ESAおよびSMA用のDuo IdP SAML SSOの設定

内容

はじめに

このドキュメントでは、Cisco ESAおよびSMAのSAML SSO用にDuo Access Gateway(DAP)を設定する方法について説明します。

環境

- Cisco ESA/SMA:AsyncOS最新バージョン
- Duo Access Gateway：導入され、ESA/SMA管理インターフェイスから到達可能
- 認証ソース： Active Directory、OpenLDAP、Azure AD、または別のSAML IDプロバイダー（属性マッピング用）

問題

このドキュメントでは、Duo側の設定についてのみ説明します。Cisco ESA/SMA Service Provider(SP)の設定については説明していません。

前提条件

用語

- アイデンティティプロバイダー(IdP)
- シングルサインオン(SSO)
- E メール セキュリティ アプライアンス（ESA）
- セキュリティ管理アプライアンス(SMA)

- アサーションコンシューマサービス(ACS)
- サービスプロバイダー(SP)

要件

作成を開始する前に、次の点に注意してください。

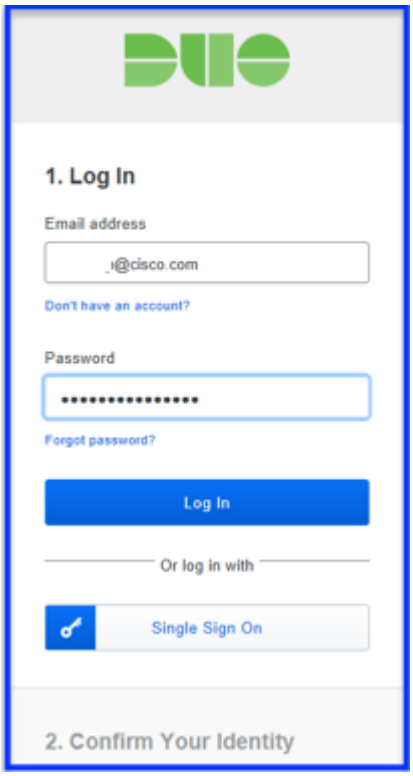
- Duo Access Gatewayが展開され、認証ソースが構成されていることを確認してください。
- 認証ソースが設定されたDuo Access Gatewayを導入します。
- 複数のAssertion Consumer Service(ACS)URLがサポートされていない場合、DuoではESAごとに個別のアプリケーションが必要になる場合があります。

この設定は、次の2つのフェーズで構成されます。

1. Duoクラウドアプリケーションを設定します。
2. 新しいクラウドアプリケーションをDuo Access Gatewayに追加します。

クラウドアプリケーションの作成

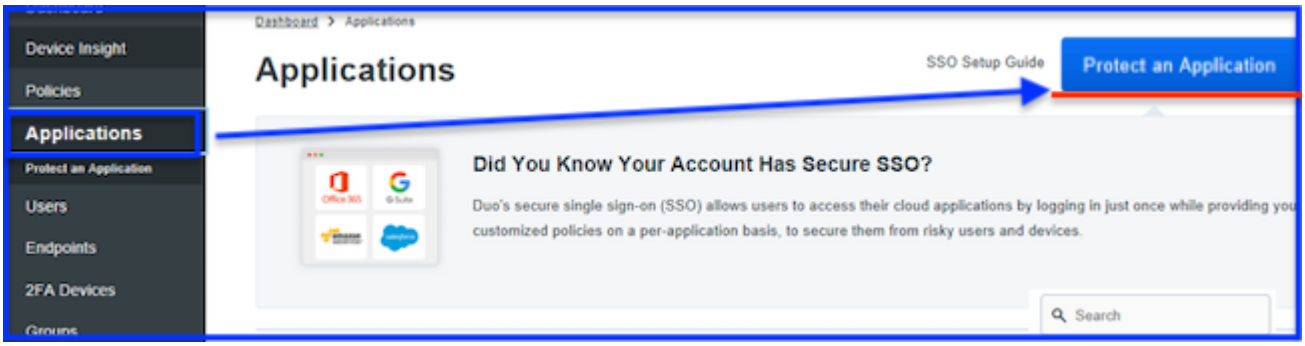
1. https://admin.duosecurity.com/にログインします。



