Duo IdP SAML SSO für ESA und SMA konfigurieren

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration des Duo Access Gateway für SAML SSO für Cisco ESA und SMA beschrieben.

Umwelt

- Cisco ESA/SMA: Aktuelle AsyncOS-Version
- Duo Access-Gateway: bereitgestellt und über die ESA/SMA-Management-Schnittstelle erreichbar
- Authentifizierungsquelle: Active Directory, OpenLDAP, Azure AD oder ein anderer SAML-Identitätsanbieter (für die Attributzuordnung)

Problem

In diesem Dokument wird nur die Konfiguration auf der Duo-Seite beschrieben. Die Konfiguration der Cisco ESA/SMA Service Provider (SP) wird nicht abgedeckt.

Voraussetzungen

Terminologie

- Identitätsanbieter (IdP)

- Single Sign-On (SSO)
- E-Mail Security Appliance (ESA)
- Security Management Appliance (SMA)
- Assertion Consumer Service (ACS)
- Service Provider

Anforderungen

Bevor Sie beginnen:

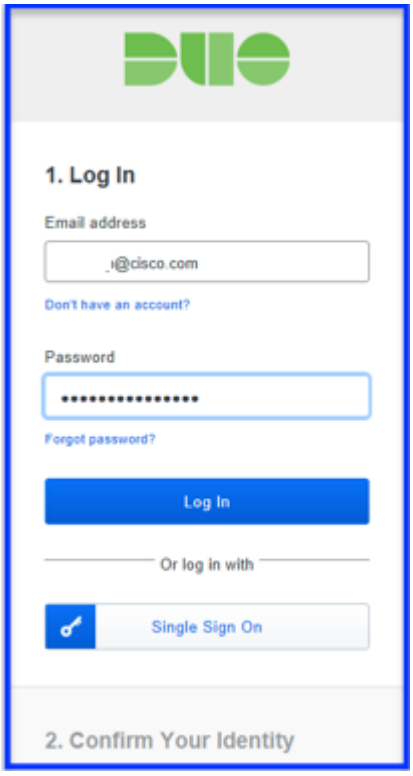
- Stellen Sie sicher, dass das Duo Access Gateway bereitgestellt wird und über eine konfigurierte Authentifizierungsquelle verfügt.
- Stellen Sie Duo Access Gateway mit einer konfigurierten Authentifizierungsquelle bereit.
- Duo kann für jede ESA eine separate Anwendung benötigen, wenn mehrere ACS-URLs (Assertion Consumer Service) nicht unterstützt werden.

Die Konfiguration erfolgt in zwei Phasen:

1. Konfigurieren Sie die Duo Cloud-Anwendung.
2. Fügen Sie die neue Cloud-Anwendung dem Duo Access Gateway hinzu.

Erstellen der Cloud-Anwendung

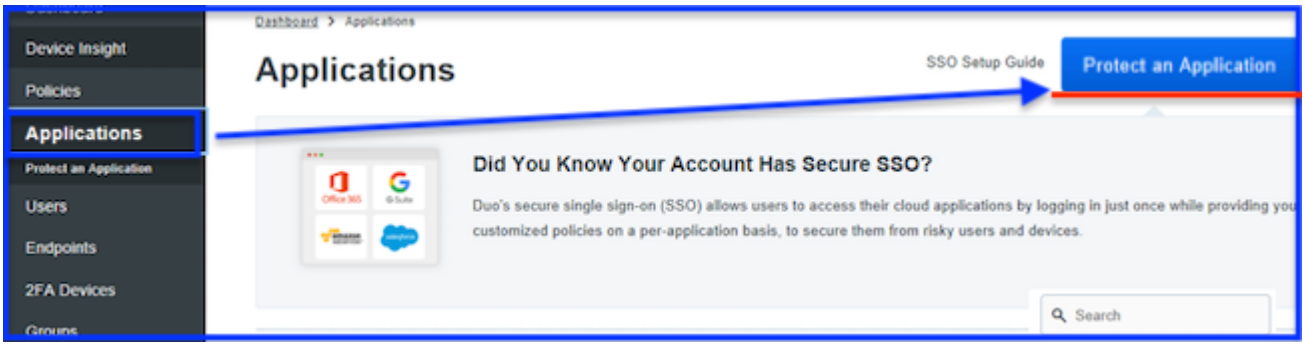
1. Melden Sie sich bei https://admin.duosecurity.com/ an.



