Servicios web

Listado de los webservice disponibles y cómo se usan

- Gestión de endpoints
- Consulta de alertas
- Envío de datos semánticos
- Analítica del triángulo del fraude
- Correlación de eventos o workflows
- Model Context Protocol

Gestión de endpoints

Antes de intentar consumir este servicio debe indicar en las cabeceras de la petición (**headers**) los parámetros de autenticación para identificarse ante el sistema. Use la llave **username** para indicar el nombre de usuario (con el mismo que inicia sesión en la interfaz web y **password** para indicar su contraseña.

Algunas consultas deben tener las siguientes cabeceras. Más abajo en la tabla de operaciones se indican cuales de ellas son necesarias dependiendo de la operación.

Header	Valor	Explicación
page	1	Consultar pagina numero 1
size	100	Ventana de resultados por pagina
datefrom	2022-01-01	Rango de fecha "desde"
dateto	2022-02-28	Rango de fecha "hasta"

Para que el intercambio de datos entre el cliente y el servidor sea legible, use adicionalmente la cabecera **Content-Type** con el valor **application/json**.

Operación	Método	Headers	URL Ejemplo
Obtener datos de un endpoint	**GET**	**username, password, page, size**	https://url/rest/endPoints?query=jason
Obtener los datos de todos los endpoints	**GET**	**username, password, page, size**	https://url/rest/endPoints?query=all
Crear o actualizar un endpoint	**PUT**	**username, password**	https://url/rest/endPoints?query=create&token=TOKEN&os=6.1&v=1.3.1 &domain=mydomain.loc&id=jason_abn76dk_agt&ip=172.16.1.1
Eliminar un endpoint	**DELETE**	**username, password**	https://url/rest/endPoints?query=delete&endpoint=jason

Este servicio web se usa para crear un agente personalizado, es decir, el cliente (organización) puede desarrollar clientes que envíen datos a The Fraud Explorer y para ello el primer paso es crear el agente, luego, se tienen disponibles otras operaciones administrativas para realizar eliminaciones de agentes, actualización de datos y obtención de información.

Este servicio web normalmente no será usado por las organizaciones y sí usado comunmente por nuestro equipo de NOFRAUD para el desarrollo de nuevos agentes para The Fraud Explorer.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Consulta de alertas

Antes de intentar consumir un servicio debe indicar en las cabeceras de la petición (**headers**) los parámetros de autenticación para identificarse ante el sistema. Use la llave **username** para indicar el nombre de usuario (con el mismo que inicia sesión en la interfaz web y **password** para indicar su contraseña.

Algunas consultas deben tener las siguientes cabeceras. Más abajo en la tabla de operaciones se indican cuales de ellas son necesarias dependiendo de la operación.

Header	Valor	Explicación
page	1	Consultar pagina numero 1
size	100	Ventana de resultados por pagina
datefrom	2022-01-01	Rango de fecha "desde"
dateto	2022-02-28	Rango de fecha "hasta"

Las operaciones disponibles son:

Operación	Método	Headers	URL Ejemplo
Obtener los eventos de un endpoint	**GET**	**username, password, page, size, datefrom, dateto**	https://url/rest/ftaEvents?endpoint=jason
Obtener los eventos de todos los endpoints	**GET**	**username, password, page, size, datefrom, dateto**	https://url/rest/ftaEvents?endpoint=all
Obtener las alertas de AI de un endpoint	**GET**	**username, password, page, size, datefrom, dateto**	https://url/rest/ftaEvents?ai=jason
Obtener las alertas de AI de los endpoints	**GET**	**username, password, page, size, datefrom, dateto**	https://url/rest/ftaEvents?ai=all

Envío de datos semánticos

Antes de intentar consumir este servicio debe indicar en las cabeceras de la petición (**headers**) los parámetros de autenticación para identificarse ante el sistema. Use la llave **username** para indicar el nombre de usuario (con el mismo que inicia sesión en la interfaz web y **password** para indicar su contraseña.

Para enviar datos semánticos de un endpoint para ser procesadas por The Fraud Explorer, debe usar la URL https://demo.thefraudexplorer.com/rest/endPoints?id=agent_ahsg17_agt con método **POST** y enviar en el **BODY** del mensaje lo siguiente:

```
{
 "hostPrivateIP":"10.20.23.8",
 "userDomain":"mydomain.loc",
 "appTitle":"Outlook",
 "phrases":"Aqui todos dicen que cerremos la boca pero yo te estoy contando, saludos"
}
```

Se supone que antes de enviar estos datos ya debió haber creado el endpoint previamente (lea la primera página de gestión de endpoints en este mismo capítulo).

