Configurar Duo IdP SAML SSO para ESA e SMA

Contents

Introdução

Este documento descreve como configurar o Gateway de Acesso Duo para SAML SSO para Cisco ESA e SMA.

Ambiente

- Cisco ESA/SMA: Versão mais recente do AsyncOS
- Gateway de acesso Duo: implantado e acessível na interface de gerenciamento ESA/SMA
- Origem da autenticação: Ative Diretory, OpenLDAP, Azure AD ou outro provedor de identidade SAML (para mapeamento de atributo)

Problema

Este documento descreve apenas a configuração do lado Duo. Ele não cobre a configuração do provedor de serviços (SP) Cisco ESA/SMA.

Pré-requisitos

Terminologia

- Provedor de identidade (IdP)
- Logon Único (SSO)
- Dispositivo de segurança de e-mail (ESA)
- Dispositivo de gerenciamento de segurança (SMA)

- Serviço de Consumidor de Asserção (ACS)
- Provedor de serviços (SP)

Requisitos

Antes de Começar:

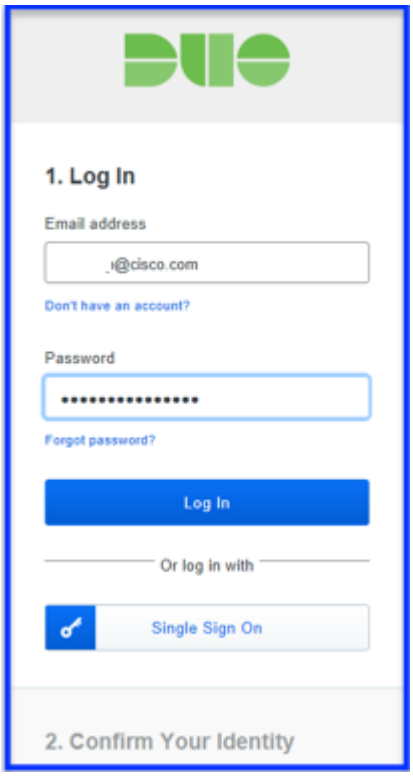
- Verifique se o Gateway de Acesso Duo está implantado e se tem uma fonte de autenticação configurada.
- Implante o Gateway de Acesso Duo com uma fonte de autenticação configurada.
- O Duo pode exigir um aplicativo separado para cada ESA se não houver suporte para vários URLs do Serviço de Consumidor de Asserção (ACS).

A configuração consiste em duas fases:

1. Configure o aplicativo de nuvem Duo.
2. Adicione o novo aplicativo de nuvem ao Gateway de Acesso Duo.

Crie o aplicativo em nuvem

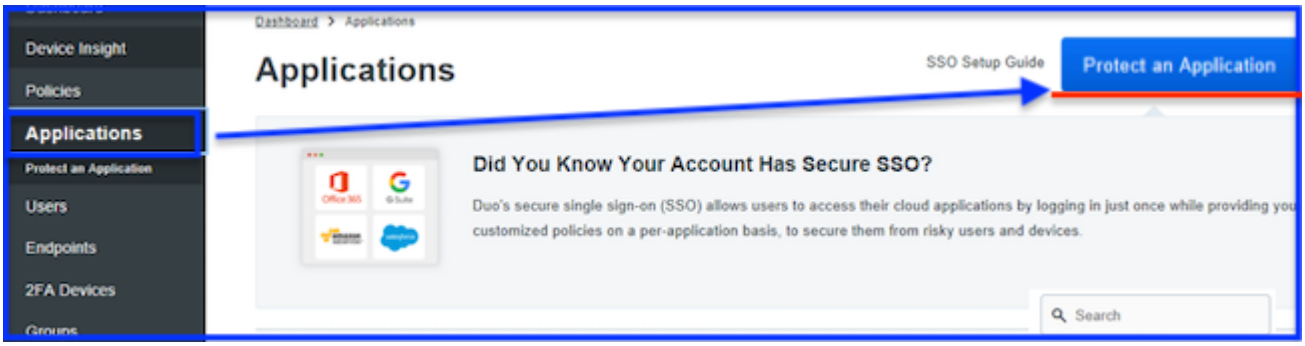
1. Faça login em https://admin.duosecurity.com/.