duo.com

duo.com

2. Navigieren Sie zu Anwendungen > Eine Anwendung schützen.

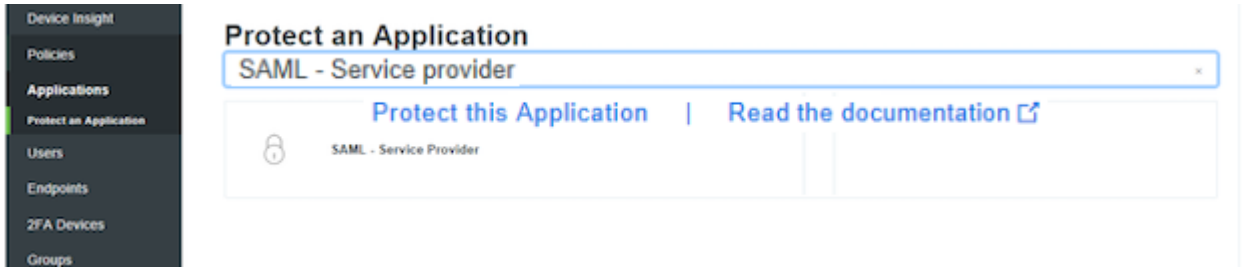


Schutz einer Anwendung

Schutz einer Anwendung

3. Suchen Sie nach SAML - Service Provider.

4. Wenn das SAML-Symbol angezeigt wird, wählen Sie Diese Anwendung schützen.



Diese Anwendung schützen

Diese Anwendung schützen

5. Füllen Sie das Service Provider-Profil aus:

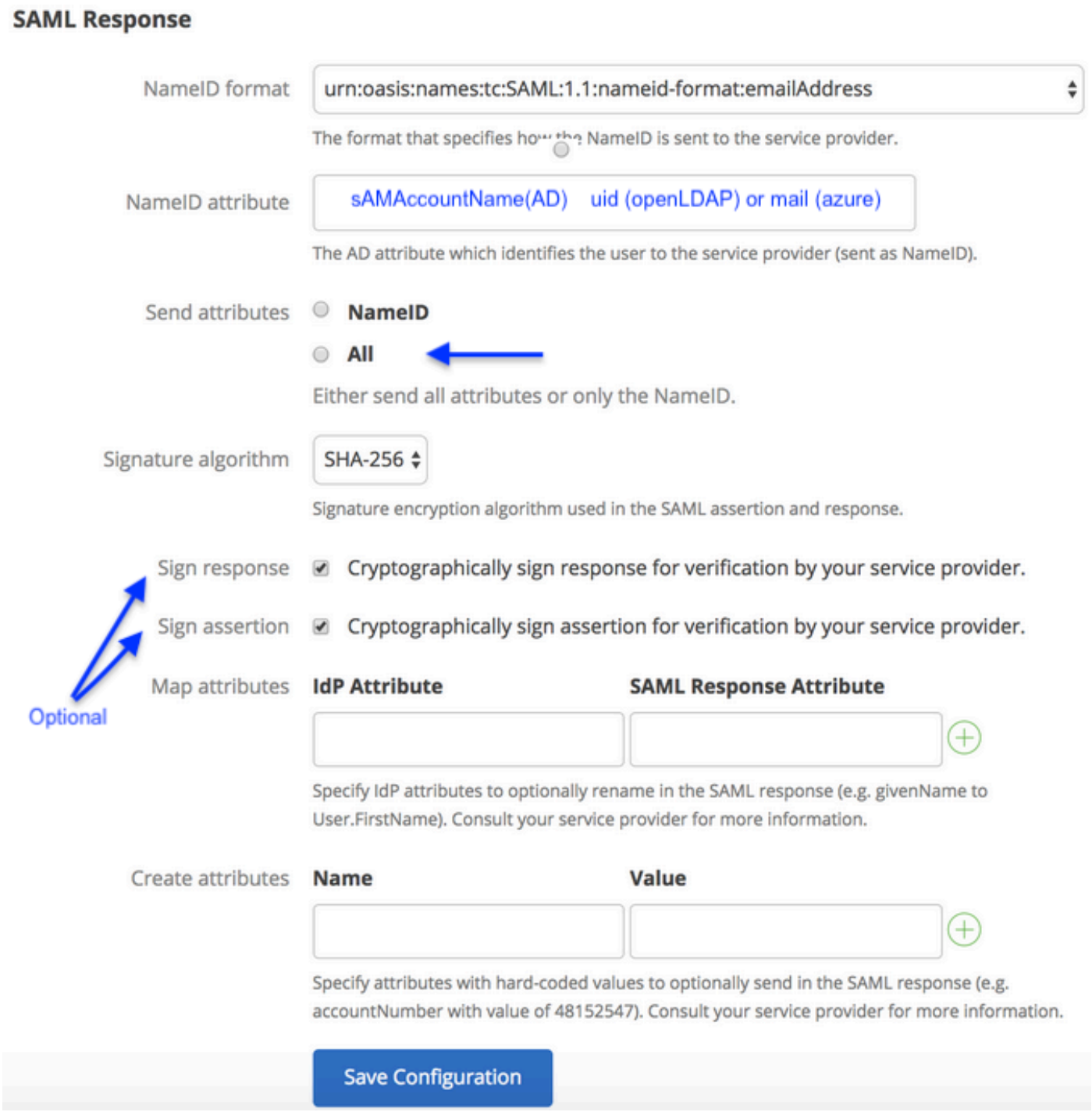
- Name des Dienstanbieters: Geben Sie einen Namen Ihrer Wahl ein.
- Entitäts-ID: Geben Sie einen gemeinsamen Namen zur Identifizierung der ESA/SMA ein.
- Assertion Consumer Service: Geben Sie die erreichbare ESA/SMA-URL ein.

