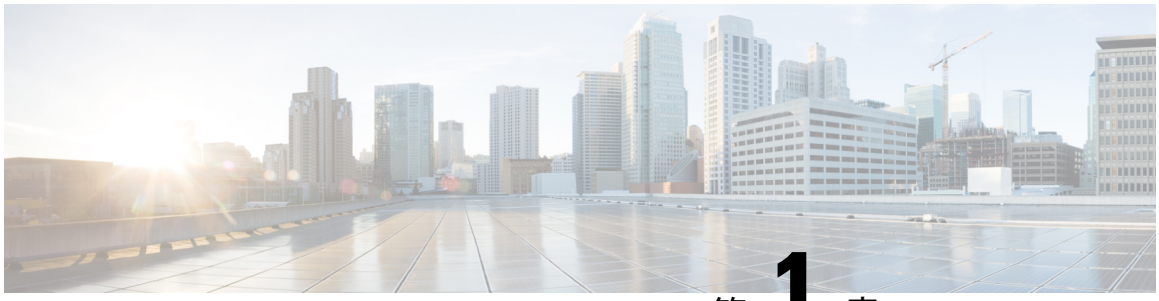
Cisco Security Cloud Sign On ID プロバイダー統合ガイド

初版：2020 年 9 月 1 日

最終更新：2022 年 4 月 19 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



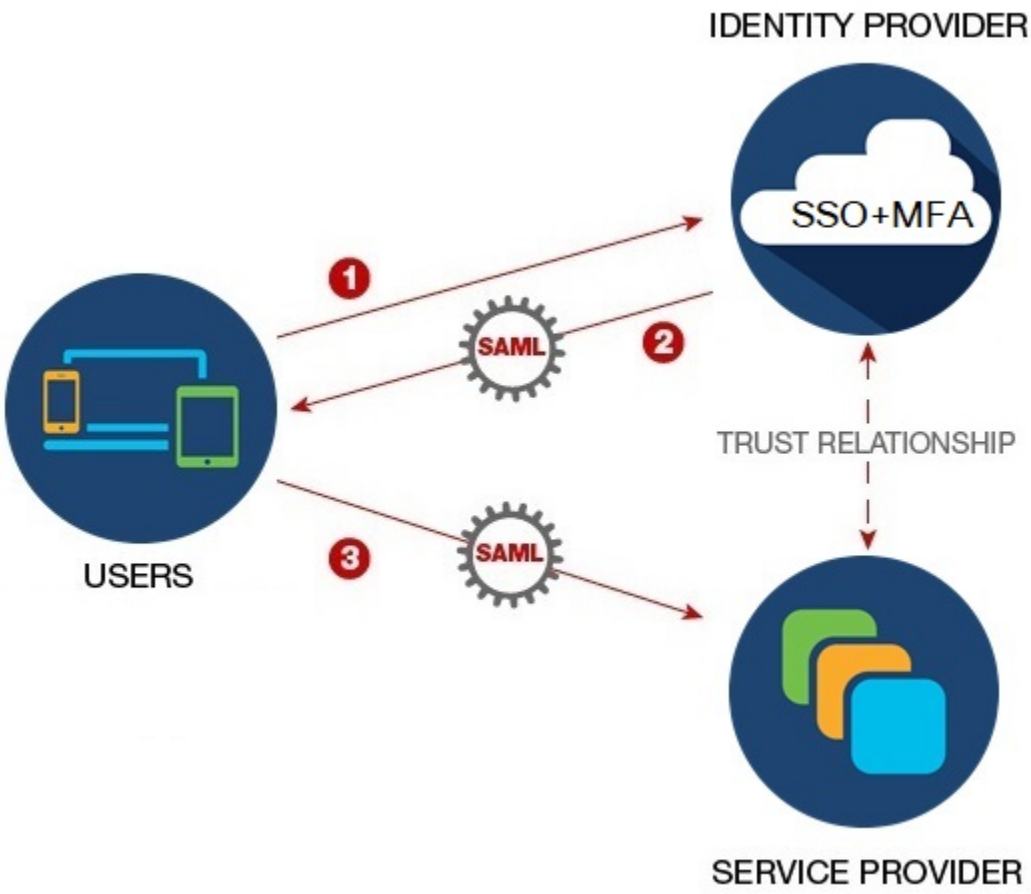
第 1 章

概要

概要

セキュリティ アサーション マークアップ言語（SAML）を使用して、独自またはサードパーティの ID プロバイダー（IdP）を Cisco Security Cloud Sign On と統合できます。SAML は、ID プロバイダー（IdP）とサービスプロバイダー（SP）の間で認証および許可データを交換するための XML ベースのオープン標準です。ここでのサービスプロバイダーは Security Cloud Sign On です。統合すると、ユーザーはシングルサインオンのクレデンシャルを使用して Security

Cloud Sign On にサインインできるようになります。



多要素認証の要件

Security Cloud Sign On では、すべてのアカウントに Duo 多要素認証が必要です。SAML（セキュリティ アサーション マークアップ言語）を使用して Secure Cloud Sign On にID プロバイダーの統合するお客様は、Duo MFA をオプトアウトできます。

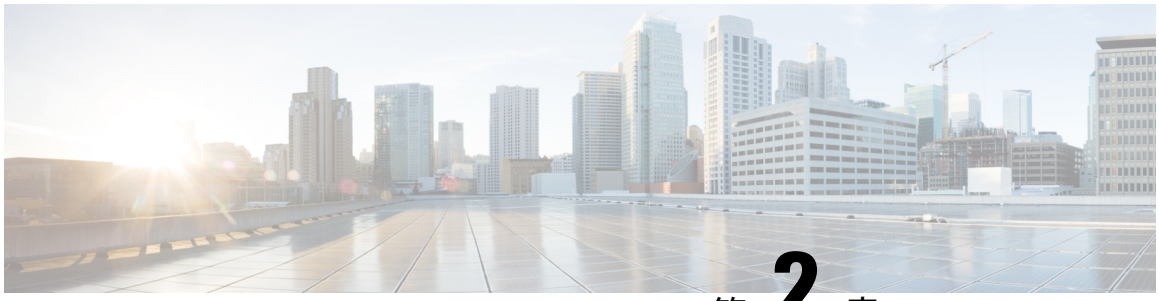
Duo MFA に登録すると、ユーザーはオプションで Google Authenticator に登録できます。Google Authenticator に登録すると、その後のサインオンは Google Authenticator チャレンジのみになり、Duo MFA チャレンジは表示されません。

Cisco Customer Identity または Microsoft によるフェデレーションサインオン（Security Cloud Sign On のページの [他のログインオプション（Other login options）]）を使用する場合、これと同じポリシーが適用されます。

既存の IdP 統合を使用しているお客様

このガイドで説明しているセルフサービスツールで作成されていない Security Cloud Sign On との IdP 統合がある場合、このツールを使用して既存の構成を更新することはできません。エンタープライズ設定ウィザード （8 ページ）統合について次の設定を変更する必要がある場合は、Cisco TAC でケースをオープンする必要があります。

- SAML シングルサインオン URL またはエンティティ ID URI
- X.509 署名証明書
- 多要素認証（MFA）設定



第 2 章

ID プロバイダーの SAML の要件

概要

IdP から Security Cloud Sign On への SAML 応答は、SAML 応答の要件 （5 ページ） で説明されているいくつかのルールに従う必要があります。

また、SAML メタデータの要件を IdP から取得する必要があります。

SAML 応答の要件

SAML 応答の属性

IdP によって送信される SAML 応答のアサーションには、次の属性名が含まれている必要があり、IdP の対応する属性にマッピングされている必要があります。

SAML アサーション属性名	IdP ユーザー属性
firstName	ユーザーの名。
lastName	ユーザーの姓。
email	ユーザーの電子メール。これは、SAML 応答の **<NameID>** 要素と一致する必要があります。

