# ESAおよびSMA管理のためのSAML SSO外部認証の設定

## 内容



## はじめに

このドキュメントでは、ESAおよびSMAシステム管理のSAML 2.0 SSO外部認証を設定する方法について説明します。

### 環境

- 製品：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)
- 対象：ESAおよびSMAシステム管理
- クラスタ動作：サービスプロバイダー(SP)およびIdPプロファイルはマシンレベルで設定され、外部認証マッピングはクラスタレベルで設定されます。

## 前提条件

- ESA/SMA Webインターフェイスへの管理アクセス
- PKCS #12(PFX)またはPEM形式（自己署名またはCA署名）で使用可能なX.509証明書およ

び秘密キー
- サードパーティのアイデンティティプロバイダー(IdP)アプリケーションおよびそのSAMLメタデータ/SSO URLへのアクセス

### 事前設定チェックリスト

- 管理者がアプライアンスへのアクセスに使用する管理インターフェイスのホスト名/FQDNを確認します。Assertion Consumer Service(ACS)のURLがそのホスト名と一致することを確認します。
- アプライアンスがクラスタ内にある場合は、SAML外部認証を有効にする前に、各メンバのマシンレベルでSAMLを設定することを検討してください。
- IdPがアプライアンスごとに個別のアプリケーションまたはレルムを必要とするかどうかを判断します。
- 必要な証明書と鍵が使用可能であることを確認します。
- ESA/SMAロールマッピングに必要なグループ属性またはロール属性がIdPから送信されることを確認します。

---

注意：このドキュメントは、エンドユーザ隔離(EUQ)SAML SSOには適用されません。

---

## バックグラウンド情報

- Cisco TACでは、サードパーティ製のIdP設定に関するテクニカルサポートは提供していません。一般的なIdPの設定例を参照できます。

SSO SAML IdP

- Duo Access Gateway(DAG)は、SAML 2.0フェデレーションを使用した一般的なクラウドサービスを備えた2要素認証を追加します。
- Active Directoryフェデレーションサービス(ADFS) - ADFS 2、3、4、Azure Active Directory (Azure AD)、SecureAUTH、およびPingFederateでテスト済み
- SAML 2.0シングルサインオンフレームワーク内でIdPがサポートする場合は、追加の2要素認証を使用できます。
- Oktaは、サービスをサポートするIdPによる認証をサポートします。