El id del endpoint deberá ser exactamente igual al indicado al momento de la creación den endpoint.

Analítica del triángulo del fraude

Se puede usar la API **REST** para enviar un texto, procesarlo y entregar el resultado de la metodología sin necesidad de usar la consola web o el dashboard para visualizar los resultados.

Antes de intentar consumir este servicio debe indicar en las cabeceras de la petición (**headers**) los parámetros de autenticación para identificarse ante el sistema. Use la llave **username** para indicar el nombre de usuario (con el mismo que inicia sesión en la interfaz web y **password** para indicar su contraseña.

Para esto, debe usar la URL con método **POST** https://demo.thefraudexplorer/rest/fraudTriangle o en caso de querer enviar varios mensajes en modo bulk https://demo.thefraudexplorer.com/rest/fraudTriangleBulk.

```
{
 "businessUnit" : "TECHNOLOGY",
 "application" : "Microsoft Word - My letter.docx",
 "phrases" : "Hola buenos dias, espero todo ande muy bien, escribo para contarte que estamos algo estresados en el area porque imaginate que un proveedor le hizo una propuesta de trabajo a uno de nuestros colaboradores y eso definitivamente representa una violacion a nuestro codigo de etica relacionada con conflictos de interes. Aqui todos dicen que cerremos la boca pero yo te estoy contando y lo quise eliminar, saludos.",
 "llmEngine" : "yes"
}
```

Esta consulta devolvería un resultado como:

```
{
   "pressureEvents": 1,
   "opportunityEvents": 3,
   "rationalizationEvents": 1,
   "suspiciousProbability": "91%",
   "messageTone": "neutral",
   "1stPersonPronouns": "yes",
   "criticalityFlag": "yes",
   "IntimityFlag": "no",
   "eventTopics": "information, suppliers",
```

```
  "eventClassification": "conocimiento, renuncia, negociaciones, ocultamiento, estres",
  "eventRisks": "concealment, psicosocial, suppliers",
  "llmResult": "suspicious",
  "phrasesMatched": {
    "pressureTerms": "estamos algo estresados",
    "opportunityTerms": "propuesta de trabajo, conflictos de interes, cerremos la boca",
    "rationalizationTerms": "quise eliminar"
  }
}
```


The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones

Correlación de eventos o workflows

Antes de intentar consumir este servicio debe indicar en las cabeceras de la petición (**headers**) los parámetros de autenticación para identificarse ante el sistema. Use la llave **username** para indicar el nombre de usuario (con el mismo que inicia sesión en la interfaz web y **password** para indicar su contraseña.

Algunas consultas deben tener las siguientes cabeceras. Más abajo en la tabla de operaciones se indican cuales de ellas son necesarias dependiendo de la operación.

Header	Valor	Explicación
page	1	Consultar pagina numero 1
size	100	Ventana de resultados por pagina
datefrom	2022-01-01	Rango de fecha "desde"
dateto	2022-02-28	Rango de fecha "hasta"

Para que el intercambio de datos entre el cliente y el servidor sea legible, use adicionalmente la cabecera **Content-Type** con el valor **application/json**.

Operación	Método	Headers	URL Ejemplo
Obtener el listado de los workflows	**GET**	**username, password, page, size**	https://url/rest/workFlows?list=all
Obtener los eventos de un workflow	**GET**	**username, password, page, size**	https://url/rest/workFlows?name=Compras

Un flujo de trabajo es aquel que permite generar alertas si se cumplen previamente unas condiciones de correlación de eventos. Los flujos de trabajo se crean en la plataforma administrativa de The Fraud Explorer.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones

Model Context Protocol

Antes de intentar consumir este servicio debe indicar en las cabeceras de la petición (**headers**) los parámetros de autenticación para identificarse ante el sistema. Use la llave **username** para indicar el nombre de usuario (con el mismo que inicia sesión en la interfaz web y **password** para indicar su contraseña.

