1. PASSOS PARA USAR O TOKEN:

1.1. Login e geração de token (access_token)

O Token pode ser gerado por duas operações:

EfetuarLogin() - Quando o cliente estabelecer a conexão inicial com o sistema em Backend.

token(), cada nova necessidade de gerar um token.

Uma vez que foi gerado, o Token deve ser enviado no Header das demais requisições

Formato:

Authorization = "bearer + espaço + string token"

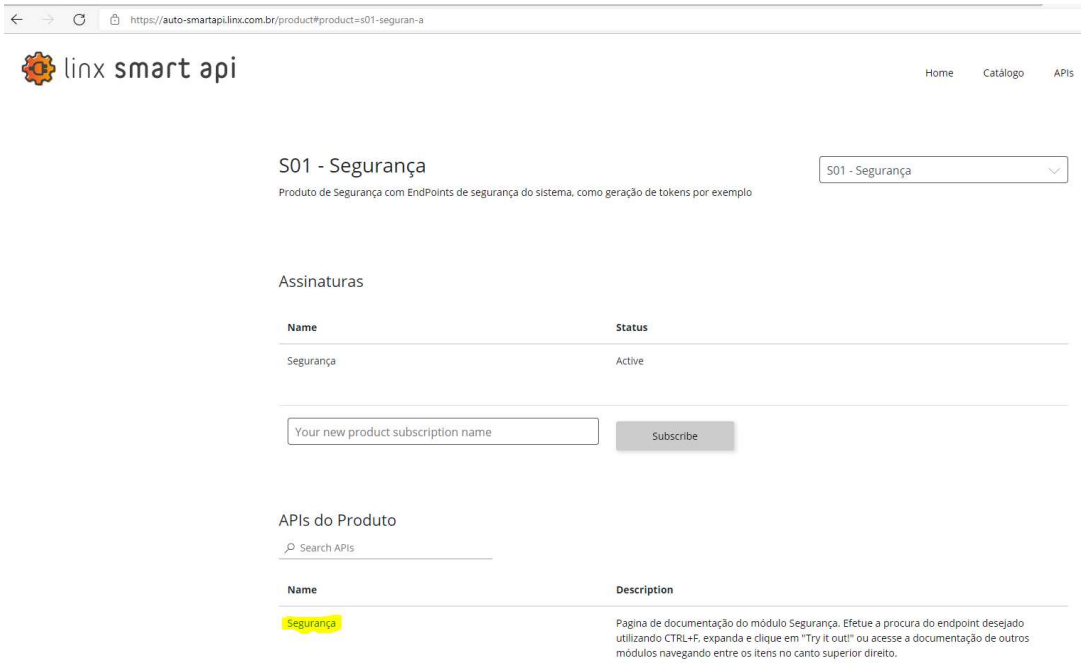
Exemplo:

Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1bmlxdWVfbmFtZSI6IkxpbnhETVMuRFRPLk1vZGVscy5TZWd1cmFuY2EuRGFkb3NVc3VhcmlvTG9naW5Nb2RlbCIsIm5iZiI6MTYyOTgxNzAwMywiZXhwIjoxNjI5ODIwNjAzLCJpYXQiOjE2Mjk4MTcwMDN9.Y-vKSi9G0zipjMfG6rqUkmj8F0lj1pl9OvAndEak66M

