Single Sign-On

Como configurar o Single Sign-On (SSO) utilizando o AD e o ADFS.

- Configurar integração com o AD (Active Directory)
- Configurar integração com o ADFS (Active Directory Federation Services)

Configurar integração com o AD (Active Directory)

Você pode utilizar os seus usuários do Active Directory para login no agilityflow, assim o usuário de rede será único, e fará um single sign-on nas aplicações do agilityflow.

Para isso iremos fornecedor 2 scripts ASP clássico e você deve configura-los no seu servidor. Abaixo segue os procedimentos para essa instalação.

O script será hospedado no servidor IIS e terá acesso ao Active Directory para autenticar usuários no Agilityflow.

Se você quiser configurar o SSO usando o padrão universal SAML, consulte nesse link, sobre o uso do SAML no Agilityflow através do ADFS.

> **Recomendação importante:** Após finalizar a configuração do AD no Agilityflow. Faça o teste em uma guia anônima do seu navegador antes de fazer o logout da sua sessão atual do Agilityflow. Assim você conseguirá fazer as mudanças necessárias no Agilityflow caso sua configuração não esteja correta. Caso você faça o logout, entre em contato conosco para auxiliarmos no passo a passo.

Pré-requisitos

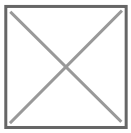
- Uma instância do Active Directory instalada no seu servidor. Você pode seguir as etapas fornecidas neste artigo para configurar e instalar o AD no seu servidor
- Garantir que todos os usuários do AD tenham o atributo de endereço de e-mail preenchido. O Agilityflow utiliza o **e-mail** e o **login** do usuário como identificador para autenticação. Portanto, além do login, é necessário que o usuário tenha o endereço de e-mail preenchido no Active Directory.

  > Caso você receba do Agilityflow a mensagem “**O usuário 'xxxx' não tem o e-mail cadastrado no AD.** ”, verifique se o endereço de e-mail está configurado para esse usuário no Active Directory, se não estiver, fale com o seu administrador de rede. Abaixo estão descritos os procedimentos para configuração do e-mail do usuário no AD.

Para preencher o e-mail do usuário no AD: acesse o seu Active Directory, no painel esquerdo clique em **Users**, agora no painel da direita, clique com o botão direito no usuário que deseja alterar o e-mail, clique em "**Properties**" e no campo "**E-mail**" inclua o e-mail do usuário. As imagens abaixo ilustram esse passo a passo:

Selecione o usuário:

Altere o e-mail:



Clique em OK e o e-mail estará incluído nesse usuário.

Esse procedimento será necessário para todos os usuários que não estão com e-mail configurado no AD.

PASSO 1: Instalando o Internet Information Services (IIS)

O Internet Information Server (Gerenciador do IIS) deve ser configurado no seu Windows Server para hospedar o arquivo de script ASP Clássico, que acessará as informações do usuário no Active Directory.

> O IIS Server deve estar instalado no mesmo domínio do Active Directory que contém os usuários.

Você pode seguir as etapas fornecidas neste artigo para instalar o IIS no Windows Server 2012. Escolha as opções a seguir ao instalar a função IIS no servidor.

- **Web Server (IIS)**
  - **Security**
    - **Windows Authentication**
  - **Application Development**
    - **ASP**
- **Management Tools**
  - **IIS Management Console**

Você precisa do **Windows Authentication** e também do **ASP** no seu servidor para hospedar e rodar o script ASP clássico que forneceremos a seguir e que será o responsável pelo login dos usuários do Active Directory no Agilityflow. Portanto, se você já instalou o IIS, verifique se esses recursos estão instalados.

PASSO 2: Editando o arquivo de script ASP clássico

1. Baixe os arquivos default.asp e config.asp que estão disponíveis na área de configuração do seu ambiente no agilityflow.

Os arquivos para download você encontra nesse link:

https://<SEU_AMBIENTE>.agilityflow.io/configuration ou através do menu: Customizar Agilityflow → Single Sign-On, AD e ADFS. → depois na ABA: "Autenticação de usuário" → "AD" você encontrará o link para download.

