "",  
    "response_id": "",  
    "customer_reference": ""  
  }'
```

Responses

● 201

```
// Created. The profile was created.
```

```
{
  "data": {
    "id": "",
    "entity_type": {
      "id": 0,
      "type": "",
      "label": ""
    },
    "customer_reference": "",
    "company_name": "",
    "risk": {
      "id": "",
      "label": "",
      "category": ""
    },
    "team": {
      "id": 0,
      "label": ""
    },
    "configuration": {
      "id": 0,
      "name": ""
    },
    "brand": {
      "id": "",
      "name": "",
      "slug": ""
    },
    "review_status": "",
    "assignee": {
      "id": "",
      "name": ""
    },
    "review_at": "",
    "updated_at": "",
    "created_at": ""
  }
}
```

4.13.4. Retrieve a profile

GET

https://api.detected.app/api/v2/public/profiles/{uuid}

Try it ▶

Production

Returns a single profile, including company details, screenings and more.

Data source providers

Company data comes from a range of data providers, and each supplies information in a different format. Some of it is normalised to a consistent format, but not all of it can be, so the response may include undocumented data.

Every field under `data.company` either contains information, is `null`, or is an empty array (`[]`). We cannot guarantee that data is present, because that depends on what the data providers supply.

Credentials

`HTTP Bearer` `AccessToken`

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Path Parameters

> `uuid` `string` *

Responses

▼ ● 200 OK

▼ object

> `data` `ProfileResource`

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

x-ratelimit-reset

retry-after

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> `message` `string`

▼ ● 404 Not Found. The requested resource does not exist, or is not available to your account.

All Of `ProfileListResour...` ▼

107 / 169

Created at Oct 06, 2026

▼ object

> message string

- ▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request GET \
  --url https://api.detected.app/api/v2/public/profiles/{uuid} \
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "data": {}
}
```

4.13.5. Delete a profile

DELETE`https://api.detected.app/api/v2/public/profiles/{uuid}`

Try it ▶

Production

Deletes a profile. All active monitoring for the profile is stopped first. If monitoring cannot be fully stopped, the profile is not deleted and a `502` response is returned. You can safely retry the request.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> `uuid string *`

Responses

✓ • **204** No Content. Monitoring was stopped and the profile was deleted.

Response Headers

`X-RateLimit-Limit``X-RateLimit-Remaining``x-ratelimit-reset``retry-after`✓ • **401** Unauthorized. The access token is missing, invalid or has expired.✓ `object`> `message string`• **404** Not Found. The profile does not exist, or is not available to your account.✓ • **429** Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.✓ `object`> `message string`✓ • **502** Bad Gateway. Monitoring could not be fully stopped, so the profile was not deleted. It is safe to retry.✓ `object``message string`

Request

 Curl

```
curl --request DELETE \  
  --url https://api.detected.app/api/v2/public/profiles/{uuid} \  
  --header 'accept: application/json'
```

Responses

 204

```
// No Content. Monitoring was stopped and the profile was deleted.
```

4.13.6. Update a profile

PATCH

https://api.detected.app/api/v2/public/profiles/{uuid}

Try it ▶

Production

Updates a profile. You can update `customer_reference` , `risk_id` , `configuration_id` , `team_id` , `assignee_id` , `brand_id` and `review_status` .

Setting `review_status` to `Archived` or `Declined` stops all ongoing monitoring for the profile and its representatives, including company alert monitoring and screening monitoring. Monitoring cannot be restarted. The status change only succeeds once the provider has confirmed that monitoring has stopped.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>` . The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Path Parameters

> `uuid` `string` *

Body Parameters

▼

`body` `ProfileUpdateRequest`

Description

Profile update request

>

`assignee_id` `string`

>

`risk_id` `string`

>

`team_id` `string`

>

`customer_reference` `string`

>

`configuration_id` `integer`

>

`brand_id` `string<uuid>`

Format: uuid

>

`review_status` `string<Processed | Needs Review | Additional Info Required | A...`

Select... ▼

Responses

▼

● 200

`OK`

▼

`object`

>

`data` `ProfileResource`

All Of `ProfileListResour...` ▼

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

x-ratelimit-reset

retry-after

✓ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> message string

✓ ● 404 Not Found. The requested resource does not exist, or is not available to your account.

▼ object

> message string

✓ ● 422 Unprocessable Content. The request was understood but failed validation. The response lists the fields that failed and why.

▼ object

> message string

> example_field string[]

✓ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

● 502 Bad Gateway. Monitoring could not be fully stopped when setting `review_status` to `Archived` or `Declined`, so the status was not changed. It is safe to retry, because monitoring that has already stopped is skipped.

