



**fluiig**  
FLOWING  
PRODUCTIVITY



**IDENTITY**

---

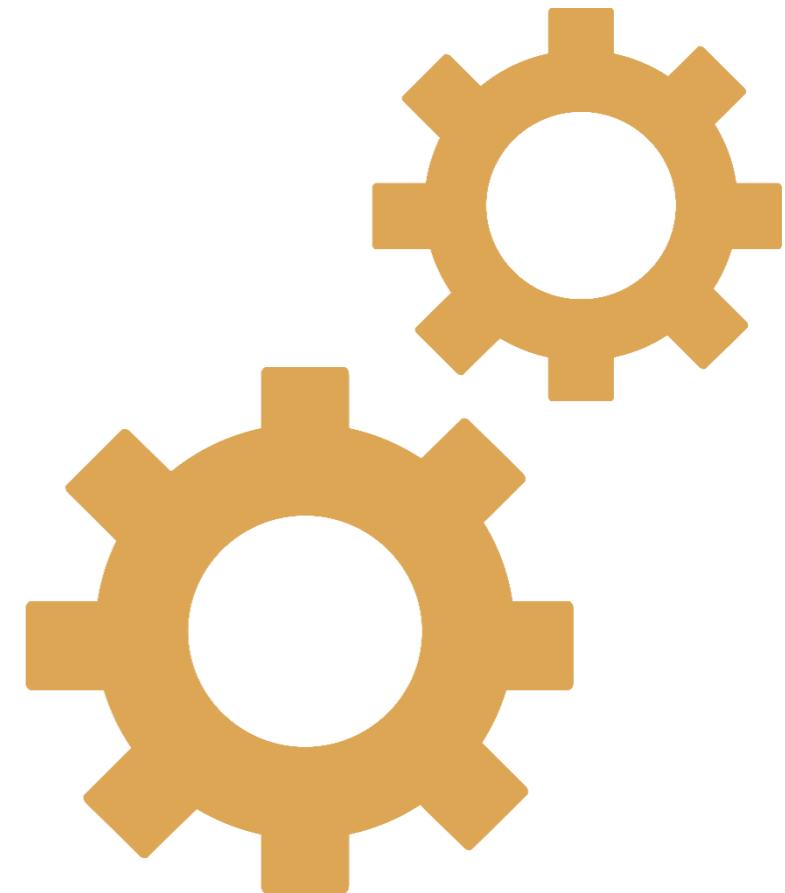
TREINAMENTO DE DESENVOLVIMENTO

1)

ARQUITETURA

## ARQUITETURA

- O fluig Identity permite gerenciar usuários e perfis de aplicações de forma centralizada
- Para atender este objetivo, diferentes arquiteturas podem ser utilizadas, de acordo com o nível de controle e integração que se deseja alcançar



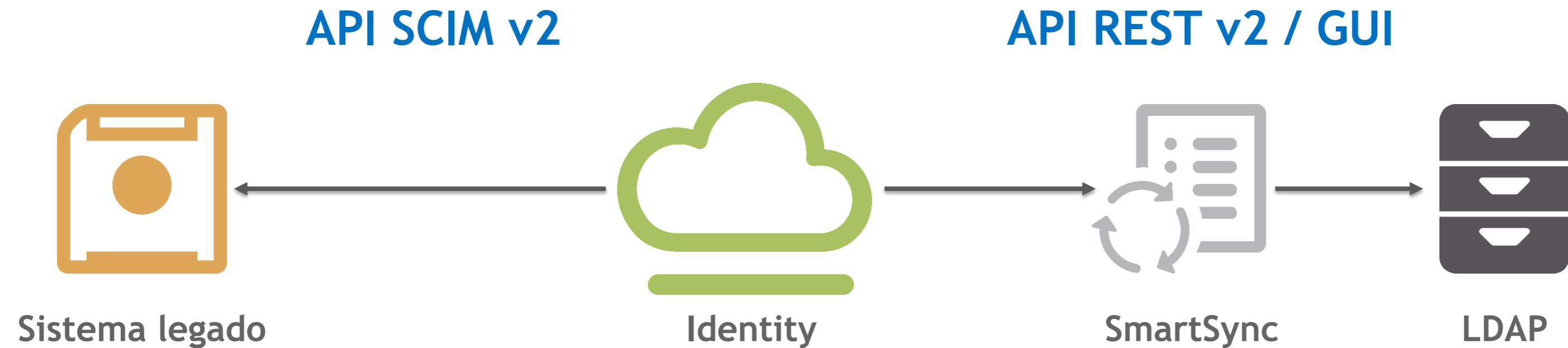
O Identity expõe **serviços REST** para prover acesso a usuários, grupos e aplicações bem como seus respectivos perfis.

Para isto, são utilizadas duas APIs:

- **API REST v2** para manipulação de usuários, grupos e aplicações
- **API SCIM v2** para provisionamento de usuários e perfis

Esse componente utiliza dois protocolos para integração com aplicações:

- **SAML v2** para autenticação de aplicações
- **SCIM v2** para provisionamento e desprovisionamento de usuários e perfis



2

)) LEVANTAMENTO INICIAL

- Produtos TOTVS tem no roadmap a integração com Identity via SAML e via SCIM
- Outros produtos devem ser analisados antes de se iniciar um projeto
- **Importante realizar este levantamento!**
  - Identificar se o sistema existente aceita o protocolo SAML e se há algum meio de integração REST

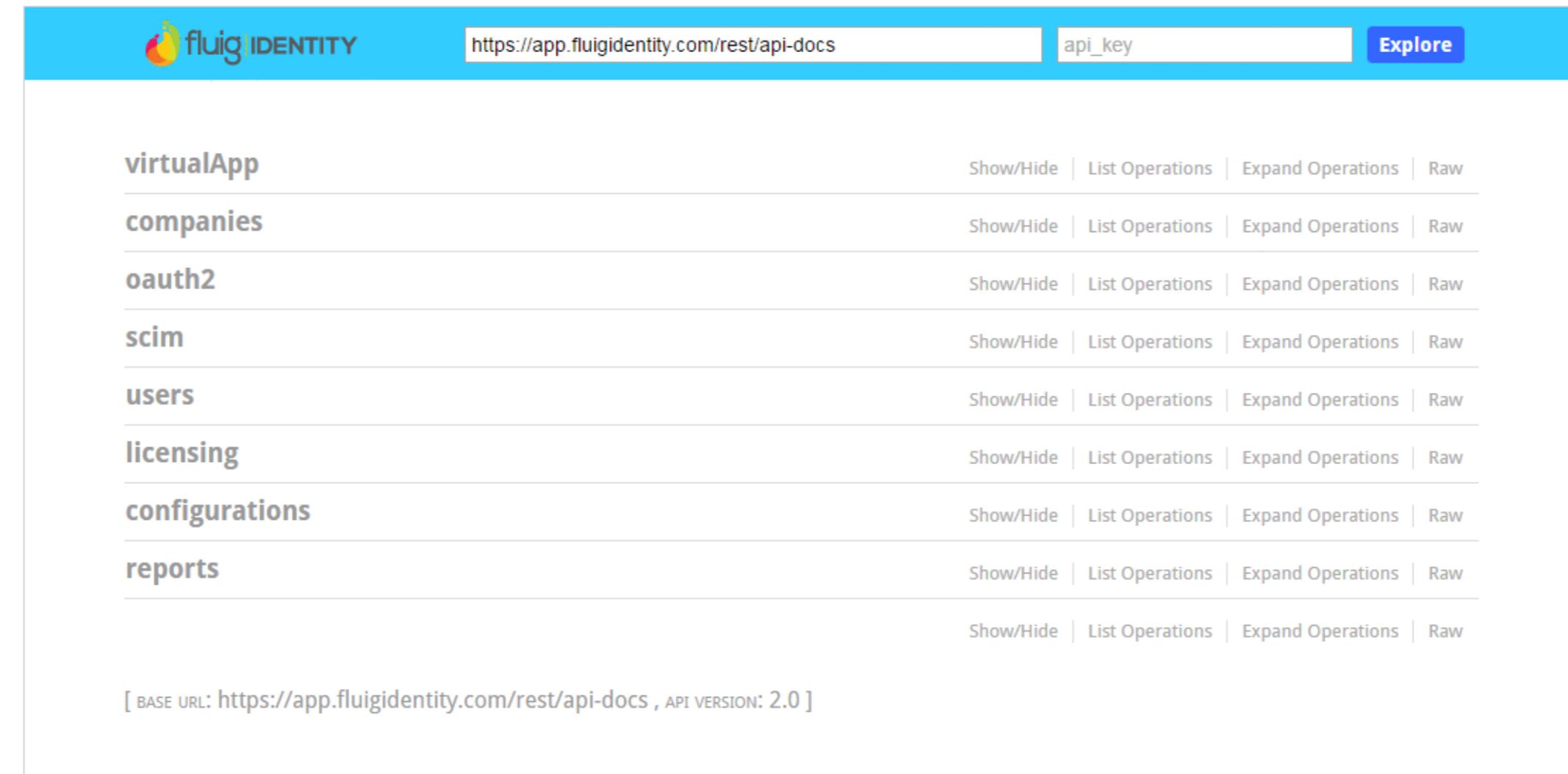


- Login integrado com LDAP?
  - Quantos domínios? Quantos usuários?
  - Usuários com e-mail preenchido no LDAP?
- Utiliza ou pretende utilizar Single Sign-On (SSO)?
- Quantos sistemas devem ser integrados?
- Qual tecnologia é utilizada pelas aplicações?
  - Linguagem, banco de dados, web ou desktop?
- Utiliza protocolo SAML?
- Que tipo de integração?
  - SSO (SAML)?
  - Provisionamento (SCIM)?



3)

SWAGGER



The screenshot shows the Swagger UI interface for the fluig/IDENTITY API. At the top, there's a header bar with the fluig/IDENTITY logo, the URL <https://app.fluigidentity.com/rest/api-docs>, an input field for 'api\_key', and a blue 'Explore' button. Below the header is a sidebar on the left containing links to various API endpoints: 'virtualApp', 'companies', 'oauth2', 'scim', 'users', 'licensing', 'configurations', and 'reports'. To the right of each endpoint link are four buttons: 'Show/Hide', 'List Operations', 'Expand Operations', and 'Raw'. At the bottom of the interface, a note indicates the base URL is <https://app.fluigidentity.com/rest/api-docs> and the API version is 2.0.

