Configuración de Duo IdP SAML SSO para ESA y SMA

Contenido

Introducción

Este documento describe cómo configurar Duo Access Gateway para SAML SSO para Cisco ESA y SMA.

Entorno

- ESA/SMA de Cisco: AsyncOS última versión
- Puerta de enlace de acceso doble: implementable y accesible desde la interfaz de gestión ESA/SMA
- Fuente de autenticación: Active Directory, OpenLDAP, Azure AD u otro proveedor de identidad SAML (para asignación de atributos)

Problema

Este documento describe solamente la configuración de dos lados. No cubre la configuración de Cisco ESA/SMA Service Provider (SP).

Prerequisites

Terminology

- Proveedor de identidad (IdP)

- Inicio de sesión único (SSO)
- Dispositivo de seguridad de correo electrónico (ESA)
- Dispositivo de administración de seguridad (SMA)
- Servicio al consumidor de aserción (ACS)
- Proveedor de servicios (SP)

Requirements

Antes de comenzar:

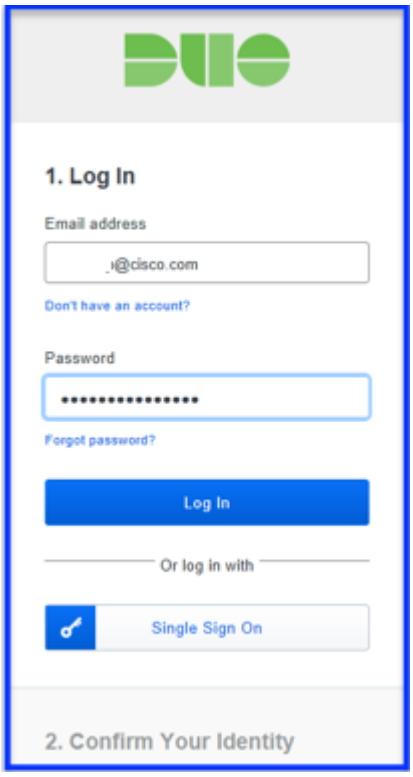
- Asegúrese de que Duo Access Gateway esté implementado y que tenga una fuente de autenticación configurada.
- Implemente Duo Access Gateway con una fuente de autenticación configurada.
- Duo puede requerir una aplicación independiente para cada ESA si no se admiten varias URL de Assertion Consumer Service (ACS).

La configuración consta de dos fases:

1. Configure la aplicación de nube Duo.
2. Agregue la nueva aplicación en la nube a Duo Access Gateway.

Crear la aplicación en la nube

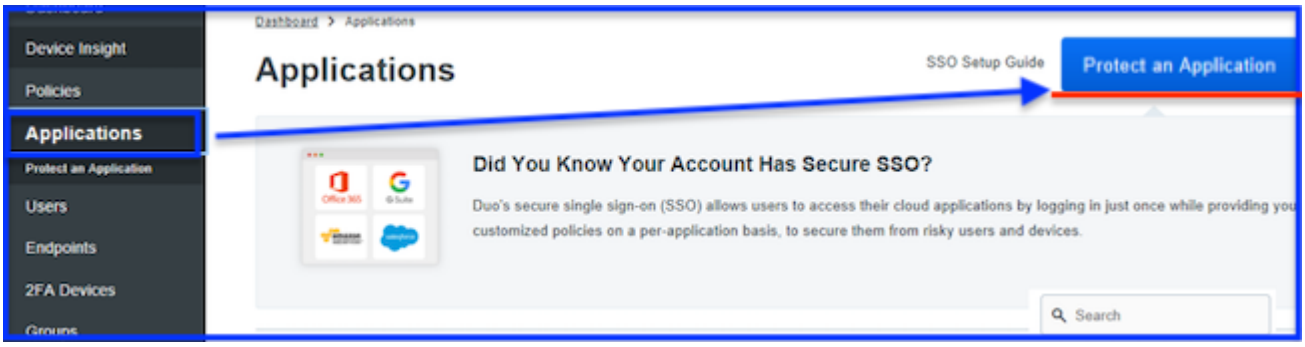
1. Inicie sesión en https://admin.duosecurity.com/.



