**Documentation Technique des API (REST)**

**API Predict du modèle.**

#### **Points de Terminaisons (Endpoints)**

L'API REST, créée avec FastAPI, expose plusieurs points de terminaison pour l'authentification et les prédictions de CO2. Voici les détails de chaque point de terminaison :

POST /token

* Description : Authentifie l'utilisateur et retourne un jeton d'accès.
* Paramètres de Requête :
  + username (string) : Nom d'utilisateur.
  + password (string) : Mot de passe.
* Réponse : Jeton d'accès (type Bearer).

Exemple de Requête **:**

curl -X POST "http://127.0.0.1:8000/token" -d "username=admin&password=secret"

Exemple de Réponse :

{

"access\_token": "secrettoken",

"token\_type": "bearer"

}

POST /predict/

* Description : Prédiction des émissions de CO2 basée sur les données fournies.
* Paramètres de Requête :
  + year (int) : Année des données.
  + state\_name (string) : Nom de l'état.
  + sector\_name (string) : Nom du secteur.
  + fuel\_name (string) : Nom du carburant.
* Authentification : Nécessite un jeton d'accès (Bearer Token).
* Réponse : Prédiction des émissions de CO2.

Exemple de Requête :

curl -X POST "http://127.0.0.1:8000/predict/" -H "Authorization: Bearer secrettoken" -H "Content-Type: application/json" -d '{"year": 2020, "state\_name": "California", "sector\_name": "Transportation", "fuel\_name": "Gasoline"}'

Exemple de Réponse :

{

"prediction du CO2": 12345.67

}

#### **Règles d'Authentification et d'Autorisation**

L'API utilise OAuth2 avec le schéma Password pour l'authentification. Voici les détails des règles d'authentification et d'autorisation :

1. Authentification :
   * Les utilisateurs doivent s'authentifier en envoyant leurs identifiants (nom d'utilisateur et mot de passe) au point de terminaison /token.
   * Si les identifiants sont corrects, un jeton d'accès (Bearer Token) est retourné, qui doit être utilisé pour accéder aux points de terminaison protégés.
2. Autorisation :
   * Le jeton d'accès doit être inclus dans le header Authorization pour accéder aux points de terminaison protégés, comme /predict/.
   * Le jeton est vérifié par la fonction authenticate\_token. Si le jeton est invalide, une réponse 401 Unauthorized est retournée.

#### Respect des Standards du Modèle REST

L'API respecte les standards REST suivants :

* Statelessness : Chaque requête contient toutes les informations nécessaires pour être traitée, sans dépendance à des états antérieurs.
* Clarity : Les points de terminaison sont clairs et suivent des conventions de dénomination cohérentes.
* HTTP Verbs : Utilisation appropriée des verbes HTTP (POST pour créer des jetons et effectuer des prédictions).
* Authentication : Utilisation de OAuth2 pour sécuriser les points de terminaison protégés.