たとえば、次の XML スニペットは、Security Cloud Sign On ACL URL への SAML 応答に含まれる **<AttributeStatement>** 要素の例です。

```
<saml2:AttributeStatement>
  <saml2:Attribute Name="firstName"
```

```
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml2:AttributeValue
          xmlns:xs="http://www.w3.org/2001/XMLSchema"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">John

      </saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="lastName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml2:AttributeValue
          xmlns:xs="http://www.w3.org/2001/XMLSchema"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Doe

      </saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml2:AttributeValue
          xmlns:xs="http://www.w3.org/2001/XMLSchema"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">jdoe@example.com
      </saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

NameID 要素

IdP からの SAML 応答の **<NameID>** 要素には、その値として有効な電子メールアドレスが含まれている必要があり、電子メールは SAML 応答の属性 （5 ページ） の **email** 属性の値と一致する必要があります。

<NameID> の **Format** 属性は、**urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified** または **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress** に設定されている必要があります。

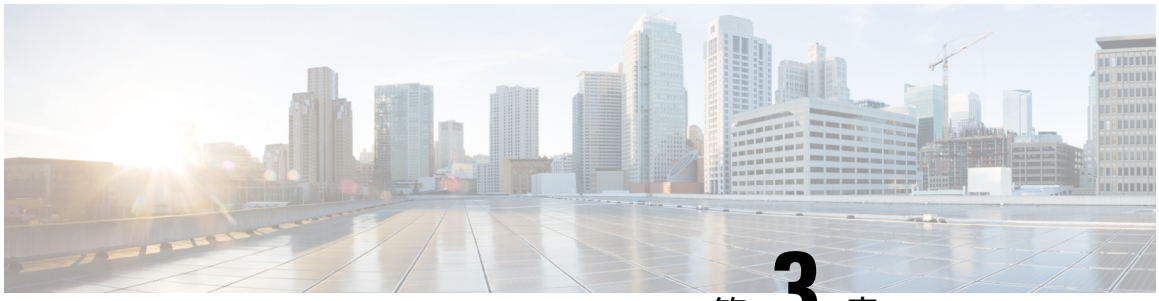
`<NameID>` 要素の例を次に示します。