2. Abra o arquivo config.asp e atribua esses valores às variáveis:

- **agilityflowUrl**: url onde o seu sistema do agilityflow está hospedado, geralmente as aplicações ficam na url: https://<SEU_AMBIENTE>.agilityflow.io/ . é importante que a url termine com a barra **/**

- **LDAP_UserName_WithAccessToReader**: Nome de usuário da conta do AD que tem pelo menos privilégio de leitura para todos os usuários no AD. (preencha com no formato: "dominioDaMinhaEmpresa\usuarioadmin")
- **LDAP_UserPassword_WithAccessToReader**: Senha dessa conta de usuário

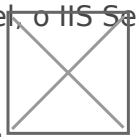
- **agilityflowADToken**: token de segurança gerado pelo agilityflow que será o código de segurança com o seu AD. Esse token pode ser copiado através do menu: Customizar Agilityflow → Single Sign-On, AD e ADFS → depois na ABA: "Autenticação de usuário" → "AD" copiei do campo "Token"

Exemplo de preenchimento do arquivo config.asp

agilityflowUrl = "https://nomedaempresa.agilityflow.io"
LDAP_UserName_WithAccessToReader = "dominioDaMinhaEmpresa\usuarioadmin"
LDAP_UserPassword_WithAccessToReader = "xxxxxxxxxx"
agilityflowADToken = "xxxxxxxxxxxxxxxxxxxxxxxxxx"

PASSO 3: Configurando o script ASP no IIS

1. Crie um website ou um application dentro do seu website padrão no IIS. Para criar um novo website no IIS, consulte a seção Criar um novo website neste artigo.
2. Clique no website e clique duas vezes em **ASP** no painel direito. Defina a opção **Enable Parent Paths** para **true**.

3. Clique no website novamente e clique duas vezes em **Authentication**. Clique com o botão direito do mouse em **Windows Authentication** e clique em **Enable**. Desative todos os outros tipos de autenticação. O IIS usará a autenticação integrada do Windows (**Integrated Windows Authentication**). Para tornar isso possível, o IIS Server deve ser instalado no domínio do Active Directory que contém os usuários.

4. Agora clique com o botão direito do mouse no website, clique em **Explore** e cole os 2 arquivos - **default.asp** e **config.asp** que já estão configurados.

PASSO 4: Configurar o Single Sign-on no Agilityflow

1. Vá para o menu Customizar Agilityflow → Single Sign-On, AD e ADFS.
2. Na aba "Autenticação de usuário (Login) / Single Sign-On" no campo **Tipo de Autenticação** selecione **"AD"**
3. No campo "**URL para realizar o login**" - Digite o URL que o Agilityflow chamará quando os usuários tentarem fazer login. Essa URL deve apontar para o website com o script ASP que você acabou de criar, nos passos anteriores. Cole a URL de navegação do arquivo default.asp. Exemplo: se o seu website foi criado na URL: **https://www.xyz.com/agilityflowAuthService** então você deve preencher esse campo com o a URL: **https://www.xyz.com/agilityflowAuthService/default.asp** verifique se todas as chamadas do IIS feitas para esse script estão com **Windows Authentication** e não **Anonymous Authentication**.

Pronto, agora abra uma guia anônima do seu navegador e tente realizar o login no agilityflow.

Se você enfrentar algum problema durante a configuração, entre em contato conosco.

Pronto, as configurações foram finalizadas.

> **Recomendação importante:** Após finalizar a configuração do AD no Agilityflow. Faça o teste em uma guia anônima do seu navegador antes de fazer o logout da sua sessão atual do Agilityflow. Assim você conseguirá fazer as mudanças necessárias no Agilityflow caso sua configuração não esteja correta. Caso você faça o logout, entre em contato conosco para auxiliarmos no passo a passo.

Configurar integração com o ADFS (Active Directory Federation Services)

O agilityflow oferece suporte Single Sign-on (SSO) por meio do SAML 2.0. O ADFS é um serviço fornecido pela Microsoft como uma função padrão do Windows Server que fornece um login da Web usando as credenciais existentes do Active Directory.

