ID サービスプロバイダーの手順

このガイドでは、Security Cloud Sign On をさまざまなアイデンティティ（ID）サービスプロバイダーと統合する手順について説明します。

Auth0 の Security Cloud Sign On との統合

このガイドでは、Auth0 SAML Addon を Security Cloud Sign On と統合する方法について説明します。

始める前に

開始する前に、「ID プロバイダー統合ガイド」を読み、プロセス全体を理解してください。これらの手順は、前述のガイドの特に「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する」および「ステップ 3：IdP から Security Cloud に SAML メタデータを提供する」について、Auth0 SAML 統合に固有の詳細を補足します。

手順

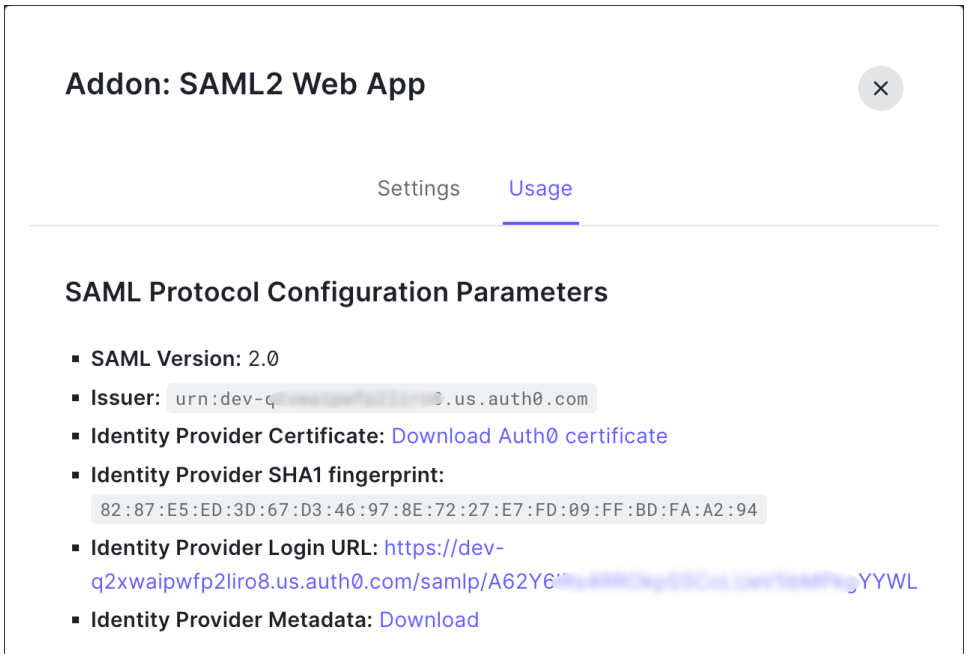
ステップ 1 Auth0 と統合する エンタープライズ で Security Provisioning and Administration にサインインします。

a) 「ステップ 1：初期設定」の説明に沿って、新しい ID プロバイダーを作成し、Duo MFA からオプトアウトするかどうかを決定します。

b) 「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する」で、**パブリック証明書**をダウンロードし、次の手順で使用する [エンティティID（Entity ID）] と [シングルサインオンサービスURL（Single Sign-On Service URL）] の値をコピーします。

ステップ 2 新しいブラウザタブで、管理者として Auth0 組織にサインインします。すぐに戻るので、Security Provisioning and Administration ブラウザタブは開いたままにしておきます。

a) [アプリケーション（Applications）] メニューから [アプリケーション（Applications）] を選択します。
b) [アプリケーションの作成（Create Application）] をクリックします。
c) [名前（Name）] フィールドに「**Secure Cloud Sign On**」または他の名前を入力します。
d) アプリケーションタイプとして [通常の Web アプリケーション（Regular Web Applications）] を選択し、[作成（Create）] をクリックします。
e) [アドオン（Addons）] タブをクリックします。
f) [SAML2 Web App（SAML2 Web App）] トグルをクリックしてアドオンを有効にします。
[SAML2 Web アプリケーションの構成（SAML2 web App configuration）] ダイアログが開きます。

