Configurar Autenticação Externa de SSO SAML com AD FS para ESA e SMA

Contents

Introdução

Este documento descreve como configurar o Ative Diretory Federation Services como provedor de identidade SAML para autenticação externa no Cisco ESA e SMA.

Pré-requisitos

Este documento fornece uma visão do aplicativo de terceiros que os engenheiros não podem ver de outra forma.

- Etapas de configuração da autenticação externa da SAML (Security Assertion Markup Language) com os Serviços de Federação do Ative Diretory (AD FS) 2012 e 2016 para as versões mais recentes do Cisco Email Security Appliance (ESA) e do Security Management Appliance (SMA).
- Etapas básicas baseadas em laboratório que não incluem configurações específicas de implantação especializada.
- Um exemplo funcional de um ambiente de laboratório que pode ser diferente de uma implantação de produção.

⚠ Caution: Conclua a configuração do provedor de serviços (SP) antes deste procedimento. Consultar.

Requisitos

- Serviços de Federação do Microsoft Ative Diretory (AD FS) 2012 ou 2016
- Cisco Email Security Appliance (ESA) e Security Management Appliance (SMA) versão mais recente.

Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

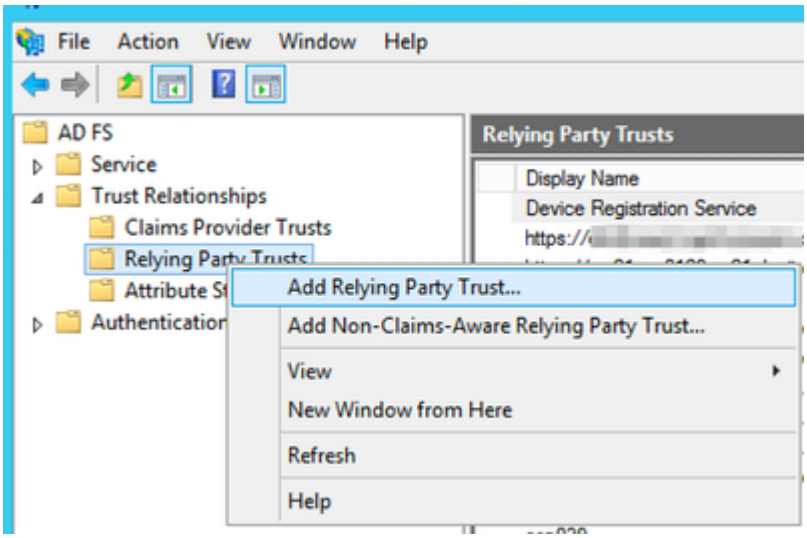
Etapas para Configuração de IDP do ADFS para SAML

Configurar a Confiança da Terceira Parte Confiável

Use uma das duas opções para criar a confiança da terceira parte confiável no AD FS.

Método A: Criar o Objeto de Confiança da Terceira Parte Confiável Importando Metadados SP

1. Abra o console AD FS Management em Administrative Tools.
2. No console de Gerenciamento do AD FS, expanda Relações Confiáveis, clique com o botão direito do mouse em Relações de Confiança de Terceira Parte Confiável e selecione Adicionar Relação de Confiança de Terceira Parte Confiável.