Com essa configuração você pode utilizar os seus usuários do Active Directory para login no agilityflow, assim o usuário da rede será usado no single sign-on do agilityflow.

> **Recomendação importante:** Após finalizar a configuração do ADFS no agilityflow. Faça o teste em uma guia anônima do seu navegador antes de fazer o logout da sua sessão atual do agilityflow. Assim você conseguirá fazer as mudanças necessárias no agilityflow caso sua configuração não esteja correta. Caso você faça o logout, entre em contato conosco para auxiliarmos no passo a passo.

Pré-requisitos

1. Uma instância do Active Directory instalada no seu servidor. Você pode seguir as etapas fornecidas neste artigo para configurar e instalar o AD no seu servidor.
2. Uma instância do ADFS instalada no seu servidor. Você pode seguir as etapas fornecidas neste artigo para configurar e instalar o ADFS no seu servidor
3. Garantir que todos os usuários do AD tenham o atributo de endereço de e-mail preenchido. O agilityflow utiliza o **e-mail** e o **login** do usuário como identificador para autenticação. Portanto, além do login, é necessário que o usuário tenha o endereço de e-mail preenchido no Active Directory.

   Então, caso você receba do agilityflow a mensagem “**O usuário 'xxxx' não tem o e-mail cadastrado no AD.** ”, verifique se o endereço de e-mail está configurado para esse usuário no Active Directory, se não estiver, fale com o seu administrador de rede. Abaixo estão descritos os procedimentos para configuração do e-mail do usuário no AD.

   Para preencher o e-mail do usuário no AD: acesse o seu Active Directory, no painel esquerdo clique em **Users**, agora no painel da direita, clique com o botão direito no

usuário que deseja alterar o e-mail, clique em "**Properties**" e no campo "**E-mail**" inclua o e-mail do usuário. As imagens abaixo ilustram esse passo a passo:

Selecione o usuário:

Altere o e-mail:

Clique em OK e o e-mail estará incluído nesse usuário.

Esse procedimento será necessário para todos os usuários que não estão com e-mail configurado no AD.

PASSO 1: Configurar o ADFS

Neste ponto, você deve estar pronto para configurar a conexão do ADFS com sua conta do agilityflow. A conexão entre o ADFS e o agilityflow é definida usando um Relying Party Trust (RPT).

Abra o **AD FS Management**, no menu da esquerda, abra a guia **Trust Relationships**, clique com o botão direito em **Relying Party Trusts** e então clique em **Add Relying Party Trust**