Trata-se de um framework para APIs que dispõe de estrutura completa para descrever, produzir, consumir e visualizar Web Services RESTful



# AUTENTICAÇÃO

The screenshot shows the Fluig Identity web interface. At the top, there is a navigation bar with the Fluig logo, a search bar containing "Comece a digitar para procurar no Fluig Identity", and several icons. Below the navigation bar, there is a horizontal menu with five items: "Novas contas", "Active Directory", "Segurança" (which has a red circle with the number 1 above it), "Customização", "Notificações via E-mail", and "Empresa". The "Segurança" item is highlighted with a blue underline. The main content area has three sections: "Senha Pessoal" (Personal Password), "Segurança com Captcha" (Security with CAPTCHA), and "Token REST API". In the "Senha Pessoal" section, there is a checked checkbox for "Habilitar senha pessoal" (Enable personal password) with a descriptive text below it. In the "Segurança com Captcha" section, there is an unchecked checkbox for "Habilitar segurança por captcha" (Enable security by CAPTCHA) with a descriptive text below it. In the "Token REST API" section, there is a "REST API v2" subsection with two entries: "ID da Empresa" (Company ID) and "ID do Cliente" (Client ID). The "ID do Cliente" entry has a red circle with the number 2 above it and a link "Baixar a Chave Privada" (Download Private Key) next to it.

**Copie o ID do Cliente da REST API v2 no Identity**



# AUTENTICAÇÃO

GIF

The screenshot shows the fluig|IDENTITY API documentation interface. At the top, there is a navigation bar with the fluig|IDENTITY logo, a URL input field containing "https://treinamentoleo.thecloudpass.com/rest/api-docs", a search bar with "api\_key", and a "Explore" button. Below the navigation bar, there is a sidebar on the left with several API endpoints listed: "virtualApp", "companies", "oauth2", "scim", "users", "licensing", "configurations", and "reports". The "oauth2" endpoint is highlighted with a yellow circle and a cursor icon pointing at it. To the right of the sidebar, there is a main content area displaying detailed information for each endpoint, including "Show/Hide", "List Operations", "Expand Operations", and "Raw" options.

virtualApp  
companies  
oauth2  
scim  
users  
licensing  
configurations  
reports

Show/Hide | List Operations | Expand Operations | Raw  
Show/Hide | List Operations | Expand Operations | Raw  
Show/Hide | List Operations | Expand Operations | Raw  
Show/Hide | List Operations | Expand Operations | Raw  
Show/Hide | List Operations | Expand Operations | Raw  
Show/Hide | List Operations | Expand Operations | Raw  
Show/Hide | List Operations | Expand Operations | Raw  
Show/Hide | List Operations | Expand Operations | Raw

[ BASE URL: <https://treinamentoleo.thecloudpass.com/rest/api-docs> , API VERSION: 2.0 ]

Cole o ID copiado no método  
GET para gerar a assertion

## AUTENTICAÇÃO

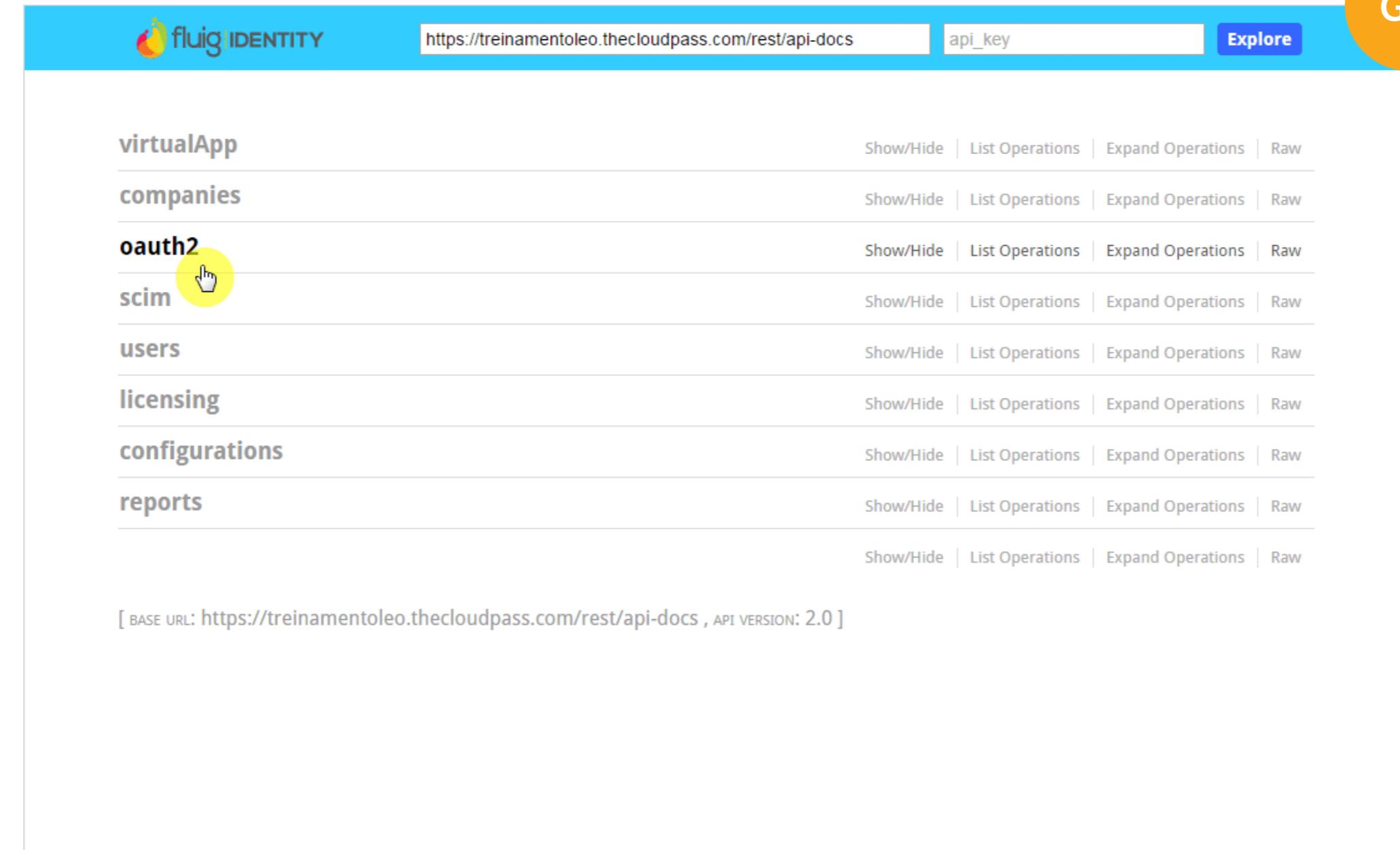
A **assertion** obtida precisa ser publicada na URL de autenticação OAuth do Identity juntamente com o **grant\_type**

O servidor irá verificar o JWT e sua assinatura e responderá com um JSON

- Copie o **access\_token**



# AUTENTICAÇÃO



The screenshot shows the fluig IDENTITY API documentation interface. At the top, there is a navigation bar with the fluig logo, the URL <https://treinamentoleo.thecloudpass.com/rest/api-docs>, a search bar with the placeholder "api\_key", and a "Explore" button. A yellow circular overlay labeled "GIF" is positioned in the top right corner.

The main content area displays a list of API endpoints under the "virtualApp" category:

- virtualApp** (highlighted in blue)
- companies**
- oauth2** (highlighted in blue)
- scim** (highlighted in blue)
- users**
- licensing**
- configurations**
- reports**

Each endpoint has associated actions: Show/Hide, List Operations, Expand Operations, and Raw. At the bottom of the page, a note indicates the base URL and API version:

[ BASE URL: <https://treinamentoleo.thecloudpass.com/rest/api-docs> , API VERSION: 2.0 ]