Adicionar Confiança da Terceira Parte Confiável

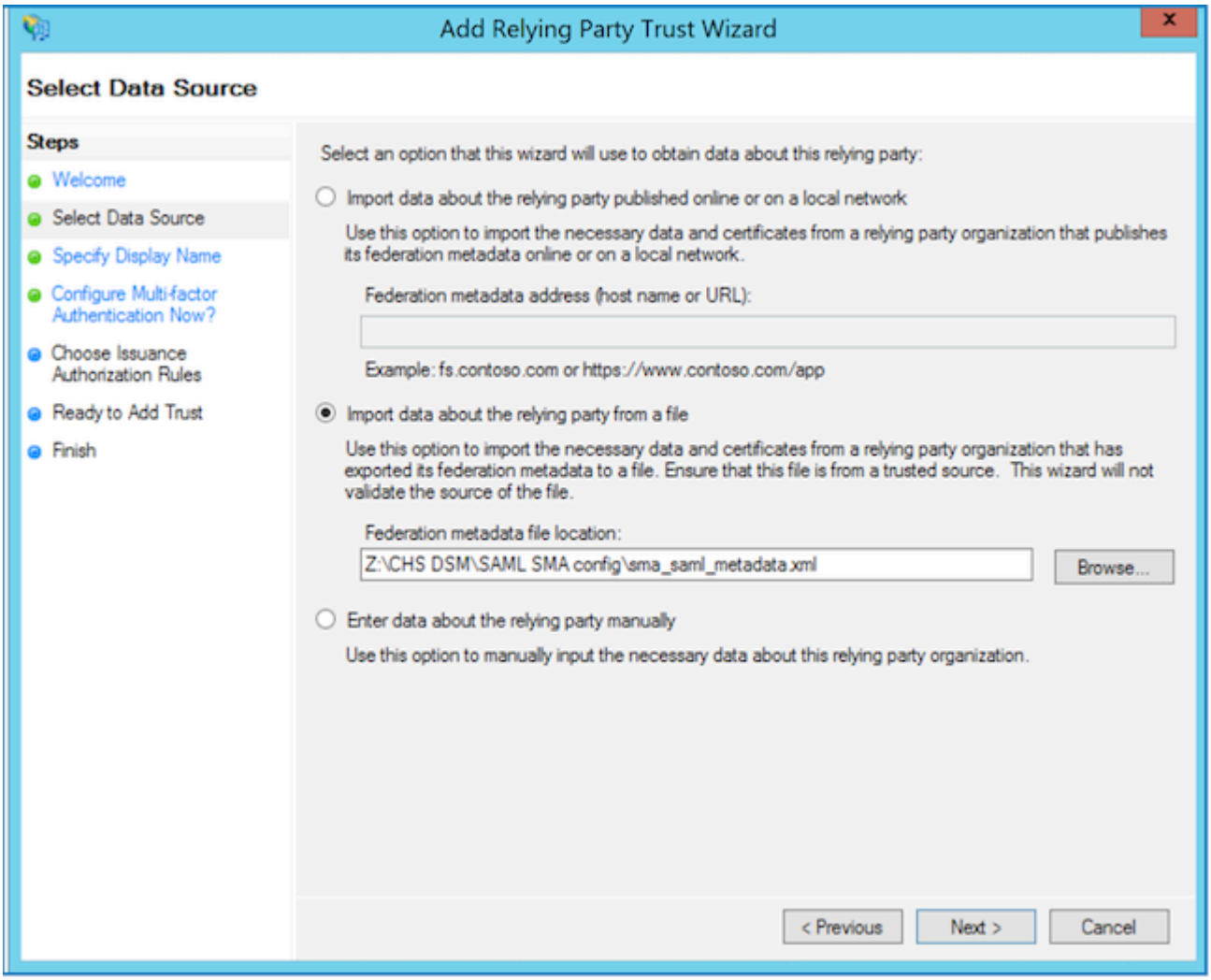
Tip: Confiança da Terceira Parte Confiável da Microsoft

Continue usando uma destas duas opções:

- Opção A: Importar dados sobre a terceira parte confiável de um arquivo. Carregue o arquivo metadata.xml do provedor de serviços (SP) do ESA ou SMA.
- Opção B: Insira os dados sobre a terceira parte confiável manualmente. Esta opção o orienta na configuração manual.

Opção A: Importar dados sobre a terceira parte confiável de um arquivo. Carregue o arquivo metadata.xml do ESA ou do provedor de serviços (SP) do SMA.