duo.com

duo.com

2. Navegue até Aplicações > Proteger uma Aplicação.

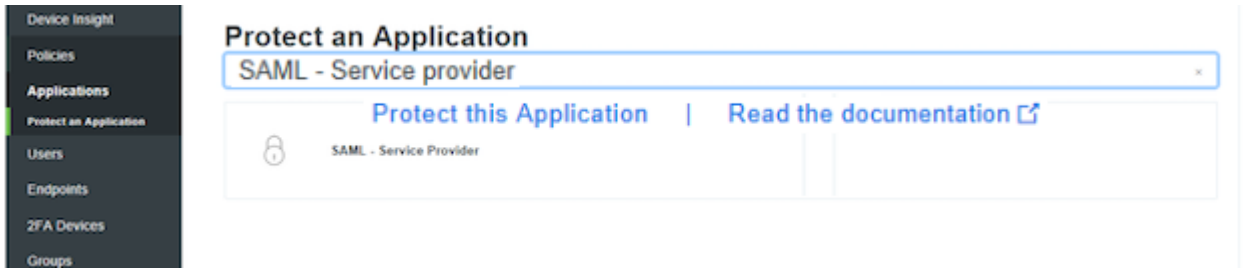


Proteger um aplicativo

Proteger um aplicativo

3. Procure SAML - Provedor de Serviços.

4. Quando o ícone SAML for exibido, selecione Proteger este Aplicativo.



Proteger este aplicativo

Proteger este aplicativo

5. Preencha o Perfil do Provedor de Serviços:

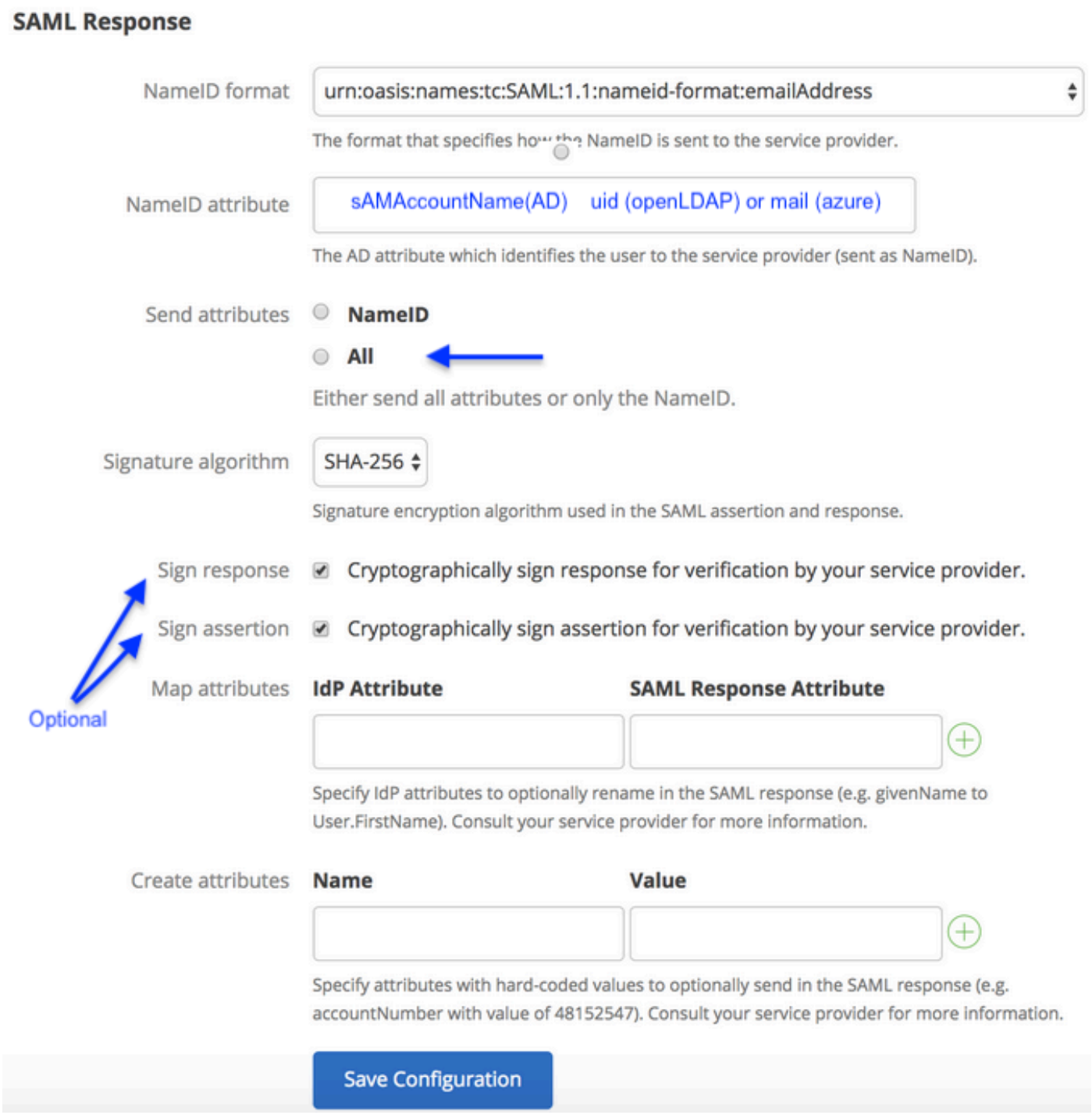
- Nome do provedor de serviços: Insira um nome de sua escolha.
- ID da entidade: Insira um nome comum para identificar o ESA/SMA.
- Serviço de consumidor de asserção: Insira o URL do ESA/SMA acessível.