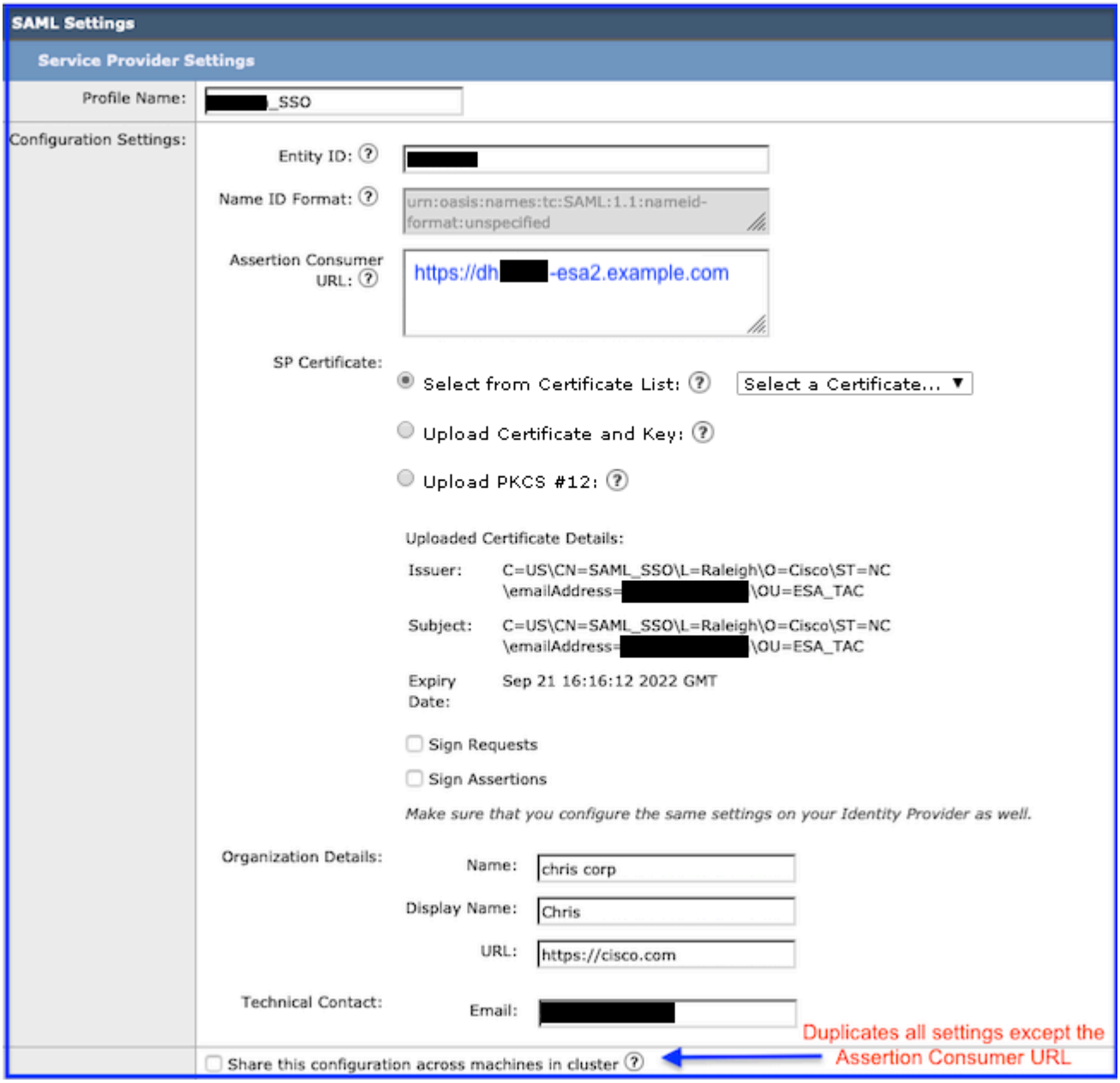
### サービスプロバイダーとしてのESA/SMAの設定

System Administration > SAML > (Machine Level) > Add Service Providerの順に移動します。

注：クラスタ内のESAでは、SAMLを有効にする前に、クラスタのすべてのメンバーに対するマシンレベルの設定が必要です。

- ページの下部にあるShare this configuration across machines in the clusterオプションを選択した場合、次の条件が適用されます。
  - アサーションコンシューマURLを除くすべてのフィールドがクラスタメンバーに複製されます。
  - Assertion Consumer URLは、管理インターフェイスのホスト名をACSとして自動入力します。
  - 代替ホスト名を使用してホストにアクセスする環境では、CESホスト型アプライアンスなど、各ホストの手動設定が必要です。
  - プロファイル名:ESAまたはSMAインターフェイスでSPインスタンスにラベルを付けるために使用される名前。
  - エンティティID: IdPが認識するSPインスタンスの名前。この名前は、SPを表すためにIdPによって使用されるラベルです。任意の名前（ESA_SPやESA_SSOなど）を指定できます。
  - Name ID Format：設定不可能なフィールド。
  - Assertion Consumer URL(ASSUMER)またはAssertion Consumer Service(ACS)：このESA/SMAホストと通信するためにIdPによって使用されるURL。
  - SP証明書:
    - 形式:PFX/PKCS12形式またはPEM形式のX.509パブリック/プライベート証明書。
    - オプション1：証明書リストから選択:ESAで作成済みの証明書をネットワーク>証明書から選択します。
    - オプション2：証明書とキーのアップロード:PEM形式の証明書とキーをアップロードします。
    - オプション3:PKCS #12のアップロード:PKCS #12ファイルをアップロードします。
    - オプション：SAMLシングルサインオン用にESA/SMAで自己署名証明書を作成します。
    - 必要に応じて、秘密キーをパスワードで保護します。

注:PEM形式の証明書を使用する場合は、各証明書と秘密キーを別々のファイルに保存してください。




サービスプロバイダー設定ページ

サービスプロバイダー設定ページ

- Sign Requests:IdPに送信されるESA/SMA SAML通信に署名するオプション。
- Sign Assertions:ESA/SMAに送信されるアサーションにIdPによる署名を要求するオプション。
- 組織の詳細：適切な会社データを入力できます。
- 設定を保存するには、SubmitとCommit Changesを実行します。
- SAML構成ページからSPメタデータをダウンロードします。