```
<saml2:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">jdoe@example.com</saml2:NameID>
```

SAML メタデータの要件

Security Cloud Sign On と統合するには、IdP の SAML アプリケーションの次のメタデータが必要です。

- **シングルサインオンサービスの初期 URL** – これは「SSO URL」または「ログイン URL」と呼ばれることもあります。この URL を使用して、IdP から Security Cloud Sign On への認証を開始できます。
- **エンティティ ID URI** – IdP のグローバルな一意の名前。これは「発行元」と呼ばれることもあります。
- **X.509 署名証明書** – IdP が SAML アサーションに署名するために使用する公開キー/秘密キーのペアの公開キー。



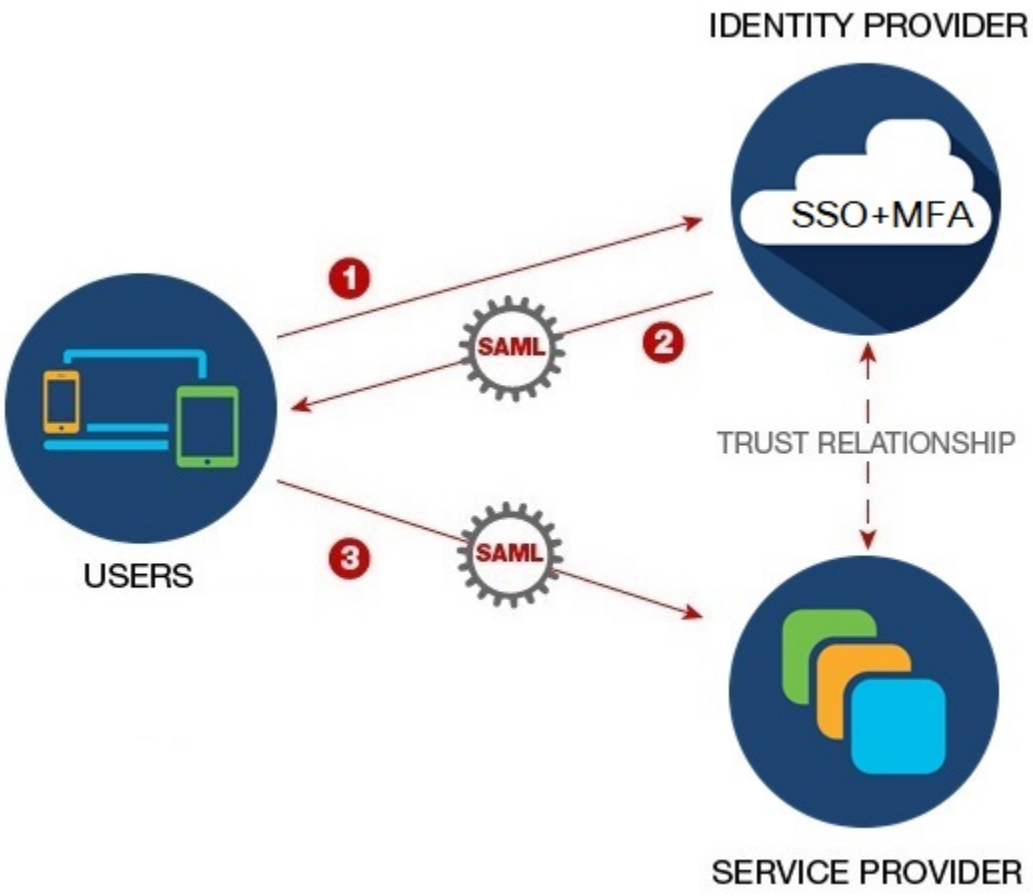
第 3 章

ID プロバイダーの統合

概要

セキュリティ アサーション マークアップ言語（SAML）を使用して、独自またはサードパーティの ID プロバイダーを Security Cloud Sign On と統合できます。SAML は、ID プロバイダー（IdP）とサービスプロバイダー（SP）の間で認証および許可データを交換するための XML ベースのオープン標準です。ここでの SP は Security Cloud Sign On です。統合すると、ユーザーは通常のシングルサインオンのクレデンシャルを使用して Security Cloud Sign On にサインイン

できるようになります。

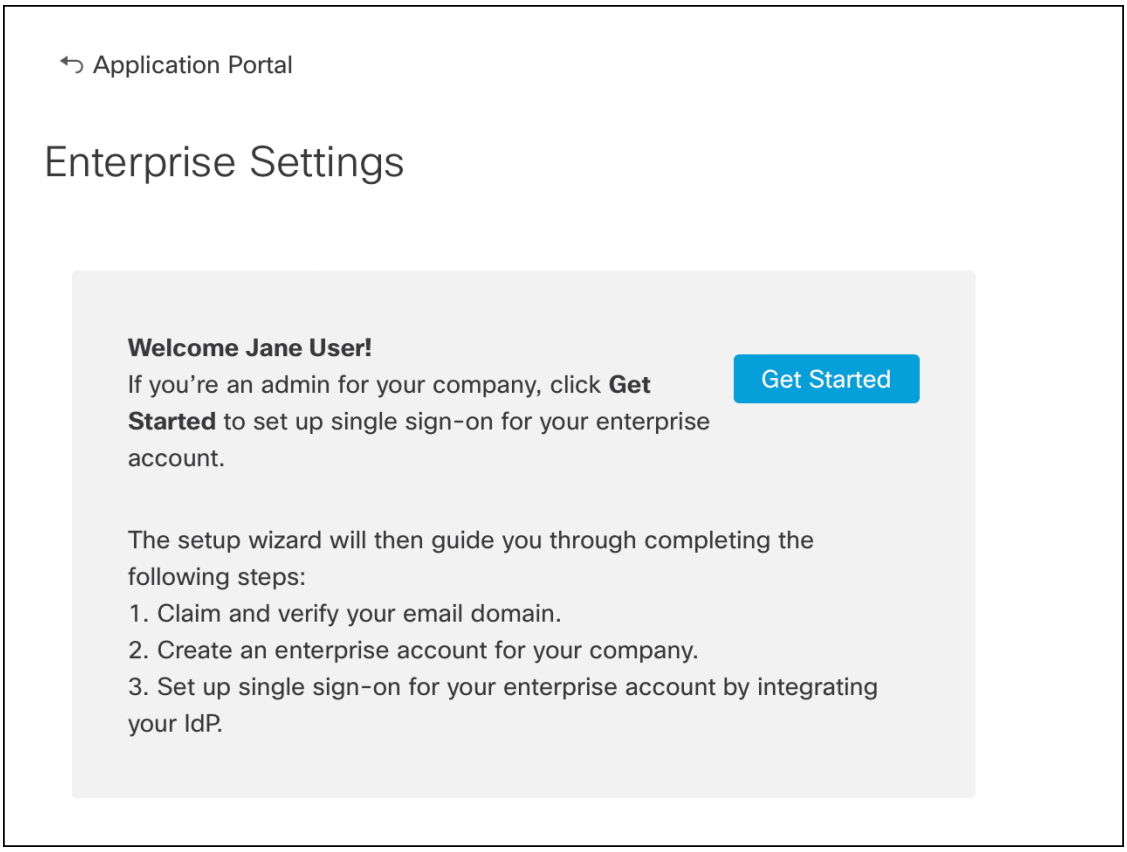


デフォルトでは、Security Cloud Sign On はすべての IdP のユーザーを Duo 多要素認証（MFA）に無料で登録します。組織ですでに MFA が IdP と統合されている場合、統合プロセス中に必要に応じて Duo ベースの MFA を無効にすることができます。

エンタープライズ設定ウィザード

エンタープライズ設定セットアップウィザードは、独自の IdP を Security Cloud Sign On と統合するための複数のステップで構成されます。各ステップを完了するたびに進行状況が保存されるため、途中で終了しても後で戻ってプロセスを完了できます。

エンタープライズ設定ウィザードを開くには、SecureX アプリケーションポータルでプロファイルアイコンをクリックし、[エンタープライズ設定（Enterprise Settings）] を選択して [始める（Get Started）] をクリックします。



設定ウィザードでは、1 つの電子メールドメインを申請し、1 つの ID プロバイダーを構成できます。次の場合は、Cisco TAC でケースをオープンする必要があります。

- 複数の ID プロバイダーを構成する必要がある
- 複数の電子メールドメインを申請する必要がある
- ステップ 2：電子メールドメインの申請と検証の後に組織名や電子メールドメインを変更する

（注） エンタープライズ設定ウィザードで作成されていない既存の IdP 統合がある場合、その統合をウィザードを使用して変更することはできません。詳細については、既存の IdP 統合を使用しているお客様 （3 ページ）を参照してください。

ステップ 1：エンタープライズの作成

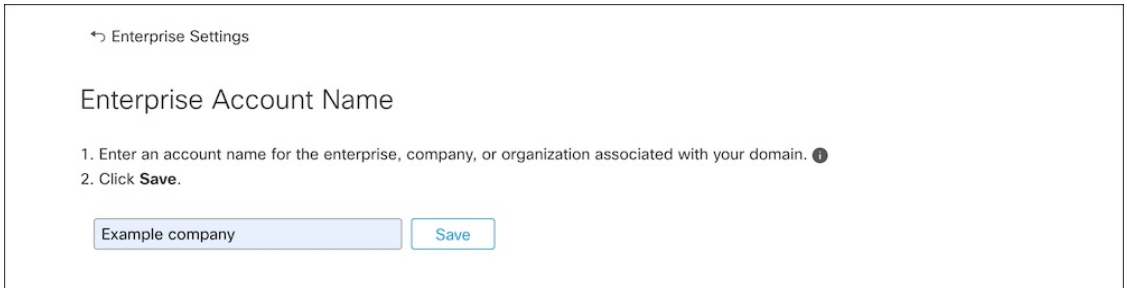
最初のステップとして、Security Cloud Sign On で名前付きのエンタープライズを作成します。このエンタープライズは、申請したドメインと ID プロバイダーの構成に関連付けられます。

ステップ 1 Security Cloud Sign On アカウントで SecureX アプリケーションポータルにサインインします。