1. Selecione a opção para importar dados sobre a terceira parte confiável de um arquivo e selecione Próximo.



Importar o arquivo de metadados ESA/SMA

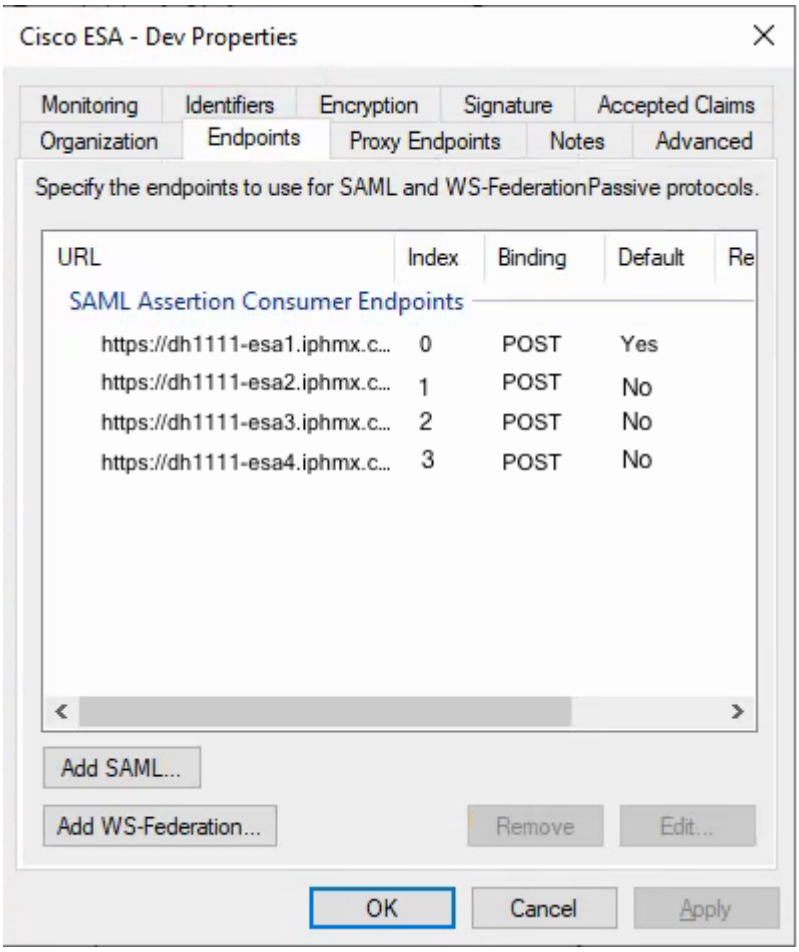
- Especifique um nome de exibição para identificar esta confiança da terceira parte confiável e selecione Avançar duas vezes.
- Para regras de autorização de emissão, selecione Permitir todos os usuários e, em seguida, selecione Avançar.
- Na página Ready to Add Trust, aceite as configurações padrão e selecione Next.
- Selecione Finish. Isso abre a caixa de diálogo Editar regras de reivindicação para o objeto de confiança da terceira parte confiável, que é abordado em Regras de transformação de emissão - Reivindicações.

Propriedades da Confiança da Terceira Parte Confiável - Pontos de Extremidade

Execute esta etapa apenas se vários ESAs estiverem presentes em um cluster.

1. Abra Propriedades de Confiança da Terceira Parte Confiável > Pontos de Extremidade.
2. Adicione cada endereço URL acessível do ESA e selecione OK.
3. Os valores de índice contam a partir de 0, ou seja, 0, 1, 2 e 3.
4. Defina apenas uma entrada como Padrão = Sim.

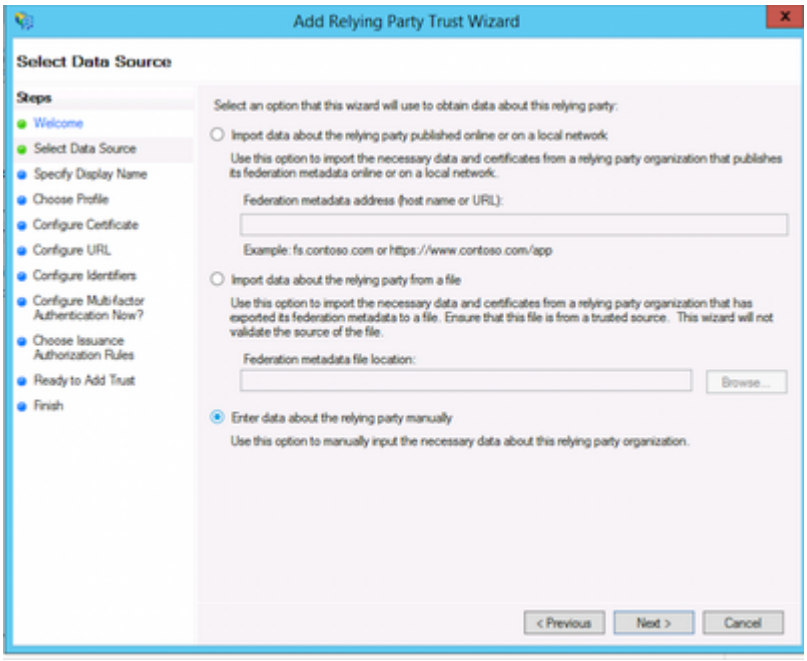
5. Defina as entradas restantes como Padrão = Não.