Request

 Curl

```
curl --request PATCH \
  --url https://api.detected.app/api/v2/public/profiles/{uuid} \
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "data": {}
}
```


4.13.7. Retrieve a profile domain

GET

`https://api.detected.app/api/v2/public/profiles/{uuid}/domain`

Try it ▶

Production

Returns the domain details for a profile, including WHOIS, social media, online presence and scam advisor analysis.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> `uuid string *`

Responses

▼ ● 200 OK

▼ object

> `data ProfileDomainResource`

Response Headers

`X-RateLimit-Limit``X-RateLimit-Remaining``x-ratelimit-reset``retry-after`

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> `message string`

▼ ● 404 Not Found. The requested resource does not exist, or is not available to your account.

▼ object

> `message string`▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object
 > message string

Request

 Curl

```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/profiles/{uuid}/domain \  
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "data": {
    "id": "",
    "type": "",
    "domain": "",
    "whois": {
      "status": "",
      "age": "",
      "ageDays": 0,
      "createdAt": "",
      "updatedAt": "",
      "expiresAt": ""
    },
    "social": {
      "title": "",
      "description": "",
      "responded": false,
      "twitter": "",
      "facebook": "",
      "linkedin": "",
      "instagram": ""
    },
    "online_presence": [
      {
        "founding_year": "",
        "phone_number": "",
        "industry": "",
        "tags": [
          ""
        ],
        "address": ""
      }
    ],
    "scam_advisor": {
      "score": 0,
      "blacklisted": false,
      "dns_threat_markers": 0,
      "dns_adult_content_markers": 0,
      "website_title": "",
      "website_description": "",
      "website_keywords": [
```

4.13.8. Create a profile domain

POST`https://api.detected.app/api/v2/public/profiles/{uuid}/domain`

Try it ▶

Production

Creates a domain for a profile, if it does not already have one. The domain is processed in the background, so the response is **202 Accepted**. Retrieve the results later with `GET /profiles/{uuid}/domain`.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> **uuid** *string* *

Body Parameters

▼ **body** *CreateProfileDomainRequest*> **domain** *string* *

Responses

▼ ● **202** Accepted. The domain has been queued for processing.

Response Headers

X-RateLimit-Limit**X-RateLimit-Remaining****x-ratelimit-reset****retry-after**▼ ● **401** Unauthorized. The access token is missing, invalid or has expired.▼ *object*> **message** *string*▼ ● **404** Not Found. The requested resource does not exist, or is not available to your account.▼ *object*> **message** *string*▼ ● **422** Unprocessable Content. The request was understood but failed validation. The response lists the fields that failed and why.

▼ object

> message string

> example_field string[]

▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request POST \  
  --url https://api.detected.app/api/v2/public/profiles/{uuid}/domain \  
  --header 'accept: application/json' \  
  --header 'content-type: application/json' \  
  --data '{  
    "domain": ""  
  }'
```

Responses

● 202

```
// Accepted. The domain has been queued for processing.
```

4.13.9. Stop profile monitoring

POST

`https://api.detected.app/api/v2/public/profiles/{uuid}/monitoring/{action}`

Try it ▶

Production

Stops ongoing monitoring for a profile. The `scope` in the request body controls how much is stopped:

- `all` : company-level alert monitoring and every screening, including representatives
- `alerts` : company-level alert monitoring only
- `screenings` : the profile's own screenings only

Each stop is confirmed with the underlying data provider before the change is saved. If a request returns a `502` response, the response lists which targets failed. You can safely retry the request, because targets that have already stopped are skipped.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> `uuid` string *> `action` string *

Select... ▼

Body Parameters

▼ `body` ProfileMonitoringActionRequest> `scope` string<all | alerts | screenings>

Select... ▼

Responses

● 200 OK. Monitoring has been stopped and confirmed with all providers.

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> `message` string

▼ ● 404 Not Found. The requested resource does not exist, or is not available to your account.

▼ object

> `message` string

▼ ● 422 Unprocessable Content. The request was understood but failed validation. The response lists the fields that failed and why.

▼ object

> message string

> example_field string[]

- ▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

- 502 Bad Gateway. Monitoring could not be stopped for one or more targets, and the response body lists which. It is safe to retry, because targets that have already stopped are skipped.

Request

 Curl

```
curl --request POST \  
  --url https://api.detected.app/api/v2/public/profiles/{uuid}/monitoring/{action} \  
  --header 'accept: application/json' \  
  --header 'content-type: application/json' \  
  --data '{  
    "scope": "all"  
  }'
```

Responses

● 200