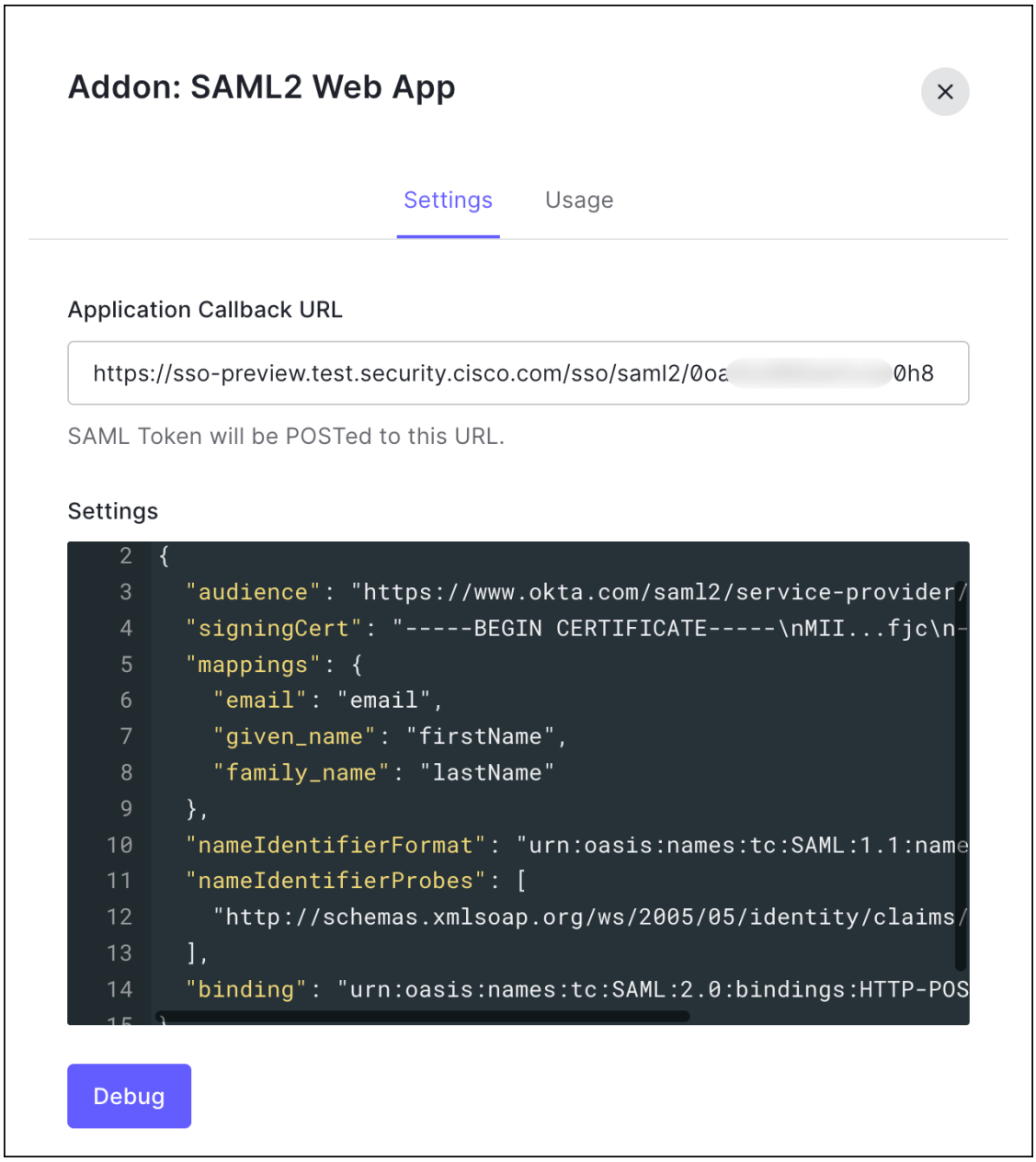


g) [使用（Usage）] タブで、Auth0 の [IDプロバイダー証明書（Identity Provider Certificate）] と [IDプロバイダーのメタデータ（Identity Provider Metadata）] ファイルをダウンロードします。
h) [設定（Settings）] タブをクリックします。
i) [アプリケーションコールバック URL（Application Callback URL）] フィールドに、エンタープライズ設定ウィザードからコピーした [シングルサインオンサービス URL（Single Sign-On Service URL）] の値を入力します。
j) [設定（Settings）] フィールドに次の JSON オブジェクトを入力します。「`audience`」の値は、提供された [エンティティ ID（オーディエンス URI）（Entity ID (Audience URI)）] の値に置き換え、「`signingCert`」は、Security Provisioning and Administration から提供された署名証明書の内容を 1 行のテキストに変換したものに置き換えます。

（注）
Cisco Security Cloud Sign On でログインするには、名と姓を入力する必要があります。Auth0 で使用されるユーザー アイデンティティ ソースによっては、SAML アサーションでユーザーの姓名を使用するために、追加の設定が必要になる場合があります。