1. Isso inicia o assistente de configuração do Relying Party Trust. Clique em **Start**.

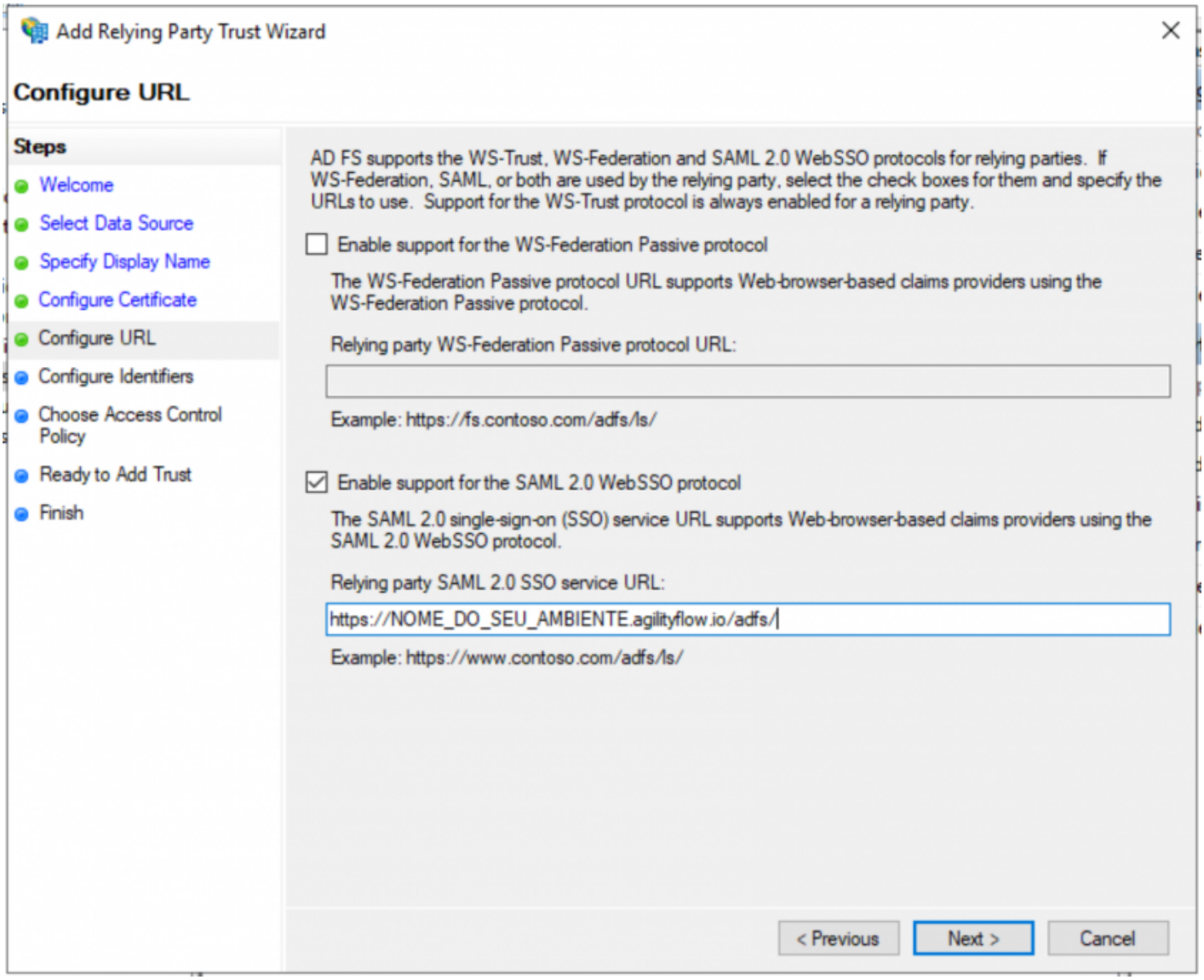
2. No passo **Select Data Source**, selecione a última opção: **Enter Data About the Party Manually.**