```
// OK. Monitoring has been stopped and confirmed with all providers.
```

4.13.10. Assign a portal user to a profile

PUT

https://api.detected.app/api/v2/public/profiles/{uuid}/portal-users

Try it ▶

Production

Assigns a portal user to a profile. Get the list of portal users with **List portal users**, or create a new portal user with **Create a portal user**.

A portal user can have one of the following roles:

- `admin` : access to the main onboarding portal
- If you do not send a role, the `admin` role is assigned. By default an invitation email is sent. Set `notify` to `false` to skip it.

Credentials

HTTP Bearer

AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Path Parameters

> `uuid` `string` *

Body Parameters

▼

body

AssignProfileUserRequest

>

`user_id`

`number` *

>

`role`

`string<admin>`

Select...

▼

>

`notify`

`boolean`

Responses

▼

●

200

OK

▼

object

>

`data`

PortalUserViewResource

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

▼

●

401

Unauthorized. The access token is missing, invalid or has expired.

▼

object

>

`message`

`string`

✓ ● 404 Not Found. The requested resource does not exist, or is not available to your account.

▼ object
 > message string

✓ ● 422 Unprocessable Content. The request was understood but failed validation. The response lists the fields that failed and why.

▼ object
 > message string
 > example_field string[]

✓ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object
 > message string

Request

[Curl](#)

```
curl --request PUT \  
  --url https://api.detected.app/api/v2/public/profiles/{uuid}/portal-users \  
  --header 'accept: application/json' \  
  --header 'content-type: application/json' \  
  --data '{  
    "user_id": ""  
  }'
```

Responses

[200](#)

```
// OK  
{  
  "data": {  
    "id": 0,  
    "name": "",  
    "email": "",  
    "profiles": [  
      {  
        "id": "",  
        "name": "",  
        "role": ""  
      }  
    ],  
    "updated_at": "",  
    "created_at": ""  
  }  
}
```

4.13.11. Retrieve profile type configuration

GET

https://api.detected.app/api/v2/public/profiles/types/{type}/{countryCode}

Try it ▶

Production

Returns the fields that can be provided when creating a profile of the given entity type in the given country, and whether each field is required.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Path Parameters

> type string *

> countryCode string *

Select... ▼

Responses

▼ ● 200 OK

▼ ProfilesTypeConfigResponse

> id integer

> type string

> label string

> fields object[]

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> message string

▼ ● 404 Not Found. The requested resource does not exist, or is not available to your account.

▼ object

> message string

- ✓ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request GET \
  --url https://api.detected.app/api/v2/public/profiles/types/{type}/{countryCode} \
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "id": 0,
  "type": "",
  "label": "",
  "fields": [
    {
      "code": "",
      "label": "",
      "is_required": false,
      "position": 0
    }
  ]
}
```

4.14. Representatives

4.14.1. Create a representative login link

POST

`https://api.detected.app/api/v2/public/representatives/{uuid}/login-links`

Try it ▶

Production

Creates a login link for a representative. The representative uses the link to sign in and complete the action given in `purpose`. Currently the only supported purpose is `verify`.

The response includes the time at which the link expires (`expires_at`).

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> `uuid string *`

Body Parameters

▼ `body PersonLoginLinkCreateRequest`> `purpose string<verify> *`

Select... ▼

Responses

▼ ● 201 Created

▼ `object`> `data PersonLinkLoginResourceResponse`

Response Headers

`X-RateLimit-Limit``X-RateLimit-Remaining``x-ratelimit-reset``retry-after`

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ `object`> `message string`

▼ ● 404 Not Found. The requested resource does not exist, or is not available to your account.

▼ object

> message string

- ▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request POST \
  --url https://api.detected.app/api/v2/public/representatives/{uuid}/login-links \
  --header 'accept: application/json' \
  --header 'content-type: application/json' \
  --data '{
    "purpose": ""
  }'
```

Responses

● 201