次の例は、JSON で given_name と family_name の属性が使用可能で、SAML アサーションで firstName と lastNam にそれぞれマッピングすることを想定しています。

```
{
  "audience": "...",
  "signingCert": "-----BEGIN CERTIFICATE-----\n...-----END CERTIFICATE-----\n",
  "mappings": {
    "email": "email",
    "given_name": "firstName",
    "family_name": "lastName"
  },
  "nameIdentifierFormat": "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified",
  "nameIdentifierProbes": [
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
  ],
  "binding": "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
}
```



k) [Addon] ダイアログの下部にある [有効化（Enable）] をクリックしてアプリケーションを有効にします。

ステップ 3 Security Provisioning and Administration に戻り、[**次へ（Next）**] をクリックします。ステップ 3：IdP から Security Cloud に SAML メタデータを提供する の画面が表示されます。

a) [XMLファイルのアップロード（XML file upload）] オプションを選択します。

b) Auth0 から提供された [IDプロバイダーのメタデータ（Identity Provider Metadata）] ファイルをアップロードします。

次のタスク

次に、「ステップ 4：SAML 統合のテスト」および「ステップ 5：統合のアクティブ化」の手順に従って、統合をテストしてアクティブ化します。

Microsoft Entra ID の Security Cloud Sign On との統合

このガイドでは、Microsoft Entra ID と Security Provisioning and Administration を統合する方法について説明します。

始める前に

開始する前に、「ID プロバイダー統合ガイド」を読み、プロセス全体を理解してください。これらの手順は、前述のガイドの特に「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する」および「ステップ 3：IdP から Security Cloud に SAML メタデータを提供する」について、Microsoft Entra ID SAML 統合に固有の詳細を補足します。

手順

ステップ 1 Microsoft Entra ID と統合するエンタープライズで Security Provisioning and Administration にサインインします。

a) 「ステップ 1：初期設定」の説明に沿って、新しい ID プロバイダーを作成し、Duo MFA からオプトアウトするかどうかを決定します。

b) 「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する」で、**パブリック証明書**をダウンロードし、次の手順で使用する [エンティティ ID（Entity ID）] と [シングルサインオンサービス URL（Single Sign-On Service URL）] の値をコピーします。

ステップ 2 新しいブラウザタブで、https://portal.azure.com に管理者としてサインインします。すぐに戻るので、Security Provisioning and Administration タブは開いたままにしておきます。

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 Microsoft Entra ID 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、[Microsoft Entra SAML Toolkit] を探します。

d) [Microsoft Entra SAML Toolkit] をクリックします。

e) [名前（Name）] フィールドに「**`Security Cloud 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、以下を行います。

- [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、Security Provisioning and Administration から提供された [エンティティID（Entity ID）] の URL を入力します。
- [応答URL（アサーションコンシューマサービスURL）（Reply URL (Assertion Consumer Service URL)）] で、[応答URLの追加（Add Reply URL）] をクリックし、Security Provisioning and Administration からの [シングルサインオンサービスURL（Single Sign-On Service URL）] を入力します。
- [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。

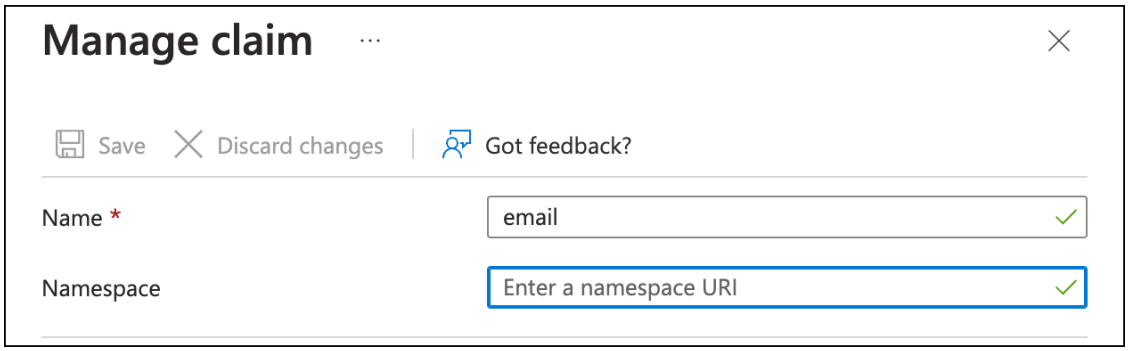
i) [属性と要求（Attributes & Claims）] パネルで、[編集（Edit）] をクリックします。

- [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。
- [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）] を「**user.primaryauthoritativeemail**」に設定します。

j) [追加の要求（Additional Claims）] パネルで [編集（Edit）] をクリックし、Microsoft Entra ID 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。

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

次に示すように、要求ごとに [名前空間（Namespace）] フィールドは必ずクリアしてください。



k) [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。

l) この手順で後ほど使用するために、[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 [Microsoft Entra識別子（Microsoft Entra Identifier）] の値をコピーします。

ステップ 3 Security Provisioning and Administration に戻り、[**次へ（Next）**] をクリックします。ステップ 3：IdP から Security Cloud に SAML メタデータを提供する の画面が表示されます。

a) [手動構成（Manual Configuration）] オプションを選択します。

b) [シングルサインオンサービスURL（アサーションコンシューマサービスURL）（Single Sign-on Service URL (Assertion Consumer Service URL)）] フィールドに、Azure から提供された [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、Microsoft Entra ID によって提供される [Microsoft Entra識別子（Microsoft Entra Identifier）] の値を入力します。

d) Azure で提供された**署名証明書**をアップロードします。

（注）
Azure によって提供される署名証明書ファイルの拡張子は **.cer** です。ただし、Security Provisioning and Administration で証明書を受け入れるには、ファイル拡張子を **.cert** に変更してからアップロードします。