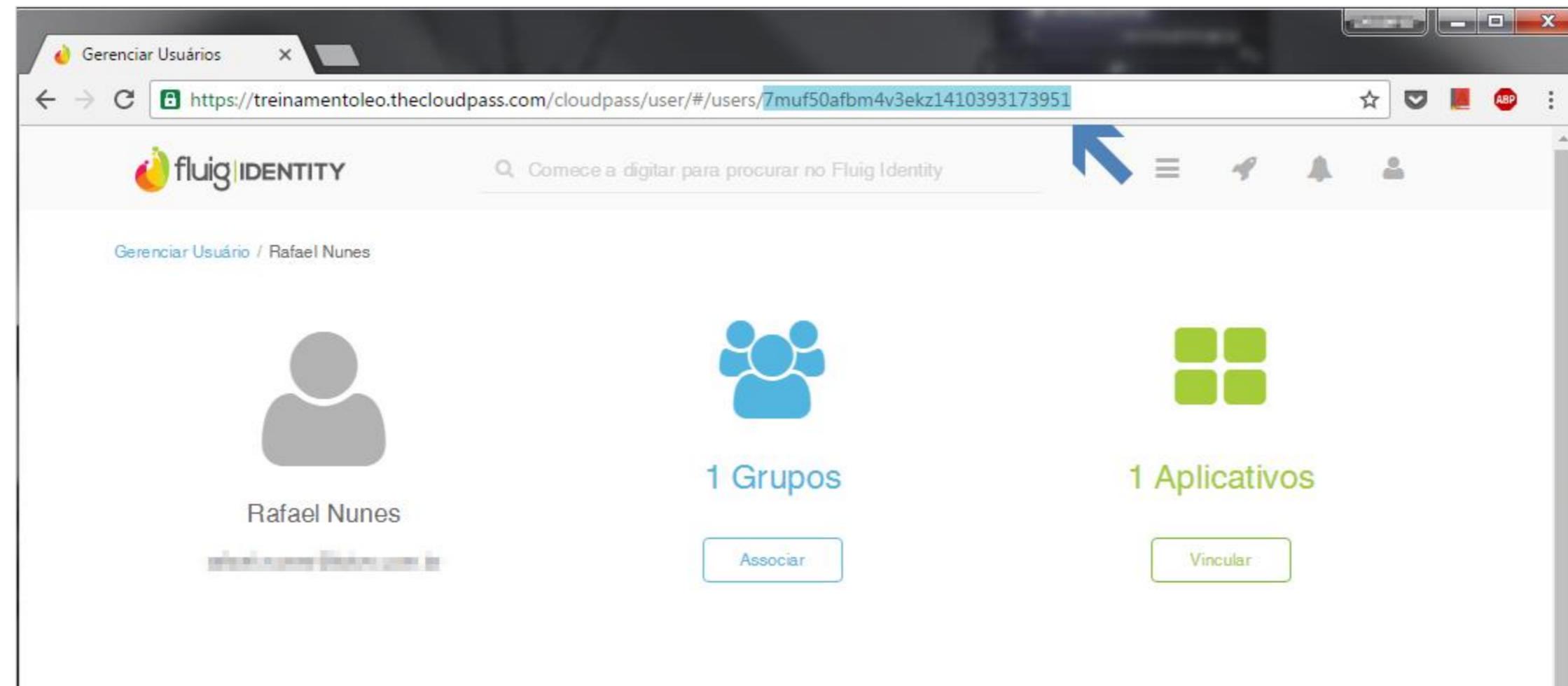
# AUTENTICAÇÃO



- Informe o valor do `access_token` no campo `api_key` no canto superior direito da tela e clique em **Explore**
- A partir deste momento, você estará **autenticado** e poderá utilizar os serviços do Identity por **1 hora**

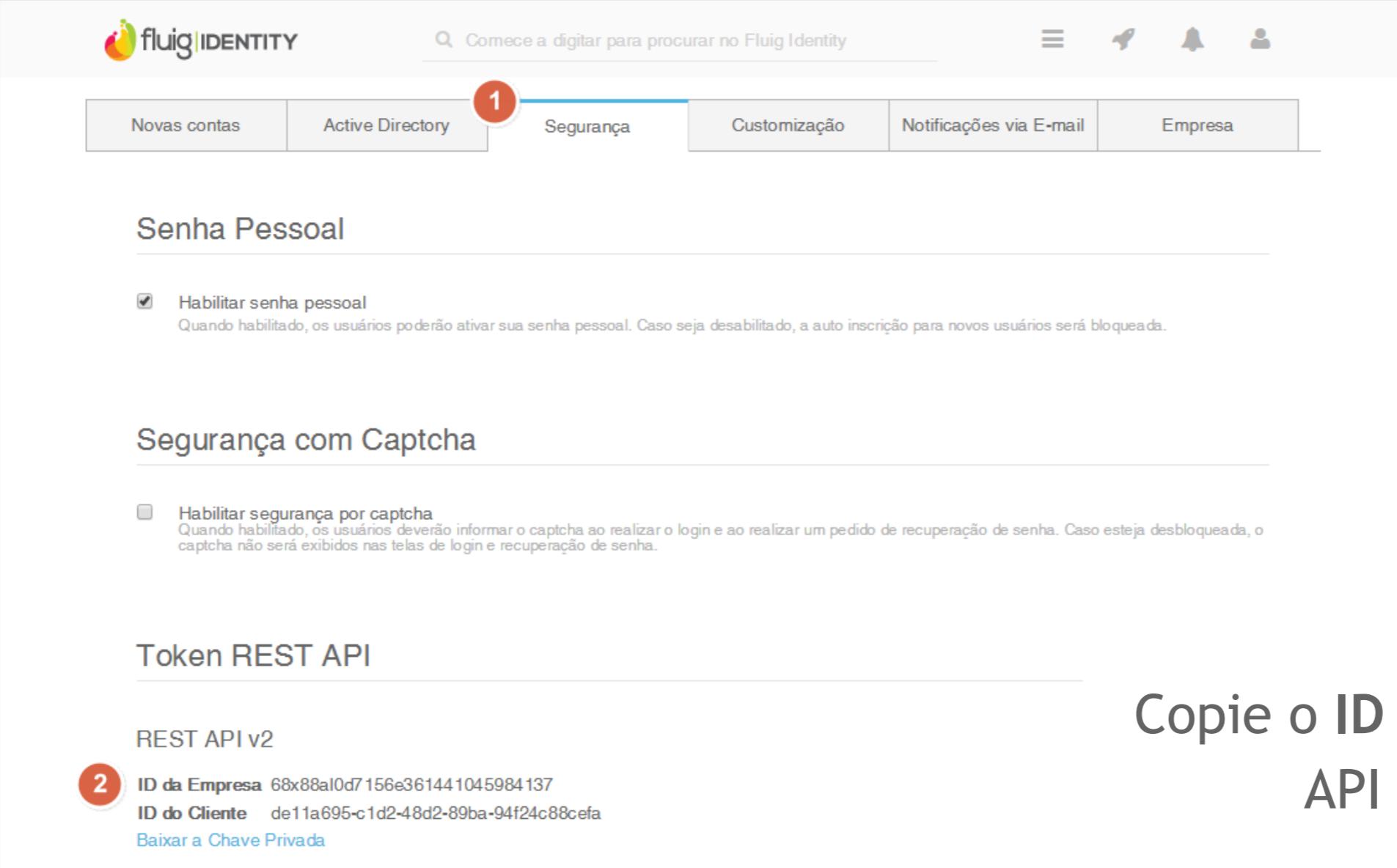


## OBTER DADOS DE UM USUÁRIO



No Identity, acesse as propriedades do usuário e **copie o ID** na barra de endereço do navegador

# OBTER DADOS DE UM USUÁRIO



The screenshot shows the Fluig Identity dashboard. At the top, there is a navigation bar with the Fluig logo, a search bar, and several icons. Below the navigation bar, there is a horizontal menu with tabs: 'Novas contas', 'Active Directory', 'Segurança' (which is highlighted with a red circle containing the number 1), 'Customização', 'Notificações via E-mail', and 'Empresa'. The main content area has three sections: 'Senha Pessoal', 'Segurança com Captcha', and 'Token REST API'. Under 'Senha Pessoal', there is a checked checkbox for 'Habilitar senha pessoal' with a descriptive subtitle. Under 'Segurança com Captcha', there is an unchecked checkbox for 'Habilitar segurança por captcha' with a descriptive subtitle. Under 'Token REST API', there is a section for 'REST API v2' containing the 'ID da Empresa' (68x88a10d7156e361441045984137) and 'ID do Cliente' (de11a695-c1d2-48d2-89ba-94f24c88cefa), along with a link to 'Baixar a Chave Privada'. A red circle containing the number 2 is placed next to the 'ID da Empresa' text.

Copie o ID da Empresa da REST  
API v2 no Identity

# OBTER DADOS DE UM USUÁRIO

GET </rest/v2/companies/{companyId}/users/{userId}> Get a company user by id

Response Class  
string

Response Content Type [application/json ▾](#)

Parameters

Parameter	Value	Description	Parameter Type	Data Type
companyId	68x88al0d7156e361441045984137	companyId	path	string
userId	7muf50afbm4v3ekz1410393173951	userId	path	string

Try it out! [Hide Response](#)

Request URL  
<https://treinamentoleo.thecloudpass.com:443/rest/v2/companies/68x88al0d7156e361441045984137/users/7muf50afbm4v3ekz1410393173951>

Response Body

```
{  
  "id": "7muf50afbm4v3ekz1410393173951",  
  "firstName": "Rafael",  
  "lastName": "Nunes",  
  "password": "",  
  "address": "",  
  "phoneNumber": "",  
  "emailAddress": "rafael.nunes@fluig.com.br",  
  "isADImport": false,  
  "annStateChanged": true.  
}
```

Informe o ID da Empresa e o ID do Usuário no método  
**GET /rest/v2/companies/{companyId}/users/{userId}**

Será retornado um JSON com os dados do usuário

4)