ステップ 2 右上隅にあるプロファイルアイコンをクリックし、[エンタープライズ設定（Enterprise Settings）] を選択します。

ステップ 3 [開始する（Get Started）] をクリックします。

ステップ 4 エンタープライズアカウントの名前を入力し、[保存（Save）] をクリックします。

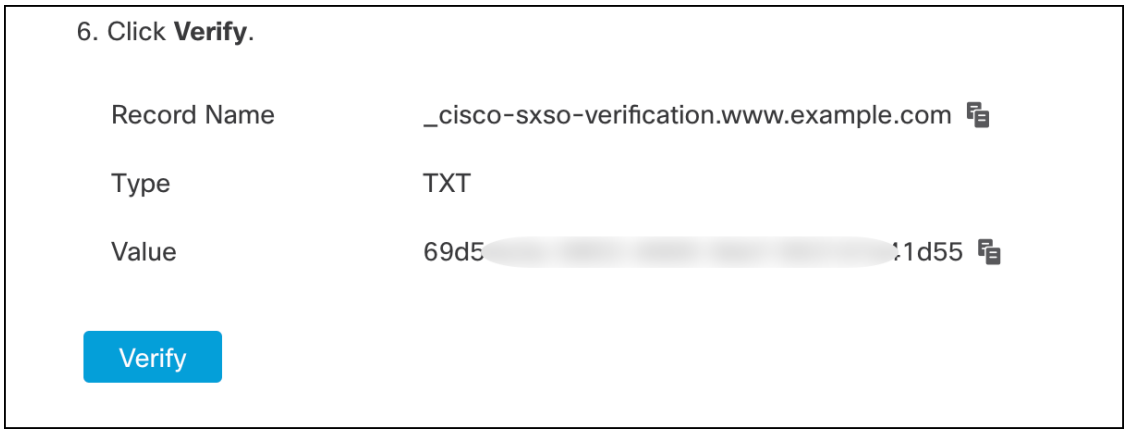


ステップ 2：電子メールドメインの申請と検証

次に、エンタープライズの電子メールドメインを申請して検証します。このステップを完了するには、ドメイン名レジストラサービスポータルで DNS レコードを作成する必要があります。ドメインの検証が完了したら、DNS レコードは削除できます。

ステップ 1 申請するドメインを入力し、[送信（Submit）] をクリックします。

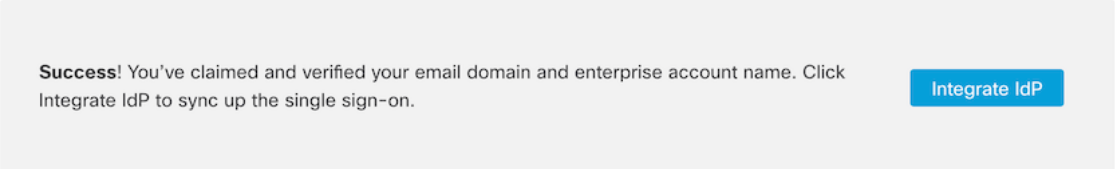
設定ウィザードに DNS TXT レコードの名前と値が表示されます。



ステップ 2 ドメイン名レジストラサービスにサインインし、指定されたレコード名と値で TXT レコードを作成します。

ステップ 3 DNS レコードが伝達されるまで待ってから、[検証（Verify）] をクリックします。

ステップ4 検証が成功したら、[IdPの統合（Integrate IdP）] をクリックして IDプロバイダーの統合を開始します。



ステップ3：SAMLメタデータの交換

このステップでは、IdP と Security Cloud Sign On の間で SAML メタデータおよび署名証明書を交換します。

始める前に

このステップを完了するには、IDプロバイダーで作成した概要に関する次の情報が必要です。

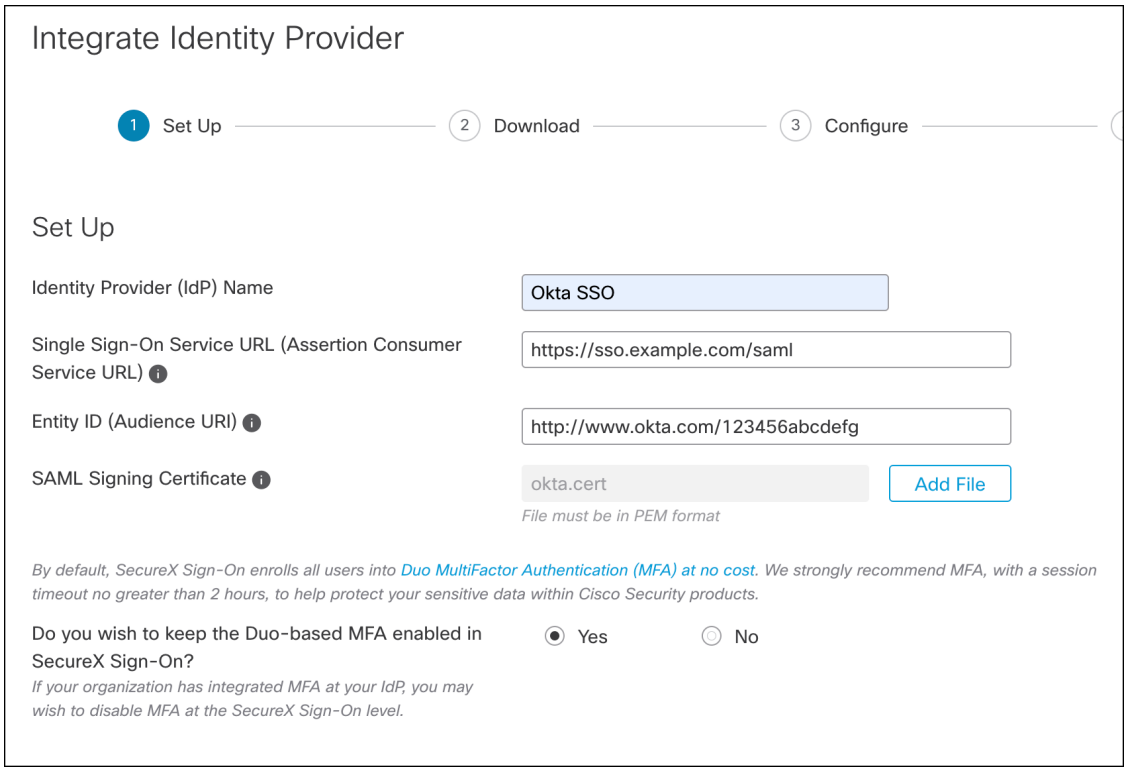
- **シングルサインオンサービスの URL** – Security Cloud Sign On から HTTP POST で SAML 認証要求を送信する URL。URL のドメインは、前にステップ2：電子メールドメインの申請と検証ドメインと一致する必要があります。
- **エンティティ ID** – ID プロバイダーを Security Cloud Sign On で一意に識別するための ID。IdP の SAML メタデータから `<EntityDescriptor>` 要素の `entityID` で確認できます。一部の IdP では **ID プロバイダー発行元**と呼ばれています。
- **SAML 署名証明書** – IdP が SAML アサーションに署名するために使用する x.509 署名証明書。

ステップ1 [セットアップ（Set Up）] 画面で [IDプロバイダー名（Identity Provider Name）] フィールドに IdP の名前を入力します。

ステップ2 IdP の SAML 統合から取得した [シングルサインオンURL（Single sign-on URL）] と [エンティティID（Entity ID）] の値を入力します。

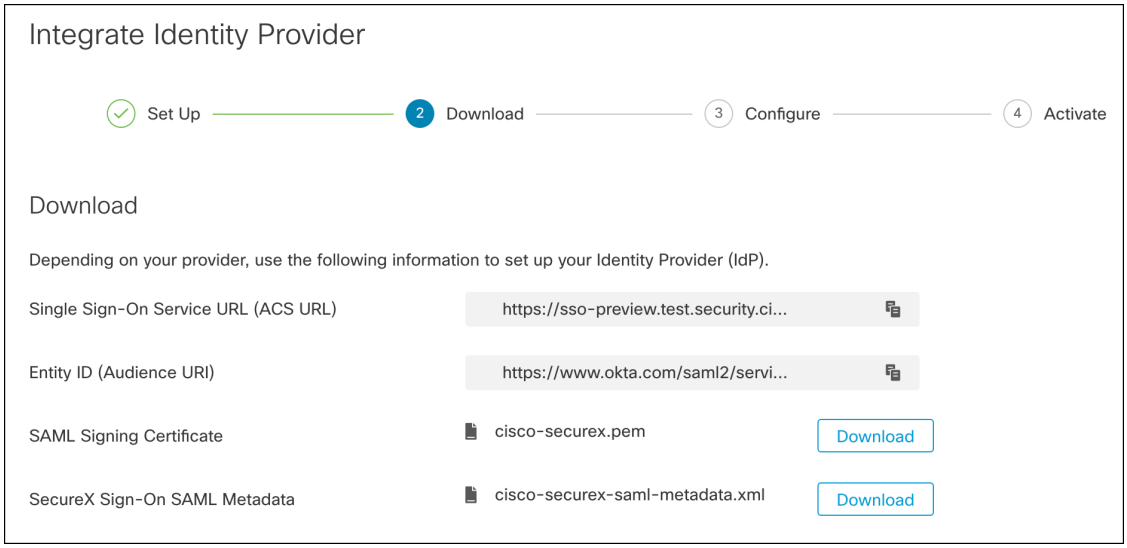
ステップ3 [ファイルの追加（Add File）] をクリックし、前に IdP からダウンロードした SAML 署名証明書を選択します。

ステップ4 Duo MFA へのユーザーの自動登録を行わない場合は、[Security Cloud Sign OnでDuoベースのMFAを有効にする（Do you wish to keep the Duo-based MFA enabled in Security Cloud Sign On?）] で [いいえ（No）] を選択します。



ステップ5 [次へ（Next）] をクリックして [ダウンロード（Download）] 画面に進みます。

ステップ6 表示された [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)）] をコピーし、SAML 署名証明書をダウンロードします。



