

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.eyJ1bmlxdWVfbmFtZSI6IkxpbnhETVMuRFRPLk1v
ZGVscy5TZWd1cmFuY2EuRGFkb3NVc3Vhcm1vTG9naW5Nb2R1bCIsIm5iZii6MTYyOTgxNzAwMywiZ
XhwIjoxNjI5ODIwNjAzLCJpYXQiOjE2Mjk4MTcwMDN9.Y-
vKSi9G0zipjMfG6rqUkmj8F01j1p190vAndEak66M

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.

The screenshot shows a web browser window with the URL <https://auto-smartapi.linx.com.br/product#product=s01-seguran-a>. The page title is "S01 - Segurança". A sub-header states: "Produto de Segurança com EndPoints de segurança do sistema, como geração de tokens por exemplo". On the left, there is a section titled "Assinaturas" with a table showing one entry: "Segurança" (Status: Active). Below this is a form with a text input "Your new product subscription name" and a "Subscribe" button. On the right, there is a section titled "APIs do Produto" with a search bar and a table showing one entry: "Segurança" (Description: "Pagina de documentação do módulo Segurança. Efete a procura do endpoint desejado utilizando CTRL+F, expanda e clique em 'Try it out!' ou acesse a documentação de outros módulos navegando entre os itens no canto superior direito").

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

The screenshot shows a web browser window with the URL <https://auto-smartapi.linx.com.br/api/segu...>. The page title is "Segurança". A dropdown menu shows "Segurança". Below it are search and filter options: "Search operations" and "Group by tag" (which is turned on). A "Token" button is visible. The main content area shows a table of operations:

| Method | Operation |
|--------|---|
| POST | Gera o token para ser usado |
| POST | Gera um novo token atualizando o anterior |

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.

The screenshot shows a section of an API documentation page for the 'Segurança' module. At the top, there are two buttons: 'API definition' and 'Changelog'. Below them is a note: 'Página de documentação do módulo Segurança. Efetue a procura do endpoint desejado utilizando CTRL+F, expanda e clique em "Try it out!" ou acesse a documentação de outros módulos navegando entre os itens no canto superior direito.' A green button labeled 'Try It' is visible in the top right corner. The main content area has a title 'Gera o token para ser utilizado no sistema.' followed by a subtitle: 'Gera um novo token para ser utilizado em todas as requisições de API. Para garantir a segurança do sistema, todas as requisições de APIs, deverão enviar esse token gerado por esse EndPoint.' A blue button labeled 'Token' is shown. Below this, there's a 'Request' section with a 'POST' method and the URL 'https://auto-gwsmartapi.linx.com.br/api-seguranca/token'. Under 'Request body', there's a 'multipart/form-data' section containing a table with four rows of parameters:

| Name | In | Required | Type | Description |
|------------|------|----------|--------|---|
| grant_type | body | false | string | Credenciais do cliente (client_credentials). |
| username | body | true | string | Nome utilizado para fazer login no sistema. Tamanho do campo: 15. |
| password | body | true | string | Senha do usuário que realiza o login. Tamanho do campo: 15. |

The 'cnpjEmpresa' parameter is also listed under 'Request body' with the same details as the other fields.

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.

Parameters

+ Add parameter

Headers

| | | |
|-----------------|-------------------------|--------|
| Cache-Control | no-cache | Remove |
| Ocp-Apim-Subscr | ***** | Remove |
| AMBIENTE | ambiente_backend | Remove |

+ Add header

Body

Form-data Raw Binary

grant_type (type: string)

username (type: string)

password (type: string)

cnpjEmpresa (type: string)

Send

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": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9eyJ
1bmlxdWVfbmFtZSI6ImFkbWluIiwiQ29kaWdvVXN1YXJpbvI6IjAiLCJyb2xl
IjpBIkVJUyIsIkNUQiIsIkNDQyIsIlBFQyIsIkZBVCIsIkZJTiiIsIk9GSSIi
lZFSSIiSiklXTSiSikZBQiIsIk1HRyIsIk1DRSiSikFGWCIsIkNBQyIsIkxPQy
IsIkNSUCiSikNNNTSiSik1DQyIsIlBETSiSiklJUyIsIk1QRiIsIkNGWCiSIlR
EQSiSIlJFVCiSikVDUyIsIkZJQiiSikZJMiiSikFXQiiSikLESSiSik5GTSi
IkVDQSiSikVDRSiSik1DSyIsIk1HUiSikxEQiIsIkxEVCIiSikxERCIiSikdNQ
SiSiklDVCIiSiklTRiIsIkZJQSiSIlRPWSiSIlNJTSiSikFVVCiSIlJTUCiSik
NUTSiSiklDTCiSIlU0QiJdLCJuYmYiojE2MDAzNTYwMzIsImV4cCI6MTY0MDM
1NjkzMiwiaWF0IjoxNjQwMzU2MDMyfQ.JbgErTluStr1KNKGOTouTlKjYndw5
9bxQZ5oa856fiQ",
    "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.