Propriedades da Confiança da Terceira Parte Confiável - Pontos de Extremidade

Opção B: Insira os dados sobre a terceira parte confiável manualmente. Esta opção o orienta na configuração manual.

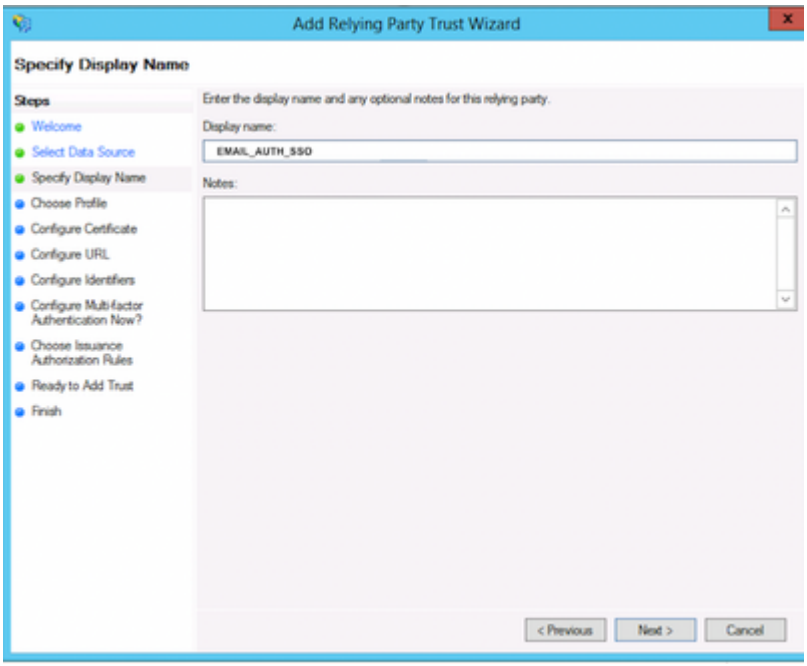
1. Selecione Inserir dados sobre a terceira parte confiável manualmente.



Adicionar terceira parte confiável manualmente

Tip: Nome de exibição é o nome escolhido para identificar o objeto de confiança da terceira parte confiável para ESA ou SMA SAML.

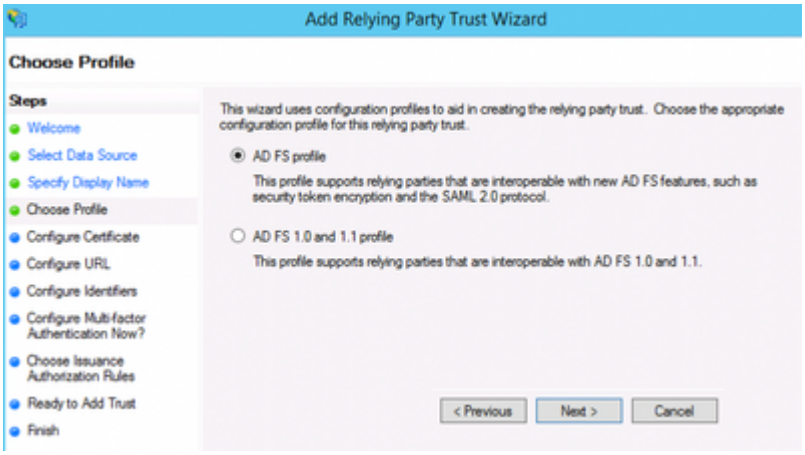
1. Insira um display name para o provedor de serviços, por exemplo, ESA_SP.