ステップ7 7. [次へ（Next）] をクリックして [構成（Configure）] 画面に進みます。

ステップ8 IdP 管理コンソールで SAML アプリケーション設定ページを開き、次の変更を行います。

a) [ACS URL（ACS URL）] と [エンティティID（Entity ID）] に割り当てられた一時的な値を前の手順で取得した値で更新します。
b) 設定ウィザードで提供されたSAML署名証明書をアップロードします。

（注） 一部のIdP（はじめになど）では、証明書の内容を1行のJSON文字列として提供する必要があります（例：`-----BEGIN CERTIFICATE-----\n...\n...\n-----END CERTIFICATE-----\n`）。

c) 設定の変更をSAMLアプリ設定に保存します。

次のタスク

次に、エンタープライズとのIdP統合をテストします。

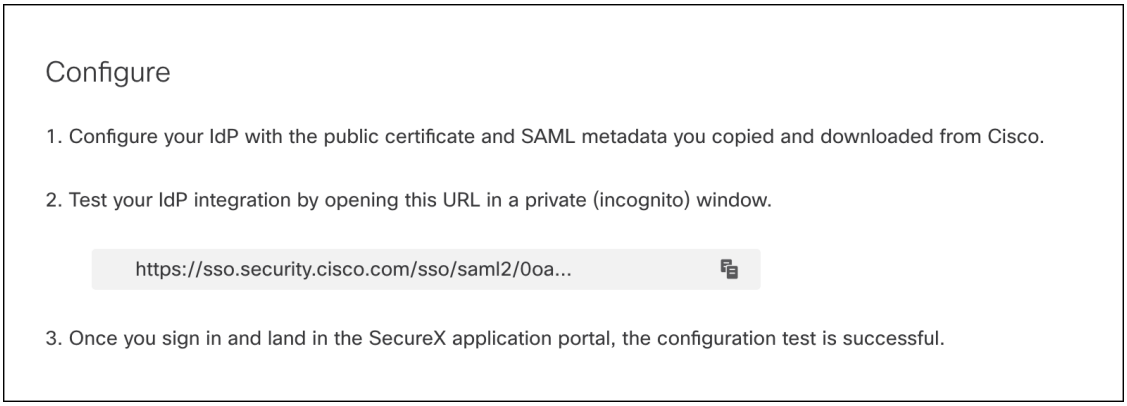
ステップ4：SSO統合のテスト

次に、エンタープライズウィザードからIdPへのSSO要求を開始してIdPの統合をテストします。SecureXアプリケーションダッシュボードに戻れば、テストが成功したことを意味します。

- プライベート（シークレット）ウィンドウでURLをテストします。
- サインインに使用する電子メールドメインは、前に申請したステップ2：電子メールドメインの申請と検証と一致する必要があります。
- 新規のユーザー（既存のSecurity Cloud Sign Onアカウントがないユーザー）と既存のユーザーでテストします。

ステップ1 エンタープライズ設定ウィザードの [構成（Configure）] 画面に戻ります。

ステップ2 **ステップ2**のSSO URLをクリップボードにコピーし、プライベート（シークレット）ブラウザウィンドウで開きます。



ステップ3 IDプロバイダーにサインインします。

- サインインに使用する電子メールドメインは、前に申請したステップ 2：電子メールドメインの申請と検証と一致する必要があります。
- Secure Cloud Sign On で最初のサインアップに使用したアカウントとは別のアカウントでテストします。たとえば、admin@example.com アカウントでサインアップして IdP 統合を作成した場合、統合のテストにそれと同じ電子メールは使用しないでください。

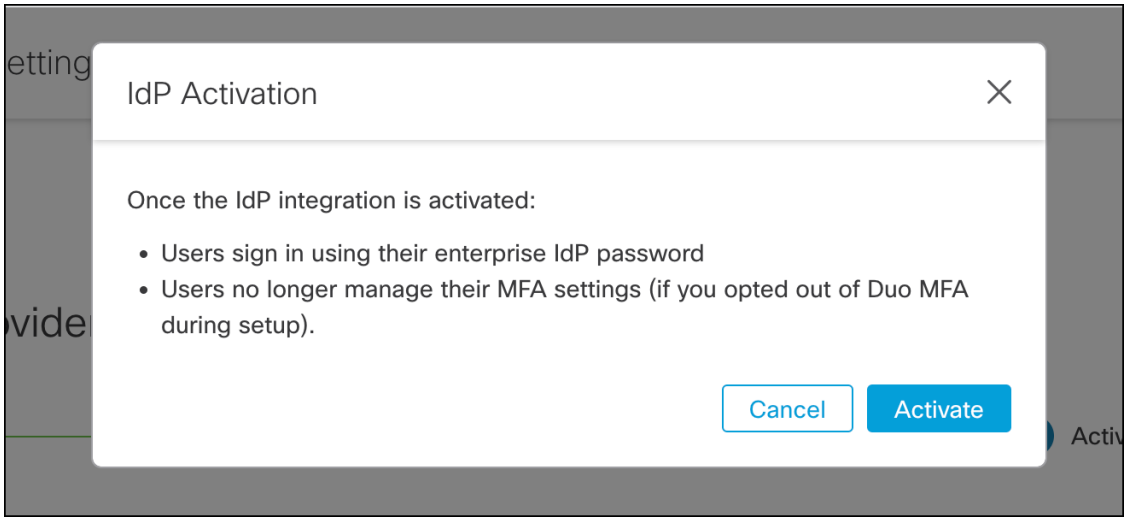
SecureX アプリケーションポータルが表示されれば、構成のテストは成功です。SSO プロセスでエラーが発生する場合は、トラブルシューティング （15 ページ） を参照してください。

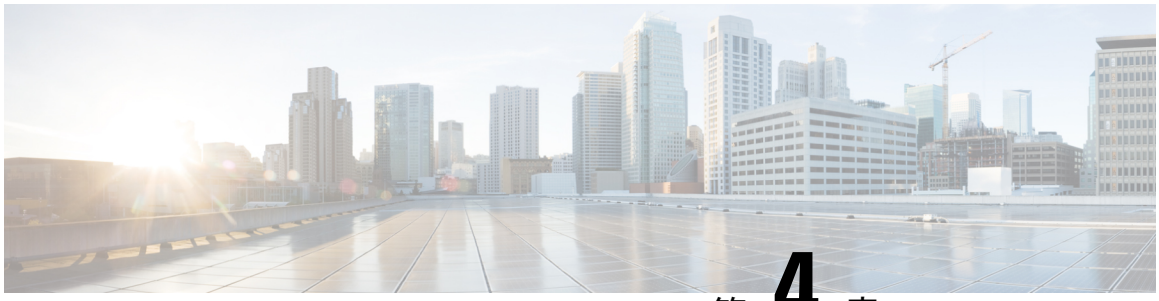
ステップ 4 統合をテストしたら、[次へ（Next）] をクリックして [アクティブ化（Activate）] ページに進みます。

ステップ 5：IdP 統合のアクティブ化

ステップ 4：SSO 統合のテストが完了し、組織で有効にする準備ができたら、IdP 統合をアクティブ化できます。アクティブ化した後は、ユーザーはエンタープライズ（IdP）の電子メールアドレスとパスワードを使用してサインインします。無料の Duo MFA 登録をオプトアウトした場合、ユーザーは MFA 設定を管理できなくなります。

IdP と Security Cloud Sign On の統合をアクティブ化するには、[IdPをアクティブ化（Activate my IdP）] をクリックし、確認ダイアログで [アクティブ化（Activate）] をクリックします。





第 4 章

トラブルシューティング

シングルサインオン/SAML のエラー

統合のテストでの HTTP 400 エラー

エンタープライズ設定ウィザードでの ステップ 4：SSO 統合のテストで HTTP 400 エラーが発生する場合は、次のトラブルシューティング手順を試してください。