HTTP response

HTTP/1.1 400 Bad Request

```
content-type: application/json; charset=utf-8
date: Mon, 27 Dec 2021 14:51:11 GMT
server: cloudflare
x-powered-by: ASP.NET
```

```
["O nome de usuário ou senha está incorreta.", "O nome de usuário ou senha está incorreta.", "Passo 0 - Método: LinxDMS.Segurança.Token ValidaLoginToken(LinxDMS.DTO.Models.Seguranca.DadosUsuarioLoginModel) - Linha: D:\\a\\1\\s\\Library\\LinxDMS.Geral\\LinxDMS.Geral\\LoginToken.cs:39\\nPasso 1 - Método: Microsoft.AspNetCore.Mvc.ActionResult`1[LinxDMS.Seguranca.Token] ValidaUsuario(LinxDMS.DTO.Models.Seguranca.DadosUsuarioLoginModel) - Linha: D:\\a\\1\\s\\WebServices\\LinxDMS\\LinxDMS\\Controllers\\Seguranca\\TokenController.cs:47\\n"]
```

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.

Unable to complete the request

Since the browser initiates the request, it requires Cross-Origin Resource Sharing (CORS) enabled on the server. Learn more

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".

The screenshot shows the Linx Smart API security catalog. At the top, there is a search bar labeled "Segurança" and a "Search operations" button. Below the search bar, there is a "Group by tag" toggle switch. Under the search bar, there is a "Token" category button. In the "Token" category, there are two entries: "POST Gera o token para ser utilizado no si..." and "POST Gera um novo token atualizando ...". The second entry is highlighted with a yellow background.

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**.

Segurança

API definition  Changelog

Página de documentação do módulo Segurança. Efetue a procura do endpoint desejado utilizando CTRL+F, expanda e clique em "Try it out!" ou acesse a documentação de outros módulos navegando entre os itens no canto superior direito.

Gera um novo token atualizando seu tempo de expiração.

Try it ▶

Utilizando o token gerado anteriormente, realiza a atualização do tempo de validade para que esse token não seja expirado. Dessa forma o tempo de expiração do token é renovado e é retornado um novo token para ser utilizado.

Token

Request

`POST https://auto-gwsmartapi.linx.com.br/api-seguranca/RefreshToken[?token]`

Request parameters

| Name | In | Required | Type | Description |
|-------|-------|----------|--------|-----------------------------|
| token | query | false | string | Token gerando anteriormente |

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

Segurança / Gera um novo token atualizando seu tempo de expiração. X

POST /RefreshToken

Authorization ▲

| | | |
|------------------|--------------------|--|
| Subscription key | Primary: Segurança | ▼ |
|------------------|--------------------|--|

Parameters

| | | |
|-------|-------------------------|--------|
| token | eyJhbGciOiJIUzI1NiIsInR | Remove |
|-------|-------------------------|--------|

+ Add parameter

Headers

| | | |
|---------------|----------|--------|
| Cache-Control | no-cache | Remove |
|---------------|----------|--------|

| | | |
|-----------------|-------|--------|
| Ocp-Apim-Subscr | ***** | Remove |
|-----------------|-------|--------|

| | | |
|----------|------------------|--------|
| Ambiente | ambiente_backend | Remove |
|----------|------------------|--------|

+ Add header

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
    1bmlxdWVfbmFtZSI6ImFkbWluIiwiQ29kaWdvVXN1YXJpbvI6IjAiLCJyb2xl
    IjpBIkVJUyIsIkNUQiIsIkNDQyIsIlBFQyIsIkZBVCIsIkZJTiIsIk9GSSIIsI
    lZFSSIIsIk1XTSIsIkZBQiIsIk1HRyIsIk1DRSIIsIkFGWCIsIkNBQyIsIkxPQy
    IsIkNSUCIsIkNNTSIsIk1DQyIsIlBETSIIsIk1JUyIsIk1QRiIsIkNGWCIsIlR
    EQSIIsIlJFVCIsIkVDUyIsIkZJQiIsIkZJMiIsIkFXQiIsIk1ESSIsIk5GTSIs
    IkVDDQSIIsIkVDRSIIsIk1DSyIsIk1HUyIsIkxEQiIsIkxEVCIsIkxERCIsIkdnQ
    SIIsIk1DVCIsIk1TRiIsIkZJQSIIsIlRPWSIsIlNJTSIsIkFVVCIsIlJTUCIsIk
    NUTSIIsIk1DTCIsIlU0QiJdLCJuYmYiOjE2NDA2MzE2MjksImV4cCI6MTY0MDY
    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.

HTTP response

HTTP/1.1 400 Bad Request

```
content-type: application/json; charset=utf-8
date: Mon, 27 Dec 2021 18:59:03 GMT
server: cloudflare
x-powered-by: ASP.NET
```

```
["Token: Erro ao identificar o usuario.", "Token: Erro ao identificar o usuario.", "Passo 0 - Método: LinxDMS.Seguranca.Token RefreshToken(System.String) - Linha: D:\\a\\1\\s\\Library\\LinxDMS.Seguranca\\LinxDMS.Seguranca\\TokenProvider.cs:60\\n Passo 1 - Método: Microsoft.AspNetCore.Mvc.ActionResult RefreshToken(System.String) - Linha: D:\\a\\1\\s\\WebServices\\LinxDMS\\LinxDMS\\Controllers\\Seguranca\\TokenController.cs:79\\n"]
```

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.

Unable to complete the request

Since the browser initiates the request, it requires Cross-Origin Resource Sharing (CORS) enabled on the server. Learn more