Crie um nome para o Perfil do provedor de serviços

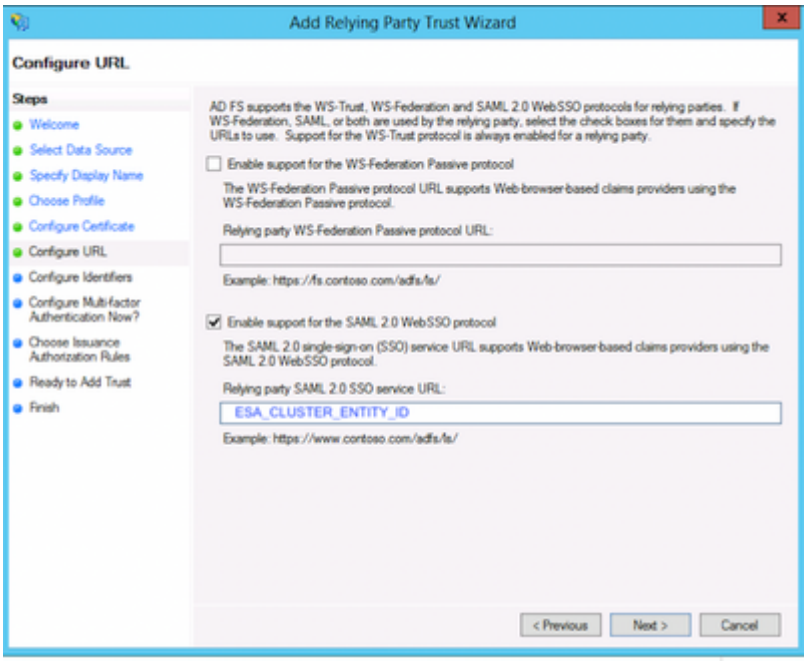
Tip: A função das regras de reivindicação e das regras de transformação de emissão

1. Escolha a opção de perfil Perfil do AD FS.



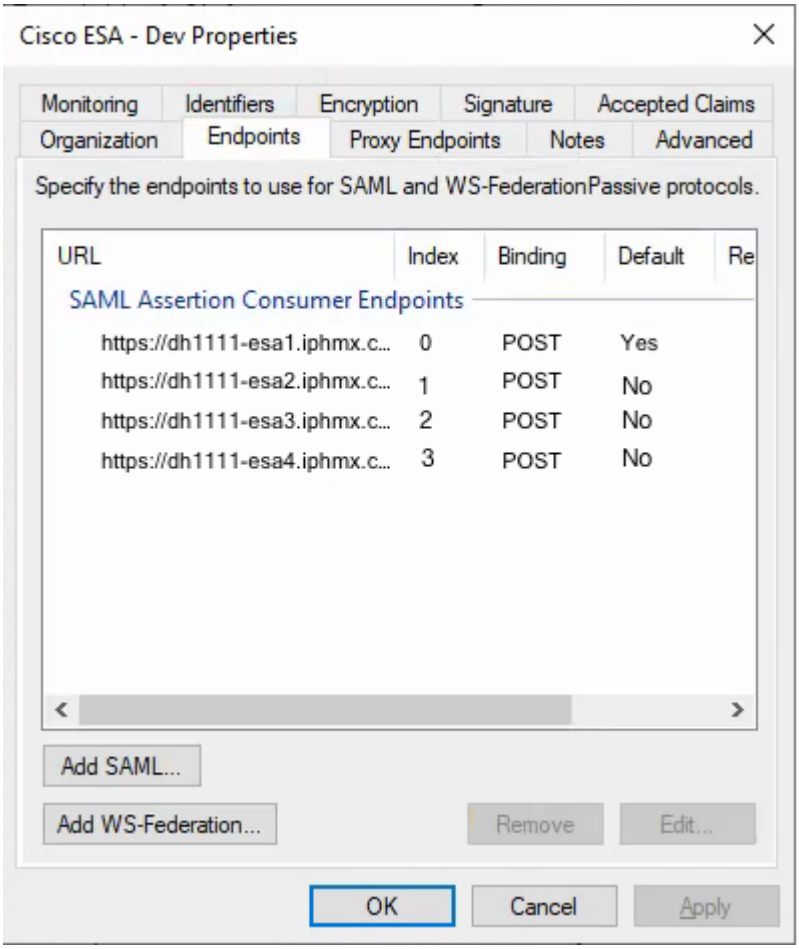
Opção de Perfil do AD FS para Utilizar o SAML 2.0

1. Carregue o certificado público da configuração do provedor de serviços (SP) do ESA.
2. Para Configurar URL, escolha Ativar suporte para o SSO do SAML 2.0.
3. Insira a URL do serviço SSO SAML 2.0 da terceira parte confiável com o valor do perfil SP ID da entidade.