ユーザーのサインオン電子メールドメインが申請したドメインと一致することを確認する

テストに使用しているユーザーアカウントの電子メールドメインがステップ 2：電子メールドメインの申請と検証と一致していることを確認してください。
たとえば、`example.com` のような最上位ドメインを申請した場合、ユーザーは `<username>@signon.example.com` ではなく `<username>@example.com` でサインインする必要があります。

SAML 応答の <NameID> 要素が電子メールアドレスであることを確認する

SAML 応答の `<NameId>` 要素の値は電子メールアドレスでなければなりません。電子メールアドレスは、ユーザーの SAML 属性で指定された **email** と一致する必要があります。詳細については、「SAML 応答の属性 （5 ページ）」を参照してください。

SAML 応答に正しい属性要求が含まれていることを確認する

IdP から Security Cloud Sign On への SAML 応答には、必須のユーザー属性である **firstName**、**lastName**、および **email** が含まれます。詳細については、SAML 応答の要件 （5 ページ）を参照してください。

エンタープライズウィザードのエラー

ドメインの検証時のエラー

ステップ2：電子メールドメインの申請と検証でエラーが発生する場合は、次のトラブルシューティング手順を試してください。

しばらく待ってから再試行する

しばらく待ってから、もう一度 [検証（Verify）] をクリックしてみてください。DNS レコードの更新が DNS サーバーに伝達されるまでの時間は、サービスプロバイダーによって異なります。

TXT DNS レコードの名前と値を確認する

ドメインレジストラで作成した TXT DNS レコードの名前と値がエンタープライズ設定ウィザードで表示される内容と一致することを確認してください。

シングルサインオンのテスト時のエラー

ステップ 4：SSO 統合のテストでエラーが発生する場合は、SAML 設定の問題やユーザーアカウントの問題である可能性があります。トラブルシューティングの手順については、シングルサインオン/SAML のエラー （15 ページ） を参照してください。

シスコのセキュリティ製品との統合

シスコのセキュリティ製品でのサインオンのエラー

Security Cloud Sign On にはサインオンできるがシスコのセキュリティ製品の 1 つ以上にサインオンできない場合は、次の点を確認してください。

Security Cloud Sign On のオプトインが必要な製品かどうかを確認する

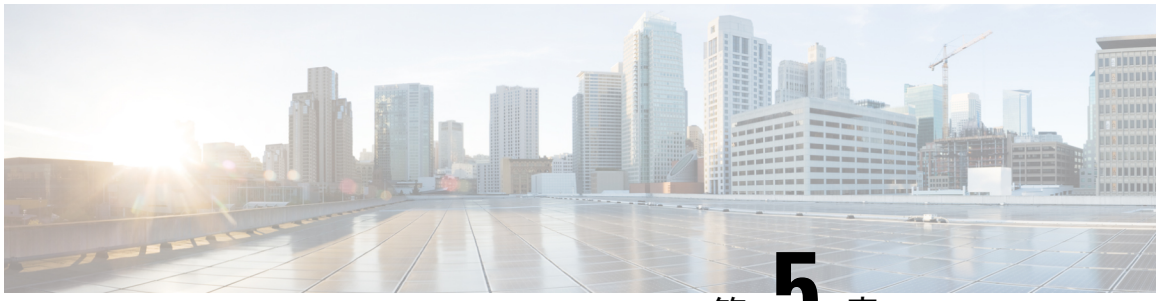
シスコのセキュリティ製品には、Cisco Umbrella のように Security Cloud Sign On がデフォルトでサポートされる製品もあれば、オプトインが必要な製品もあります。オプトインが必要なシスコのセキュリティ製品については、サポートされるセキュリティ製品のリストで確認できます。

Security Cloud Sign On の識別情報が製品の識別情報と一致することを確認する

各ユーザーの Security Cloud Sign On の識別情報（電子メール）が製品の識別情報と一致する必要があります。たとえば、**user@example.com** というユーザー名の Security Cloud Sign On アカウントがあるとします。この Security Cloud Sign On アカウントを使用して Umbrella で正常に認証するには、同じ電子メールを持つ既存の Umbrella アカウントが必要です。

第 I 部

ID プロバイダー統合ガイド



第 5 章

Auth0 社

概要

ここでは、Security Cloud Sign On と統合する Auth0 SAML アプリケーションを作成する方法について説明します。