ステップ 4 Security Provisioning and Administration で [次へ（Next）] をクリックします。

次のタスク

「ステップ 4：SAML 統合のテスト」および「ステップ 5：統合のアクティブ化」に従って、統合をテストしてアクティブ化します。

Duo の Security Cloud Sign On との統合

このガイドでは、Duo SAML アプリケーションを Security Cloud Sign On と統合する方法について説明します。

始める前に

開始する前に、「ID プロバイダー統合ガイド」を読み、プロセス全体を理解してください。これらの手順は、前述のガイドの特に「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する」および「ステップ 3：IdP から Security Cloud に SAML メタデータを提供する」について、Duo SAML 統合に固有の詳細を補足します。

手順

ステップ 1 Duo と統合する エンタープライズ で Security Provisioning and Administration にサインインします。

a) 「ステップ 1：初期設定」の説明に沿って、新しい ID プロバイダーを作成し、Duo MFA からオプトアウトするかどうかを決定します。

b) 「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する」で、**パブリック証明書**をダウンロードし、次の手順で使用する [エンティティID（Entity ID）] と [シングルサインオンサービスURL（Single Sign-On Service URL）] の値をコピーします。

ステップ 2 新しいブラウザタブで、管理者として Duo 組織にサインインします。すぐに戻るので、Security Provisioning and Administration タブは開いたままにしておきます。

a) 左側のナビゲーションメニューから **[アプリケーション（Applications）]** > **[アプリケーションの保護（Protect an Application）]**をクリックします。

b) 検索バーで、**Cisco Security Cloud Sign On** と検索します。

c) [汎用サービスプロバイダー（Generic Service Provider）] アプリケーションの横にある [保護（Protect）] をクリックし、保護タイプとして [Duoがホストする SSOによる2FA（2FA with SSO hosted by Duo）] を選択します。

汎用 SAML サービスプロバイダーの構成ページが開きます。

d) [メタデータ（Metadata）] セクションを選択します。

e) [エンティティID（Entity ID）] の値をコピーし、後で使用するために保存します。

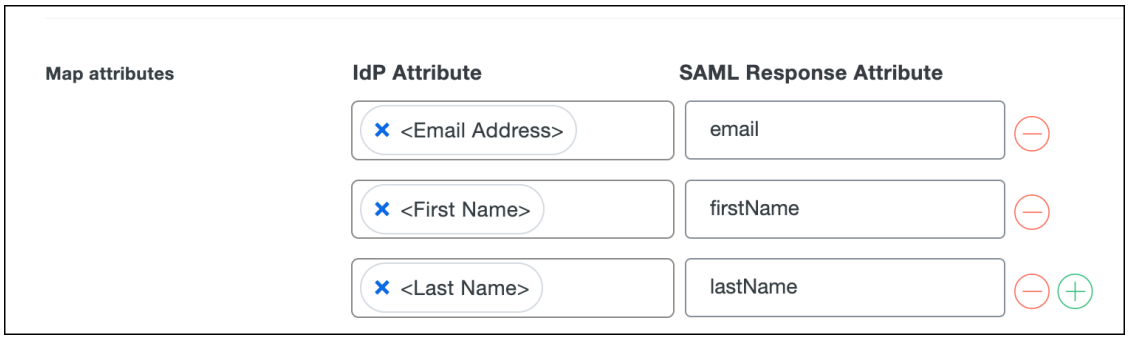
f) [シングルサインオンURL（Single Sign-On URL）] の値をコピーし、後で使用するために保存します。

g) 後で使用するため、[ダウンロード（Downloads）] セクションで [証明書のダウンロード（Download certificate）] をクリックします。

h) [SAML応答（SAML Response）] セクションで次の手順を実行します。

- [NameID形式（NameID format）] で [urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified] または [urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress] を選択します。
- [NameID属性（NameID attribute）] で [<Email Address>] を選択します。
- [属性のマッピング（Map Attributes）] セクションで、Duo IdP ユーザー属性とSAML 応答属性の次のマッピングを入力します。