Regras de Autorização de Emissão - Permitir Todos os Usuários

1. Para regras de autorização de emissão, escolha Permitir que todos os usuários acessem esta terceira parte confiável.



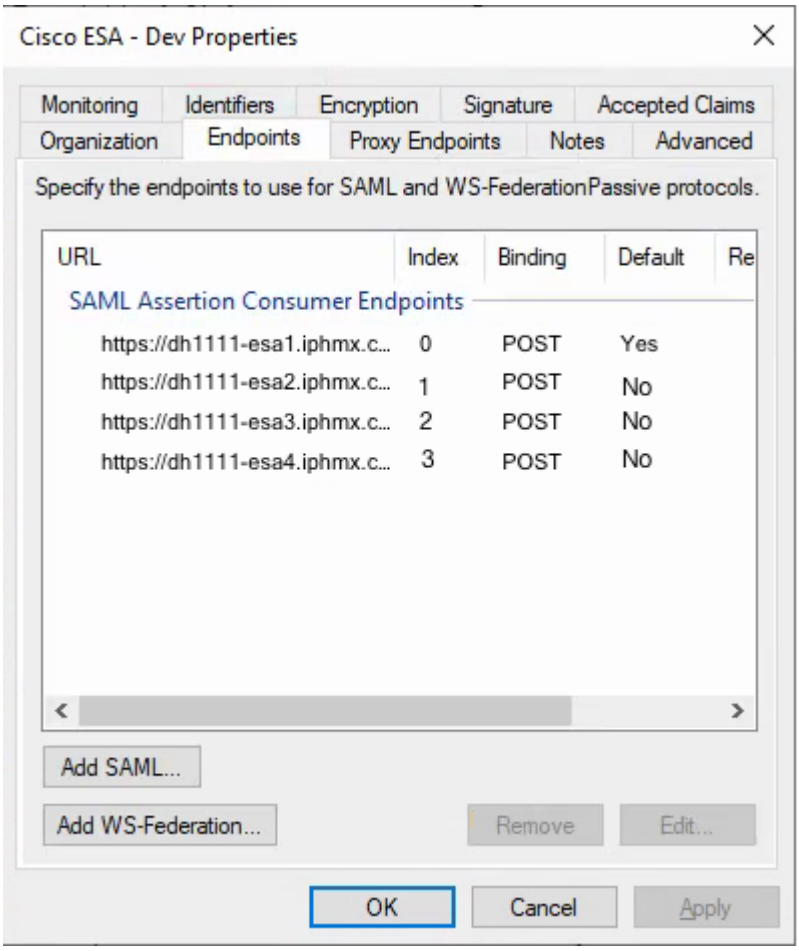
Escolher Regras de Autorização de Emissão

1. Selecione Próximo para ir para a página Finalizar.

Configurar Pontos de Extremidade de Confiança da Terceira Parte Confiável (Somente Clusters)

Execute esta etapa apenas se vários ESAs estiverem presentes em um cluster.

1. Abra Propriedades de Confiança da Terceira Parte Confiável > Pontos de Extremidade.
2. Adicione cada endereço de URL acessível do ESA e clique em OK.
3. Defina endpoint index values começando em 0 (por exemplo, 0, 1, 2, 3).
4. Defina apenas um ponto final como Padrão = Sim. Defina os pontos de extremidade restantes como Padrão = Não

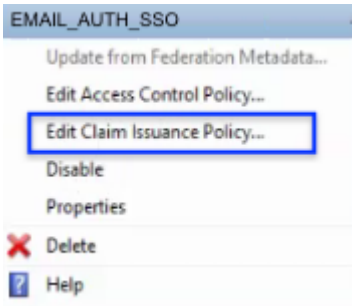


Regras de Autorização de Emissão - Permitir Todos os Usuários

- A etapa Finalizar inicia a caixa de diálogo Editar regras de declaração para o objeto de confiança da terceira parte confiável, abordado em Regras de transformação de emissão.