はじめに

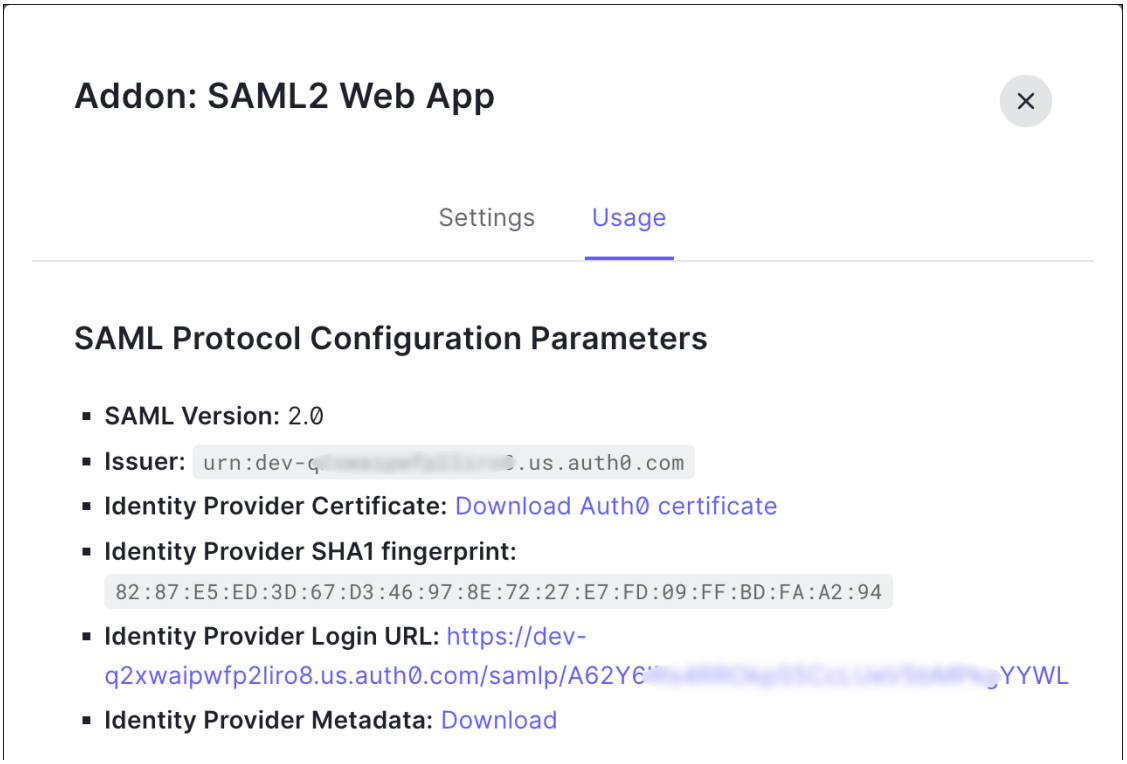
始める前に

- 管理者権限で Auth0 管理コンソールにサインインできる必要があります。
- ステップ 1：エンタープライズの作成 （9 ページ） と ステップ 2：電子メールドメインの申請と検証 （10 ページ） が完了している必要があります。

ステップ 1 Auth0 ダッシュボードにサインインし、次の手順を実行します。

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 App の構成ダイアログが開きます。



g) [発行元（Issuer）] フィールドと [IDプロバイダーログインURL（Identity Provider Login URL）] フィールドの値をコピーします。

h) [Auth0証明書のダウンロード（Download Auth0 certificate）] をクリックして ID プロバイダー証明書をダウンロードします。

ステップ 2 エンタープライズ設定ウィザードの [IDプロバイダーの統合（Integrate Identity Provider）] 画面を開き、次の手順を実行します。

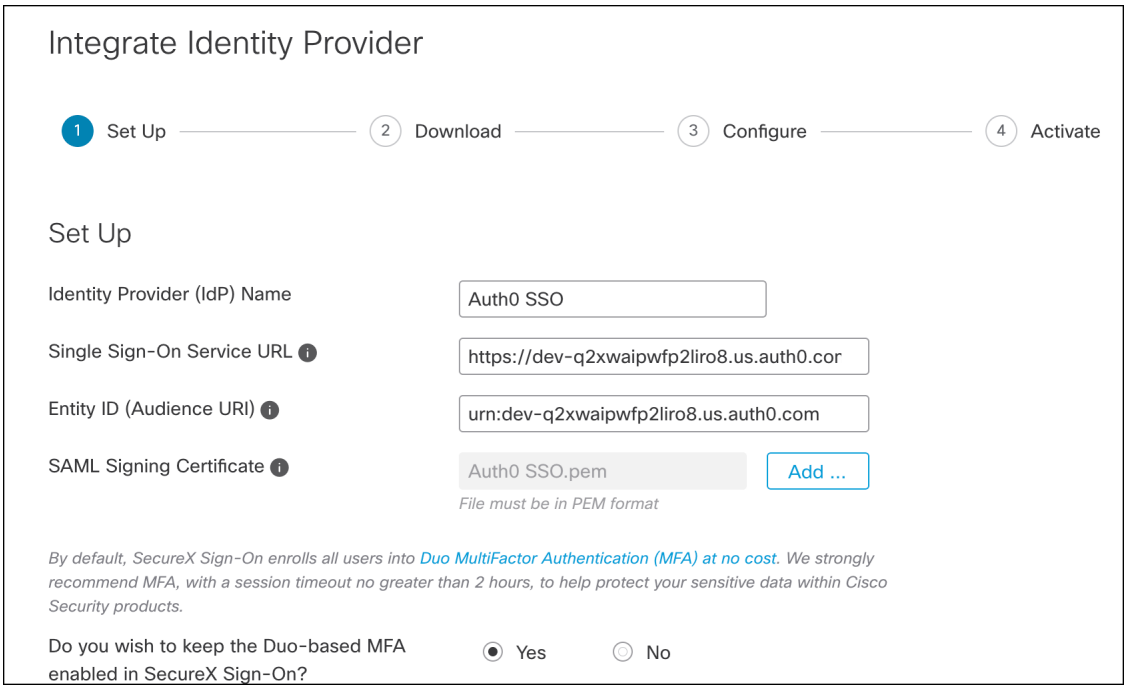
a) [IDプロバイダー名（Identity Provider Name）] フィールドに IdP の名前（例：**Auth0 SSO**）を入力します。

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、SAML アドオンダイアログからコピーした [IDプロバイダーログインURL（Identity Provider Login URL）] の値を入力します。

c) [エンティティID（Entity ID）] フィールドに、SAML アドオンダイアログからコピーした [発行元（Issuer）] フィールドの値を入力します。

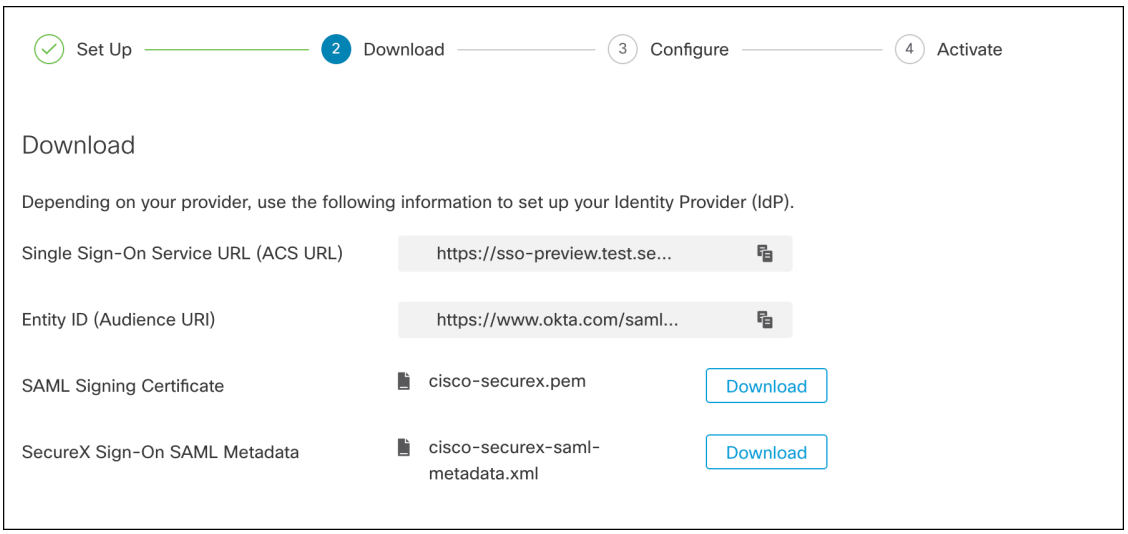
d) [ファイルの追加（Add File）] をクリックし、Auth0 からダウンロードした SAML 署名証明書を選択します。

e) 必要に応じて、Duo ベースの無料の MFA サービスからユーザーをオプトアウトします。



f) [次へ（Next）] をクリックして [ダウンロード（Download）] 設定ページに進みます。

g) 後で使用するために [シングルサインオンサービスURL（Single Sign-On Service URL）] と [エンティティID（Entity ID）] の値をコピーし、SAML 署名証明書（cisco-securex.pem）をダウンロードします。



h) [次へ（Next）] をクリックして [構成（Configure）] 画面に進みます。

ステップ 3 Auth0 コンソールのアドオン設定ダイアログに戻ります。

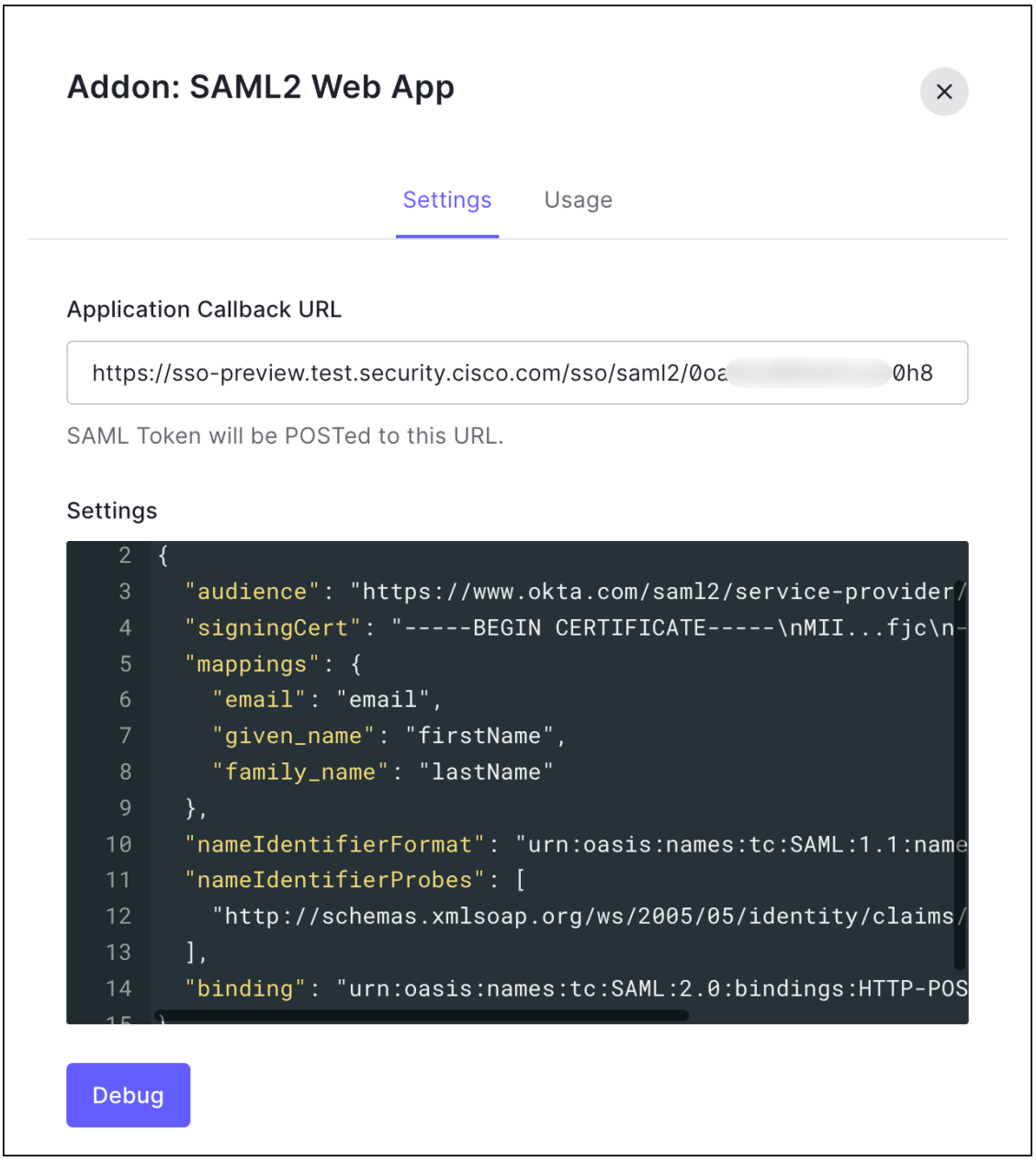
a) [設定（Settings）] タブをクリックします。

b) [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。

c) 必要に応じて、[デバッグ（Debug）] をクリックしてサンプル SAML 応答の構造と内容を確認します（応答をデバッグするには、Auth0 ユーザーを SAML アプリケーションに割り当てる必要があります）。

d) [設定（Settings）] フィールドに次の JSON オブジェクトを入力します。<ENTITY_ID_URI> を、前にコピーした [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、<SIGNING_CERT> を、ダウンロードした SecureX Sign On 署名証明書（PEM ファイル）を 1 行の文字列に変換した内容に置き換えます。

