

Configurar Duo IdP SAML SSO para ESA e SMA

Contents

[Introdução](#)

[Ambiente](#)

[Problema](#)

[Pré-requisitos](#)

[Terminologia](#)

[Requisitos](#)

[Crie o aplicativo em nuvem](#)

[Adicionar novo CloudApplication ao Gateway de Acesso Duo](#)

[Próximas etapas \(configuração ESA/SMA\)](#)

[Verificação](#)

[Informações Relacionadas](#)

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 Directory, 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:

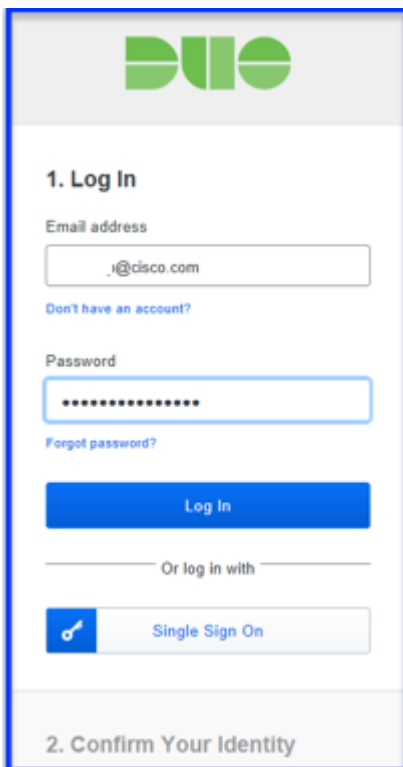
- Verifique se o Gateway de Acesso Duo está implantado e se tem uma fonte de autenticação configurada.
- Implante o Gateway de Acesso Duo com uma fonte de autenticação configurada.
- O Duo pode exigir um aplicativo separado para cada ESA se não houver suporte para vários URLs do Serviço de Consumidor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

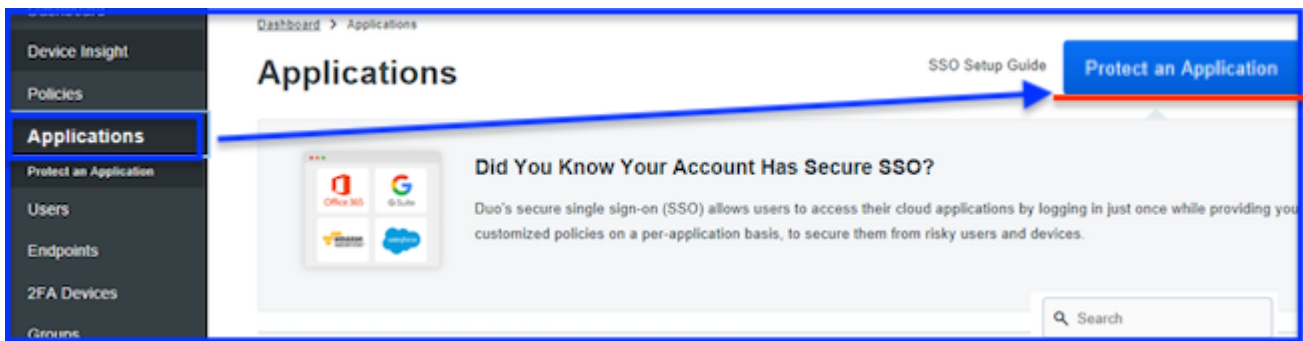


The image shows a screenshot of the Duo Admin Center login interface. At the top is the Duo logo. Below it is the heading '1. Log In'. There are two input fields: 'Email address' with a placeholder ending in '@cisico.com' and 'Password' with masked characters. A blue 'Log In' button is positioned below the password field. To the left of the password field are links for 'Don't have an account?' and 'Forgot password?'. Below the 'Log In' button is a section for 'Or log in with' which includes a 'Single Sign On' button with a key icon. At the bottom of the screenshot, the heading '2. Confirm Your Identity' is visible.

duo.com

duo.com

2. Navegue até Aplicações > Proteger uma Aplicação.

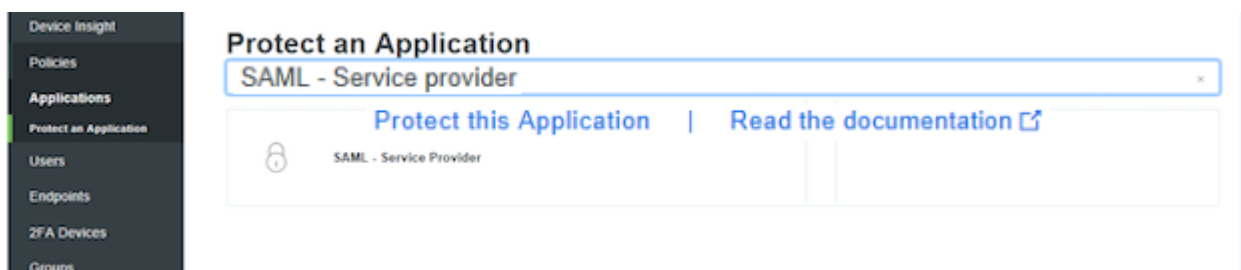


Proteger um aplicativo

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.

SAML Response

NameID format

The format that specifies how the NameID is sent to the service provider.

NameID attribute

The AD attribute which identifies the user to the service provider (sent as NameID).

Send attributes NameID

All

Either send all attributes or only the NameID.

Signature algorithm

Signature encryption algorithm used in the SAML assertion and response.

Sign response Cryptographically sign response for verification by your service provider.

Sign assertion Cryptographically sign assertion for verification by your service provider.

Map attributes **IdP Attribute**

SAML Response Attribute

Specify IdP attributes to optionally rename in the SAML response (e.g. givenName to User.FirstName). Consult your service provider for more information.

Create attributes **Name**

Value

Specify attributes with hard-coded values to optionally send in the SAML response (e.g. accountNumber with value of 48152547). Consult your service provider for more information.

Save Configuration

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.

Applications

Name	Type	Login URL	Logo		
SAML - Service Provider 1	Company_ESA01	https://[REDACTED]		Edit Logo	Delete
SAML - Service Provider	Company_ESA02	https://[REDACTED]		Edit Logo	Delete
SAML - Service Provider 2	Company_ESA03	https://[REDACTED]		Edit Logo	Delete

Metadata

[Recreate Certificate](#)

Information for configuring applications with Duo Access Gateway [Download XML metadata.](#)

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.