IdP属性（IdP Attribute）	SAML応答属性（SAML Response Attribute）
<Email Address>	**email**
<First Name>	**firstName**
<Last Name>	**lastName**



i) [設定（Settings）] の [名前（Name）] フィールドに「**Security Cloud Sign On**」または他の値を入力します。

ステップ 3 Security Provisioning and Administration に戻り、[**次へ（Next）**] をクリックします。ステップ 3：IdP から Security Cloud に SAML メタデータを提供する の画面が表示されます。

a) [手動構成（Manual Configuration）] オプションを選択します。
b) [シングルサインオンサービスURL（アサーションコンシューマサービスURL）（Single Sign-on Service URL (Assertion Consumer Service URL)）] フィールドに、Duo から提供された [シングルサインオンURL（Single Sign-On 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、Duo から提供された [エンティティID（Entity ID）] の値を入力します。
d) Duo からダウンロードした**署名証明書**をアップロードします。

次のタスク

次に、「ステップ 4：SAML 統合のテスト」および「ステップ 5：統合のアクティブ化」の手順に従って、統合をテストしてアクティブ化します。

Google ID の Security Cloud Sign On との統合

このガイドでは、Google ID SAML アプリケーションを Security Cloud Sign On と統合する方法について説明します。

始める前に

開始する前に、「ID プロバイダー統合ガイド」を読み、プロセス全体を理解してください。これらの手順は、前述のガイドの特に「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する」および「ステップ 3：IdP から Security Cloud に SAML メタデータを提供する」について、Google ID 統合に固有の詳細を補足します。

手順

ステップ 1 Google と統合するエンタープライズで Security Provisioning and Administration にサインインします。

a) 「ステップ 1：初期設定」の説明に沿って、新しい ID プロバイダーを作成し、Duo MFA からオプトアウトするかどうかを決定します。

b) 「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する」で、**パブリック証明書**をダウンロードし、次の手順で使用する [エンティティID（Entity ID）] と [シングルサインオンサービスURL（Single Sign-On Service URL）] の値をコピーします。

ステップ 2 新しいブラウザタブで、スーパー管理者権限を持つアカウントを使用してGoogle管理コンソールにサインインします。Security Provisioning and Administration タブは開いたままにします。

a) 管理コンソールで、メニュー ☰ > [アプリ（Apps）] > [ウェブアプリとモバイルアプリ（Web and mobile apps）] に移動します。

b) [アプリを追加（Add App）] > [カスタムSAMLアプリの追加（Add custom SAML app）] をクリックします。

c) [アプリの詳細（App Details）] で以下を行います。

- アプリケーション名に「**`Secure Cloud Sign On`**」または他の値を入力します。
- 必要に応じて、アプリケーションに関連付けるアイコンをアップロードします。

d) [続行（Continue）] をクリックして、[Google ID プロバイダー（Google Identity Provider）] の詳細ページに移動します。

e) [メタデータのダウンロード（Download Metadata）] をクリックして、後で使用するために Google SAML メタデータファイルをダウンロードします。

f) [続行（Continue）] をクリックして、[サービスプロバイダーの詳細（Service provider details）] ページに移動します。

g) [ACS URL（ACS URL）] フィールドに、Security Provisioning and Administration から提供された [シングルサインオンサービスURL（Single Sign-On Service URL）] を入力します。

h) [エンティティID（Entity ID）] フィールドに、Security Provisioning and Administration から提供された [エンティティID（Entity ID）] の URL を入力します。

i) [署名付き応答（Signed Response）] オプションをオンにします。

j) [名前IDの形式（Name ID Format）] で [UNSPECIFIED（UNSPECIFIED）] または [EMAIL（EMAIL）] を選択します。

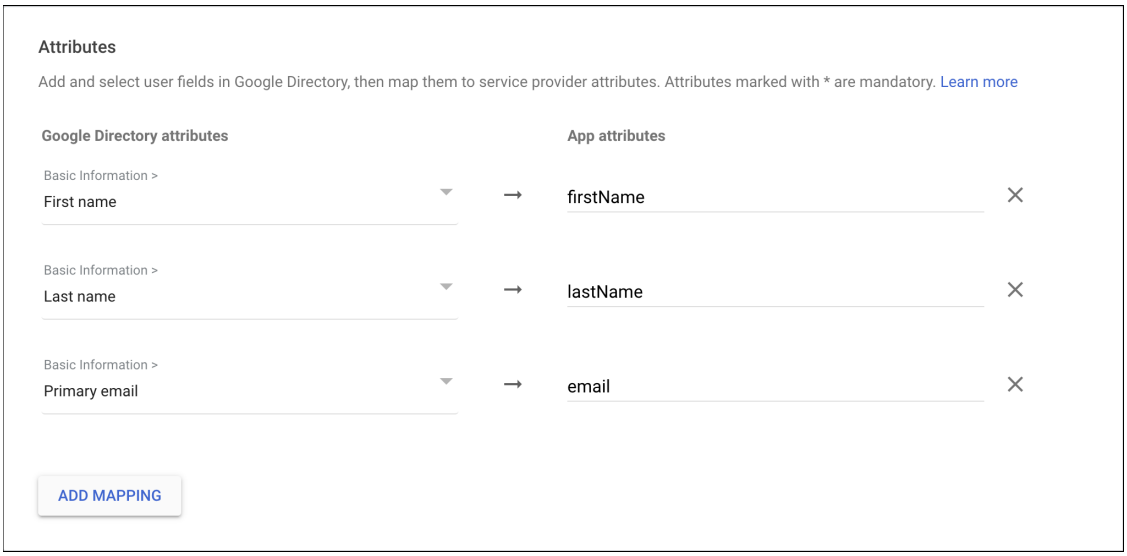
k) [名前ID（Name ID）] で [基本情報 > 主要電子メール（Basic Information > Primary email）] を選択します。