```
// Created
{
  "data": {
    "purpose": "",
    "link": "",
    "expires_at": ""
  }
}
```

4.14.2. Download the IDV report for a representative

GET

https://api.detected.app/api/v2/public/representatives/{uuid}/verifications/{type}/report

Try it ▶

Production

Downloads the identity verification (IDV) report for a representative, as a ZIP file containing a single `report.pdf` generated by the IDV provider.

Constraints

- Only `idv` is supported as the `{type}` path parameter.
- Only representatives verified with the `id_scan` provider support report downloads.
- Reports are available for **31 days** from the date of the IDV record. After that, the provider deletes the underlying data and the endpoint returns `410 Gone`.

Credentials

`HTTP Bearer` `AccessToken`

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Path Parameters

> `uuid` `string` *

> `type` `string` *

Select... ▼

Header Parameters

> `accept` `string`

Select... ▼

Responses

✓ ● **200** OK. The response body is a ZIP file containing the IDV report.

Response Headers

> `Content-Type` `string`

> `Content-Disposition` `string`

> `Content-Length` `integer`

> `Cache-Control` `string`

> `Pragma` `string`

> `Expires` `string`

> `X-Content-Type-Options` `string`

✓ ● **401** Unauthorized. The access token is missing, invalid or has expired.

129 / 169

Created at Oct 06, 2026

▼ object

> message string

▼ ● 404 Not Found. The requested resource does not exist, or is not available to your account.

▼ object

> message string

▼ ● 410 Gone. The report is no longer available because the 31 day retention period has passed.

▼ object

message string

▼ ● 422 Unprocessable Content. The request was understood but failed validation. The response lists the fields that failed and why.

▼ object

> message string

> example_field string[]

Request

 Curl

```
curl --request GET \
  --url https://api.detected.app/api/v2/public/representatives/{uuid}/verifications/{type}/report \
  --header 'accept: application/octet-stream'
```

Responses

● 200

// OK. The response body is a ZIP file containing the IDV report.

4.14.3. Run a verification for a representative

POST`https://api.detected.app/api/v2/public/representatives/{uuid}/verifications/{type}`

Try it ▶

Production

Runs a verification for a representative. Currently the supported type is `id3`.

Each type of verification can use different providers, and the data returned under the `info` key is specific to the provider. The examples show what a response might look like, but the structure and content of this data are determined by the external providers and may change without notice.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> `uuid string *`> `type string *`

Select... ▼

Responses

▼ ● **201** Created. The verification has completed and the result is in the response.▼ `object`> `data PersonVerificationsResourceResponse`

Response Headers

`X-RateLimit-Limit``X-RateLimit-Remaining`● **202** Accepted. The verification has started but has not completed. Retrieve the result later with `GET /representatives/{uuid}/verifications`.▼ ● **401** Unauthorized. The access token is missing, invalid or has expired.▼ `object`> `message string`▼ ● **404** Not Found. The requested resource does not exist, or is not available to your account.▼ `object`> `message string`

- ✓ ● 422 Unprocessable Content. The request was understood but failed validation. The response lists the fields that failed and why.

✓ object

- > message string
- > example_field string[]

- ✓ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

✓ object

- > message string

Request



```
curl --request POST \
  --url https://api.detected.app/api/v2/public/representatives/{uuid}/verifications/{type} \
  --header 'accept: application/json'
```

Responses

● 201

```
// Created. The verification has completed and the result is in the response.
{
  "data": {
    "type": "",
    "provider": "",
    "info": {}
  }
}
```

4.14.4. List representative verifications

GET

`https://api.detected.app/api/v2/public/representatives/{uuid}/verifications`

Try it ▶

Production

Returns the verifications held for a representative. Each item shows the verification `type`, the `provider` that carried it out, and the provider's result under `info`.

The verification types are:

- `idv`
- `id3`
- `digital_foot_print`

Each type of verification can use different providers, and the data returned under the `info` key is specific to the provider. The examples show what a response might look like, but the structure and content of this data are determined by the external providers and may change without notice.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> `uuid string *`

Query Parameters

> `type string`

Responses

✓ ● 200 OK

▼ object

> `data` `PersonVerificationsResourceResponse`

Response Headers

`X-RateLimit-Limit``X-RateLimit-Remaining`

✓ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> `message string`

✓ ● 404 Not Found. The requested resource does not exist, or is not available to your account.

▼ object

> message string

- ▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request GET \
  --url https://api.detected.app/api/v2/public/representatives/{uuid}/verifications \
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "data": {
    "type": "",
    "provider": "",
    "info": {}
  }
}
```

4.14.5. List representatives

GET

https://api.detected.app/api/v2/public/representatives

Try it ▶

Production

Returns a list of representatives for your account. A representative can be a natural person or a legal entity, and may or may not be linked to a profile. The list includes representatives added through the portal or case management, and those converted from external data sources. Use the query parameters to filter the results.

The representative types are: `director`, `identity`, `ownership`, `declaratory`, `principal`, `director_company`, `treasurer`, `secretary`, `syndicator`, `member`, `agent`, `designated_member`, `club_manager`, `authorised_representative`, `authorised_signatory`, `trustee_company`, `trustee`, `partner_company`, `partner`, `syndicate_manager`, `individual`, `lead_partner`, `shareholder`, `shareholder_company`, `shareholder_entity`.

