

API REST

- [Service Documentation: "Post Risk"](#)
- [Service Documentation: "Post Update"](#)
- [Servicio de Desenrollamiento](#)

Service Documentation:

"Post Risk"

This service allows you to submit a request to process and assess the risk associated with a specific transaction or activity. The request will contain relevant information about the transaction or activity, as well as any other data necessary to conduct an accurate risk assessment. Upon receiving the request, the system will analyze the provided data using various risk assessment models and algorithms to determine the likelihood that the transaction is fraudulent or represents some other type of risk.

Risk

Service Overview

- **Service Name:** Post `risk`
- **URL:** `{URL_Base}/api/v1/risk`
- **Method:** POST
- **Functionality:** The Post Risk service facilitates the submission of requests for processing and evaluating the risk associated with a particular transaction or activity. Users can send relevant information about the transaction or activity, along with any additional data necessary for a thorough risk assessment. Upon receiving the request, the system employs various risk assessment models and algorithms to analyze the provided data. The outcome of this analysis indicates the likelihood of the transaction being fraudulent or representing other types of risks.

Request Parameters:

- **cid:** The customer ID that we will provide you
- **csid:** Bank session ID
- **userID:** Bank user ID
- **additionalData:** Key value pair dictionary (the generic values can be viewed above)

Response Structure

The API responds with a JSON object listing the risk levels configured within the system. Each entry in the response includes:

- **score:** Score assigned to the validation of the queried customer's session" is a numerical value that represents the level of risk associated with the validation process of a specific customer's session.

Example Response

“

```
{
  "score": 0
}
```

Example CURL Request

To query the risk for a specific project, utilize the following `curl` command:

“

```
curl -X 'POST' \
  'https://fraud-detector-api.statsd.io/api/v1/risk' \
  -H 'accept: application/json' \
  -H 'apiKey: [Your_API_Key]' \
  -H 'Content-Type: application/json' \
  -d '{
    "cid": "[Your_Cid]",
    "csid": "demo0883d839",
    "userID": "1193539722",
    "additionalData": {}
  }'
```

Make sure you replace {BaseURL} with the actual base URL of the service, and your_api_key with the API key provided to you.

Service Documentation:

"Post Update"

The "Post Update" service enables data updating via an HTTP POST request. Its primary function is to facilitate the modification of records or information within the system, such as user profiles, configurations, and content. This helps maintain up-to-date and accurate data within the application or system where it's implemented.

Update

Service Overview

- **Service Name:** Post Update
- **URL:** {URL_Base}/api/v1/Update
- **Method:** POST
- **Functionality:** service allows users to modify existing records or information within the system by sending an HTTP POST request to the designated endpoint. This functionality is crucial for keeping the data within the application or system current and accurate. Users can update various types of data, such as user profiles, configurations, content, or any other relevant information managed by the system. The service processes the POST request and applies the specified changes to the appropriate records, ensuring that the system reflects the most recent updates made by users or administrators.

Request Parameters:

- **cid:** The customer ID that we will provide you
- **csid:** Bank session ID
- **userID:** Bank user ID
- **additionalData:** Key value pair dictionary (the generic values can be viewed above)

Response Structure

The API responds with a JSON object listing the risk levels configured within the system. Each entry in the response includes:

- **success:** Operation Status Code

Example Response

“

```
{
  "success": 1
}
```

Example CURL Request

To query the risk for a specific project, utilize the following `curl` command:

“

```
curl -X 'POST' \
  'https://fraud-detector-api.statsd.io/api/v1/update' \
  -H 'accept: application/json' \
  -H 'apiKey: [Your_API_Key]' \
  -H 'Content-Type: application/json' \
  -d '{
    "cid": "[Your_Cid]",
    "csid": "demo0883d839",
    "userID": "1193539722",
    "additionalData": {}
  }'
```

Make sure you replace {BaseURL} with the actual base URL of the service, and your_api_key with the API key provided to you.