1.1.1 Exemplificando a Geração do Token na Linx Smart API:

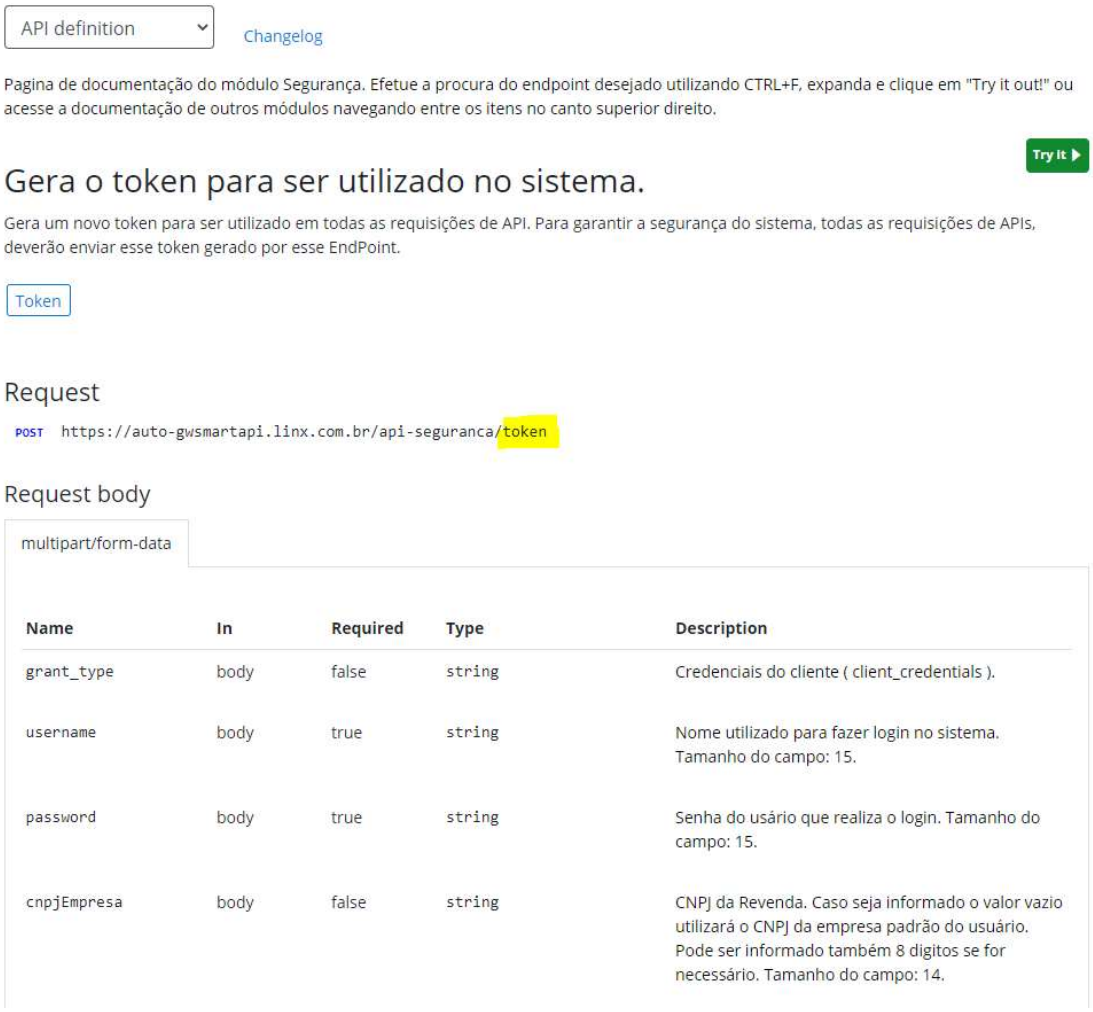
Passo 1. [Catálogo] . No catálogo do Portal **Linx Smart API**, localizar o quadro segurança:

Passo 2. [Segurança]. Clicar no Link "Segurança" para obter a lista de API's relacionadas com esta função.



Passo 3. [Endpoint]. Selecionar o Endpoint que Gera o Token "/token".

Passo 4. [Endpoint]. Selecionar o Endpoint que gera um novo Token. Serão mostrados os detalhes sobre os dados de entrada que podem ser enviados na requisição para a API. Bem como um botão [Try It] que deve ser acionado para efetuar o teste.



Passo 5. [Teste]. Ao clicar em [Try It], será apresentada a tela que permite informar os dados de entrada. Para o endpoint "/token" os dados obrigatórios são:

Header: AMBIENTE

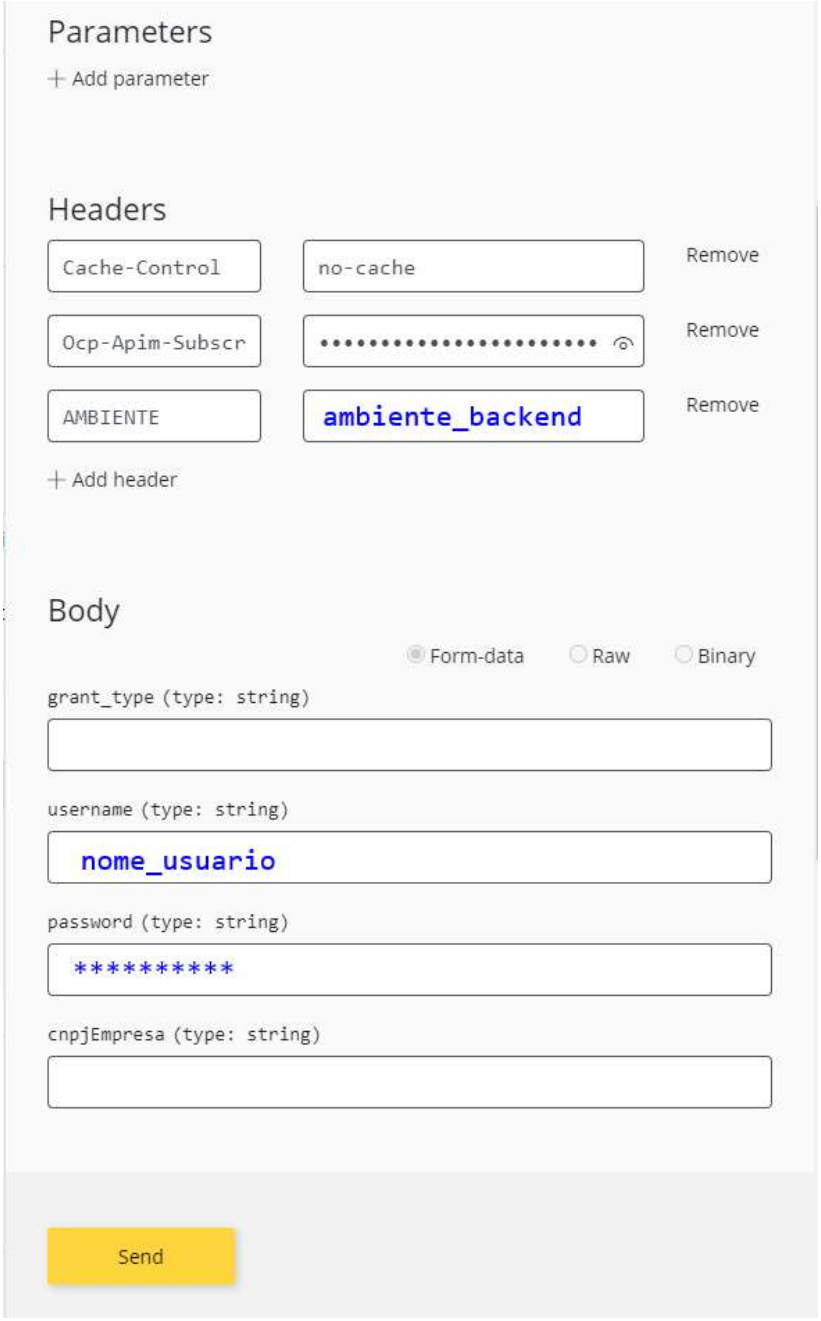
Informar o nome do backend fornecido pela LINX nos dados de cadastro. Caso não seja informado, a API de geração de token não responderá corretamente, e será emitido um **erro** de CORS (Cross-Origin Resource Sharing).

BODY:

username [USUÁRIO DO LINXDMS]

password [SENHA DO LINXDMS]

Credenciais do LINXDMS. Estes são os dados mais sensíveis para utilização das API's. E após geração do token não são mais requeridos.