3. No passo **Specify Display Name**, insira um nome para esse Relying Party Trust. Informe o nome **agilityflow**.

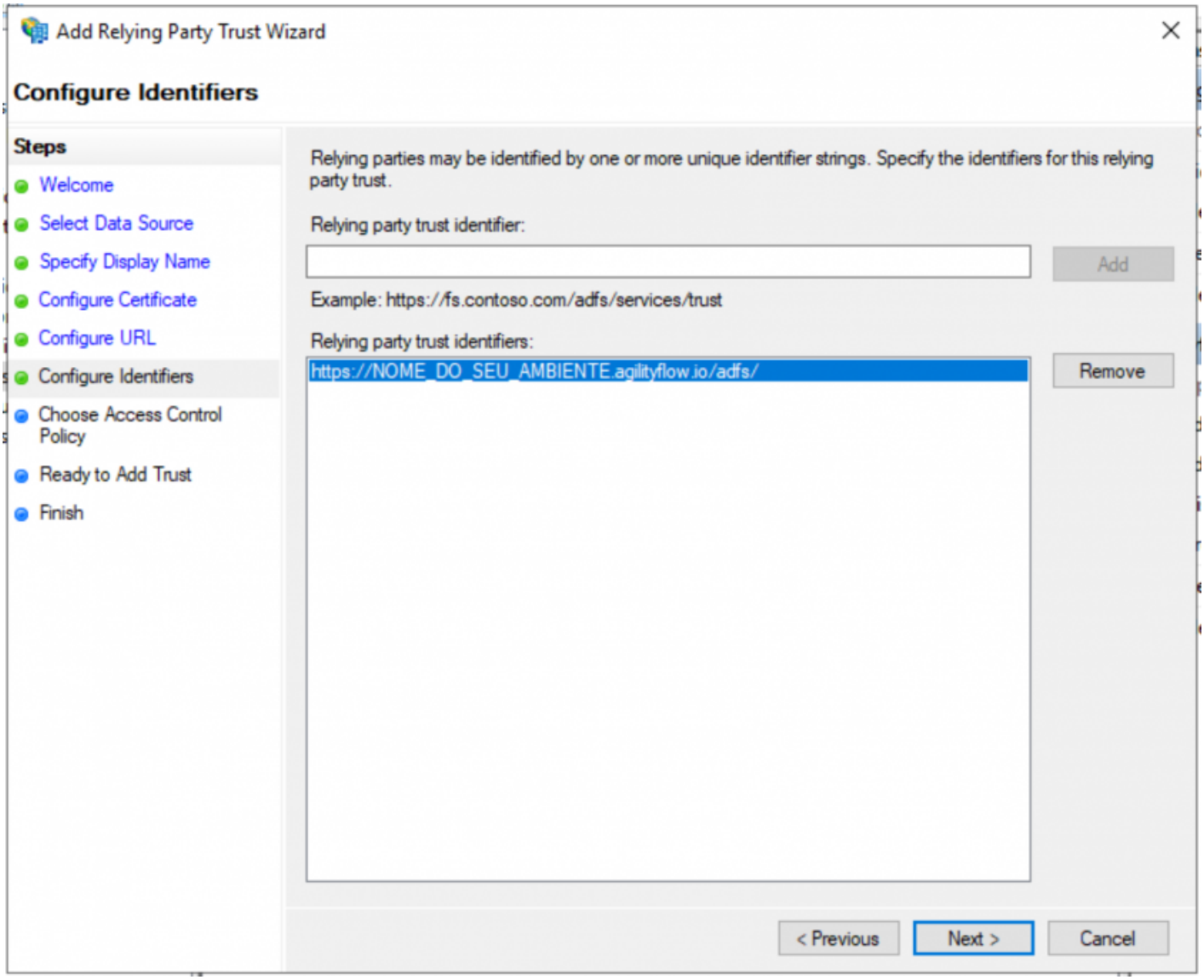
4. No passo **Choose Profile**, mantenha a opção **ADFS FS profile**

5. No passo **Configure Certificate**, mantenha as configurações da forma que estão e clique em **Next**.

6. No passo **Configure URL**, marque a opção **Enable support for the SAML 2.0 WebSSO protocol** e em **Relying party SAML 2.0 SSO service URL** informe **https://<SEU_AMBIENTE>.agilityflow.io/adfs/**



7. No passo **Configure identifiers** informe **https://<SEU_AMBIENTE>.agilityflow.io/adfs/** em **Relying party trust identifier** e clique em **Add**, na sequencia, clique em **Next.**



8. No passo **Configure Multi-factor Authentication Now?**, mantenha as configurações da forma que estão e clique em **Next.**

9. No passo **Choose Issuance Authorization Rules**, mantenha a opção **Permit all users to access the relying party** marcada e clique em **Next.**

10. No passo **Ready to Add Trust,** mantenha as configurações da forma que estão e clique em **Next.**

11. No passo **Finish,** mantenha marcada a opção **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** e clique em **Close**;

12. Na nova janela que abrirá, clique em **Add rule**

13. No passo **Choose Rule Type,** no campo **Claim rule Template** selecione a opção **Send LDAP Attributes as Claims** e clique em **Next.**

14. No passo **Configura Claim Rule** preencha da seguinte forma:

Em **Claim rule name** informe "**LDAP E-mail, Username".** Em **Attribute store** selecione **Active Directory.** Na tabela **Mapping of LDAP attributes to outgoing claim types** preencha da seguinte forma:

LDAP Attribute	**Outgoing claim type**
SAM-Account-Name	Name ID
E-Mail-Addresses	E-Mail Address