l) [続行（Continue）] をクリックして、[属性マッピング（Attribute mapping）] ページに進みます。

m) Google ディレクトリ属性とアプリケーション属性との次のマッピングを追加します。

Googleディレクトリの属性（Google Directory attributes）	**アプリの属性（App attributes）**
名（First name）	firstName

Googleディレクトリの属性（Google Directory attributes）	アプリの属性（App attributes）
姓（Last name）	lastName
Primary email	email



n) [終了（Finish）] をクリックします。

ステップ 3 Security Provisioning and Administration に戻り、[**次へ（Next**）] をクリックします。ステップ 3：IdP から Security Cloud に SAML メタデータを提供する の画面が表示されます。

a) [XMLファイルのアップロード（XML file upload）] オプションを選択します。
b) 以前に Google 社からダウンロードした SAML メタデータファイルをアップロードします。
c) [次へ（Next）] をクリックして [テスト（Testing）] ページに進みます。

次のタスク

次に、「ステップ 4：SAML 統合のテスト」および「ステップ 5：統合のアクティブ化」の手順に従って、統合をテストしてアクティブ化します。

Okta の Security Cloud Sign On との統合

このガイドでは、Okta SAML アプリケーションを Security Provisioning and Administration と統合する方法について説明します。

始める前に

開始する前に、「ID プロバイダー統合ガイド」を読み、プロセス全体を理解してください。これらの手順は、前述のガイドの特に「ステップ 2：ID プロバイダーに Security Cloud SAML

メタデータを提供する」および「ステップ 3：IdP から Security Cloud に SAML メタデータを提供する」について、Okta SAML 統合に固有の詳細を補足します。

手順

ステップ 1 Okta と統合するエンタープライズで Security Provisioning and Administration にサインインします。

a) 「ステップ 1：初期設定」の説明に沿って、新しい ID プロバイダーを作成し、Duo MFA からオプトアウトするかどうかを決定します。

b) 「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する」で、**パブリック証明書**をダウンロードし、次の手順で使用する [エンティティID（Entity ID）] と [シングルサインオンサービスURL（Single Sign-On Service URL）] の値をコピーします。

ステップ 2 新しいブラウザタブで、管理者として Okta 組織にサインインします。すぐに戻るので、Security Provisioning and Administration タブは開いたままにしておきます。

a) [アプリケーション（Applications）] メニューから [アプリケーション（Applications）] を選択します。

b) [アプリケーション統合の作成（Create App Integration）] をクリックします。

c) [SAML 2.0（SAML 2.0）] を選択し、[次へ（Next）] をクリックします。

d) [全般設定（General Settings）] タブで、統合の名前（例：**Security Cloud Sign On**）を入力し、必要に応じてロゴをアップロードします。

e) [次へ（Next）] をクリックして [SAMLの構成（Configure SAML）] ページに進みます。

f) [シングルサインオンURL（Single sign-on URL）] フィールドに、Security Provisioning and Administration から提供された [シングルサインオンサービスURL（Single sign-on Service URL）] を入力します。

g) [オーディエンスURI（Audience URI）] フィールドに、Security Provisioning and Administration から提供された [エンティティID（Entity ID）] を入力します。

h) [名前IDの形式（Name ID Format）] で [指定なし（Unspecified）] または [電子メールアドレス（EmailAddress）] を選択します。

i) [アプリケーションユーザー名（Application username）] で [Oktaユーザー名（Okta username）] を選択します。

j) [属性ステートメント（オプション）（Attribute Statements (optional)）] セクションで、次の名前 SAML 属性のマッピングを Okta ユーザープロファイルに追加します。

名前（Name）（SAMLアサーション）	値（Value）（Okta プロファイル）
email	user.email
firstName	user.firstName
lastName	user.lastName

k) [Show Advanced Settings] をクリックします。

l) [次へ（Next）] をクリックします。

m) [署名証明書（Signature Certificate）] で、[ファイルの参照（Browse files...）] をクリックし、以前に Security Provisioning and Administration からダウンロードした公開署名証明書をアップロードします。