## ESA/SMAアプライアンスと連携するためのアイデンティティプロバイダー(IdP)の設定

注：一部のIdPでは、ESAごとに個別のアプリケーションまたはレルムが必要です（例：DUO）。

これらのリンクは、発行時点での複数のIdPの設定例を示しています。
Cisco TACでは、サードパーティ製品に対するテクニカルサポートは提供していません。これらの例は参考資料として提供されています。

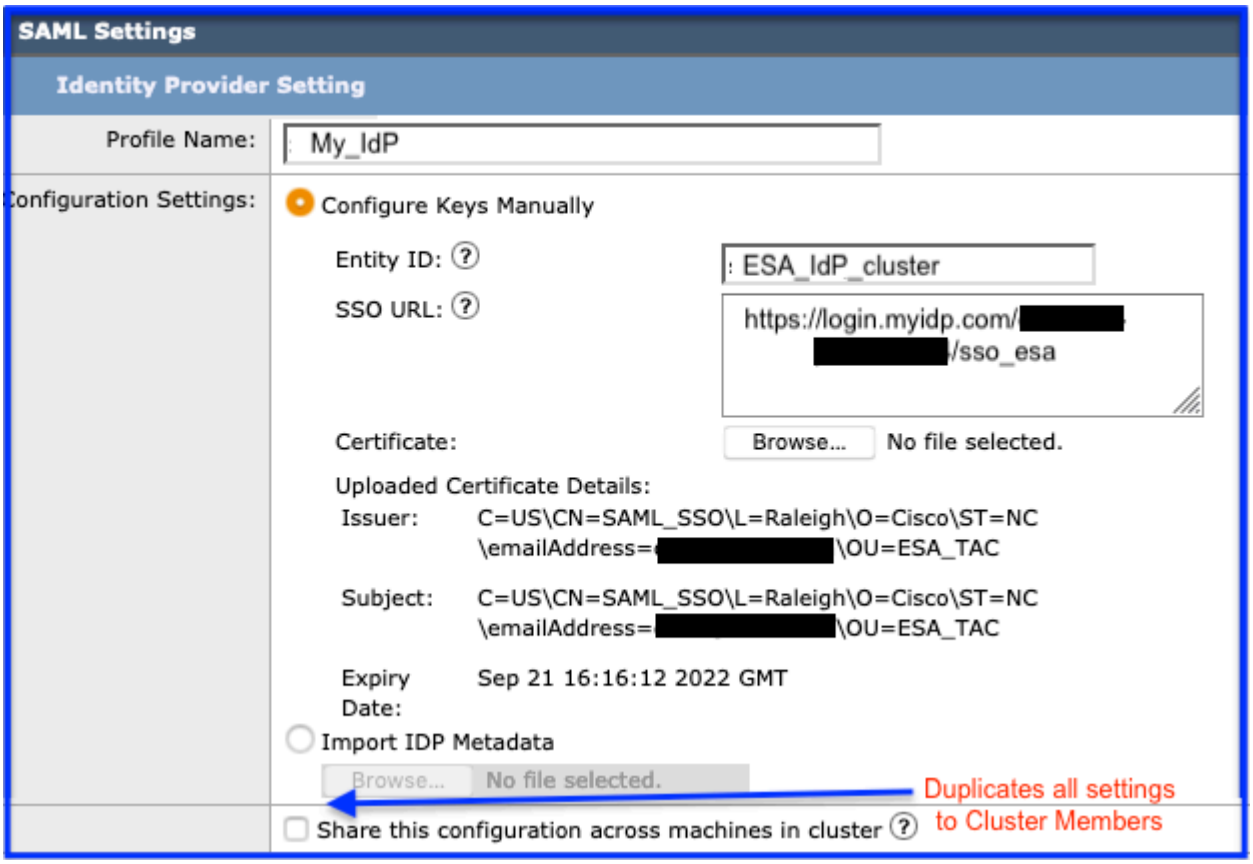
## ESA/SMAでのIDP設定

1. 「システム管理」>「SAML」に移動します。

2. 「IDプロバイダの追加」を選択します。

- 次の2つのオプションを使用できます。
- IdPメタデータのインポート
- キーの手動設定:
  - エンティティID: IdPを識別するために使用される任意の値です
  - SSO URL:SPがSAML認証要求を送信するURL
  - 秘密キーと公開証明書を別々のファイルにアップロードする