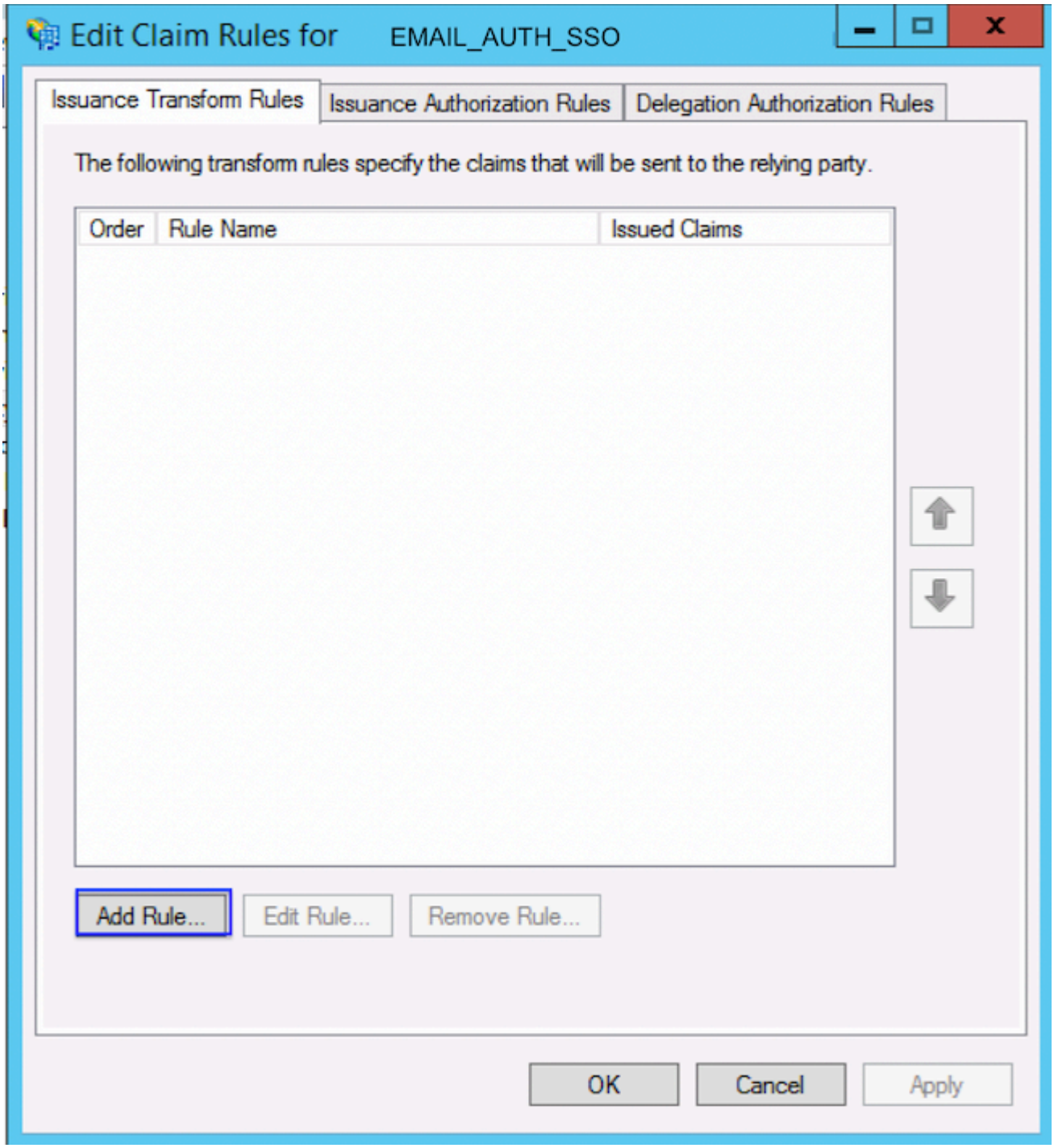
Regras de Transformação de Emissão - Reivindicações

- Selecione Editar Política de Emissão de Declarações.



Editar Política de Emissão de Declarações

- Selecione Adicionar regra.