duo.com

duo.com

2. [アプリケーション] > [アプリケーションの保護] に移動します。

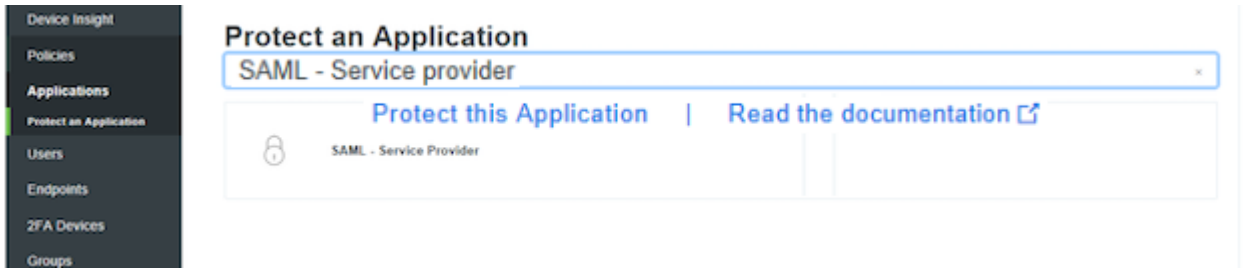


アプリケーションの保護

アプリケーションの保護

3. SAML – サービスプロバイダーを検索します。

4. SAMLアイコンが表示されたら、Protect this Applicationを選択します。



このアプリケーションの保護

このアプリケーションの保護

5. サービスプロバイダープロファイルを完成させます。

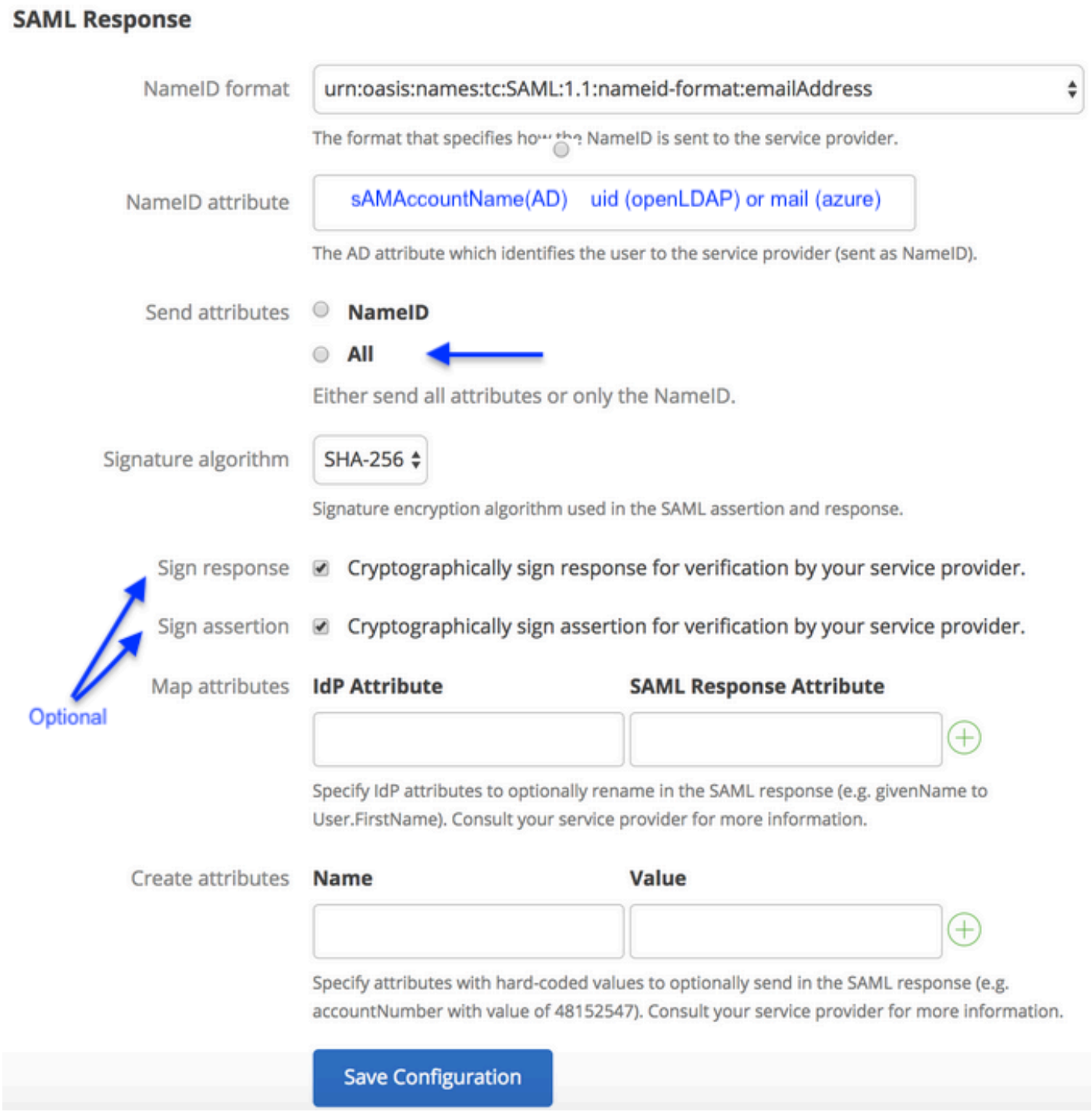
- サービスプロバイダ名：任意の名前を入力します。
- エンティティID:ESA/SMAを識別する一般的な名前を入力します。
- アサーションコンシューマサービス：到達可能なESA/SMA URLを入力します。