6. Verwenden Sie die folgenden NameID-Attributwerte basierend auf der Authentifizierungsquelle:

Attribut	Active Directory	OpenLDAP	SAML Identity Provider (IdP)	Azure AD
Mail-Attribut	Post	Post	Post	Post
Benutzername-Attribut	sAMAccountName	UID	Post	Post
Vorname-Attribut	Vorname	Keim	Vorname	Vorname
Nachname-Attribut	sn	sn	sn	Nachname

- Das Senden von Attributen ist optional. Wählen Sie entweder NameID oder ALL.
- Die Signaturantwort und die Signaturassertion sind optional. Diese Einstellungen müssen für IdP und SP übereinstimmen.

7. Wählen Sie Konfiguration speichern.



SAML-Antwort

SAML-Antwort

8. Laden Sie abschließend die Konfigurationsdatei herunter.

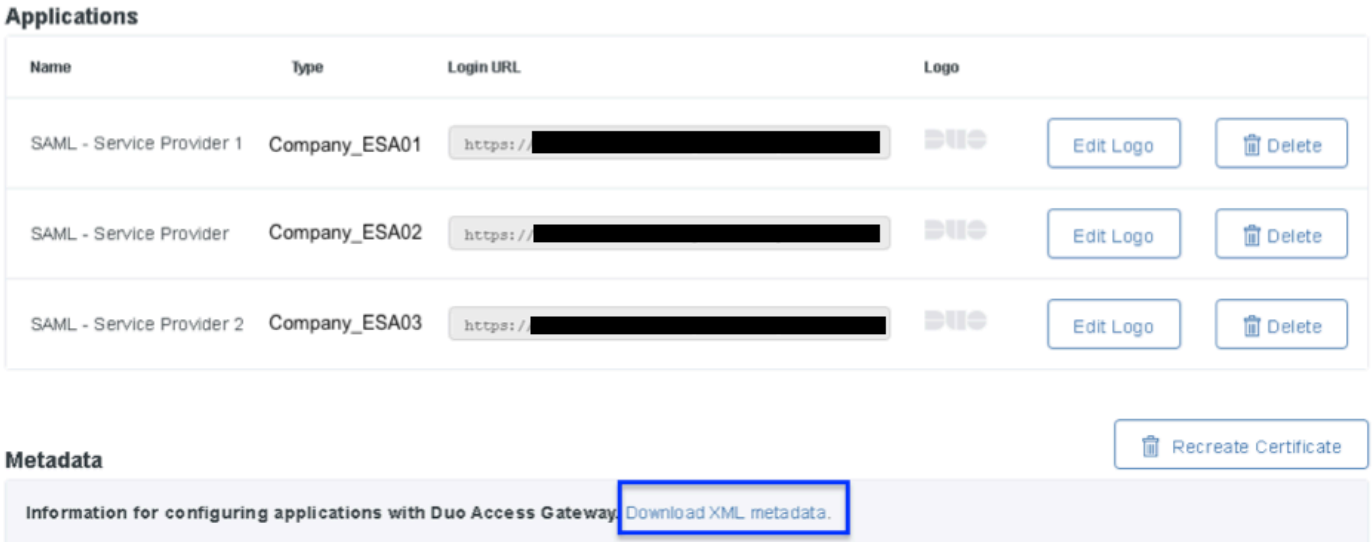
Hinzufügen einer neuen Cloud-Anwendung zum Duo Access Gateway

1. Melden Sie sich beim Duo Access Gateway an.

2. Navigieren Sie zu Anwendung > Anwendung hinzufügen > Konfigurationsdatei > Datei auswählen.

3. Wählen Sie die in Schritt 1 erstellte Anwendungskonfiguration und anschließend UPLOAD.

4. Laden Sie die XML-Metadaten für die Verwendung auf den SP-Hosts als IdP-Konfiguration herunter.



Ansicht von Anwendungen und Herunterladen von XML-Metadaten

Ansicht von Anwendungen und Herunterladen von XML-Metadaten

5. Kehren Sie zur ESA/SMA zurück, um die SAML SSO-Konfiguration abzuschließen.

- Erwartetes Ergebnis: Die Anwendung Duo Access Gateway wird erstellt, und die IdP-XML-Metadaten können in die ESA/SMA importiert werden.

6. Verwenden Sie die heruntergeladenen Metadaten in der nachfolgenden ESA/SMA-Prozedur.

Nächste Schritte (ESA/SMA-Konfiguration)

In diesem Artikel wird nur die Duo-seitige Konfiguration behandelt. Befolgen Sie die Anweisungen, um die Einrichtung auf der ESA/SMA abzuschließen.

Verifizierung

- Vergewissern Sie sich, dass die Anwendung im Duo Access Gateway unter Anwendungen angezeigt wird.
- Bestätigen Sie, dass die IdP-XML-Metadaten erfolgreich heruntergeladen wurden und in die ESA/SMA importiert werden können.

Zugehörige Informationen

- Duo Dokumentation für SAML SSO

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.