This endpoint is paginated. Use the `page` parameter to request further pages. The `meta` and `links` objects in the response describe the current page and link to the others.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Query Parameters

> `order_by` string

> `sort_by` string

> `page` string

> `id` string

> `is_company` string

> `customer_reference` string

> `profile_id` string

> `email` string

> `types` string

Select... ▼

Select... ▼

Responses

▼ ● 200 OK

▼ object

- > **data** `RepresentativesResource[]`
- > **links** `LinksResource`
- > **meta** `MetaResource`

Response Headers

X-RateLimit-Limit**X-RateLimit-Remaining****x-ratelimit-reset****retry-after**▼ ● **401** Unauthorized. The access token is missing, invalid or has expired.

▼ object

- > **message** `string`

▼ ● **429** Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

- > **message** `string`

Request



```
curl --request GET \  
--url https://api.detected.app/api/v2/public/representatives \  
--header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "data": [
    {
      "id": "",
      "profile_id": "",
      "customer_reference": "",
      "is_company": false,
      "review_status": {
        "status": "",
        "verified_at": "",
        "updated_at": "",
        "created_at": ""
      },
      "types": [
        ""
      ],
      "full_name": "",
      "title": "",
      "professional_profile": "",
      "country": "",
      "country_code": "",
      "country_of_residence": "",
      "residence_country_code": "",
      "personal_number": "",
      "first_name": "",
      "last_name": "",
      "dob": "",
      "email": "",
```

4.14.6. Create a representative

POST

https://api.detected.app/api/v2/public/representatives

Try it ▶

Production

Creates a representative and links it to a profile. Include the `profile_id` of the profile the representative will be linked to. Both natural persons and legal entities are supported.

The representative types are: `director`, `identity`, `ownership`, `declaratory`, `principal`, `director_company`, `treasurer`, `secretary`, `syndicator`, `member`, `agent`, `designated_member`, `club_manager`, `authorised_representative`, `authorised_signatory`, `trustee_company`, `trustee`, `partner_company`, `partner`, `syndicate_manager`, `individual`, `lead_partner`, `shareholder`, `shareholder_company`, `shareholder_entity`.

Credentials

`HTTP Bearer` `AccessToken`

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Body Parameters

▼

body

PersonCreateRequest

>

name

object

*

>

email

string

*

>

title

string<Mr | Mrs | Ms | Miss | Mx | Dr | Rev>

>

profile_id

string

*

>

review_status

string<pending | needs_review | verified | rejected | fraud | ...

>

types

string[]

*

>

dob

string

>

role_type

string[]

>

professional_profile

string

>

job_title

string

>

residence_country_code

string

>

birth_country_code

string

>

nationality

string

>

address

object

>

personal_number

string

>

shareholder_type

string<Direct | Indirect>

>

share_percentage

number

+

+

+

Responses

▼

● 201

Created

▼

object

>

data

RepresentativesResource

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

▼

● 400

Bad Request. The request could not be processed because it is invalid. The message field explains why.

▼ object

> message string

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> message string

▼ ● 422 Unprocessable Content. The request was understood but failed validation. The response lists the fields that failed and why.

▼ object

> message string

> example_field string[]

▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request POST \
  --url https://api.detected.app/api/v2/public/representatives \
  --header 'accept: application/json' \
  --header 'content-type: application/json' \
  --data '{
    "name": {
      "first_name": "",
      "last_name": ""
    },
    "email": "",
    "profile_id": "",
    "types": []
  }'
```

Responses

● 201

```
// Created
{
  "data": {
    "id": "",
    "profile id": ""
```

4.14.7. Retrieve a representative

GET

https://api.detected.app/api/v2/public/representatives/{uuid}

Try it ▶

Production

Returns a single representative, including their review status, type details and AML screening results.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Path Parameters

> **uuid** string *

Responses

▼ ● 200 OK

▼ object

> **data** RepresentativesResource

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

x-ratelimit-reset

retry-after

▼ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> **message** string

▼ ● 404 Not Found. The requested resource does not exist, or is not available to your account.

▼ object

> **message** string

▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object
 > message string

Request

 Curl