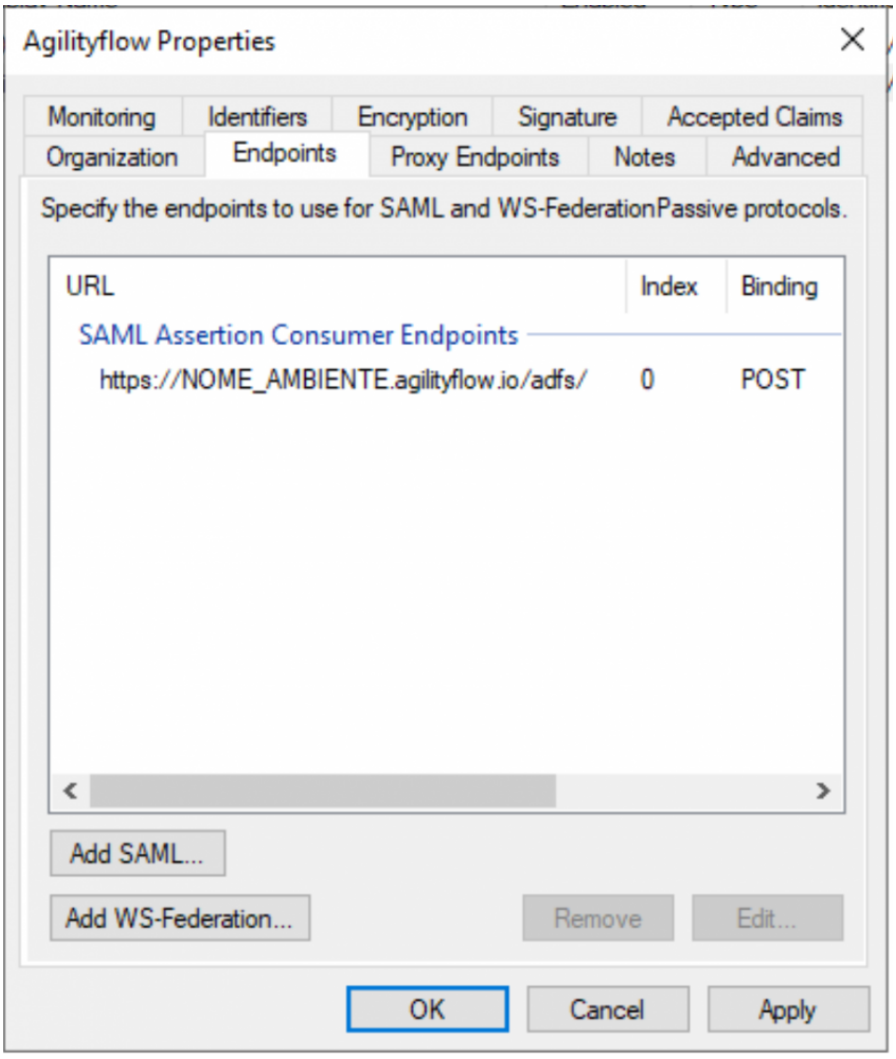
Depois clique em **Finish e OK**

15. Depois de confirmar e fechar o **Claim Rules dialog,** Vá até a lista de **Relying Party Trusts** e

clique com o botão direito em **agilityflow** e selecione a opção **Properties.**

16. Na aba **Advanced**, selecione **SHA-256** no campo **Secure hash algorithm.**

17. Na aba **Endpoints**, clique em **Add SAML** para adicionar um novo endpoint



18. Na nova janela que abrirá chamada **Add an Endpoints**, preencha os campos da seguinte forma:

- Em **Endpoint type** escolha **SAML Logout**
- Em **Binding** mantenha a opção **POST**

- Em **Trusted URL** informe a URL concatenando as seguintes informações
  1. O endereço da web do seu servidor ADFS, exemplo: "**https://www.seudominio.com"**
  2. O endpoint SAML configurado no ADFS. Por padrão (se você não alterou essa configuração) será: **"/adfs/ls"**
  3. E por fim, concatene os parâmetros "**?wa=wsignout1.0**"