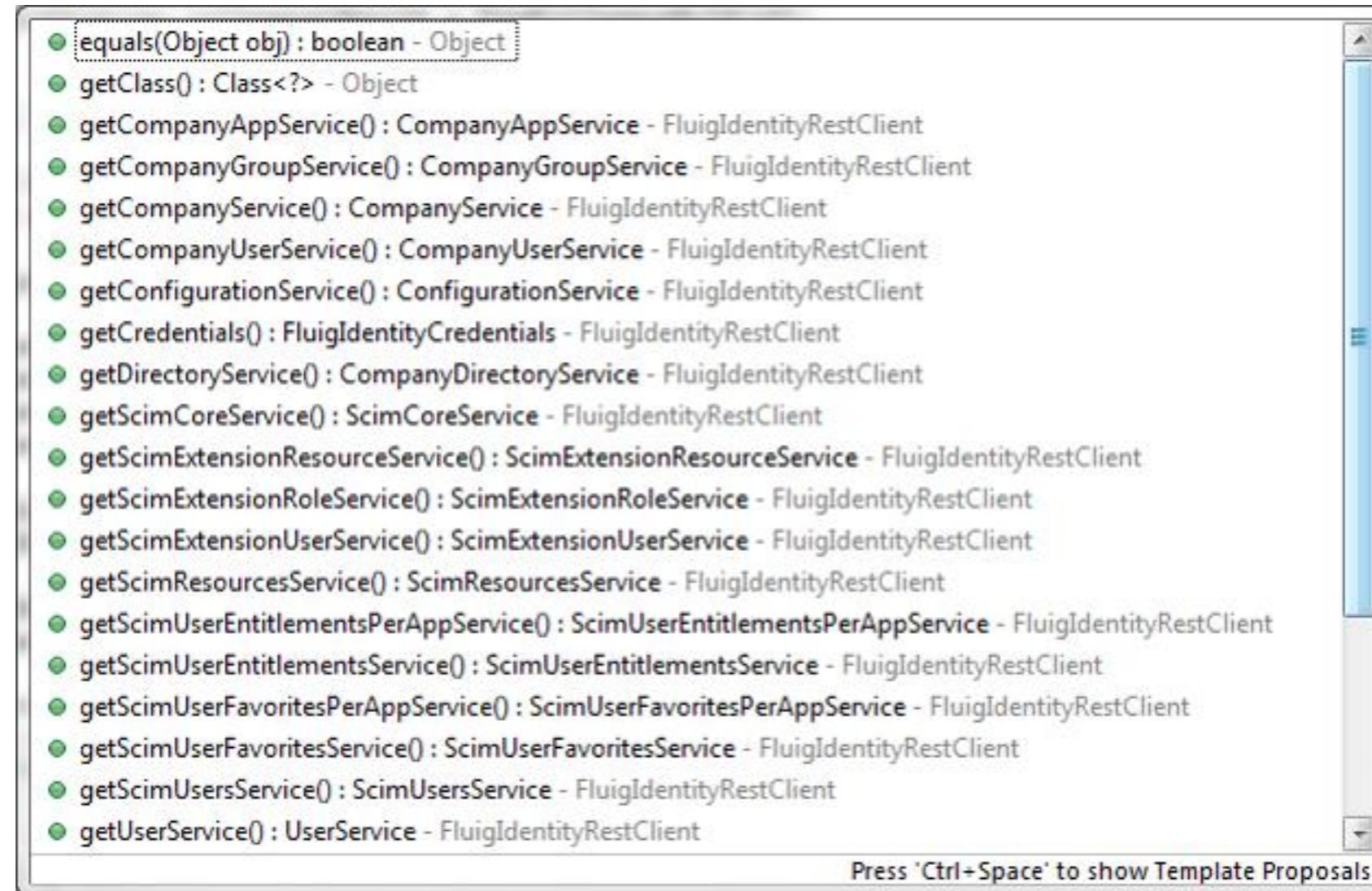
**REST CLIENT**

- API utilizada para operações de manipulação de empresas, usuários, grupos e aplicações, bem como a integração entre estes elementos
- O esquema de autenticação e autorização das APIs REST v2 é baseado no padrão OAuth 2.0 utilizando JWT (JSON Web Token)
- Cada empresa criada no Identity possui um **client-id** e uma **chave privada**, que permitirão o acesso aos dados da empresa via API REST
- Para obter os serviços disponíveis no fluig Identity via API, é necessário realizar o download do arquivo **rest-client.jar**: 

- Após incluir o rest-client.jar como dependência, é necessário configurar o objeto **FluigIdentityCredentials** informando o ID do Cliente, o caminho do certificado gerado pelo Identity e a URL do contexto
- Será obtido o objeto **FluigIdentityRestClient**, que contém todos os serviços do fluig Identity, tais como consultar usuários e grupos existentes no contexto

```
FluigIdentityCredentials credentials = new Fluig.IdentityCredentials(  
    "f2008cf1-a835-4ab0-bb7e-608447875058", // ID do Cliente  
    "C:\\\\PS_FluigIdentity.pk8", // Caminho da chave PK8  
    "https://suaempresa.fluigidentity.com"); // URL do contexto Identity  
  
FluigIdentityRestClient cliente = new FluigIdentityRestClient(credentials);
```

# REST CLIENT



Serviços disponíveis no objeto FluigIdentityRestClient, demonstrado no slide anterior

## REST CLIENT

```
UserCompanyAccountDTO accountDTO = new UserCompanyAccountDTO();  
accountDTO.setCompanyId(getCompanyIdIdentity());  
accountDTO.setEmailAddress(email);  
accountDTO.setFirstName(nome);  
accountDTO.setLastName(sobrenome);  
accountDTO.setPassword("Fluig@123");  
  
accountDTO = client.getCompanyUserService().createUser(getCompanyIdIdentity(),  
accountDTO, true);
```

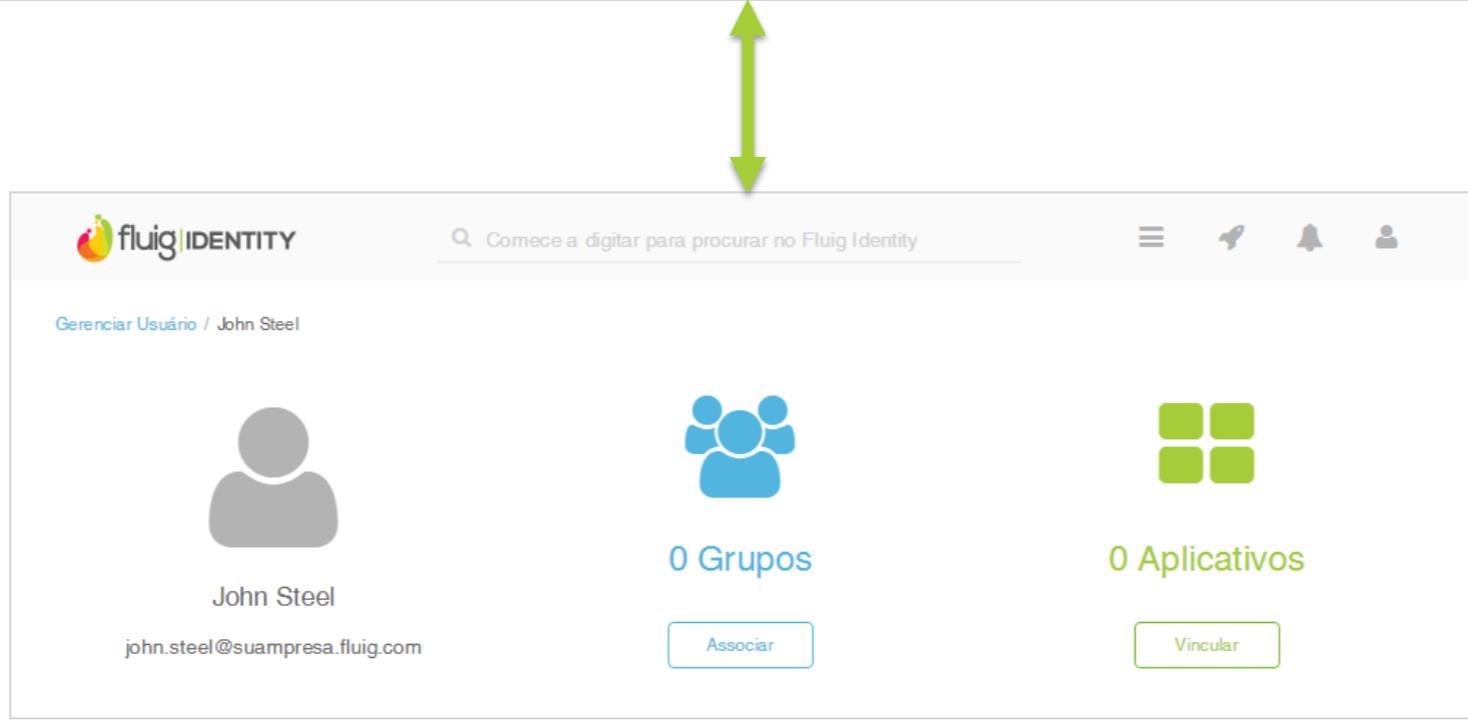
Exemplo de inclusão de usuário no Identity por meio da API REST v2

Models REST do fluig Identity: 

# RENT CLIENT

```
{"id":"i1t90by5x7ubdzazl405023949562","firstname":"John","lastName":"Steel","password":"","address":"","phoneNumber":"","emailAddress":"john.steel@suaempresa.fluig.com","isADImport":false,"appStatechanged":false,"adToken":"","jobTitle":"","dateCreated":"2014-04-14_17:24:28","companyName":"","role":"USER","userLoginType" :"CP_LOGIN","userOrigin":"CP_ADMIN","assignedAppCount":0,"userStatus":"ACTIVATED","previousUserStatus":"INVITED","resetKey":"","companyLogoPath":"","enableOTP":false,"personalId":"i1t90by5x7ubdzazl405023949562","department":"qkygwtx5q8yp24f11402082355416","customFields":{}, "extFields":{},"companyId":"wOejm0700eq6vitp1402681820034"}
```

## Retorno do Identity



The screenshot shows the fluig IDENTITY user management interface. At the top, there's a navigation bar with the fluig logo, a search bar containing "Comece a digitar para procurar no Fluig Identity", and several icons. Below the header, the page title is "Gerenciar Usuário / John Steel". The main content area displays a user profile for "John Steel" with the email "john.steel@suaempresa.fluig.com". To the right of the profile, there are two sections: "0 Grupos" (Groups) with a blue icon and "0 Aplicativos" (Applications) with a green icon. At the bottom of each section are buttons labeled "Associar" (Associate) and "Vincular" (Link). A double-headed vertical arrow is positioned between the JSON data block and the screenshot.

Usuário Criado



MÃOS À OBRA!