duo.com

duo.com

2. Vaya a Aplicaciones > Proteger una aplicación.

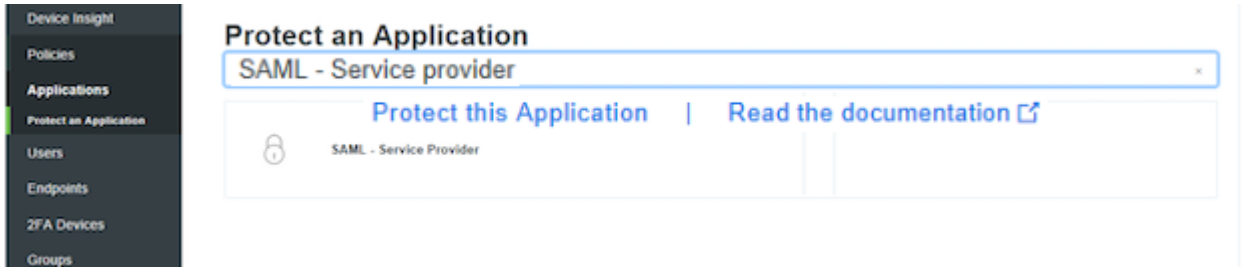


Proteger una aplicación

Proteger una aplicación

3. Busque SAML - Service Provider.

4. Cuando aparezca el icono SAML, seleccione Proteger esta Aplicación.



Proteger esta aplicación

Proteger esta aplicación

5. Complete el perfil del proveedor de servicios:

- Nombre del proveedor de servicios: Introduzca el nombre que desee.
- ID de entidad: Introduzca un nombre común para identificar el ESA/SMA.
- Servicio al consumidor de aserción: Introduzca la URL de ESA/SMA accesible.

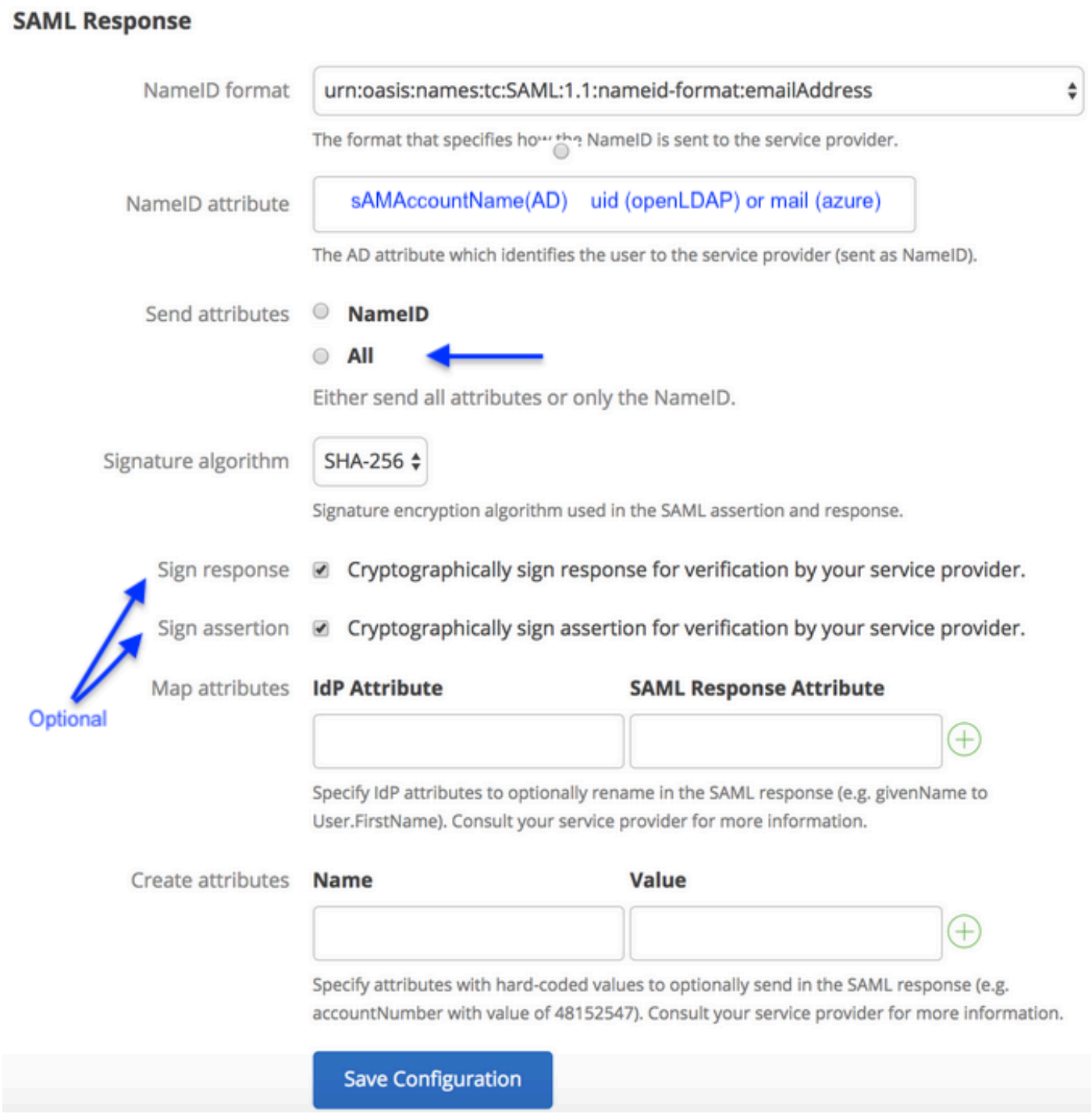
6. Utilice estos valores de atributo NameID basados en el origen de autenticación:

Atributo	Directorio activo	OpenLDAP	Proveedor de identidad SAML (IdP)	Azure AD
Atributo de correo	correo	correo	correo	correo
Atributo Username	sAMAccountName	uid	correo	correo
Atributo de nombre	nombreDado	gn	nombreDado	nombreDado
Atributo de apellido	sn	sn	sn	apellidar

- Enviar atributos es opcional. Seleccione NameID o ALL.

- La respuesta de firma y la aserción de firma son opcionales. Esta configuración debe coincidir en el IdP y el SP.

7. Seleccione Guardar Configuración.



Respuesta SAML

Respuesta SAML

8. Finalmente, descargue el archivo de configuración.

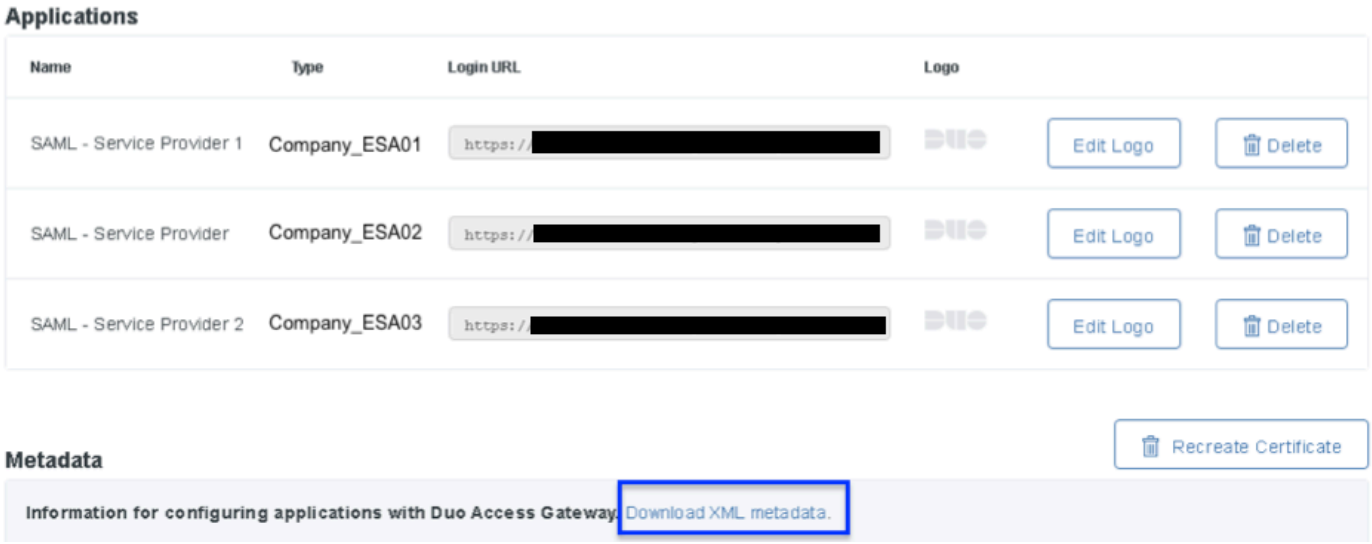
Incorporación de una nueva aplicación basada en la nube al gateway de acceso dúo

1. Inicie sesión en Duo Access Gateway.

2. Vaya a Aplicación > Agregar aplicación > Archivo de configuración > Elegir archivo.

3. Seleccione la configuración de aplicación creada en el paso 1 y, a continuación, seleccione CARGAR.

4. Descargue los metadatos XML para su uso en los hosts SP como configuración IdP.



Vista de aplicaciones y descarga de metadatos XML

Vista de aplicaciones y descarga de metadatos XML

5. Vuelva al ESA/SMA para completar la configuración de SSO de SAML.

- Resultado esperado: se crea la aplicación Duo Access Gateway y los metadatos XML de IdP están listos para importarse en el ESA/SMA.

6. Utilice los metadatos descargados en el procedimiento ESA/SMA subsiguiente.

Siguientes pasos (configuración ESA/SMA)

En este artículo se trata únicamente la configuración de dos lados. Para completar la configuración en el ESA/SMA, siga las instrucciones.

Verificación

- Confirme que la aplicación aparece en Duo Access Gateway bajo Applications.
- Confirme que los metadatos XML de IdP se descarguen correctamente y estén listos para importar en el ESA/SMA.

Información Relacionada

- Documentación de Duo para SAML SSO

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).