Configuration de Duo IdP SAML SSO pour ESA et SMA

Table des matières

Introduction

Ce document décrit comment configurer Duo Access Gateway pour SAML SSO pour Cisco ESA et SMA.

Environnement

- Cisco ESA/SMA : Dernière version d'AsyncOS
- Passerelle d'accès duo : déployée et accessible depuis l'interface de gestion ESA/SMA
- Source d'authentification : Active Directory, OpenLDAP, Azure AD ou un autre fournisseur d'identité SAML (pour le mappage d'attributs)

Problème

Ce document décrit uniquement la configuration côté Duo. Elle ne couvre pas la configuration du fournisseur de services Cisco ESA/SMA.

Conditions préalables

Terminologie

- Fournisseur d'identité (IdP)
- Authentification unique (SSO)

- Appliance de sécurité de la messagerie (ESA)
- Appliance de gestion de la sécurité (SMA)
- Service client d'assertion (ACS)
- Fournisseur de services (SP)

Exigences

Avant de commencer :

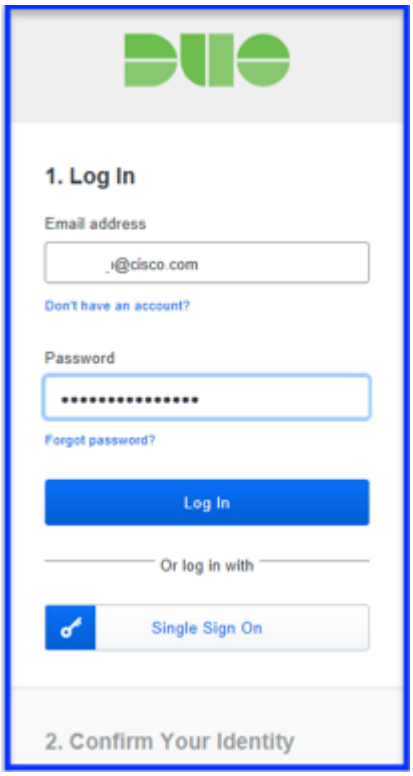
- Assurez-vous que la passerelle d'accès duo est déployée et qu'elle dispose d'une source d'authentification configurée.
- Déployez la passerelle d'accès duo avec une source d'authentification configurée.
- Duo peut nécessiter une application distincte pour chaque ESA si plusieurs URL ACS (Assertion Consumer Service) ne sont pas prises en charge.

La configuration se compose de deux phases :

1. Configurer l'application cloud Duo.
2. Ajoutez la nouvelle application cloud à Duo Access Gateway.

Créer l'application cloud

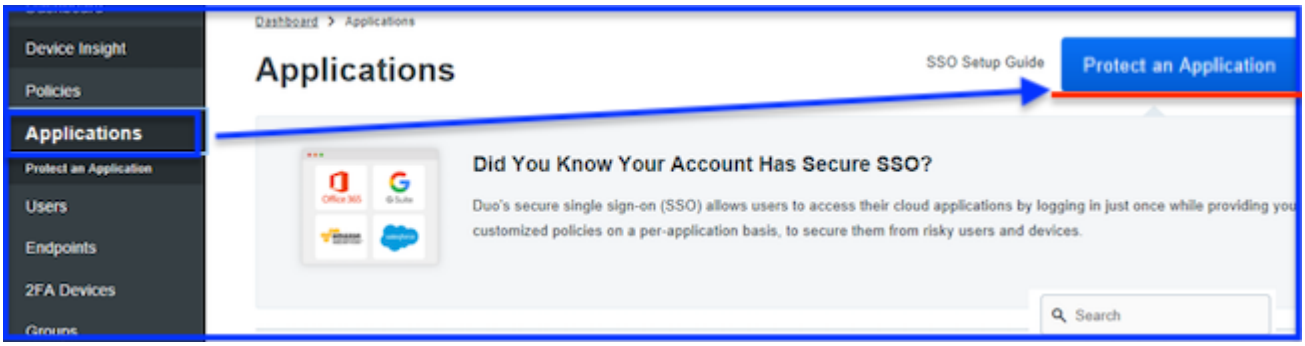
1. Connectez-vous à https://admin.duosecurity.com/.