## EXERCÍCIOS DE FIXAÇÃO

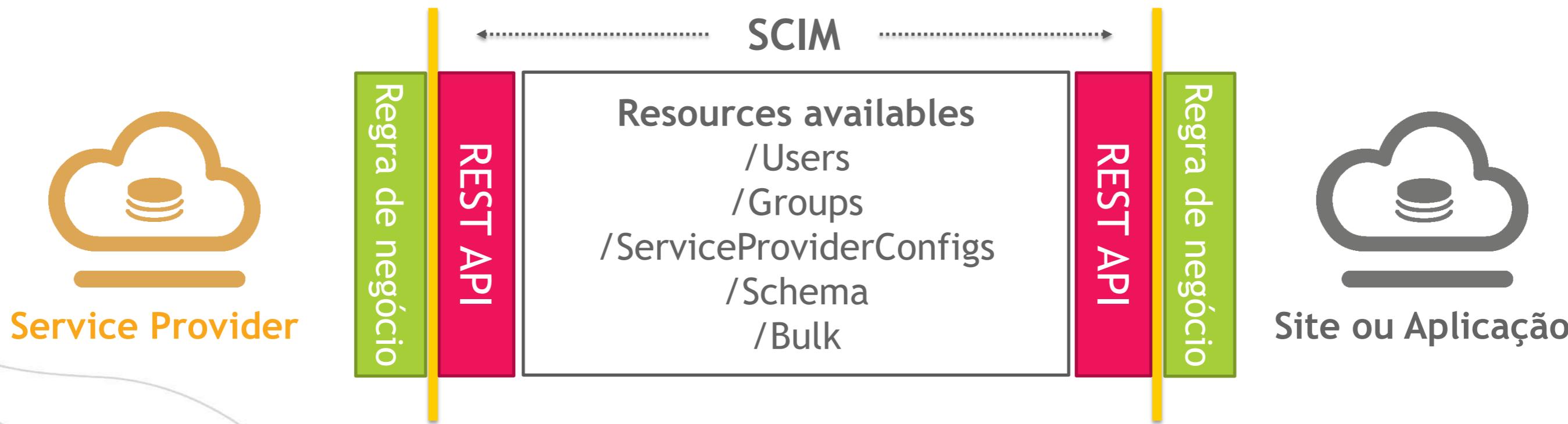
Imagine que está em um projeto de Identity. As atividades são detalhadas abaixo:

1. Utilizar o Swagger através da interface gráfica para buscar um Usuário existente no Identity
2. Realizar uma busca do mesmo usuário utilizando uma API

6

) SCIM

- **SCIM**: padrão aberto para automatizar a troca de informações de identidade entre domínios ou sistemas. É usado na integração dos ERPs
- APIs baseadas em SCIM são um subconjunto de APIs REST do fluig Identity: <https://app.fluigidentity.com/rest/swagger-ui/index.html#!/scim>



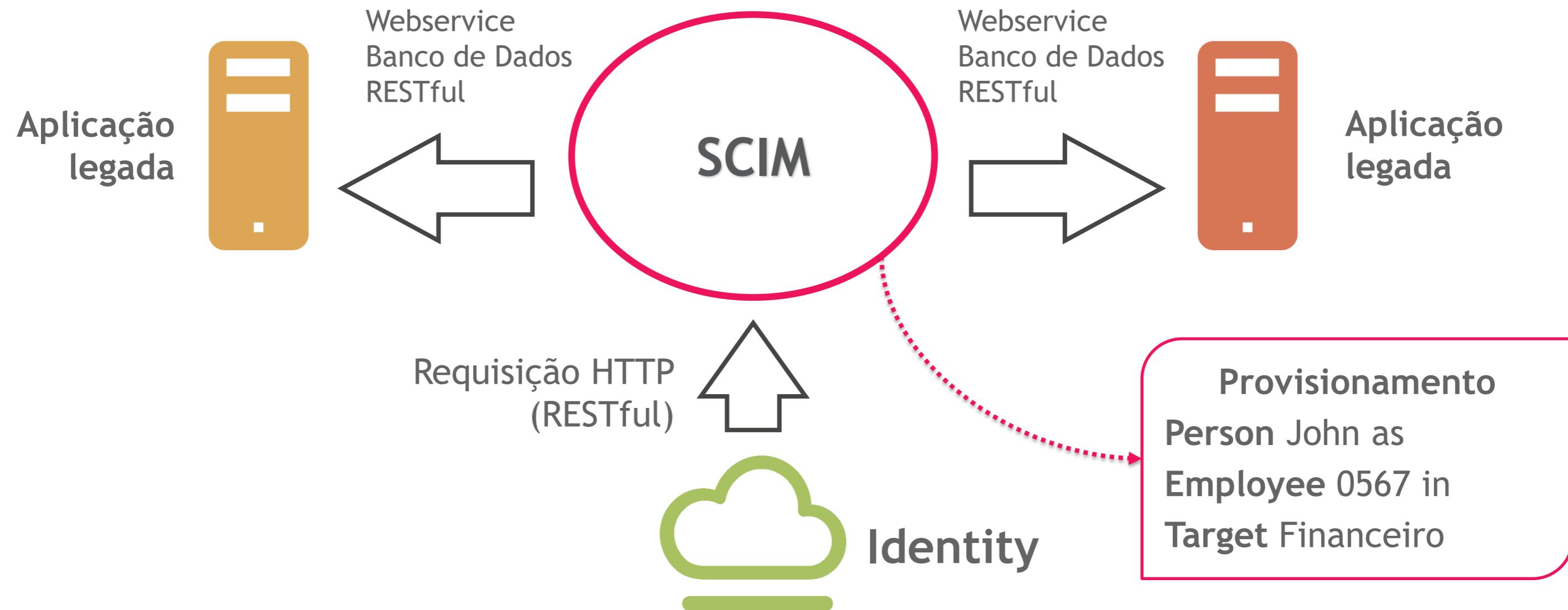
As solicitações SCIM são feitas através de operações de HTTP e as respostas são devolvidas no corpo do HTTP de retorno

O formato poderá ser JSON ou XML, dependendo do pedido, o status da solicitação indicado tanto no código de status HTTP e o corpo da resposta

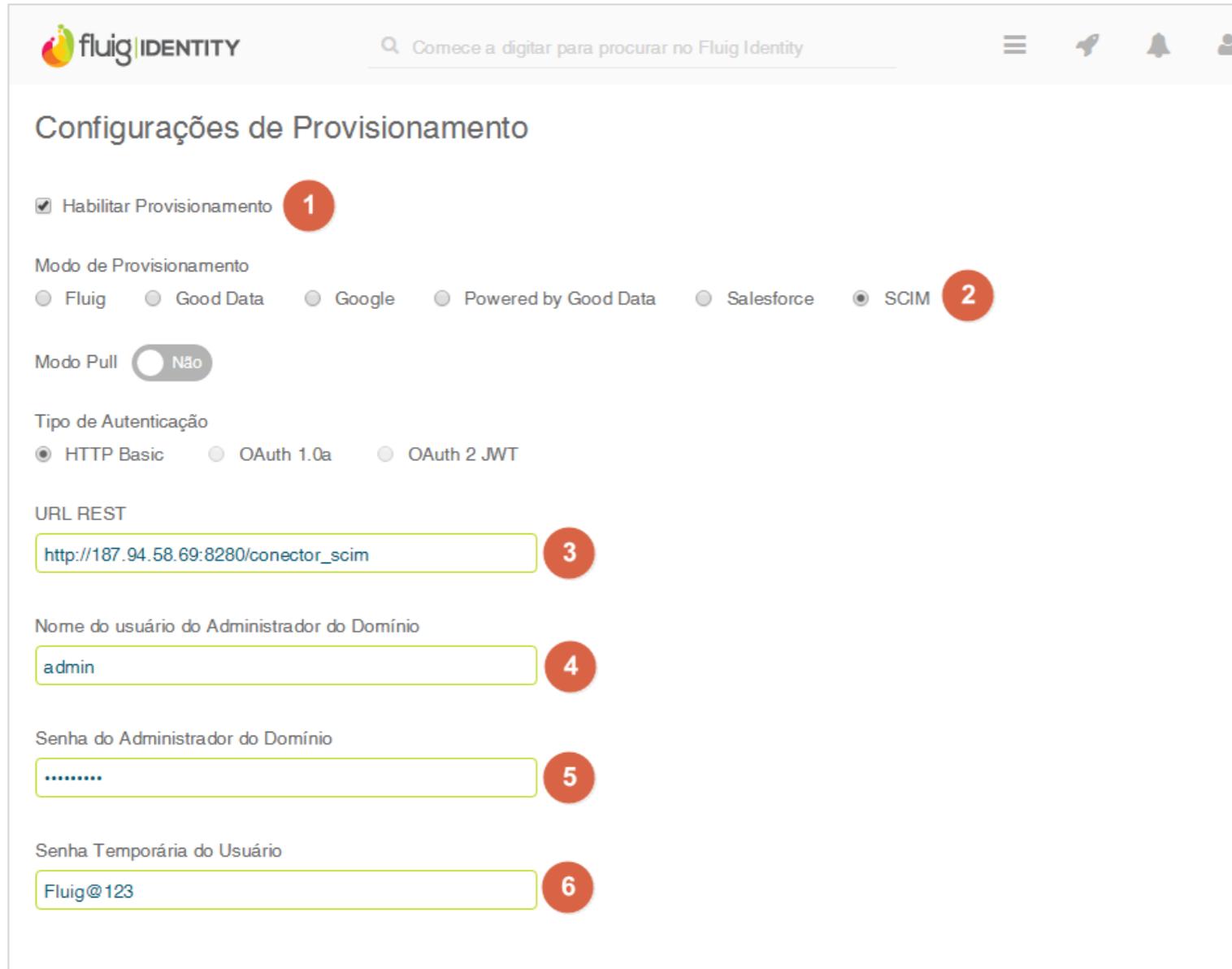
Operações e ações esperadas para HTTP:

Operação	Descrição	Exemplo
<b>GET</b>	Recupera um recurso completo ou parcial.	/Users/{id} or /Groups/{id}
<b>POST</b>	Cria um novo recurso	/Users or /Groups
<b>PUT</b>	Modifica um recurso com um recurso especificado pelo consumidor	/Users/{id} or /Groups/{id}
<b>DELETE</b>	Exclui um recurso	/Users/{id} or /Groups/{id}

# PROVISIONAMENTO & DESPROVISIONAMENTO DE USUÁRIOS



# CONFIGURAÇÃO DE APLICATIVOS SCIM



The screenshot shows the 'Configurações de Provisionamento' (Provisioning Settings) page in the Fluig Identity interface. The page includes fields for provisioning mode (selected as SCIM), authentication type (HTTP Basic), URL REST, and administrator credentials (username: admin, temporary password: Fluig@123).