```
curl --request GET \  
  --url https://api.detected.app/api/v2/public/representatives/{uuid} \  
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "data": {
    "id": "",
    "profile id": ""
  }
}
```

4.14.8. Delete a representative

DELETE`https://api.detected.app/api/v2/public/representatives/{uuid}`

Try it ▶

Production

Deletes a representative. This cannot be undone. Screening monitoring for the representative is stopped before the deletion.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> **uuid** string *

Responses

✓ • **204** No Content. The representative was deleted.

Response Headers

X-RateLimit-Limit**X-RateLimit-Remaining****x-ratelimit-reset****retry-after**✓ • **401** Unauthorized. The access token is missing, invalid or has expired.

✓ object

> **message** string✓ • **404** Not Found. The requested resource does not exist, or is not available to your account.

✓ object

> **message** string✓ • **429** Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

✓ object

> **message** string

Request



```
curl --request DELETE \  
  --url https://api.detected.app/api/v2/public/representatives/{uuid} \  
  --header 'accept: application/json'
```

Responses



```
// No Content. The representative was deleted.
```

4.14.9. Stop screening monitoring for a representative

POST

`https://api.detected.app/api/v2/public/representatives/{uuid}/monitoring/{action}`

Try it ▶

Production

Stops screening monitoring for a single representative. Each stop is confirmed with the underlying data provider before the change is saved. If a request returns a `502` response, the response lists which targets failed. You can safely retry the request, because targets that have already stopped are skipped.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> `uuid string *`> `action string *`

Select... ▼

Responses

● **200** OK. Monitoring has been stopped and confirmed with all providers.

▼ ● **401** Unauthorized. The access token is missing, invalid or has expired.

▼ object

> `message string`

▼ ● **404** Not Found. The requested resource does not exist, or is not available to your account.

▼ object

> `message string`

▼ ● **429** Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> `message string`

● **502** Bad Gateway. Monitoring could not be stopped for one or more targets, and the response body lists which. It is safe to retry, because targets that have already stopped are skipped.

Request



```
curl --request POST \  
  --url https://api.detected.app/api/v2/public/representatives/{uuid}/monitoring/{action} \  
  --header 'accept: application/json'
```

Responses



```
// OK. Monitoring has been stopped and confirmed with all providers.
```

4.14.10. Reset the verification flow for a representative

DELETE`https://api.detected.app/api/v2/public/representatives/{uuid}/verify-flow`

Try it ▶

Production

Resets the verification flow for a representative on a given profile and sends them a fresh verification link by email. This is the same as the "Reset verification" action in case management. If the representative has no active verification flow, nothing happens and no email is sent.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Path Parameters

> **uuid** `string<uuid>` *

Format: uuid

Query Parameters

> **notify** `string`

Responses

✓ ● **204** No Content. The verification flow was reset and the representative was emailed a new link, or there was no active flow and nothing was done.

Response Headers

X-RateLimit-Limit**X-RateLimit-Remaining****x-ratelimit-reset****retry-after**

✓ ● **401** Unauthorized. The access token is missing, invalid or has expired.

✓ ● **object**> **message** `string`

✓ ● **429** Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

✓ ● **object**> **message** `string`

Request



```
curl --request DELETE \  
  --url https://api.detected.app/api/v2/public/representatives/{uuid}/verify-flow \  
  --header 'accept: application/json'
```

Responses

● 204

// No Content. The verification flow was reset and the representative was emailed a new link, or there was no active flow and nothing to reset.

4.15. Search

4.15.1. Search for an entity

POST

https://api.detected.app/api/v2/public/search

Try it ▶

Production

Searches for a company or other entity using criteria such as its name, company number and VAT number. We query several data providers and return the most relevant results. Each result is scored against your search criteria using fuzzy matching. Some providers also do fuzzy matching, and others do not. Each result shows which provider supplied it.

Creating a profile from a search result

You can create a profile directly from a search result. Send the `lookup_id` from the response, and the `response_id` of the result you want, to `POST /profiles`. See the examples on that endpoint.

Credentials

`HTTP Bearer` `AccessToken`

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Body Parameters

▼ body SearchRequest

> type string<company | sole_trader | partnership | charity | government_ent... *

Select... ▼

> name string *

> vat_number string

> company_reference string

> company_number string

> address object *

Responses

▼ ● 200 OK

▼ SearchResponse

- > data object[]
- > status string<EMPTY | PARTIAL | MATCH>
- > lookup_id integer

Response Headers

X-RateLimit-Limit**X-RateLimit-Remaining****x-ratelimit-reset****retry-after**

- ▼ ●
- 401**
- Unauthorized. The access token is missing, invalid or has expired.

▼ object

- > message string

- ▼ ●
- 404**
- Not Found. The requested resource does not exist, or is not available to your account.

▼ object

- > message string

- ▼ ●
- 422**
- Unprocessable Content. The request was understood but failed validation. The response lists the fields that failed and why.

▼ object

- > message string
- > example_field string[]

- ▼ ●
- 429**
- Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the
- Retry-After**
- header before trying again.

▼ object

- > message string

Request