duo.com

duo.com

2. Accédez à Applications > Protéger une application.

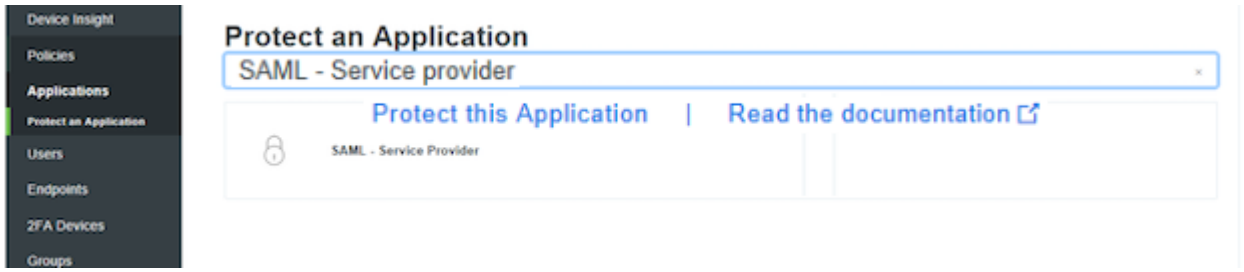


Protéger une application

Protéger une application

3. Recherchez SAML - Service Provider.

4. Lorsque l'icône SAML apparaît, sélectionnez Protéger cette application.



Protéger cette application

Protéger cette application

5. Complétez le profil de fournisseur de services :

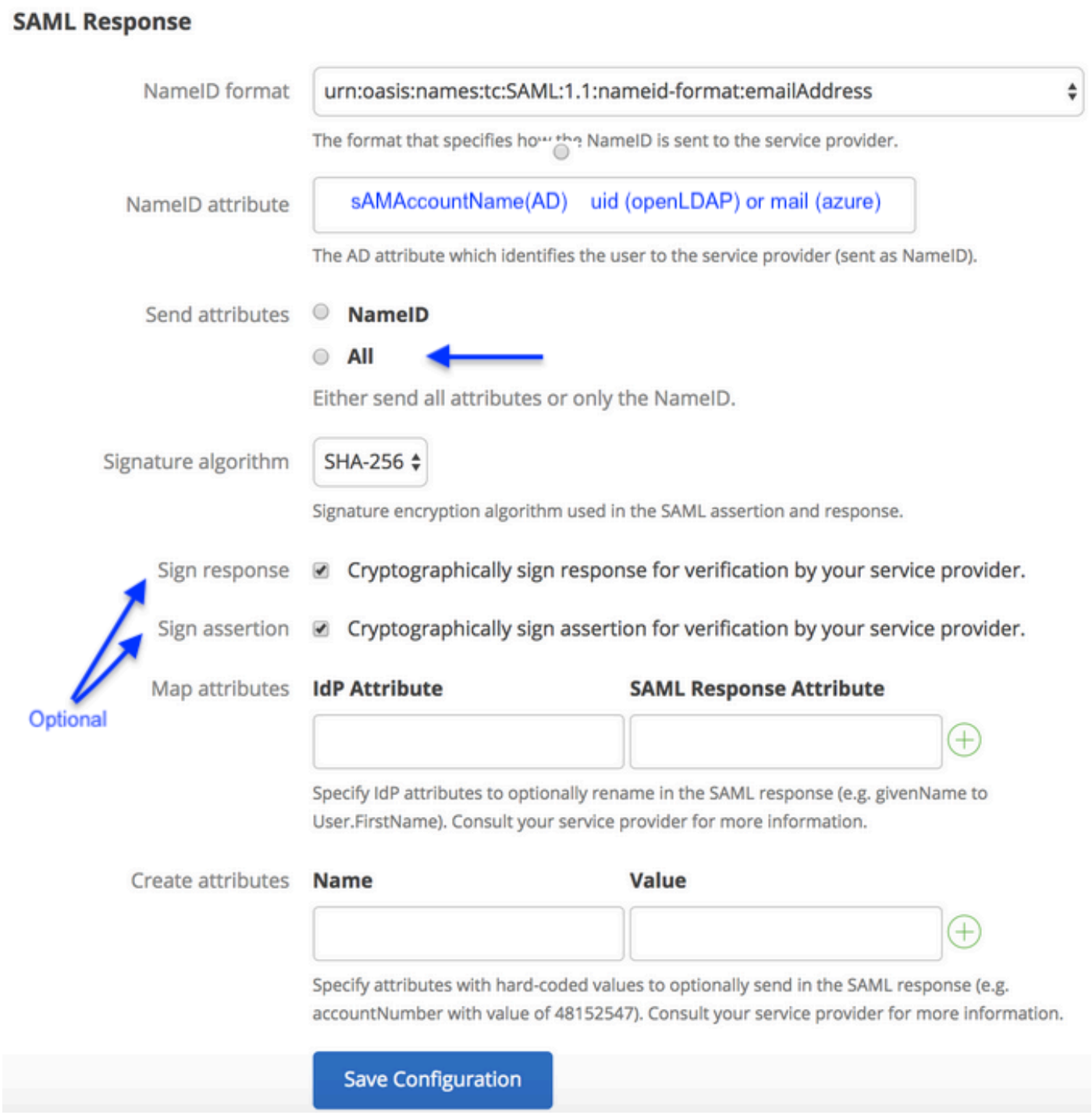
- Nom du fournisseur de services : Saisissez le nom de votre choix.
- ID d'entité : Entrez un nom commun pour identifier l'ESA/SMA.
- Assertion Consumer Service : Saisissez l'URL ESA/SMA accessible.