（注）

応答とアサーションは、RSA-SHA256 アルゴリズムで署名する必要があります。

n) [サインオン（Sign On）]、[設定（Settings）]、[サインオン方法（Sign on method）] の順に選択し、[詳細の表示（Show details）] をクリックします。
o) [次へ（Next）] をクリックして Okta にフィードバックを送信し、[完了（Finish）] をクリックします。
p) [サインオンURL（Sign on URL）] と [発行者（Issuer）] の値をコピーし、**署名証明書**をダウンロードして Security Provisioning and Administrationに提供します。

ステップ 3 Security Provisioning and Administration に戻り、[**次へ（Next**）] をクリックします。ステップ 3：IdP から Security Cloud に SAML メタデータを提供する の画面が表示されます。

a) [手動構成（Manual Configuration）] オプションを選択します。
b) [シングルサインオンサービスURL（アサーションコンシューマサービスURL）（Single Sign-on Service URL (Assertion Consumer Service URL)）] フィールドに、Okta から提供された [サインオンURL（Sign on 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、Okta から提供された [発行者（Issuer）] の値を入力します。
d) Okta から提供された**署名証明書**をアップロードします。

次のタスク

次に、「ステップ 4：SAML 統合のテスト」および「ステップ 5：統合のアクティブ化」の手順に従って、統合をテストしてアクティブ化します。

Ping ID の Security Cloud Sign On との統合

このガイドでは、Ping SAML アプリケーションを Security Cloud Sign On と統合する方法について説明します。

始める前に

開始する前に、「ID プロバイダー統合ガイド」を読み、プロセス全体を理解してください。これらの手順は、前述のガイドの特に「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する」および「ステップ 3：IdP から Security Cloud に SAML メタデータを提供する」について、Ping 統合に固有の詳細を補足します。

手順

ステップ 1 Ping と統合するエンタープライズで Security Provisioning and Administration にサインインします。

a) 「ステップ 1：初期設定」の説明に沿って、新しい ID プロバイダーを作成し、Duo MFA からオプトアウトするかどうかを決定します。

b) 「ステップ 2：ID プロバイダーに Security Cloud SAML メタデータを提供する」で、後で使用するために **Security Cloud Sign On SAML メタデータ**ファイルをダウンロードします。

ステップ 2 新しいブラウザタブで、Ping 管理コンソールにサインインします。Security Provisioning and Administration ブラウザタブを開いたままにします。

a) [接続（Connections）] > [アプリケーション（Applications）] に移動します。

b) [+] ボタンをクリックして [アプリケーションの追加（Add Application）] ダイアログを開きます。

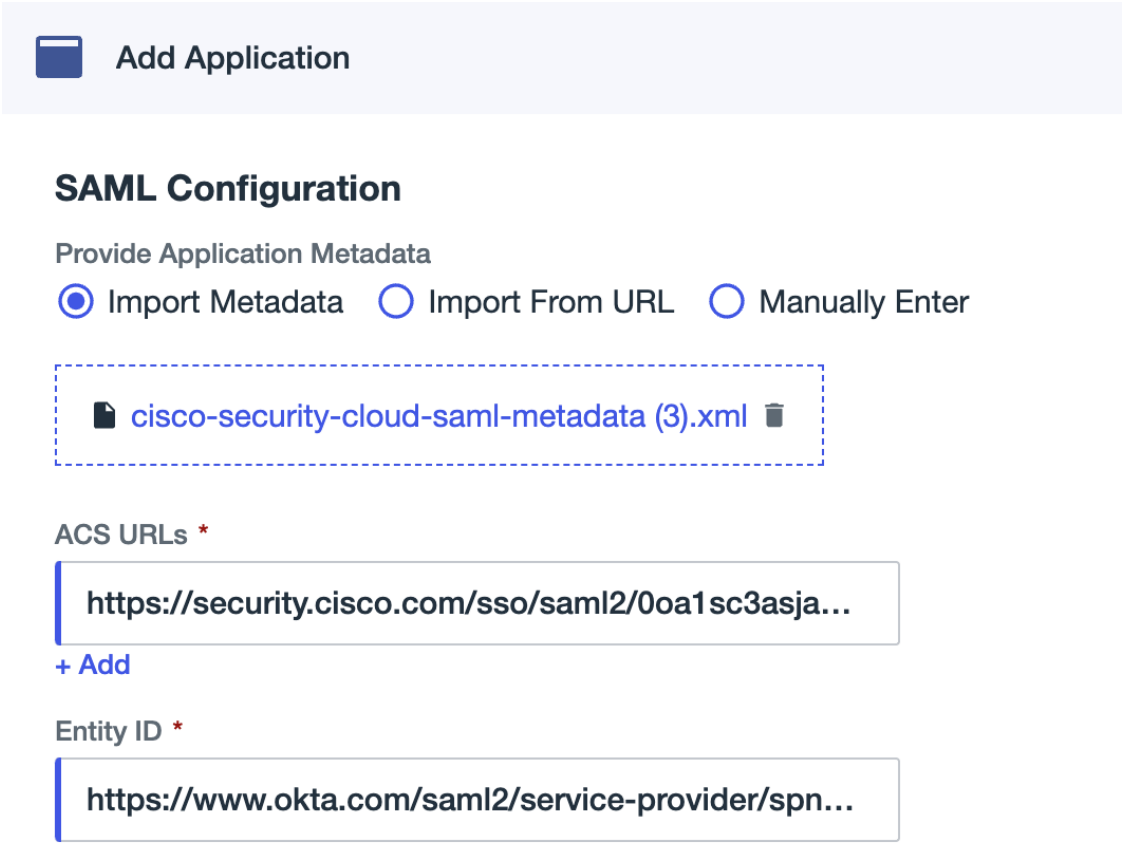
c) [アプリケーション名（Application Name）] フィールドに「**`Secure Cloud Sign On`**」または他の名前を入力します。