```
curl --request POST \
  --url https://api.detected.app/api/v2/public/search \
  --header 'accept: application/json' \
  --header 'content-type: application/json' \
  --data '{
    "type": "",
    "name": "",
    "address": {
      "country_code": "",
      "city": ""
    }
  }'
```

Responses

● 200

```
// OK
{
  "data": [
    {
      "type": "",
      "name": "",
      "company_reference": "",
      "provider": "",
      "provider_reference": "",
      "jurisdiction_code": "",
      "company_type": "",
      "current_status": "",
      "address": "",
      "vat_number": "",
      "province_code": "",
      "post_code": "",
      "city": "",
      "confidence": 0,
      "response_id": 0
    }
  ],
  "status": "",
  "lookup_id": 0
}
```

4.15.2. Retrieve search type configuration

GET

https://api.detected.app/api/v2/public/search/types/{type}/{countryCode}

Try it ▶

Production

Returns the search configuration for an entity type in a country: whether search is enabled, and which search fields you can use with `POST /search`.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Path Parameters

> type string *

> countryCode string *

Responses

▼

● 200 OK

▼

SearchTypeResponse

> company EntityTypeConfig

> sole_trader EntityTypeConfig

> partnership EntityTypeConfig

> charity EntityTypeConfig

> government_entity EntityTypeConfig

> syndicate EntityTypeConfig

> association EntityTypeConfig

> trust EntityTypeConfig

> fund EntityTypeConfig

Response Headers

X-RateLimit-Limit

X-RateLimit-Remaining

▼

● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> message string

- ▼ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request GET \
  --url https://api.detected.app/api/v2/public/search/types/{type}/{countryCode} \
  --header 'accept: application/json'
```

Responses

● 200

```
// OK
{
  "company": {
    "type": "",
    "label": "",
    "search_enabled": false,
    "search_fields": {
      "address.country_code": {
        "is_required": false,
        "label": "",
        "position": 0
      },
      "customer_reference": {
        "is_required": false,
        "label": "",
        "position": 0
      },
      "name": {
        "is_required": false,
        "label": "",
        "position": 0
      },
      "address.city": {
        "is_required": false,
        "label": "",
        "position": 0
      },
      "address.state": {
        "is_required": false,
        "label": "",
        "position": 0
      },
      "company_number": {
        "is_required": false,
        "label": "",
        "position": 0
      },
      "domain": {
        "is_required": false,
        "label": "",
        "position": 0
      }
    }
  },
  "sole_trader": {
    "type": "",
    "label": "",
    "search_enabled": false,
    "search_fields": {
      "address.country_code": {
        "is_required": false,
        "label": "",
        "position": 0
      },
      "customer_reference": {
        "is_required": false,
```

```
    "label": "",
    "position": 0
  },
  "name": {
    "is_required": false,
    "label": "",
    "position": 0
  },
  "address.city": {
    "is_required": false,
    "label": "",
    "position": 0
  },
  "address.state": {
    "is_required": false,
    "label": "",
    "position": 0
  },
  "company_number": {
    "is_required": false,
    "label": "",
    "position": 0
  },
  "domain": {
    "is_required": false,
    "label": "",
    "position": 0
  }
},
"partnership": {
  "type": "",
  "label": "",
  "search_enabled": false,
  "search_fields": {
    "address.country_code": {
      "is_required": false,
      "label": "",
      "position": 0
    }
  },
  "customer_reference": {
    "is_required": false,
    "label": "",
    "position": 0
  },
  "name": {
    "is_required": false,
    "label": "",
    "position": 0
  },
  "address.city": {
    "is_required": false,
    "label": "",
    "position": 0
  },
  "address.state": {
    "is_required": false,
    "label": "",
    "position": 0
  }
}
```

```
    },
    "company_number": {
      "is_required": false,
      "label": "",
      "position": 0
    },
    "domain": {
      "is_required": false,
      "label": "",
      "position": 0
    }
  }
},
"charity": {
  "type": "",
  "label": "",
  "search_enabled": false,
  "search_fields": {
    "address.country_code": {
      "is_required": false,
      "label": "",
      "position": 0
    },
    "customer_reference": {
      "is_required": false,
      "label": "",
      "position": 0
    },
    "name": {
      "is_required": false,
      "label": "",
      "position": 0
    },
    "address.city": {
      "is_required": false,
      "label": "",
      "position": 0
    },
    "address.state": {
      "is_required": false,
      "label": "",
      "position": 0
    },
    "company_number": {
      "is_required": false,
      "label": "",
      "position": 0
    },
    "domain": {
      "is_required": false,
      "label": "",
      "position": 0
    }
  }
},
"government_entity": {
  "type": "",
  "label": "",
  "search_enabled": false,
```

```
"search_fields": {
  "address.country_code": {
    "is_required": false,
    "label": "",
    "position": 0
  },
  "customer_reference": {
    "is_required": false,
    "label": "",
    "position": 0
  },
  "name": {
    "is_required": false,
    "label": "",
    "position": 0
  },
  "address.city": {
    "is_required": false,
    "label": "",
    "position": 0
  },
  "address.state": {
    "is_required": false,
    "label": "",
    "position": 0
  },
  "company_number": {
    "is_required": false,
    "label": "",
    "position": 0
  },
  "domain": {
    "is_required": false,
    "label": "",
    "position": 0
  }
},
"syndicate": {
  "type": "",
  "label": "",
  "search_enabled": false,
  "search_fields": {
    "address.country_code": {
      "is_required": false,
      "label": "",
      "position": 0
    },
    "customer_reference": {
      "is_required": false,
      "label": "",
      "position": 0
    },
    "name": {
      "is_required": false,
      "label": "",
      "position": 0
    },
    "address.city": {
```

```
    "is_required": false,
    "label": "",
    "position": 0
  },
  "address.state": {
    "is_required": false,
    "label": "",
    "position": 0
  },
  "company_number": {
    "is_required": false,
    "label": "",
    "position": 0
  },
  "domain": {
    "is_required": false,
    "label": "",
    "position": 0
  }
},
"association": {
  "type": "",
  "label": "",
  "search_enabled": false,
  "search_fields": {
    "address.country_code": {
      "is_required": false,
      "label": "",
      "position": 0
    },
    "customer_reference": {
      "is_required": false,
      "label": "",
      "position": 0
    },
    "name": {
      "is_required": false,
      "label": "",
      "position": 0
    },
    "address.city": {
      "is_required": false,
      "label": "",
      "position": 0
    },
    "address.state": {
      "is_required": false,
      "label": "",
      "position": 0
    },
    "company_number": {
      "is_required": false,
      "label": "",
      "position": 0
    },
    "domain": {
      "is_required": false,
      "label": "",