Servicio de Desenrollamiento

Este servicio consta de dos partes: autenticación y desenrollamiento. La autenticación genera un token de autorización necesario para consumir el servicio de desenrollamiento, que permite eliminar la asociación de un cliente a un proyecto específico.

1. Autenticación

Para acceder al servicio de desenrollamiento, primero es necesario autenticarse y obtener un token de autorización (`Bearer token`). Este proceso de autenticación se realiza mediante la siguiente ruta:

Endpoint de Autenticación:

```
curl --location 'https://apigw-dev.ado-tech.com/api/token/{realm}' \  
--data-urlencode 'client_id=user' \  
--data-urlencode 'client_secret=credentials' \  
--data-urlencode 'grant_type=client_credentials'
```

Parámetros de Autenticación

- `client_id`: Identificador único del cliente. En este ejemplo, es `user`.
- `client_secret`: Credenciales secretas específicas del cliente, necesarias para la autenticación.
- `grant_type`: Tipo de permiso requerido para obtener el token. En este caso, es `client_credentials`.

Respuestas de Autenticación

Si la autenticación es exitosa, el servicio responderá con un token de autorización en formato Bearer. Este token es necesario para realizar la solicitud de desenrollamiento en el siguiente paso.

```
{
  "access_token": "eyJhbGciOiJSUzI1NiIsI... ",
  "token_type": "Bearer",
  "expires_in": 300
}
```

- `access_token`: El token generado por el servicio.
- `token_type`: El tipo de token generado por el servicio. En estos caso será de tipo `Bearer`.
- `expires_in`: El tiempo de vida del token generado en milisegundos.

En caso de error, el servicio de autenticación puede devolver uno de los siguientes códigos de respuesta, junto con mensajes de error relevantes:

- **400 Bad Request:** Credenciales incorrectas o incompletas.

```
{
  "error": "Credenciales inválidas."
}
```

2. Desenrollamiento de Cliente

Una vez obtenido el token de autenticación, puede utilizarse para consumir el servicio de desenrollamiento del cliente. Este servicio elimina la asociación de un cliente con el proyecto especificado.

Endpoint de Desenrollamiento de Cliente:

```
curl --location 'https://apigw-dev.ado-tech.com/api/identity-manager/unroll-client' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer {token}' \
--data '{
  "projectName": "ProjectName",
  "documentType": 1,
  "documentNumber": "123456789"
}'
```

Parámetros del Cuerpo de la Solicitud

- `projectName`: Nombre del proyecto del que se desea desarrollar al cliente. Ejemplo: `"ProjectName1"`.
- `documentType`: Tipo de documento de identificación del cliente. Este valor es un número entero que representa el tipo de documento.
- `documentNumber`: Número de documento de identificación del cliente.

“ **Nota:** El valor `{token}` en el encabezado `Authorization` debe ser reemplazado con el token de autorización obtenido en el paso de autenticación.

Respuestas del Servicio de Desenrollamiento

El servicio de desenrollamiento devolverá una respuesta indicando el éxito o el fallo del desenrollamiento solicitado. Las posibles respuestas incluyen:

200 OK: Desenrollamiento exitoso; el cliente ha sido desenrollado del proyecto.

400 Bad Request: No se ha encontrado el usuario con el documento y el tipo de documento especificados

```
{ "error": "Can't found User with specified credentials" }
```

401 Unauthorized: Token de autorización no proporcionado.

```
{ "error": "Token inválido." }
```

```
{ "error": "Token no proporcionado." }
```

401 Unauthorized: Token de autorización inválido, expirado.

```
{ "error": "Token inválido." }
```

404 Not Found: No se encuentra el proyecto, debe a que este mal escrito o no este habilitado para esta función.

```
{ "error": "The specified project was not found" }
```

Este servicio está diseñado para facilitar la eliminación segura de la relación de un cliente con un proyecto específico, utilizando autenticación basada en tokens para garantizar la seguridad y la integridad de las solicitudes.