d) 必要に応じて、説明を追加し、アイコンをアップロードします。

e) [アプリケーションの種類（Application Type）] で [SAMLアプリケーション（SAML application）] を選択し、[構成（Configure）] をクリックします。

f) [SAML構成（SAML Configuration）] ダイアログで、[メタデータのインポート（Import Metadata）] オプションを選択し、[ファイルの選択（Select a file）] をクリックします。

g) Security Provisioning and Administration からダウンロードした **Security Cloud Sign On SAML メタデータ**ファイルを見つけます。



h) [保存（Save）] をクリックします。

i) [設定（Configuration）] タブをクリックします。

j) [メタデータのダウンロード（Download Metadata）] をクリックして、Security Provisioning and Administration に提供する SAML メタデータファイルをダウンロードします。

k) [属性のマッピング（Attribute Mappings）] タブをクリックします。

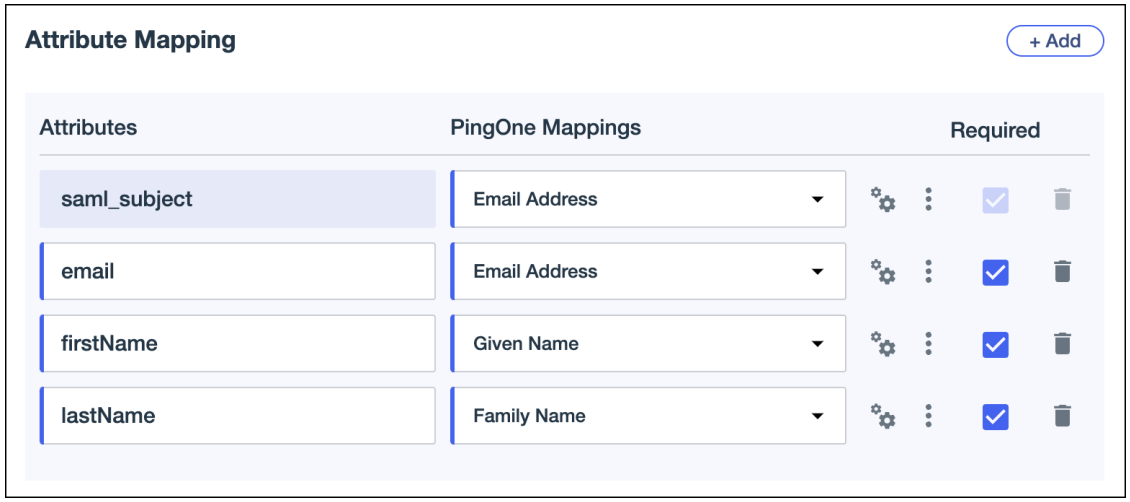
l) [編集（Edit）]（鉛筆アイコン）をクリックします。

m) 必須の [saml_subject（saml_subject）] 属性について、[電子メールアドレス（Email Address）] を選択します。

n) [+追加（+Add）] をクリックし、SAML 属性と PingOne ユーザー ID 属性の次のマッピングを追加し、それぞれのマッピングで [必須（Required）] オプションを有効にします。

属性	PingOne マッピング（PingOne Mappings）
firstName	電子メール アドレス（Email Address）
lastName	Given Name
email	Family Name

[属性マッピング（Attribute Mapping）] パネルは次のようになります。



o) [保存（Save）] をクリックしてマッピングを保存します。

ステップ 3 Security Provisioning and Administration に戻り、[**次へ（Next）**] をクリックします。ステップ 3：IdP から Security Cloud に SAML メタデータを提供する の画面が表示されます。

a) [XMLファイルのアップロード（XML file upload）] オプションを選択します。

b) 以前に Ping からダウンロードした SAML メタデータファイルをアップロードします。

c) [次へ（Next）] をクリックして [テスト（Testing）] ページに進みます。

次のタスク

次に、「ステップ 4：SAML 統合のテスト」および「ステップ 5：統合のアクティブ化」の手順に従って、統合をテストしてアクティブ化します。

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。