6. 認証ソースに基づいて、次のNameID属性値を使用します。

Attribute	Active Directory	OpenLDAP	SAML IDプロバイダー(IdP)	Azure AD
メール属性	メール	メール	メール	メール
ユーザ名属性	sAMAccountName	uid	メール	メール
名の属性	givenName	gn	givenName	givenName
名属性	sn	sn	sn	姓

- 送信属性はオプションです。NameIDまたはALLのいずれかを選択します。
- Sign responseおよびSign assertionはオプションです。これらの設定は、IdPとSPで一致している必要があります。

7. Save Configurationを選択します。



SAML応答

SAML応答

8. 最後に、コンフィギュレーションファイルをダウンロードします。

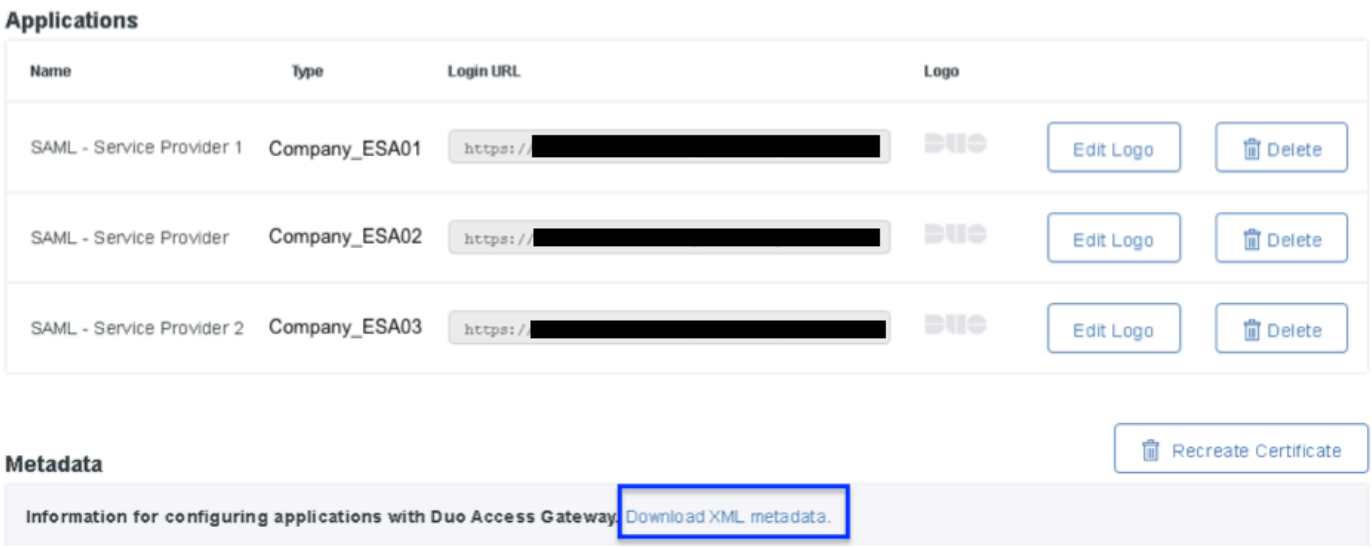
Duo Access Gatewayへの新しいクラウドアプリケーションの追加

1. Duo Access Gatewayにログインします。

2. Application > Add Application > Configuration file > Choose Fileの順に移動します。

3. ステップ1で作成したアプリケーション設定を選択し、UPLOADを選択します。

4. SPホストで使用するXMLメタデータをIdP構成としてダウンロードします。



アプリケーションの表示およびXMLメタデータのダウンロード

アプリケーションの表示およびXMLメタデータのダウンロード

5. ESA/SMAに戻り、SAML SSOの設定を完了します。

- 期待される結果：Duo Access Gatewayアプリケーションが作成され、IdP XMLメタデータをESA/SMAにインポートする準備が整いました。

6. ダウンロードしたメタデータを以降のESA/SMA手順で使用します。

次のステップ（ESA/SMA設定）

この記事では、Duo側の設定についてのみ説明します。ESA/SMAのセットアップを完了するには、指示に従います。

検証

- アプリケーションがDuo Access GatewayのApplicationsの下に表示されることを確認します。
- IdP XMLメタデータが正常にダウンロードされ、ESA/SMAでインポートする準備が整っていることを確認します。

関連情報

- SAML SSOのDuoドキュメント

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。