6. Utilisez ces valeurs d'attribut NameID en fonction de la source d'authentification :

Attribut	Active Directory	OpenLDAP	Fournisseur d'identité SAML (IdP)	Azure AD
Attribut Mail	poste	poste	poste	poste
Attribut Nom d'utilisateur	sAMAccountName	uid	poste	poste
Attribut de prénom	givenName	canon	givenName	givenName
Attribut Nom	sn	sn	sn	nom de famille

- Les attributs d'envoi sont facultatifs. Sélectionnez NameID ou ALL.
- La réponse et l'assertion Sign sont facultatives. Ces paramètres doivent correspondre sur le fournisseur d'identité et le fournisseur de services.

7. Sélectionnez Enregistrer la configuration.



Réponse SAML

Réponse SAML

8. Enfin, téléchargez le fichier de configuration.

Ajouter une nouvelle application cloud à la passerelle d'accès Duo

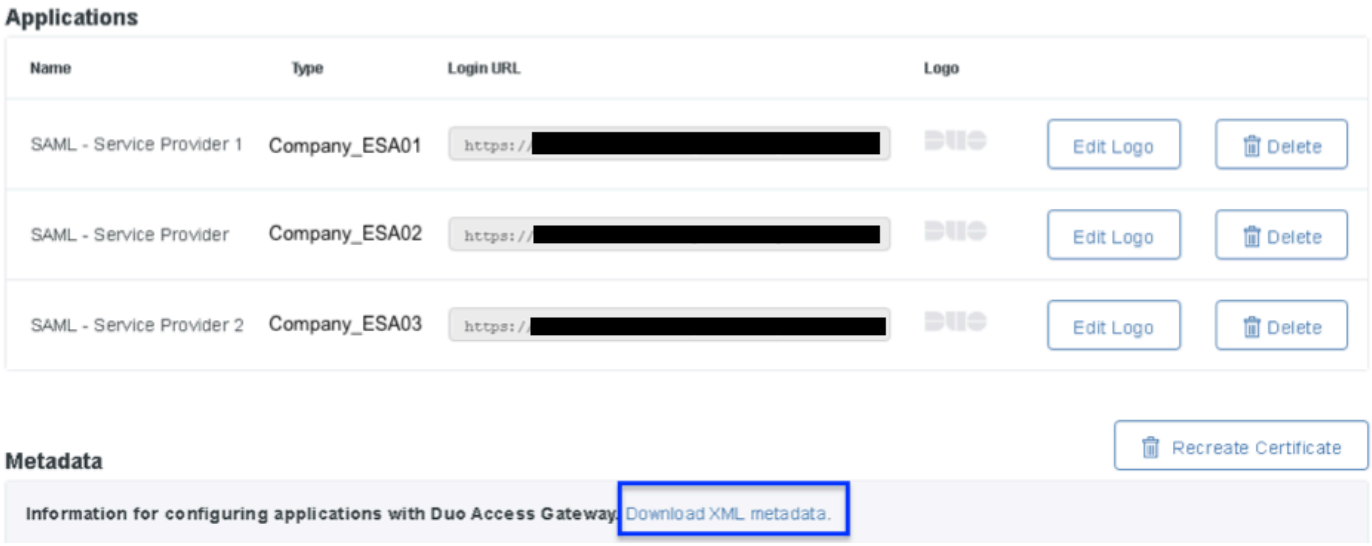
1. Connectez-vous à la passerelle d'accès Duo.

2. Accédez à Application > Ajouter une application > Fichier de configuration > Sélectionnez

Fichier.

3. Sélectionnez la configuration d'application créée à l'étape 1, puis sélectionnez UPLOAD.

4. Téléchargez les métadonnées XML à utiliser sur les hôtes SP comme configuration IdP.



Affichage des applications et téléchargement des métadonnées XML

Affichage des applications et téléchargement des métadonnées XML

5. Revenez à l'ESA/SMA pour terminer la configuration de l'authentification unique SAML.

- Résultat escompté : l'application Duo Access Gateway est créée et les métadonnées XML IdP sont prêtes à être importées dans ESA/SMA.

6. Utiliser les métadonnées téléchargées dans la procédure ESA/SMA suivante.

Étapes suivantes (configuration ESA/SMA)

Cet article couvre uniquement la configuration côté Duo. Pour terminer la configuration sur l'ESA/SMA, suivez les instructions.

Vérification

- Vérifiez que l'application apparaît dans la passerelle d'accès duo sous Applications.
- Vérifiez que les métadonnées XML IdP ont été téléchargées correctement et qu'elles sont prêtes à être importées sur ESA/SMA.

Informations connexes

- Documentation Duo pour SAML SSO

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.