Passo 6. [Retorno]. Quando os parâmetros enviados atendem plenamente os requisitos da API, o retorno enviado terá a estrutura json mostrada a seguir:

Http json:

```
{
  "access_token": "string",
  "token_type"  : "string",
  "expires_in"  : 0
}
```

Exemplo 1 do retorno 200 recebido:

Se todos os parâmetros foram enviados corretamente, a API devolverá um token com validade de 900 segundos. Este token deverá ser utilizado na requisição de todas as demais API's do sistema, para que seja atendida a nova regra de segurança e controle de acessos.

```
HTTP/1.1 200 OK

content-type: application/json; charset=utf-8
date: Fri, 24 Dec 2021 14:27:15 GMT
server: cloudflare
x-powered-by: ASP.NET

{
    "access_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ
1bmlxdWVfbmFtZSI6ImFkbWluIiwiQ29kaWdvVXN1YXJpbyI6IjAiLCJyb2xl
IjpbIkVJUyIsIkNUQiIsIkNDQyIsIlBFQyIsIkZBVCIsIkZJTiIsIk9GSSIsI
lZFSSIsIklXTSIsIkZBQiIsIklHRyIsIklDRSIsIkFGWCIsIkNBQyIsIkxPQy
IsIkNSUCIsIkNNTSIsIk1DQyIsIlBETSIsIklJUyIsIklQRiIsIkNGWCIsIlR
EQSIsIlJFVCIsIkVDUyIsIkZJQiIsIkZJMiIsIkFXQiIsIklESSIsIk5GTSIs
IkVDQSIsIkVDRSIsIklDSyIsIklHUyIsIkxEQiIsIkxERCIsIkdNQ
SIsIklDVCIsIklTRiIsIkZJQSIsIlRPWSIsIlNJTSIsIkFVVCIsIlJTUCIsIk
NUTSIsIklDTCIsIlU0QiJdLCJuYmYiOjE2NDAzNTYwMzIsImV4cCI6MTY0MDM
1NjkzMiwiaWF0IjoxNjQwMzU2MDMyfQ.JbgErTluStr1KNKGOTouTlKjYndw5
9bxQZ5oa8S6fiQ",
    "token_type": "bearer",
    "expires_in": 900
}
```

Exemplo 2, retorno 400:

Neste exemplo solicitamos um token enviando a senha de usuário errada. O retorno neste caso contém uma STRING com as informações sobre o erro.

Exemplo 3, retorno com erro de CORS:

Um erro comum na requisição de geração de TOKEN é a falta do parâmetro AMBIENTE nos dados de Logon. Neste caso haverá uma falha crítica na resposta, com erro de CORS.

2. PASSOS PARA RENOVAR A VALIDADE DO TOKEN:

Considerando que a validade de um token é 900 segundos ou 15 minutos, haverá necessidade de renovar a validade dele quando se aproxima o momento de expirar.

2.1. Renovação do Token:

Razões para efetuar um refresh do Token:

Prorrogar o uso do Token por mais 15 minutos sem requerer logon.

Apesar de a validade de um Token ser limitada em 900 segundos, é possível renovar a validade do Token sem requerer um novo logon, pela simples execução de um refresh antes de expirar completar o tempo.

Este processo pode ser repetido indefinidamente, caso seja sempre feito dentro do prazo.

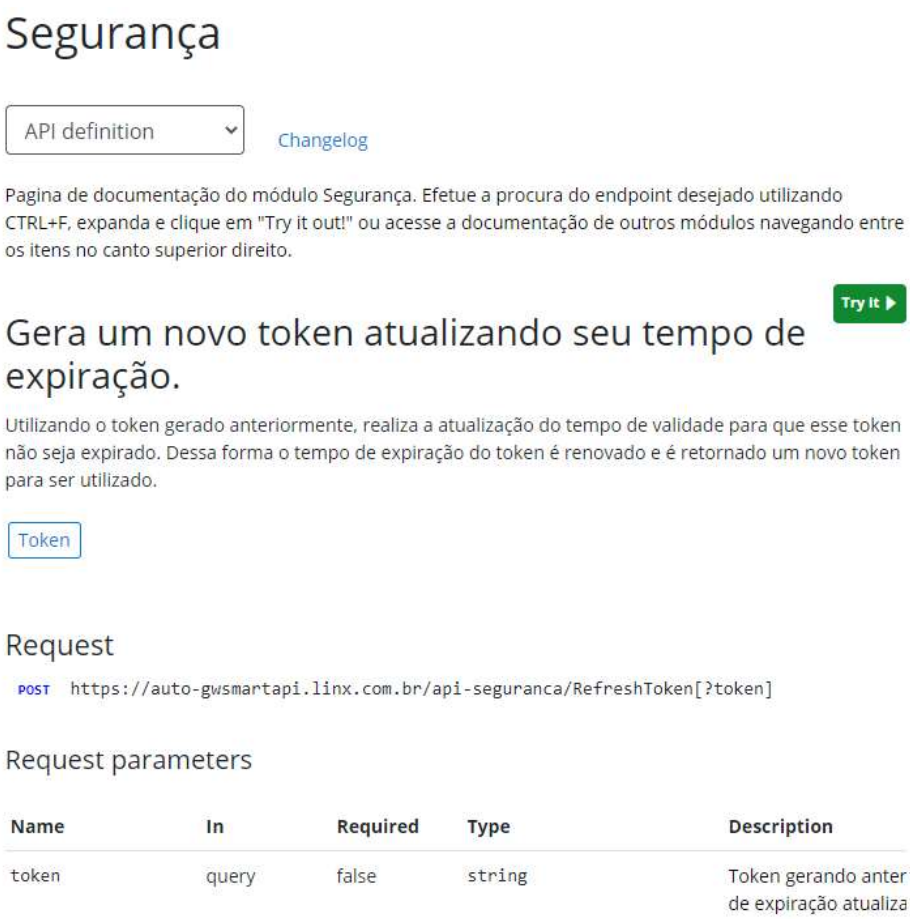
Ao mudar a Sessão/Revenda:

Um novo Token será gerado e retornado na operação TrocarRevendaSessão(). O qual deve ser enviado nas próximas requisições.

2.1.1 Exemplificando a Renovação do Token na Linx Smart API:

Passo 1. [Endpoint]. Ainda na SmartApi, catálogo segurança, selecionar o Endpoint "/RefreshToken ".

Passo 2. [Endpoint]. Todos os detalhes sobre a documentação do Endpoint "/RefreshToken " são apresentados. Para seguir com o teste, deve clicar no botão Try It .



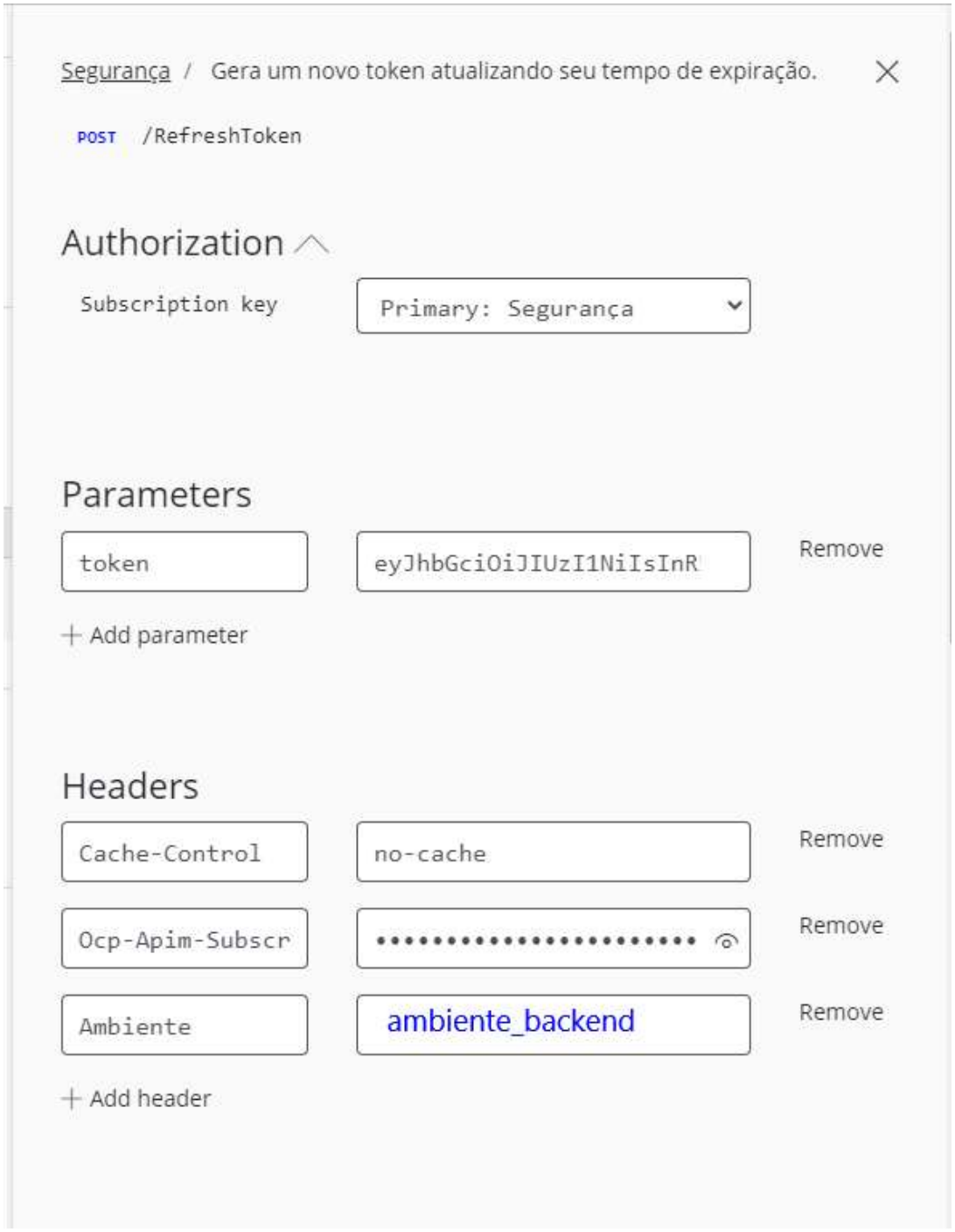
Passo 3. [Teste]. Neste ponto, para enviar um token para a renovação, é preciso informar o parâmetro "token" com a string do token obtida na geração.