  A sua url final deverá ficar parecida com essa : **https://www.seudominio.com/adfs/ls?wa=wsignout1.0**

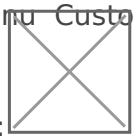
Após isto, clique em **OK**;

19. Isto conclui a configuração do ADFS, clique em Apply e depois em OK;

PASSO 2: Configurar o Single Sign-on no agilityflow

> **Recomendação importante:** Após finalizar a configuração do ADFS no agilityflow. Faça o teste em uma guia anônima do seu navegador antes de fazer o logout da sua sessão atual do agilityflow. Assim você conseguirá fazer as mudanças necessárias no agilityflow caso sua configuração não esteja correta. Caso você faça o logout, entre em contato conosco para auxiliarmos no passo a passo.

Acesse via browser a sua instância do agilityflow.

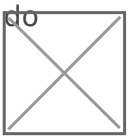
1. Vá para o menu Customizar agilityflow → Single Sign-On, AD e ADFS, será aberta a seguinte tela: 
2. Na aba "**Autenticação de usuário (Login) / Single Sign-On"** no campo **Tipo de Autenticação** selecione **"ADFS"**
3. No campo "**URL para realizar o login**" - Digite a URL do seu servidor ADFS que o agilityflow chamará quando os usuários tentarem fazer login. Essa URL geralmente termina em **IdpInitiatedSignOn.aspx**. Por exemplo, se o link de início for **https://www.seudominio.com/adfs/ls/**, a página de login será **https://www.seudominio.com/adfs/ls/IdpInitiatedSignOn.aspx.**

4. No campo "**Url para realizar o logoff**" insira a mesma URL que você inseriu no campo "**Trusted URL**", descrito aqui nesse tópico essa é a URL que o agilityflow chamará para o usuário fazer logout do ADFS. Essa URL geralmente termina em "**?wa=wsignout1.0**". Por exemplo, se o link de início for **https://www.seudominio.com/adfs/ls**, a página de logout será

   https://www.seudominio.com/adfs/ls?wa=wsignout1.0

5. Para o preenchimento do campo **Certificado (X. 509),** você precisará voltar ao seu servidor ADFS e seguir o seguintes passos:
   1. Abra o seu Windows Server, abra **Administrative Tools** no menu Iniciar do Windows ou em **Control Panel** e abra o aplicativo **AD FS Management.**

   2. No menu da esquerda, abra a guia **Service** → **Certificates**

   3. No painel da direita, clique duas vezes no certificado Token-signing que você deseja usar.

   4. Clique na aba **Details** e clique em **Copy to File**

   5. Clique em **Next** no assistente de exportação e selecione a opção **Base-64 encoded X.509 (.CER)**

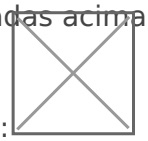
      

   6. Salve o arquivo de certificado em seu sistema de arquivos local

   7. Abra o certificado que você acabou de salvar em um editor de texto.

8. Apague do conteúdo do certificado as linhas inicias e linhas finais
   Linha inicial para apagar **"-----BEGIN CERTIFICATE-----"**
   Linha final para apagar **"-----END CERTIFICATE-----"**
   Essas informações não podem constar no campo **Certificado (X. 509)** do agilityflow
9. Depois de apagar as duas linhas citadas acima, copie o conteúdo desse certificado

   que deve ser algo como esse abaixo:
10. Agora volte na sua instância do agilityflow e cole o conteúdo desse certificado no campo de texto **Certificado (X. 509).**

Salve e pronto, as configurações foram finalizadas.

Se você enfrentar algum problema durante a configuração, entre em contato conosco.

> **Recomendação importante:** Após finalizar a configuração do ADFS no agilityflow. Faça o teste em uma guia anônima do seu navegador antes de fazer o logout da sua sessão atual do agilityflow. Assim você conseguirá fazer as mudanças necessárias no agilityflow caso sua configuração não esteja correta. Caso você faça o logout, entre em contato conosco para auxiliarmos no passo a passo.