MANUAL DE INTEGRAÇÃO - API IDENTITY PROVIDER

1. CONHECENDO A API

O Identity Provider é uma Rest API que fornece manutenção de dados para os usuários e da permissão de acesso aos diferentes módulos de um sistema.

2. CRIANDO UM CLIENT

Para ter acesso ao Identity Provider você precisará criar um client, que irá controlar seus usuários e suas respectivas permissões.

ENDPOINT

/client-create

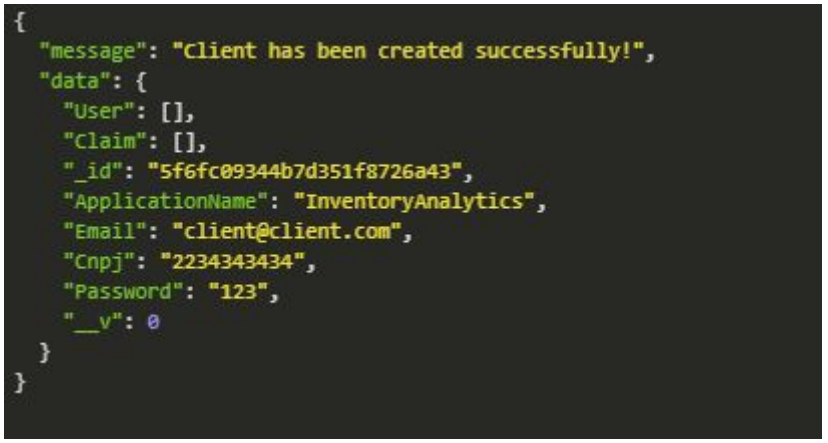
HEADER

Content-Type: application/json

EXEMPLO DE BODY JSON

```
{
  "ApplicationName": "InventoryAnalytics",
  "Email" : "client@client.com",
  "Cnpj": 2234343434,
  "Password": "123"
}
```

EXEMPLO DE RESPOSTA DO IDENTITY PROVIDER



```
{
  "message": "Client has been created successfully!",
  "data": {
    "User": [],
    "Claim": [],
    "_id": "5f6fc09344b7d351f8726a43",
    "ApplicationName": "InventoryAnalytics",
    "Email": "client@client.com",
    "Cnpj": "2234343434",
    "Password": "123",
    "__v": 0
  }
}
```

*Agora você poderá criar um **token JWT** para que seu cliente tenha acesso aos demais endpoints.*

3. AUTENTICANDO UM CLIENT E GERANDO TOKEN JWT **(CLIENT_TOKEN)**

Esse passo é necessário para acessar os demais endpoints do sistema. Para gerar um token (CLIENT_TOKEN) você deverá se autenticar no sistema, esse token é válido por 60 minutos.

ENDPOINT

/client-auth

HEADER

Content-Type: application/json

EXEMPLO DE BODY JSON

```
{
  "Email" : "client@client.com",
  "Password": "123"
}
```

EXEMPLO DE RESPOSTA DO IDENTITY PROVIDER


```
{
  "auth": true,
  "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI1ZjZmYzA5MzQ0YjdkMzUxZjg3MjZhNDMiLCJFbW
FpbCI6ImNsaWVudEBjbGllbnQuY29tIiwiQ25waiI6IjIyMzQzNDM0MzQiLCJpYXQiOjE2MDExNTkzMjgsImV4cC
I6MTYwMTE2MjkyOH0.Y2bhOPnYussf89CntFeuTt7xy35O4lvQBFE0kP07kPM",
  "expiresIn": 3600
}
```


Agora você poderá acessar todos os endpoints protegidos do identity provider.

***Auth**: Seu estado de autenticação*

***Token**: Token JWT*

Expires In: Tempo de expiração do token, sempre será de 1 hora, você deverá levar em conta isso ao implementar em seu sistema, uma boa lógica de renovação de token é o suficiente.

4. CRIANDO UM NOVO USUÁRIO

ENDPOINT

/user-create

HEADER

Content-Type: application/json

Authorization: ***CLIENT_TOKEN***

EXEMPLO DE BODY JSON

```
{
  "Name" : "user@user.com",
  "Email" : "user@user.com",
  "Password": "123"
}
```

EXEMPLO DE RESPOSTA DO IDENTITY PROVIDER

```
{
  "message": "User has been created successfully!",
  "data": {
    "_id": "5f6fc482cb2b96388cff84d9",
    "Name": "user@user.com",
    "Password": "123",
    "Email": "user@user.com",
    "Client": "5f6fc09344b7d351f8726a43",
    "__v": 0
  }
}
```

5. CRIANDO UMA NOVO CLAIM

ENDPOINT

/claim-create

HEADER

Content-Type: application/json

Authorization: ***CLIENT_TOKEN***

EXEMPLO DE BODY JSON

```
{
  "Name": "Modulo-Documentos"
}
```

EXEMPLO DE RESPOSTA DO IDENTITY PROVIDER

```
{
  "message": "Claim has been created successfully!",
  "data": {
    "_id": "5f6fc539e461163454a160d2",
    "Name": "Modulo-Documentos",
    "Client": "5f6fc09344b7d351f8726a43",
    "__v": 0
  }
}
```

