Azure AD

概要

ここでは、Azure AD SAML アプリケーションを作成し、それを Security Cloud Sign On と統合する方法を示します。

（注）

- Azure AD ユーザーのユーザープリンシパル名（UPN）は、ユーザーの電子メールアドレスと同じとは限らないことに注意してください。
- SAML 応答の `<NameID>` 要素と `email` ユーザー属性には、ユーザーの電子メールアドレスを含める必要があります。詳細については、「SAML 応答の要件」を参照してください。
- 指定された電子メールアドレスは、既存の製品のアクセス制御で使用されているものと一致する必要があります。一致しない場合は、製品のアクセス制御を更新する必要があります。

はじめに

始める前に

- 管理者権限で Azure ポータルにサインインできる必要があります。
- エンタープライズ設定ウィザードの ステップ 1：エンタープライズの作成 と ステップ 2：電子メールドメインの申請と検証 が完了している必要があります。

ステップ 1 https://portal.azure.com にサインインします。

アカウントで複数のテナントにアクセスできる場合は、右上隅でアカウントを選択します。ポータルセッションを必要な Azure AD テナントに設定します。

a) [Azure Active Directory] をクリックします。
b) 左側のサイドバーで[エンタープライズアプリケーション（Enterprise Applications）] をクリックします。
c) [+新しいアプリケーション（+ New Application）] をクリックし、[Azure AD SAML Toolkit（Azure AD SAML Toolkit）] を探します。
d) [Azure AD SAML Toolkit（Azure AD SAML Toolkit）] をクリックします。
e) [名前（Name）] フィールドに「**SecureX Sign On**」またはその他の値を入力し、[作成（Create）] をクリックします。
f) [概要（Overview）] ページで、左側のサイドバーの [管理（Manage）] の下にある [シングルサインオン（Single Sign On）] をクリックします。
g) [シングルサインオン方式の選択（select single sign on method）] で [SAML（SAML）] を選択します。
h) [基本的なSAML構成（Basic SAML Configuration）] パネルで [編集（Edit）] をクリックします。
   - [識別子（エンティティID）（Identifier (Entity ID)）] で [識別子の追加（Add Identifier）] をクリックし、**https://example.com** または他の有効な URL の一時的な値を入力します。この一時的な値は後で置き換えます。
   - [応答URL（Assertion Consumer Service URL）（Reply URL (Assertion Consumer Service URL)）] で [応答URLの追加（Add reply URL）] をクリックし、**https://example.com** または他の有効な URL の一時的な値を入力します。この一時的な値は後で置き換えます。
   - [サインオンURL（Sign on URL）] フィールドに「**https://sign-on.security.cisco.com/**」と入力します。
   - [保存（Save）] をクリックし、[基本的なSAML構成（Basic SAML Configuration）] パネルを閉じます。
i) [必要な要求（Required claim）] で [一意のユーザー識別子（名前ID）（Unique User Identifier (Name ID)）] 要求をクリックして編集します。
j) [ソース属性（Source attribute）] フィールドを `user.userprincipalname` に設定します。

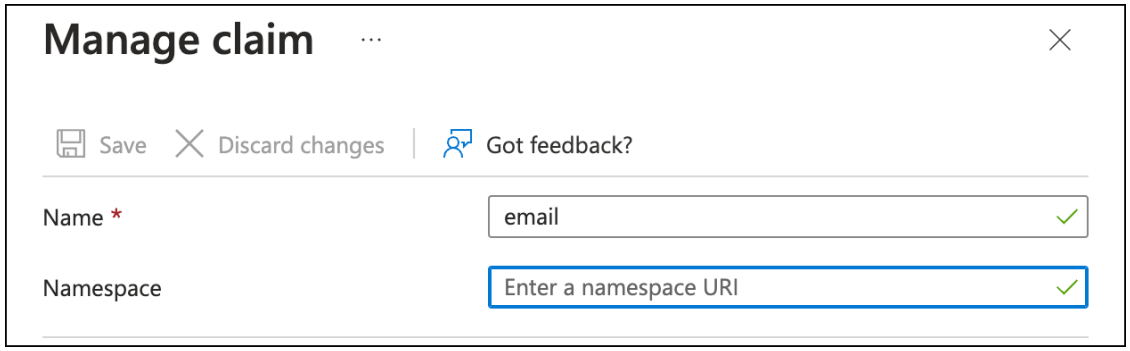
   ここでは、**user.userprincipalname** の値が有効な電子メールアドレスを表していることを前提としています。それ以外の場合は、[ソース（Source）] で **user.primaryauthoritativeemail** を使用するように設定します。
k) [追加の要求（Additional Claims）] パネルで [編集（Edit）] をクリックし、Azure AD ユーザープロパティと SAML 属性の間の次のマッピングを作成します。

   ここでは、**user.userprincipalname** の値が有効な電子メールアドレスを表していることを前提としています。それ以外の場合は、**email** 要求の [ソース属性（Source attribute）] で **user.primaryauthoritativeemail** を使用するように設定します。