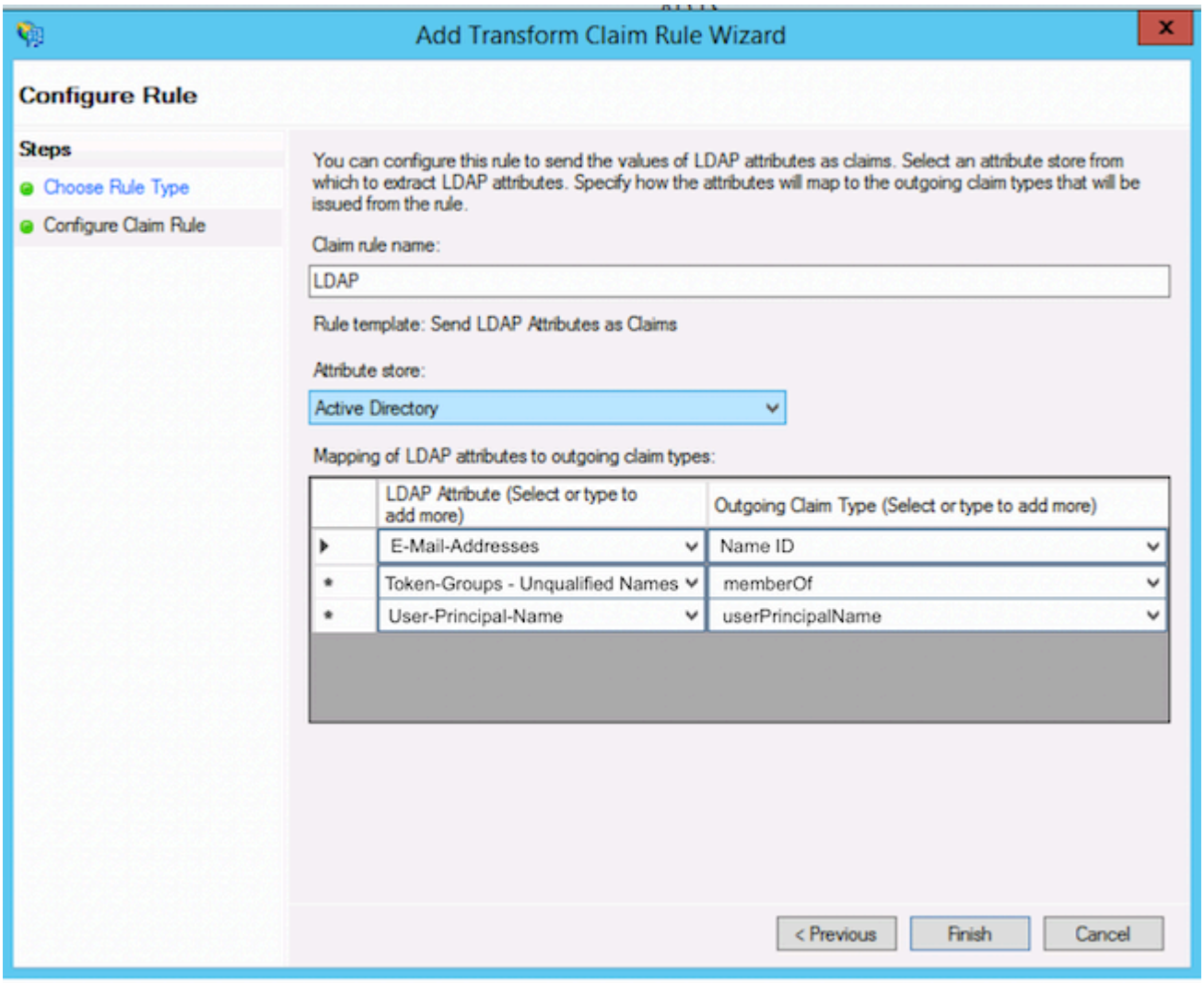


Adicionar regra de transformação de emissão

Os valores mostrados aqui são valores comuns que permitem que o ESA preencha nomes de grupo nas configurações de autenticação externa.

Tip: Os valores no mapeamento podem variar com base na preferência do administrador.

Tip: No exemplo listado, insira os tipos de declaração de saída memberOf e userPrincipalName manualmente. Selecione Nome ID na lista suspensa.



Transformar Regra de Declaração

- Selecione Finish.

Fazer download de metadados IdP e carregá-los no ESA

Depois de concluir a configuração da regra de confiança da terceira parte confiável e da declaração, exporte os metadados do provedor de identidade (IdP) e carregue-os no ESA.

⚠ Caution: Reiniciar o serviço AD FS pode interromper sessões de autenticação ativas. Execute esta etapa durante uma janela de manutenção, se necessário.

- Reinicie o serviço AD FS, se necessário.
- Execute estes comandos:

```
net stop adfssrv
net start adfssrv
```

- Faça download do arquivo de metadados deste URL:

https://myserver.domain.com/FederationMetadata/2007-06/FederationMetadata.xml

- Terminar e voltar ao cluster ESA.

Verificar

1. No ESA ou SMA, confirme se a importação de metadados IdP foi concluída com êxito.
2. Teste um logon administrativo usando o SSO (logon único) SAML.
3. Verifique se as declarações de grupo esperadas são recebidas e se o mapeamento de função é preenchido conforme esperado na configuração de autenticação externa.

Informações Relacionadas

-

- Cisco Email Security Appliance – Guias do usuário final
- Dispositivo de gerenciamento de segurança de conteúdo da Cisco - Guias do usuário final

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.