3. この設定をクラスタ内のマシン間で共有し、クラスタ内のすべてのESA間で設定を複製します。

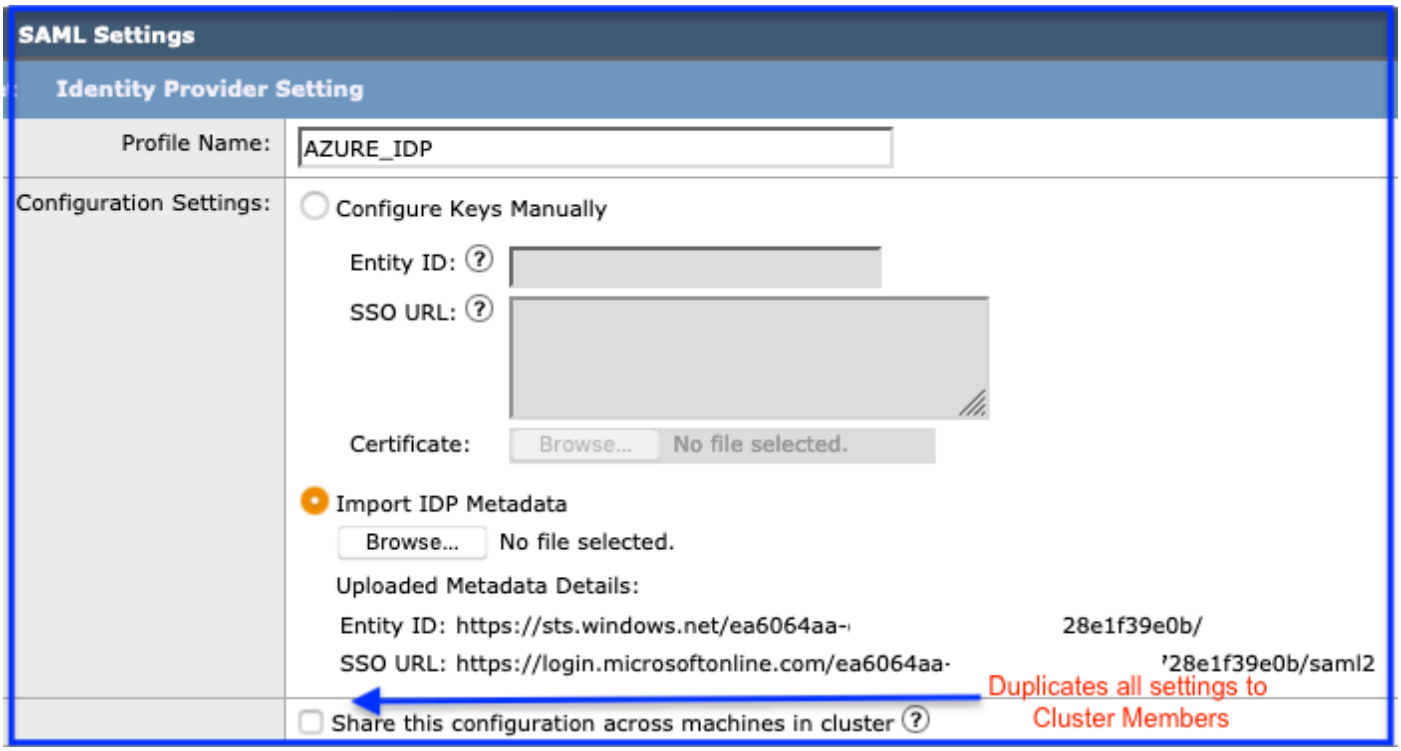



IdPコンテンツの手動入力

IdPコンテンツの手動入力

4. IdPからのメタデータのアップロード

- Import IdP Metadataを選択します。
- IdPから保存されたメタデータファイルを参照し、設定を保存します。
- 導入に適用される場合、クラスタ内のマシン間でこの設定を共有するオプションを使用できます。




