



Cette API permet de générer un token à partir d'un login (celui de la secrétaire) et de son mot de passe.

L'URL de base utilisée pour notre API d'authentification est la suivante :

1

```
I6InNlY3JldGFpcmUxIiwizXhwIjo1MTM0OTA0NjE2MDAwfQ.SDzDxv-Rge  
2gu304VQguIgg0PIWj0mGsJtk7icJNcE0"  
}
```

GET /authapi

Vérifie l'authentification de la personne connectée. Renvoie l'identifiant ainsi que le mot de passe de cette personne.

Réponse

Renvoie un document JSON avec les champs suivants :

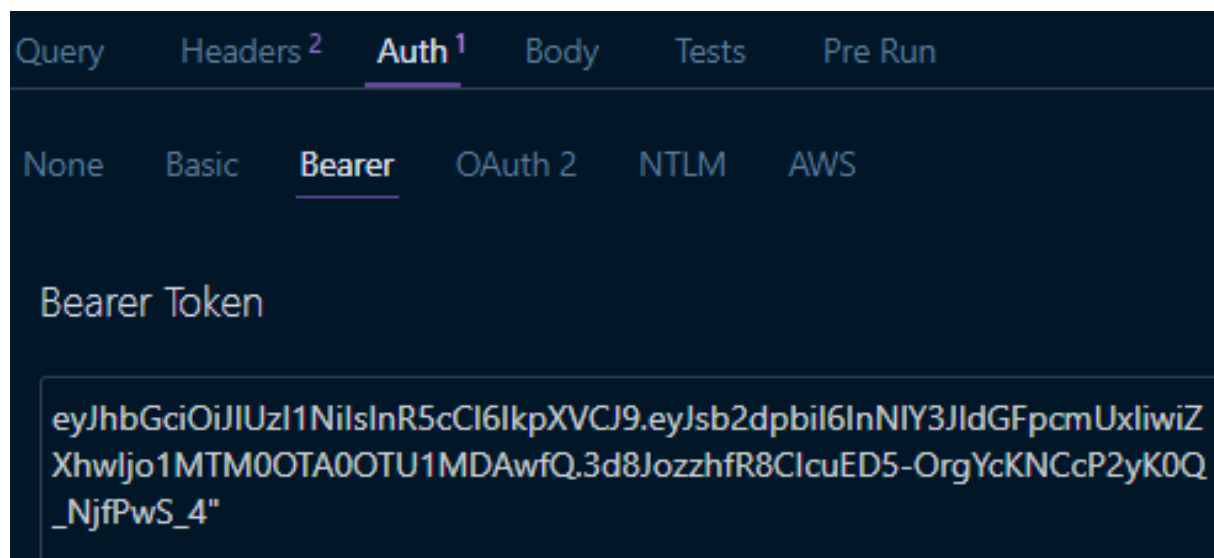
- `login` : identifiant de connexion de la personne souhaitant s'authentifier.
- `mdp` : le mot de passe de la personne s'authentifant.

Exemple

Requête :

```
GET /authapi
```

Token généré après la requête `POST` à mettre dans Auth, dans Bearer :



Réponse :

```
{  
  "login": "secretaire1",
```

```
"mdp": "password1234!"  
}
```

Erreurs

Cette API peut renvoyer les erreurs suivantes :

- **405 Bad Request** : La méthode n'est pas autorisée.
- **401 Unauthorized** : Une condition permettant d'avoir accès aux données n'est pas remplie. Ici, avec le cas de **GET** où le token ou le mot de passe ou le login est invalide.
- **404 Not Found** : La ressource de la requête est introuvable.
- **500 Internal Server Error** : Une erreur inattendue s'est produite dans le serveur.