6. ADICIONANDO UMA CLAIM A UM USUÁRIO

ENDPOINT

/manage-access-create

HEADER

Content-Type: application/json

Authorization: ***CLIENT_TOKEN***

EXEMPLO DE BODY JSON

```
{
  "IdUser": "5f6fc19c8e97d00f902e7e4f",
  "IdClaim": "5f6fc0b844b7d351f8726a44"
}
```

Atenção:

- **IdUser**: É o id do usuário que você criou, para ver como recuperar confira o capítulo 7. Utilizar o campo _id.
- **IdClaim**: É o id da claim que você criou, para ver como recuperar confira o capítulo 8.Utilizar o campo _id.

EXEMPLO DE RESPOSTA DO IDENTITY PROVIDER

```
{
  "message": "Manage Access has been created successfully!",
  "data": {
    "_id": "5f6fc1b28e97d00f902e7e50",
    "User": "5f6fc19c8e97d00f902e7e4f",
    "Claim": "5f6fc0b844b7d351f8726a44",
    "Client": "5f6fc09344b7d351f8726a43",
    "__v": 0
  }
}
```

7. RECUPERANDO UM USUÁRIO EXISTENTE

7.1 - RECUPERAR TODOS OS USUÁRIOS DE UM CLIENT

ENDPOINT

/user

HEADER

Content-Type: application/json

Authorization: ***CLIENT_TOKEN***

EXEMPLO DE RESPOSTA DO IDENTITY PROVIDER


```
[
  {
    "_id": "5f6fc482cb2b96388cff84d9",
    "Name": "user@user.com",
    "Password": "123",
    "Email": "user@user.com",
    "Client": "5f6fc09344b7d351f8726a43",
    "__v": 0
  },
  {
    "_id": "5f6fcc3c7079065024462ae6",
    "Name": "leonardo oliveira",
    "Password": "teste",
    "Email": "teste@teste.com",
    "Client": "5f6fc09344b7d351f8726a43",
    "__v": 0
  }
]
```

7.2 - RECUPERAR APENAS UM USUÁRIO DE UM CLIENT

ENDPOINT

*/user-details/**EMAIL_USER***

HEADER

Content-Type: application/json

*Authorization: **CLIENT_TOKEN***

EXEMPLO DE RESPOSTA DO IDENTITY PROVIDER

8. RECUPERANDO UM CLAIM EXISTENTE

8.1 - RECUPERAR TODOS OS CLAIMS DE UM CLIENT

ENDPOINT

/claim

HEADER

Content-Type: application/json

Authorization: ***CLIENT_TOKEN***

EXEMPLO DE RESPOSTA DO IDENTITY PROVIDER


```
[
  {
    "_id": "5f6fc539e461163454a160d2",
    "Name": "Modulo-Documentos",
    "Client": "5f6fc09344b7d351f8726a43",
    "__v": 0
  },
  {
    "_id": "5f6fcd377079065024462ae7",
    "Name": "Modulo-Contabilidade",
    "Client": "5f6fc09344b7d351f8726a43",
    "__v": 0
  }
]
```

8.2 - RECUPERAR APENAS UM CLAIM DE UM CLIENT

ENDPOINT

*/user-details/**NOME_MODULO***

HEADER

Content-Type: application/json

*Authorization: **CLIENT_TOKEN***

EXEMPLO DE RESPOSTA DO IDENTITY PROVIDER

9. AUTENTICANDO UM USUÁRIO E GERANDO TOKEN JWT **(USER_TOKEN)**

ENDPOINT

/user-auth

HEADER

Content-Type: application/json

Authorization: ***CLIENT_TOKEN***

EXEMPLO DE RESPOSTA DO IDENTITY PROVIDER

Agora você poderá acessar todos os endpoints protegidos do Identity Provider.

Auth*: Seu estado de autenticação*

Token*: Token JWT*

Expires In: Tempo de expiração do token, sempre será de 1 hora, você deverá levar em conta isso ao implementar em seu sistema, uma boa lógica de renovação de token é o suficiente.

10. RECUPERANDO CLAIMS DE UM USUÁRIO

ENDPOINT

/user-claims

HEADER

Content-Type: application/json

Authorization: ***USER_TOKEN***

EXEMPLO DE RESPOSTA DO IDENTITY PROVIDER

11. VERIFICANDO SE O USUÁRIO TEM UMA DETERMINADA CLAIM

ENDPOINT

*/user-has-permission/****CLAIM_NAME***

HEADER

Content-Type: application/json

Authorization: ***USER_TOKEN***

EXEMPLO DE RESPOSTA DO IDENTITY PROVIDER

12. ACESSO AOS MÓDULOS DO SEU SISTEMA

Para impedir o acesso do usuário aos módulos do seu sistema, você pode tanto utilizar das informações contidas do token do usuário, quanto realizar requisições para descobrir se ele tem acesso a uma determinada claim, abordado no capítulo 10 e 11.