Idpからのメタデータのアップロード

Idpからのメタデータのアップロード

## ESA/SMAでのSAMLを使用した外部認証の有効化

LDAP外部認証と同様に、SAMLシングルサインオンでは、グループを管理者ロールに割り当てるためのマッピングが必要です。

1. System Administration > Users (Cluster Level) > External Authentication > Enableの順に移動します。

2.認証タイプとしてSAMLを選択します。

3. 名前マップと照合するための属性名（オプション）：グループマッピングから検索する属性名を入力します。

---

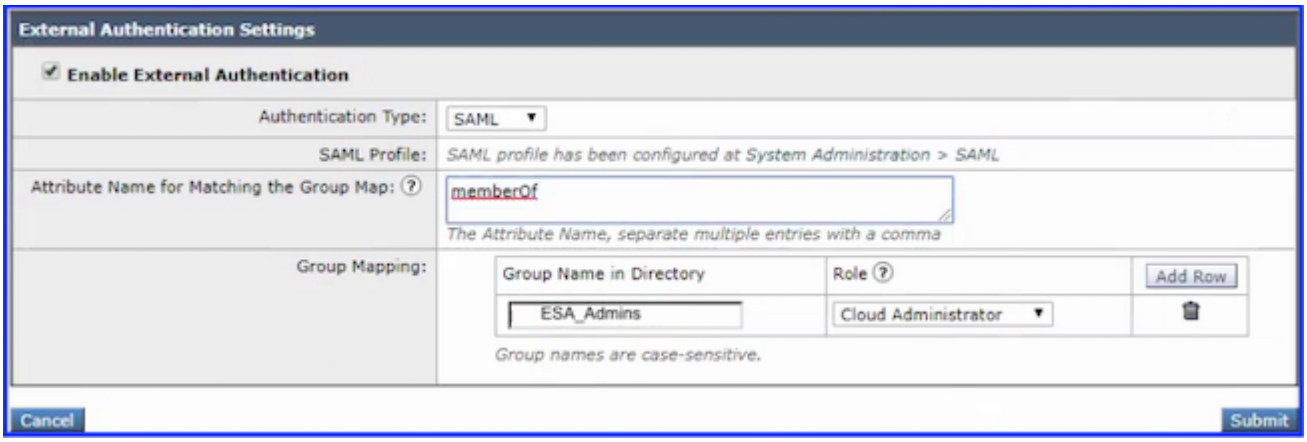
注：属性名は、アイデンティティプロバイダーがSAML応答でリレーするように設定された属性によって異なります。アプライアンスは、グループマッピングフィールドで設定された属性に対してSAML応答で指定された属性名の一致エントリを検索します。このフィールドが設定されていない場合、アプライアンスはSAML応答に存在するすべての属性を、設定されているグループマッピングフィールドと照合します。

---

4. 事前定義またはカスタムのユーザロールに基づいて、SAMLディレクトリで定義されているグ

ループ名属性を入力します。

- Group Mappingフィールドには、group属性が含まれている必要があります。SAMLアサーションまたは応答を認証するために、未指定グループ属性を追加できます。




外部認証の設定

外部認証の設定

5. 変更を送信し、確定します。

設定が正常に完了すると、ログオンページの下部に新しいリンクが表示されます。ESA/SMAのログオンページに、管理者を企業IDプロバイダー(IdP)にリダイレクトする「シングルサインオンを使用」リンクが表示されます。

選択すると、管理者は社内SAMLログオンページにリダイレクトされます。


シングルサインオンリンクを使用すると、SAMLにリダイレクトされます。

SAMLへのシングルサインオンリンクリダイレクトを使用する

# トラブルシュート

これらのインジケータを使用して、問題がアプライアンス設定とIdP設定のどちらに関連しているかを特定します。

## SSOリダイレクトリンクがログインページに表示されない（「シングルサインオンを使用」）

System Administration > Users > External Authentication > SAMLが設定されていることを確認します。

## リダイレクトが「Single Sign-On Authentication Failed!管理者に問い合わせてください。」

エラー:「シングルサインオン認証に失敗しました！管理者に問い合わせてください。」

- IdPで認証に失敗しました。
  - これは、シングルサインオン認証ページに到達してクレデンシャルを送信するまで、設定が機能していることを示します。
  - この障害はIdP設定が原因で発生することが多く、IdP設定の追加検証が必要です。

## 「Authorization Failure!」でESA/SMAログインページに戻るリダイレクト管理者に問い合わせてください。」

エラー:「認証エラー！管理者に問い合わせてください。」

- 認証は成功しましたが、ESA/SMAで認証に失敗しました。
  - Users > External Authentication > SAML内の設定に注目してください。
    - 属性名、グループ名、およびグループマッピング。

# 関連情報

- Cisco Eメールセキュリティアプライアンス – ユーザガイド
- Ciscoコンテンツセキュリティ管理アプライアンス – ユーザガイド

- Cisco Webセキュリティ：ユーザガイド

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。