6. Use estes valores de atributo NameID com base na origem da autenticação:

Atributo	Diretório ativo	OpenLDAP	Provedor de Identidade SAML (IdP)	AD do Azure
Atributo de e-mail	correio	correio	correio	correio
Atributo de nome de usuário	sAMAccountName	UID	correio	correio
Atributo de nome	Nome fornecido	gn	Nome fornecido	Nome fornecido
Atributo de sobrenome	sn	sn	sn	sobrenome

- Enviar atributos é opcional. Selecione NameID ou ALL.
- Assinar resposta e Assinar asserção são opcionais. Essas configurações devem corresponder ao IdP e ao SP.

7. Selecione Salvar Configuração.



Resposta SAML

Resposta SAML

8. Finalmente, faça o download do arquivo de configuração.

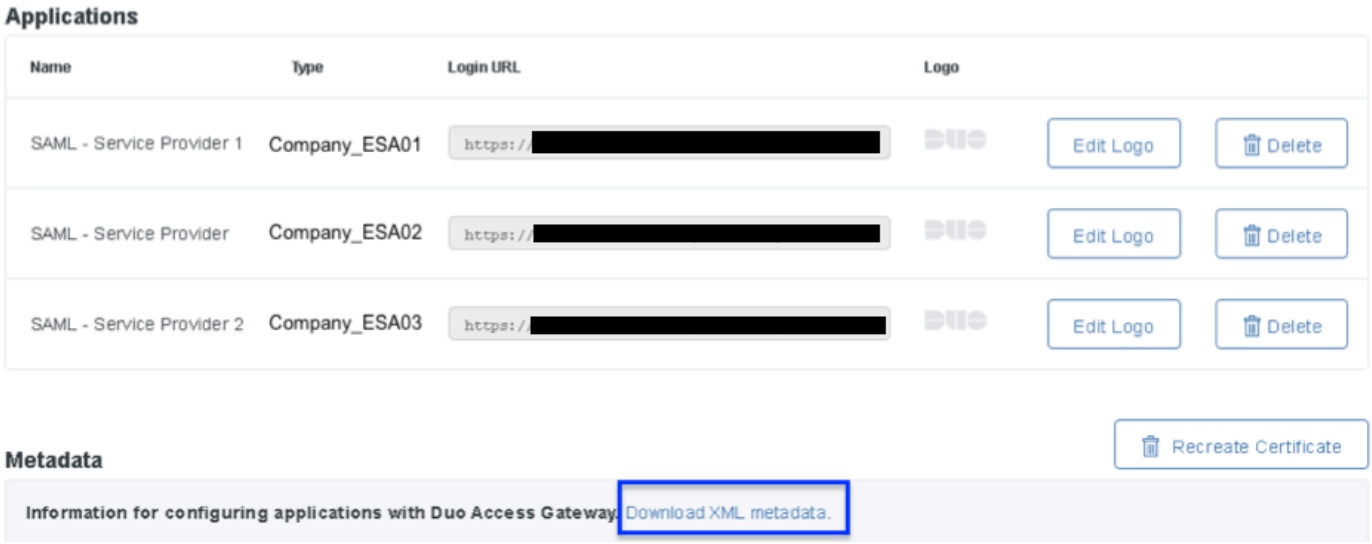
Adicionar novo aplicativo de nuvem ao Gateway de Acesso Duo

1. Faça login no Gateway de Acesso Duo.

2. Navegue até Application > Add Application > Configuration file > Choose File.

3. Selecione a configuração do aplicativo criada na Etapa 1 e, em seguida, selecione UPLOAD.

4. Faça download dos metadados XML para uso nos hosts SP como a configuração de IdP.



Exibição de aplicativos e download de metadados XML

Exibição de aplicativos e download de metadados XML

5. Retorne ao ESA/SMA para concluir a configuração do SAML SSO.

- Resultado esperado: o aplicativo Duo Access Gateway é criado e os metadados XML do IdP estão prontos para importação no ESA/SMA.

6. Use os metadados descarregados no procedimento ESA/SMA subsequente.

Próximas etapas (configuração ESA/SMA)

Este artigo aborda apenas a configuração do lado Duo. Para concluir a configuração no ESA/SMA, siga as instruções.

Verificação

- Confirme se o aplicativo aparece no Gateway de Acesso Duo em Aplicativos.
- Confirme se os metadados XML do IdP foram baixados com êxito e se estão prontos para importação no ESA/SMA.

Informações Relacionadas

- Documentação do Duo para SSO SAML

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.