Algunas consultas deben tener las siguientes cabeceras. Más abajo en la tabla de operaciones se indican cuales de ellas son necesarias dependiendo de la operación.

Header	Valor	Explicación
endpoint	jason_and716_agt	Identificación del endpoint
desde	2022-01-01	Rango de fecha "desde"
hasta	2022-02-28	Rango de fecha "hasta"

Las operaciones disponibles son:

Operación	Método	Headers	URL Ejemplo
Obtener el resumen general de las alertas	**GET**	**username, password, desde, hasta**	https://url/rest/mcp?general
Obtener una vista detallada de las alertas de un endpoint	**GET**	**username, password, endpoint, desde, hasta**	https://url/rest/mcp?detalle

Puede configurar su LLM para crear dos herramientas (tools) en Python que consuman este servicio API. Este script en Python implementa las dos herramientas (vista general y vista detallada de alertas):

```
from mcp.server.fastmcp import FastMCP
from datetime import datetime, timedelta
import httpx
import json

params = json.load(open('config.json'))

mcp = FastMCP("NOFRAUD")

#
# Descripcion de la herramienta: hace un resumen de todas las alertas que existen en un rango de fechas
```

```
#

@mcp.tool()
async def visionGeneral(desde: str, hasta: str) -> str:
    """
    Hace un resumen general de todas las alertas que existen en un rango de fechas.
    Esta herramienta solo se debe usar cuando se solicita un resumen general, no cuando se solicitan detalles.
    Cuando se solicitan detalles se debe usar la otra herramienta 'visionDetallada'.

    Estos son algunos ejemplos para usar esta herramienta:

    1. Podrias hacerme un resumen de las alertas desde el 1 de Abril al 30 de Abril de 2025?:
       visionGeneral(2025-04-01, 2025-04-30).
    2. Me podrias indicar si entre el periodo del 1 de Enero al 31 de Marzo de 2025 existieron alertas?:
       visionGeneral(2025-01-01, 2025-03-31).

    Requisitos para el uso de esta herramienta:

    1. La fecha de inicio debe ser anterior a la fecha de fin.
    2. Las fechas deben ser en formato YYYY-MM-DD.
    """
    global params
    async with httpx.AsyncClient() as client:
        url = params["url"] + "?general"
        headers = {
            "Content-Type": "application/json",
            "username": params["username"],
            "password": params["password"],
            "desde": str(desde),
            "hasta": str(hasta),
        }
        response = await client.get(url, headers=headers)
        response.raise_for_status()

    return response.json()

@mcp.tool()
async def visionDetallada(endpoint: str, desde: str, hasta: str) -> str:
    """
    Detalla las alertas que tiene un endpoint en especifico en un rango de fechas.
    Esta herramienta solo se debe usar cuando se solicitan detalles, no cuando se solicita un resumen.
```

```
    Cuando se solicita un resumen se debe usar la herramienta 'visionGeneral'.

    Estos son algunos ejemplos para usar esta herramienta:

    1. Podrias mostrarme las alertas del endpoint 'jhondoe' del 1 de Abril al 30 de Abril de 2025?:
       visionDetallada('jhondoe', 2025-04-01, 2025-04-30).
    2. Podrias detallarme las alertas del endpoint 'jhondoe@nofraud.la' del 1 de Enero al 31 de Marzo de 2025?:
       visionDetallada('jhondoe@nofraud.la', 2025-01-01, 2025-03-31).

    Requisitos para el uso de esta herramienta:

    1. El endpoint debe ser un nombre de usuario o un email. No se acepta 'todos' como endpoint.
    2. La fecha de inicio debe ser anterior a la fecha de fin.
    3. Las fechas deben ser en formato YYYY-MM-DD.
    """
    global params
    async with httpx.AsyncClient() as client:
        url = params["url"] + "?detalle"
        headers = {
            "Content-Type": "application/json",
            "username": params["username"],
            "password": params["password"],
            "endpoint": endpoint,
            "desde": str(desde),
            "hasta": str(hasta),
        }
        response = await client.get(url, headers=headers)
        response.raise_for_status()

    return response.json()

if __name__ == "__main__":
    mcp.run()
```

El archivo de configuración que debe crear según su instancia de The Fraud Explorer:

```
{
    "username": "mcp-username",
    "password": "su_password_mcp",
    "url": "https://demo.thefraudexplorer.com/rest/mcp"
}
```