1. Habilite o checkbox 'Habilitar Provisionamento'.

2. Selecione 'SCIM' no dropdown 'Modo de Provisionamento'.

3. Insira a URL REST: `http://187.94.58.69:8280/conector_scim`.

4. Insira o nome de usuário do Administrador do Domínio: `admin`.

5. Insira a senha do Administrador do Domínio: `.....`.

6. Insira a Senha Temporária do Usuário: `Fluig@123`.

1. Habilitar Provisionamento
2. Selecionar SCIM
3. URL do sistema que receberá chamadas REST
4. Usuário para acessar o sistema via HTTP Basic
5. Senha para acessar o sistema via HTTP Basic
6. Senha temporária configurada no objeto FluigUser

## SCIM + IDENTITY

Para que o Identity consiga se integrar com o sistema legado utilizando o protocolo SCIM é necessário ter um sistema:

- Que receba requisições em REST (JSON), devido ao fato do Identity realizar apenas chamadas em REST
- Configurado com autenticação HTTP Basic
- Ter o arquivo rest-client.jar como dependência do projeto

Para que o Identity realize as chamadas REST para o conector SCIM é necessário disponibilizar os serviços com a seguinte URL:

**http://[hostname]:[port]/scim/v2/extensions/Users/{id}**

Endereço da aplicação

Recurso Principal

Subtipo do Recurso Principal

Identificador do Recurso

## SCIM URL

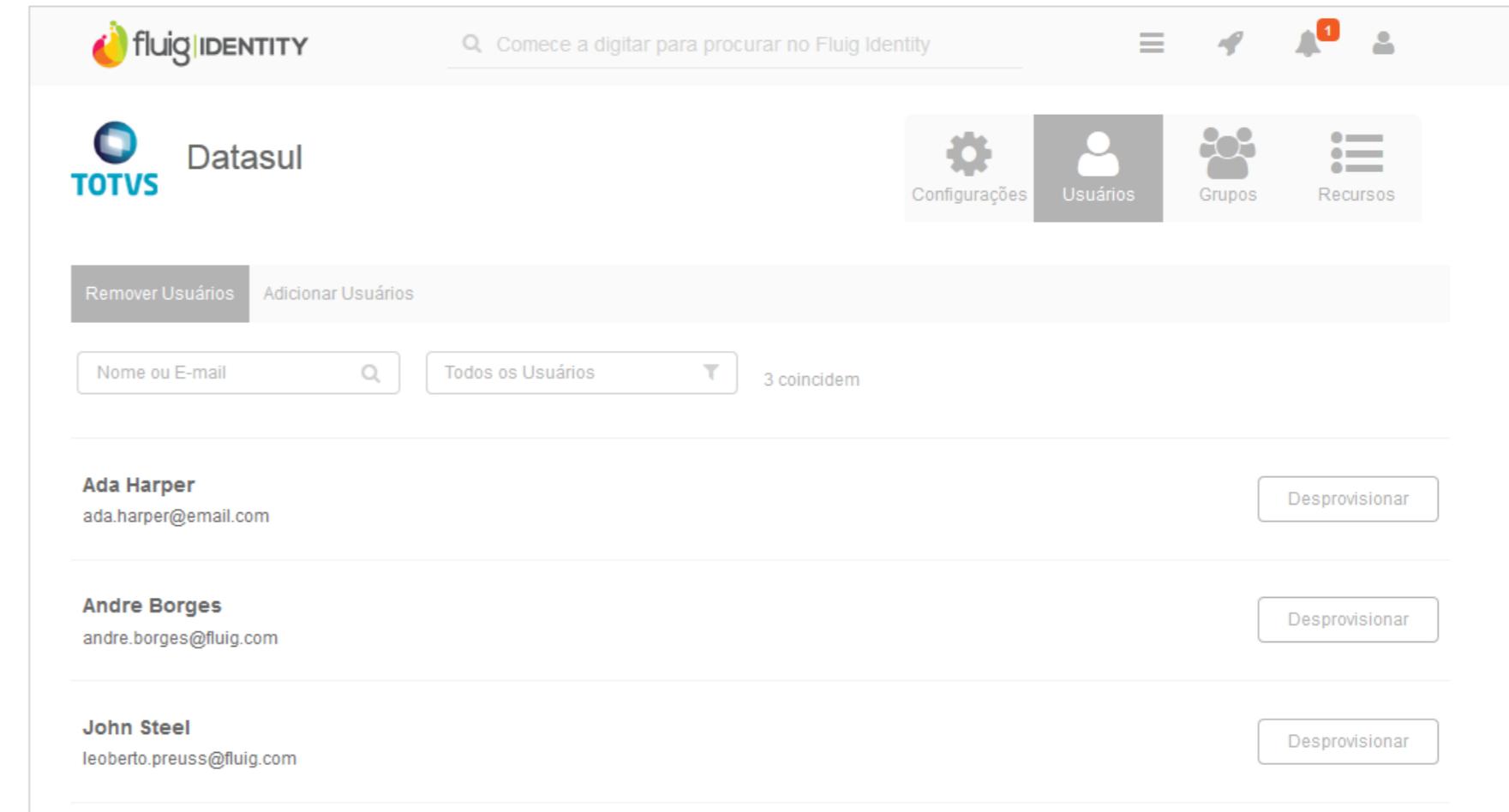
Recurso	[hostname]:[port]/scim/v2/extensions	Método	Descrição
User	/Users	POST	Essa API será chamada do fluig Identity para criar um usuário
	/{userId}	DELETE	Essa API será chamada do fluig Identity para remover um usuário
Entitlements	/Entitlements/Users/{userId}	POST	Essa API será chamada do fluig Identity para associar um usuário a um grupo ou lista de grupos
	/Entitlements/Users/{userId}/remove	POST	Essa API será chamada do fluig Identity para dissociar um usuário de um Resource

## SCIM URL

Recurso	[hostname]:[port]/scim/v2/extensions	Método	Descrição
Resources	/Resources	POST	Essa API será chamada do fluig Identity para criar um recurso
	/Resources/{resourceId}	PUT	Essa API será chamada do fluig Identity para atualizar um recurso
	/Resources/{resourceId}	DELETE	Essa API será chamada do fluig Identity para remover um recurso
	/ping	GET	Método responsável por receber chamadas do Identity p/ verificar se o conector está funcionando
	/sync	GET	Essa API será chamada do fluig Identity para iniciar a sincronização de dados do sistema legado

# PROVISIONAMENTO & DESPROVISIONAMENTO DE USUÁRIOS

Ao criar um usuário no Identity e associar este ao aplicativo SCIM, o sistema enviará uma requisição, em até 30 segundos, para provisionar este usuário no sistema legado, conforme as configurações do aplicativo em questão



The screenshot shows the Fluig Identity web application interface. At the top, there is a header with the Fluig logo, a search bar containing the placeholder "Comece a digitar para procurar no Fluig Identity", and several navigation icons: a gear for "Configurações", a person icon for "Usuários" (which is highlighted in grey), a group icon for "Grupos", and a list icon for "Recursos". Below the header, there is a section for "Datasul TOTVS" which includes their logo and a "Remover Usuários" button. A search bar below this section contains the text "Nome ou E-mail" and a dropdown menu set to "Todos os Usuários" with the subtext "3 coincidem". The main content area displays three user entries:

User	Email	Action
Ada Harper	ada.harper@email.com	Desprovisionar
Andre Borges	andre.borges@fluig.com	Desprovisionar
John Steel	leoberto.preuss@fluig.com	Desprovisionar

7)

## RAC - RESOURCE ACCESS CONTROL

## RAC - RESOURCE ACCESS CONTROL

Ao criar um aplicativo SCIM no fluig Identity e selecionar a opção **Habilitar Resource Access Control**, o sistema disponibiliza o gerenciamento dos recursos existentes no sistema legado

- Criação, exclusão e atualização de recursos
- Inclusão/remoção de usuários

Recurso de controle de acesso

Habilitar Resource Access Control

Modo RAC

Projeto (GoodData)  Projeto (Powered by GoodData)  Papel

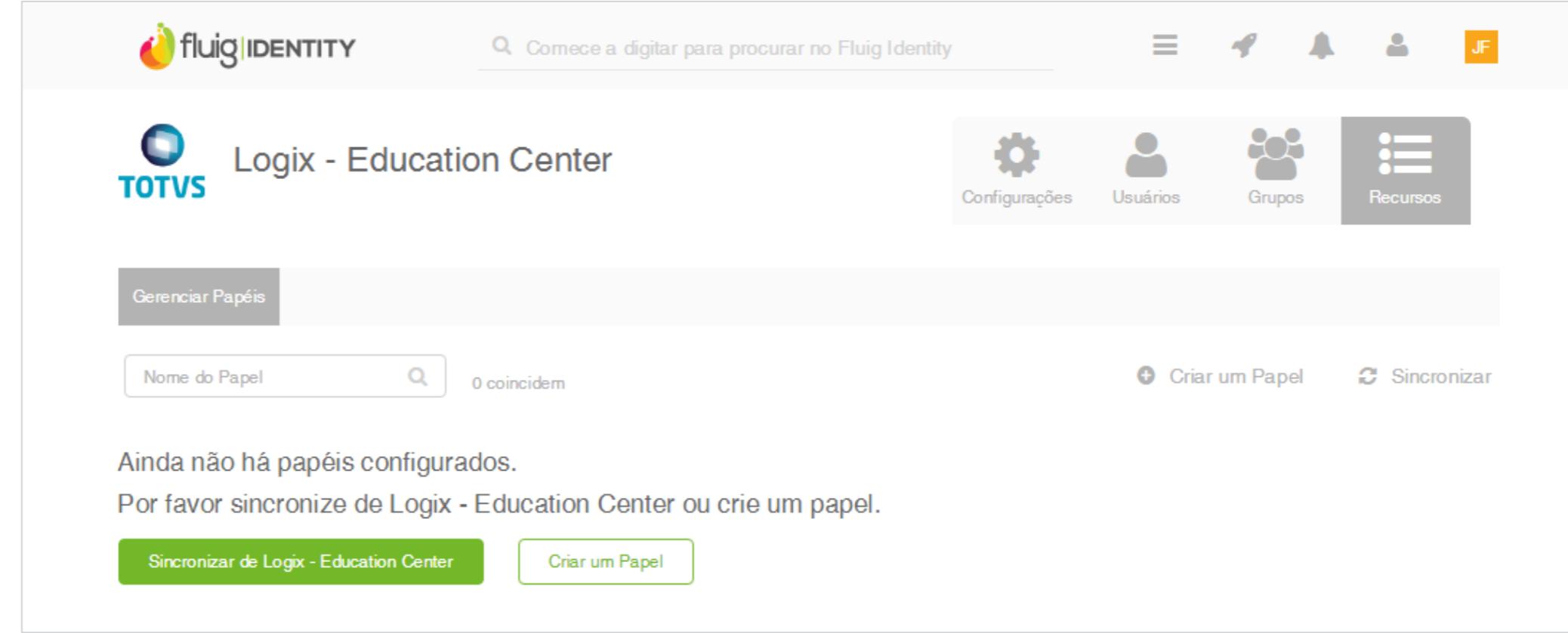
Modelo RAC (Modelo de fluxo UI)

Modelo Básico  
 Modelo Datasul  
 Modelo Fluig  
 Modelo Fluig Identity  
 Modelo Logix  
 Modelo PIMS Multiculture  
 Modelo Protheus  
 Modelo RM  
 Modelo Winthor

Limite de Caracteres no Nome do Papel  Use this field?