```

```
        "position": 0
      }
    }
  },
  "trust": {
    "type": "",
    "label": "",
    "search_enabled": false,
    "search_fields": {
      "address.country_code": {
        "is_required": false,
        "label": "",
        "position": 0
      },
      "customer_reference": {
        "is_required": false,
        "label": "",
        "position": 0
      },
      "name": {
        "is_required": false,
        "label": "",
        "position": 0
      },
      "address.city": {
        "is_required": false,
        "label": "",
```

4.15.3. List search types

GET

https://api.detected.app/api/v2/public/search/types

Try it ▶

Production

Returns the entity types that can be searched, and whether search is enabled for each.

Credentials

HTTP Bearer AccessToken

The API uses OAuth 2.0. Request an access token from `POST /oauth/token` with the client ID and client secret of your integration client, and your account slug. Send the access token in the `Authorization` header of every request, in the format `Authorization: Bearer <access_token>`. The access token carries the scopes set on your integration client in the dashboard. Access tokens expire. When one expires, request a new one.

Enter http bearer value

Responses

▼

● 200

OK

▼

SearchTypesResponse

>

company

EntityTypesConfig

>

sole_trader

EntityTypesConfig

>

partnership

EntityTypesConfig

>

charity

EntityTypesConfig

>

government_entity

EntityTypesConfig

>

incorporated_syndicate

EntityTypesConfig

>

company_syndicate

EntityTypesConfig

>

syndicate

EntityTypesConfig

>

association

EntityTypesConfig

>

trust

EntityTypesConfig

>

fund

EntityTypesConfig

>

individual

EntityTypesConfig

>

joint_individual

EntityTypesConfig

>

club

EntityTypesConfig

Response Headers

- X-RateLimit-Limit
- X-RateLimit-Remaining

✓ ● 401 Unauthorized. The access token is missing, invalid or has expired.

▼ object

> message string

✓ ● 429 Too Many Requests. You have exceeded the rate limit. Wait for the number of seconds given in the `Retry-After` header before trying again.

▼ object

> message string

Request

 Curl

```
curl --request GET \
  --url https://api.detected.app/api/v2/public/search/types \
  --header 'accept: application/json'
```

Responses

● 200

// OK