名前	名前空間	ソース属性
`email`	値なし	`user.userprincipalname`

名前	名前空間	ソース属性
firstName	値なし	user.givenname
lastName	値なし	user.surname

各要求の [名前空間（Namespace）] フィールドは必ずクリアしてください。



l) [SAML証明書（SAML Certificates）] パネルで、[証明書（Base64）（Certificate (Base64)）] 証明書の [ダウンロード（Download）] をクリックします。

m) この手順の後半で使用するために、[SAMLによるシングルサインオンのセットアップ（Set up Single Sign-On with SAML）] セクションで [ログインURL（Login URL）] と [Azure AD識別子（Azure AD Identifier）] の値をコピーします。

ステップ 2 新しいブラウザタブでエンタープライズ設定ウィザードを開きます。[IDプロバイダーの統合（Integrate Identity Provider）]>[セットアップ（Set Up）] 画面（ステップ 3：SAML メタデータの交換）が表示されます。

a) [IDプロバイダー（IdP）名（Identity Provider (IdP) Name）] フィールドに「**Azure SSO**」または統合の他の名前を入力します。

b) [シングルサインオンサービスURL（Single Sign-On Service URL）] フィールドに、Azure からコピーした [ログインURL（Login URL）] の値を入力します。

c) [エンティティID（オーディエンスURI）（Entity ID (Audience URI)）] フィールドに、Azure からコピーした [Azure AD識別子（Azure AD Identifier）] の値を入力します。

d) [ファイルの追加（Add File）] をクリックし、Azure ポータルからダウンロードした SAML 署名証明書をアップロードします。

e) 必要に応じて、無料の Duo MFA からユーザーをオプトアウトします。

f) [ダウンロード（Download）] 画面で [次へ（Next）] をクリックします。

g) この手順の後半で使用するために、[シングルサインオンサービスURL（ACS URL）（Single Sign-On Service URL (ACS URL)）] と [エンティティID（オーディエンスURI）（Entity ID (Audience URI)）] の値をコピーします。

h) [Next] をクリックします。

ステップ 3 Azure コンソールのブラウザタブに戻ります。

a) [基本的なSAML構成（Basic SAML Configuration）] セクションで [編集（Edit）] をクリックします。

b) [識別子（エンティティID）（Identifier (Entity ID)）] フィールドに入力した一時的な ID プロバイダーを、エンタープライズ設定ウィザードからコピーした [エンティティID（オーディエンスURI）（Entity ID (Audience URI)）] フィールドの値に置き換えます。

c) [応答URL（Assertion Consumer Service URL）（Reply URL (Assertion Consumer Service URL)）] フィールドに入力した一時的な ID プロバイダーを、エンタープライズ設定ウィザードからコピーした [シングルサインオンサービスURL（ACS URL）（Single Sign-On Service URL (ACS URL)）] フィールドの値に置き換えます。

d) [保存（Save）] をクリックし、[基本的なSAML構成（Basic SAML Configuration）] パネルを閉じます。

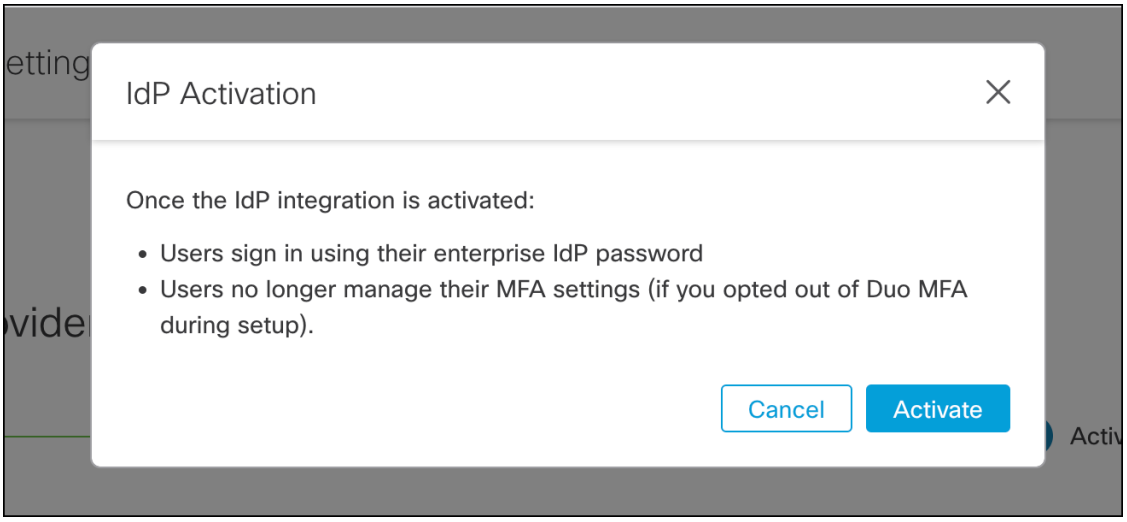
ステップ 4 エンタープライズ設定ウィザードに戻り、統合をテストします。[構成（Configure）] 画面（ステップ 4：SSO 統合のテスト）で次の手順を実行します。

a) 提供された URL をコピーし、プライベート（シークレット）ウィンドウで開きます。

b) SAML アプリケーションに関連付けられた Azure AD アカウントでサインインします。SecureXアプリケーションポータルに戻れば、テストは成功です。エラーが発生する場合は、トラブルシューティング を参照してください。

c) [次へ（Next）] をクリックして [アクティブ化（Activate）] 画面に進みます。

d) 準備ができたら、[IdPをアクティブ化（Activate my IdP）] をクリックし、ダイアログボックスで選択内容を確認します。



翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。