Parâmetro GET: token = "string token"

Header: AMBIENTE

Informar o nome do ambiente backend que atende ao usuário. Caso não seja informado, a API de geração de token não responderá corretamente, e será emitido um **erro** de CORS (Cross-Origin Resource Sharing).

Tela de entrada de Header e Parâmetros



Passo 4. [Retorno]. Quando os parâmetros enviados atendem plenamente os requisitos da API, o retorno recebido terá a estrutura json mostrada a seguir:

Exemplo 1 do retorno 200 recebido:

HTTP response

```
HTTP/1.1 200 OK

content-type: application/json; charset=utf-8
date: Mon, 27 Dec 2021 19:00:33 GMT
server: cloudflare
x-powered-by: ASP.NET

{
    "access_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ
1bmlxdWVfbmFtZSI6ImFkbWluIiwiQ29kaWdvVXN1YXJpbyI6IjAiLCJyb2xl
IjpbIkVJUyIsIkNUQiIsIkNDQyIsIlBFQyIsIkZBVCIsIkZJTiIsIk9GSSIsI
lZFSSIsIklXTSIsIkZBQiIsIklHRyIsIklDRSIsIkFGWCIsIkNBQyIsIkxPQy
IsIkNSUCIsIkNNTSIsIk1DQyIsIlBETSIsIklJUyIsIklQRiIsIkNGWCIsIlR
EQSIsIlJFVCIsIkVDUyIsIkZJQiIsIkZJMiIsIkFXQiIsIklESSIsIk5GTSIs
IkVDQSIsIkVDRSIsIklDSyIsIklHUyIsIkxEQiIsIkxERCIsIkdNQ
SIsIklDVCIsIklTRiIsIkZJQSIsIlRPWSIsIlNJTSIsIkFVVCIsIlJTUCIsIk
NUTSIsIklDTCIsIlU0QiJdLCJuYmYiOjE2NDA2MzE2MjksImV4cCI6MTY0MDY
zMjUyOSwiaWF0IjoxNjQwNjMxNjI5fQ.K36Tp1FTr8SmUSxEoLDygLxFMQG1J
z4zPACNynROD0o",
    "token_type": "bearer",
    "expires_in": 900
}
```

Exemplo 2, retorno 400:

O retorno 400 será emitido pela API quando for requisitado o Refresh de um token inválido, ou que já expirou o prazo de 900 segundos.

Exemplo 3, retorno com erro de CORS:

Pelo mesmo motivo da geração do token, o erro de CORS ocorre pela falta do HEADER AMBIENTE nos dados da requisição.