Limite de Caracteres na Descrição do Papel  Use this field?

## RAC - RESOURCE ACCESS CONTROL



The screenshot shows the fluig Identity interface for managing resource access control. At the top, there's a header with the fluig logo, a search bar containing "Comece a digitar para procurar no Fluig Identity", and various navigation icons. Below the header, the connection to "Logix - Education Center" is shown, along with its logo (TOTVS). On the right side of the header, there are four main navigation buttons: "Configurações" (Settings), "Usuários" (Users), "Grupos" (Groups), and "Recursos" (Resources), where "Recursos" is highlighted with a grey background. The main content area has a heading "Gerenciar Papéis" (Manage Roles) and a search bar with the placeholder "Nome do Papel". It displays a message stating "Ainda não há papéis configurados. Por favor sincronize de Logix - Education Center ou crie um papel." (There are no roles configured yet. Please synchronize from Logix - Education Center or create a role.) At the bottom, there are two buttons: "Sincronizar de Logix - Education Center" (Sync from Logix - Education Center) and "Criar um Papel" (Create a Role).

É necessário que o SCIM envie todos os recursos existentes no sistema legado para o Identity. Para isso é preciso selecionar a opção **Sincronizar**, no menu Recursos

- O Identity enviará um requisição GET para a URL **[hostname]:[port]/scim/v2/extensions-sync**
- O método será responsável por enviar os recursos (Grupos e Usuários) para o Identity
- Para enviar os grupos podemos utilizar o seguinte comando:

```
client.getScimResourcesService().createApplicationResourcesInBulk("IDCompany", "IDAplicativoECM", "ListaResourcesLegado");
```

Método do objeto **FluigIdentityRestClient**  
Objeto **FluigIdentityRestClient**

Método da interface **ScimResourcesService**,  
responsável por incluir todos os recursos do  
sistema legado no Identity de acordo com o  
aplicativo existente



MÃOS À OBRA!



## EXERCÍCIOS DE FIXAÇÃO

Imagine que está em um projeto de Identity, as atividades são detalhadas abaixo:

5. Usar o conector disponibilizado
6. Criar um papel
7. Associar usuários ao papel

8

)) DESENVOLVIMENTO DE APLICATIVO COM  
PROTOCOLO SAML

SAML é um mecanismo de autenticação segura de padrão aberto, baseado em XML para a troca de dados de autenticação e autorização de acesso entre um provedor de identidade (Identity Provider ou IDP), que atesta e certifica a identidade dos usuários, e um provedor de serviços (Service Provider ou SP)

- O fluig Identity suporta o Single Sign On (SSO) baseado no SAML 2.0
- A autenticação pode ser iniciada tanto pelo SP quanto pelo IDP: 🔑

## SAML

Pode ser baseado em padrões como:

- Extensible Markup Language (XML)
- XML Schema
- XML Signature
- XML Encryption (SAML 2.0 only)
- SOAP
- Hypertext Transfer Protocol (HTTP)
  - Protocolo adotado pelo fluig Identity



A equipe do fluig Identity desenvolveu um SAML Toolkit que pode ajudar qualquer aplicação habilitar/falar SAML

- SAML Toolkit: 
- Este kit de ferramenta fornece suporte para:
  - SAML 2.0
  - Tanto IDP-initiated e SP-initiated SAML SSO

# CONFIGURAR APLICATIVO SAML

- Selecionar se o aplicativo será IDP\_Initiated ou SP\_Initiated
- HTTP\_POST: Para enviar o SAML Response do IDP para o SP POST
- HTTP\_REDIRECT: usado para pequenas mensagens (como SAML request)
- URL da página de login: gerada pelo Identity
- Temporário: usado quando o nome do usuário for opaco ou temporário
- Indeterminado: nome de usuário como “a1b2xyz” (string aleatória)

Visão Geral Entrar Provisionar

Modo de Login

Aplicativo Thick  Plugin  Executável SAML  SAML

Tipo Inic SSO

IDP\_INITIATED  SP\_INITIATED

URL da página de login:

`https://jfwk.thecloudpass.com/cloudpass/IDPInitSSO/recei`

ID da Entidade Específica do Domínio

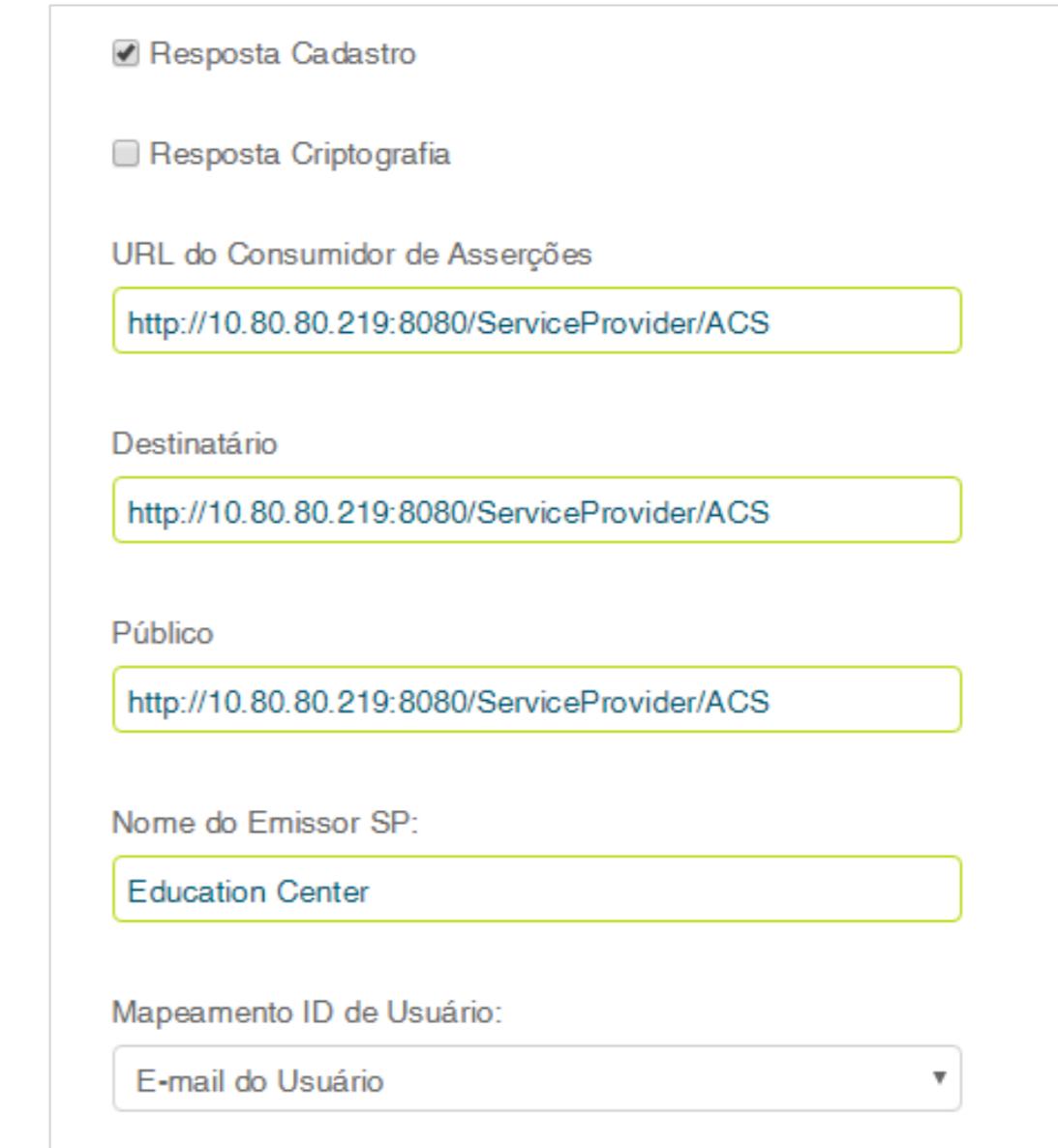
Domínio:

Formato do Name ID

Endereço De Email  Temporário  Indeterminado

## CONFIGURAR APLICATIVO SAML

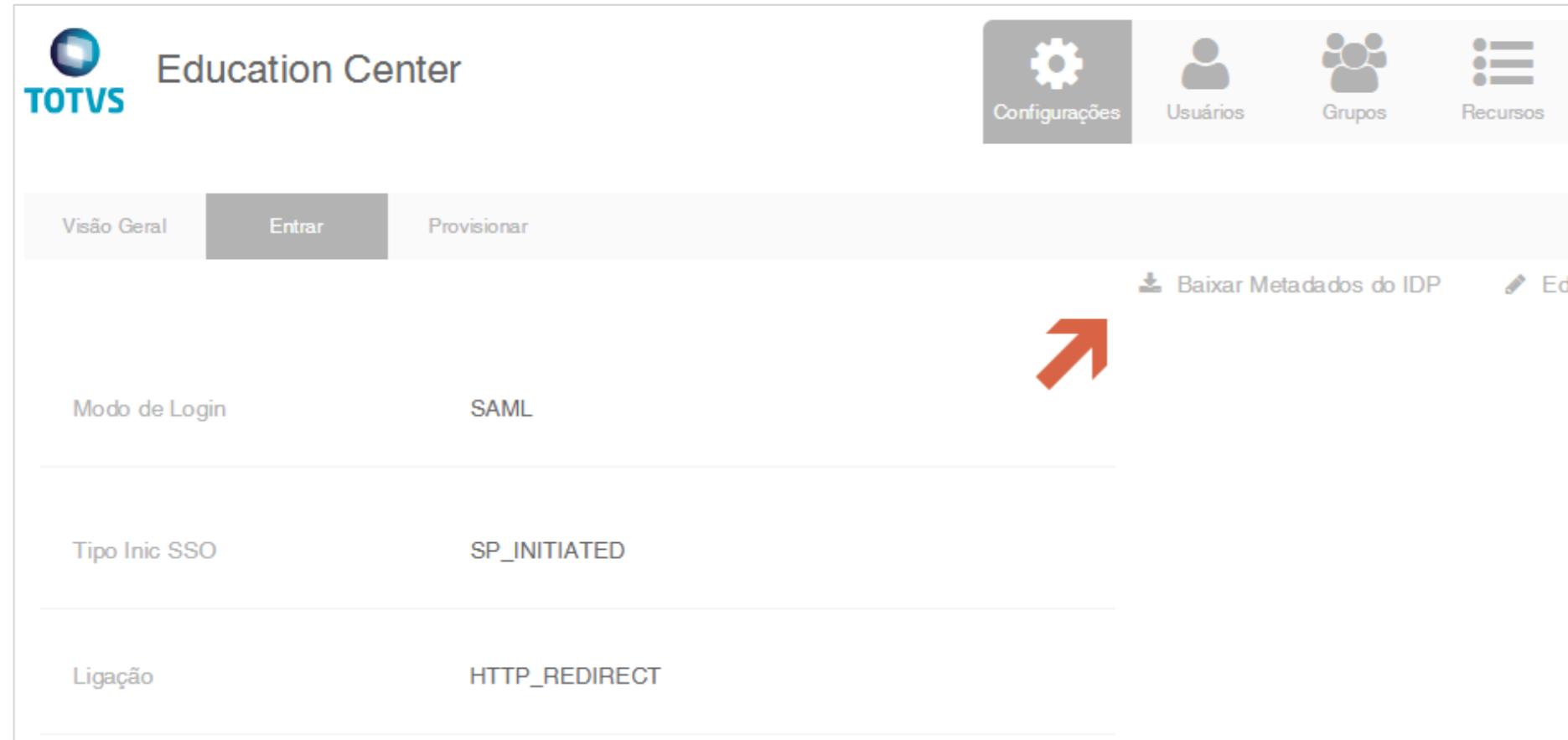
- Resposta cadastro: Recebe a assinatura no XML do SAML Response (ds:Signature)
- Resposta Criptografia: IDM não suporta
- URL Consumo de Asserções, Destinatário e Público: URL que irá receber o SAML Response do Identity
- Nome do Emissor: deve ser o mesmo no arquivo saml.properties
- Mapeamento ID de usuário: usado para ajustar automaticamente o login quando o app for atribuído para um usuário



The screenshot shows a configuration form for a SAML application. It includes the following fields:

- checkboxes for "Resposta Cadastro" (checked) and "Resposta Criptografia" (unchecked)
- "URL do Consumidor de Asserções" field containing <http://10.80.80.219:8080/ServiceProvider/ACS>
- "Destinatário" field containing <http://10.80.80.219:8080/ServiceProvider/ACS>
- "Público" field containing <http://10.80.80.219:8080/ServiceProvider/ACS>
- "Nome do Emissor SP:" field containing [Education Center](#)
- "Mapeamento ID de Usuário:" dropdown menu containing "E-mail do Usuário"

# CONFIGURAR APLICATIVO SAML



The screenshot shows the TOTVS Education Center interface. In the top left, there's a TOTVS logo and the text "Education Center". On the right, there are four navigation icons: "Configurações" (with a gear icon), "Usuários" (with a person icon), "Grupos" (with a group icon), and "Recursos" (with a list icon). Below these are three tabs: "Visão Geral" (selected), "Entrar" (disabled), and "Provisionar". Under "Visão Geral", there are two sections: "Modo de Login" (SAML) and "Tipo Inic SSO" (SP\_INITIATED). At the bottom, it says "Ligaçāo" and "HTTP\_REDIRECT". To the right of the main content area, there's a button labeled "Baixar Metadados do IDP" with a download icon, and a "Editar" button with a pencil icon. A large red arrow points from the text in the adjacent column to this "Baixar Metadados do IDP" button.

Caso o aplicativo seja configurado como SP\_Initiated é necessário baixar os Metadados e informar no “idpDestination” do arquivo saml.properties

```
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"  
Location="https://jvfwk.thecloudpass.com/cloudpass/SPInitPost/receiveSSOResponse/oaq3ssk03f16sxvi1410390042739/317nbccwwwpb2bq1461006374098"/>  
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"  
Location="https://jvfwk.thecloudpass.com/cloudpass/SPInitRedirect/receiveSSOResponse/oaq3ssk03f16sxvi1410390042739/317nbccwwwpb2bq1461006374098"/>
```

- Caso a aplicação Web seja baseada em Java, é recomendável utilizar o **Java Toolkit** que é uma aplicação desenvolvida em Java e que pode ser executada em qualquer servidor de aplicação (Tomcat, JBoss)
- Caso a aplicação seja escrita em outra linguagem recomenda-se utilizar o **REST Toolkit** que é uma aplicação disponível como um serviço REST e pode ser escrito em Java ou .NET

- Composto por duas classes:
  - **RequestGenerator**: responsável por gerar e enviar a autenticação para o IDP (apenas para SP\_Initiated)
  - **AssertionConsumerService**: responsável por receber a resposta SAML do IDP
- E três arquivos:
  - **logback.xml**: configurações do nível de logs
  - **saml.properties**: configurações sobre URL do aplicativo no Identity, caminho do certificado SAML e etc.
  - **web.xml**: conterá as classes em questão com o nome da servlet
- Exemplo: 

1. Ao acessar o endereço do sistema legado para realizar o login no sistema o sistema irá chamar um servlet do Toolkit
2. A classe **RequestGenerator** irá gerar e enviar a requisição de autenticação para o fluig Identity
3. Todas as configurações existentes no arquivo saml.properties serão enviadas para o Identity (**PropertyObject**)
4. O XML de request será gerado e enviado para o Identity de acordo com as configuração do saml.properties

5. O Identity irá validar a requisição usando o `splssuerName`, `idpDestination` e `AssertionConsumerService` URL baseado na especificação SAML
  - Se o usuário não possuir a aplicação associada ao seu perfil no Identity ele irá ter acesso apenas à tela inicial (Launchpad) do Identity
6. Feita a validação o Identity irá enviar a resposta (XML) para o ToolKit de acordo com as configurações realizadas na aplicação (URL do Consumidor de Aserções, Destinatário, Público)
7. A classe `AssertionConsumerService` receberá uma resposta SAML do Identity

8. Seguindo a especificação SAML o ToolKit irá validar o issuer name, assinatura e tempo de validade da resposta SAML
9. Com isso irá retornar para o sistema o primeiro nome, último nome e email do usuário logado no Identity
10. O sistema legado irá fazer as validações necessárias com as informações repassadas
11. Usuário com acesso ao sistema legado

## JAVA TOOLKIT - IDP\_INITIATED

1. Acessando o Identity o usuário irá selecionar o aplicativo SAML desejado
2. O Identity enviará um SAML Response (XML) para o sistema que está configurado para receber a resposta
3. Seguindo a especificação SAML o ToolKit (`AssertionConsumerService`) irá validar o issuer name, assinatura e tempo de validade da resposta SAML

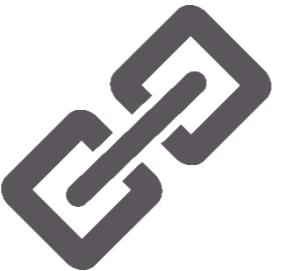
## JAVA TOOLKIT - IDP\_INITIATED

4. Com isso irá retornar para o sistema o primeiro nome, último nome e e-mail do usuário logado no Identity
5. O sistema legado irá fazer as validações necessárias com as informações repassadas
6. Usuário com acesso ao sistema legado



## XML REQUEST / RESPONSE

Exemplos:





MÃOS À OBRA!



## EXERCÍCIOS DE FIXAÇÃO

7. Baixar o Certificado SAML (fluig Identity > Configurações > Segurança)
  
8. Utilizar o projeto disponibilizado para realizar a integração do Identity com o Java Toolkit:
  - SP\_INITIATED
  - IDP\_INITIATED

## CANAIS DE COMUNICAÇÃO FLUIG

- Site: [fluig.com](http://fluig.com)
- Documentação: [dev.fluig.com](http://dev.fluig.com)
- Guia de Relacionamento: [!\[\]\(ccfcb8aa8843ab31465ed736799d3183\_img.jpg\)](#)
- Suporte: [suporte.fluig.com](http://suporte.fluig.com)
- Comunidade DEV fluig: [!\[\]\(5a3182a4731c23cc618d5c684ad69253\_img.jpg\)](#)
- Blog: [fluig.com/blog](http://fluig.com/blog)
- YouTube: [youtube.com/fluigplatform](http://youtube.com/fluigplatform)
- SlideShare: [pt.slideshare.net/fluig](http://pt.slideshare.net/fluig)
- Scribd: [scribd.com/fluigplatform](http://scribd.com/fluigplatform)



Acompanhe os canais sociais de fluig:

/fluigplatform

pt.scribd.com/fluigplatform

/fluigplatform

/company/fluig

pt.slideshare.net/fluig

/fluig.com/blog

**www.fluig.com**  
**0800 882 9191**

# OBRIGADO!

**FLUIG EDUCATION CENTER**

E-mail: [fluig.education.center@fluig.com](mailto:fluig.education.center@fluig.com)

Fone: (11) 2099-7337



**fluig**  
FLOWING  
PRODUCTIVITY