```
{
  "audience": "https://www.okta.com/saml2/...",
  "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"
}
```



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

ステップ 4 エンタープライズ設定ウィザードの [構成（Configure）] 画面に戻ります。

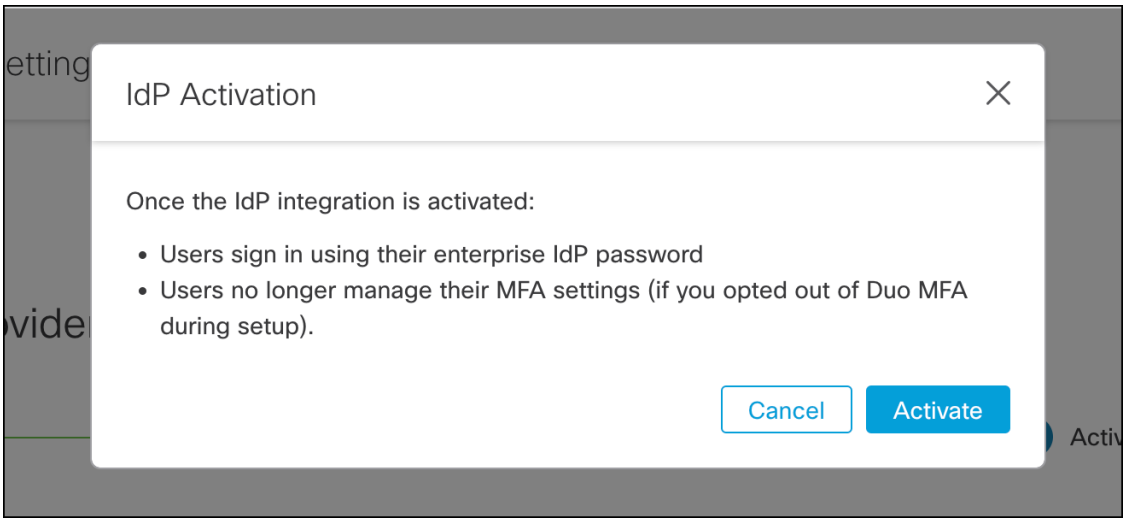
a) 表示された URL をコピーし、プライベート（シークレット）ブラウザウィンドウで開きます。
ブラウザが Auth0 SSO ページにリダイレクトされます。

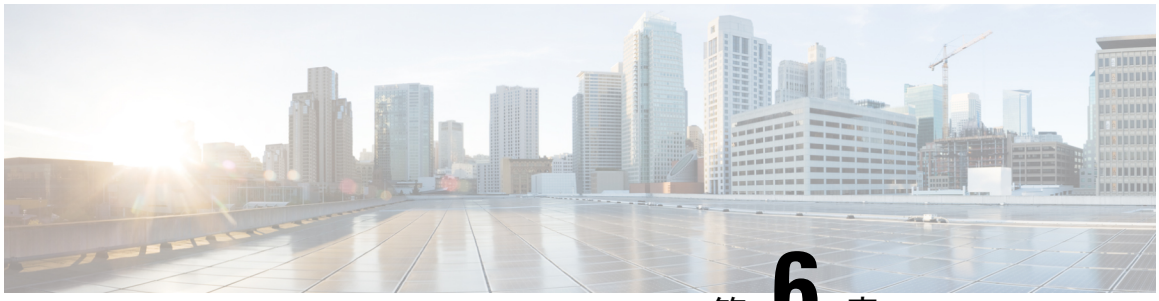
b) ステップ 2：電子メールドメインの申請と検証と一致する電子メールアドレスで Auth0 にサインインします。
SecureX アプリケーションポータルに戻れば、テストは成功です。

c) 設定ウィザードで [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) ユーザーの統合をアクティブ化するには、[IdP をアクティブ化（Activate my IdP）] をクリックします。

e) ダイアログで選択内容を確認します。





第 6 章

ADFS

概要

ここでは、ADFS SAML アプリケーションを作成し、それを Security Cloud Sign On と統合する方法について説明します。

使用する前に

始める前に

- サーバーマネージャにサインインできる必要があります。
- この手順を完了するには、少なくともローカルコンピュータに対する管理者のメンバーシップ、またはこれと同等の権限が必要です。
- ステップ 1：エンタープライズの作成 （9 ページ） と ステップ 2：電子メールドメインの申請と検証 （10 ページ） が完了している必要があります。

ステップ 1 Microsoft が提供している手順に従って、次のように要求対応の証明書利用者信頼を手動で作成します。

a) [表示名の指定（Specify Display Name）] ページで、「**`SecureX Sign-On`**」または他の名前を入力します。

b) [証明書の構成（Configure Certificate）] ページに進みます。

c) [URLの構成（Configure URL）] ページで次の手順を実行します。

- [SAML 2.0 WebSSO プロトコルのサポートを有効にする（Enable support for the SAML 2.0 WebSSO protocol）] チェックボックスをオンにします。

- [証明書利用者 SAML 2.0 SSOサービスのURL（Relying party SAML 2.0 SSO service URL）] で一時的な URL（例：**`https://example.com/sso`**）を入力します。これは、この手順の後半でシスコの実際のサービス URL に置き換えます。

d) [識別子の構成（Configure Identifiers）] ページで、一時的な URL を使用して証明書利用者信頼の識別子（例：**`https://example.com/id`**）を追加します。これは、この手順の後半でシスコの実際の識別子に置き換えます。

e) [アクセス制御ポリシーの選択（Choose Access Control Policy）] ページでアクセス制御ポリシーを選択します。

f) [完了（Finish）] ページで [閉じる（Close）] をクリックします。

ステップ 2 作成した証明書利用者を右クリックし、[要求規則の編集（Edit Claim Rules）] を選択します。

ステップ 3 「Windows Server 2016 で証明書利用者信頼の要求として LDAP 属性を送信する規則を作成するには」の手順に従って、前に作成した証明書利用者信頼の規則を次のように作成します。

a) [規則の構成（Configure Rule）] ページの [要求規則名（Claim rule name）] で、「**`Secure Sign On`**」または他の名前を入力します。

b) [属性ストア（Attribute Store）] メニューから目的の属性ストアを選択します。

c) [LDAP属性（LDAP attribute）] と [出力方向の要求の種類（Outgoing Claim Type）] の次のマッピングを作成します。

[LDAP属性（LDAP attribute）]	[出力方向の要求の種類（Outgoing Claim Type）]
E-Mail-Addresses	email
Given-Name	firstName
姓	lastName

d) [終了（Finish）] をクリックします。

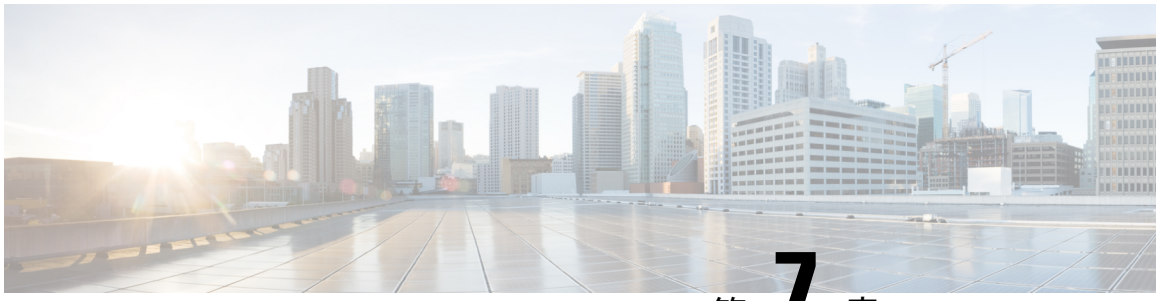
ステップ 4 「入力方向の要求を変換する規則を作成する」の手順に従って、次のように規則を作成します。

a) [規則の構成（Configure Rule）] ページで次の手順を実行します。

- [要求規則名（Claim rule name）] で「**`Send email as NameID`**」または他の名前を入力します。
- [入力方向の要求の種類（Incoming claim type）] で [E-Mail Address（E-Mail Address）] を選択します。
- [出力方向の要求の種類（Outgoing claim type）] で [Name ID（Name ID）] を選択します。
- [出力方向の名前IDの形式（Outgoing name ID format）] で、[電子メール（Email）] または [未定義（Undefined）] を選択します。
- [すべての要求値をパススルーする（Pass through all claim values）] が選択されていることを確認し、[完了（Finish）] をクリックします。

ステップ 5 SecureX アプリダッシュボードからエンタープライズ設定ウィザードを開きます。ステップ 3：SAML メタデータの交換 （11 ページ） の画面が表示されます。

a)



第 7 章

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 （5 ページ）」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 （9 ページ） と ステップ 2：電子メールドメインの申請と検証 （10 ページ） 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。

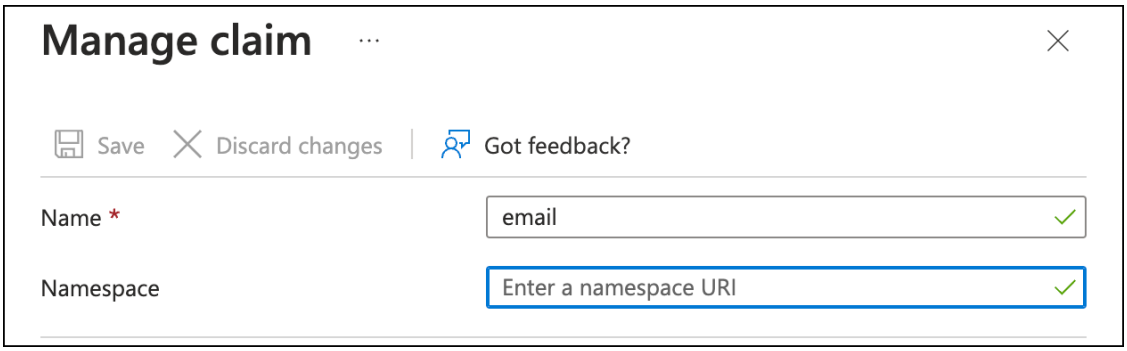
ここでは、**user.userprincipalname** の値が有効な電子メールアドレスを表していることを前提としています。それ以外の場合は、[ソース（Source）] で **user.primaryauthoritativeemail** を使用するように設定します。

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
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 （11 ページ））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。

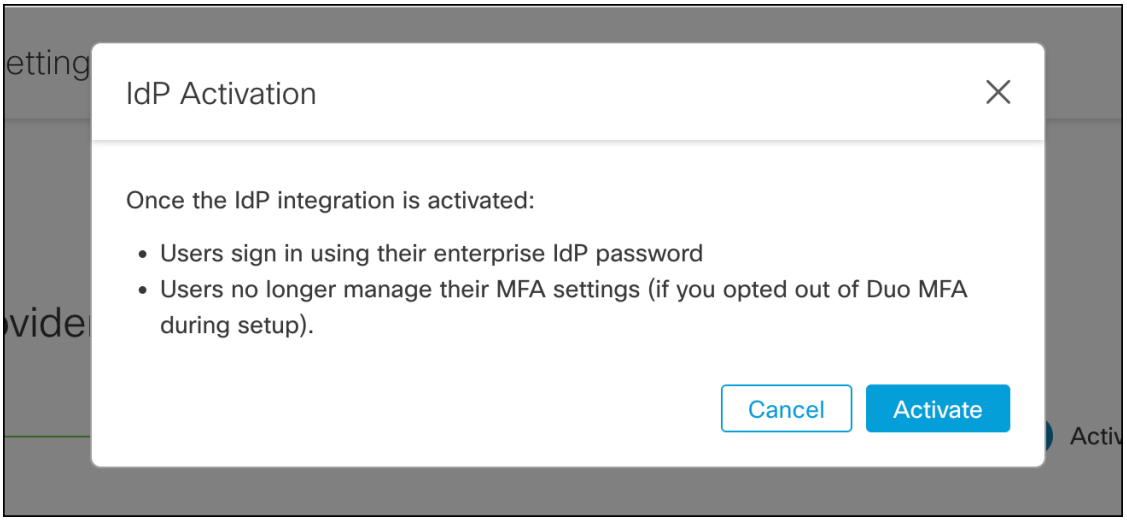
ステップ 4 エンタープライズ設定ウィザードに戻り、統合をテストします。[構成（Configure）] 画面（ステップ 4：SSO 統合のテスト （13 ページ））で次の手順を実行します。

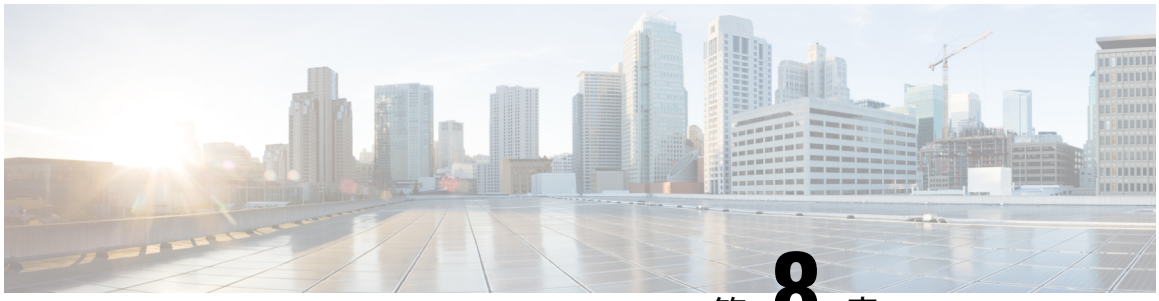
a) 提供された URL をコピーし、プライベート（シークレット）ウィンドウで開きます。

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 （15 ページ） 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。





第 8 章

Duo

概要

ここでは、Duo SAML アプリケーションを作成し、それを Security Cloud Sign On と統合する方法について説明します。

はじめに

始める前に

- 所有者ロールを持つ Duo 管理者である必要があります。
- Duo の [Duo管理（Duo Admin）] > [シングルサインオン（Single Sign-On）] > [設定済み認証ソース（Configured Authentication Sources）] で、少なくとも 1 つの認証ソースがすでに設定されている必要があります。
- 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 （9 ページ） と ステップ 2：電子メールドメインの申請と検証 （10 ページ） が完了している必要があります。

ステップ 1 Duo Admin Panel にサインインします。

a) 左側のメニューから [アプリケーション（Applications）] をクリックし、[アプリケーションの保護（Protect an Application）] をクリックします。

b) [汎用SAMLサービスプロバイダー（Generic SAML Service Provider）] を探します。

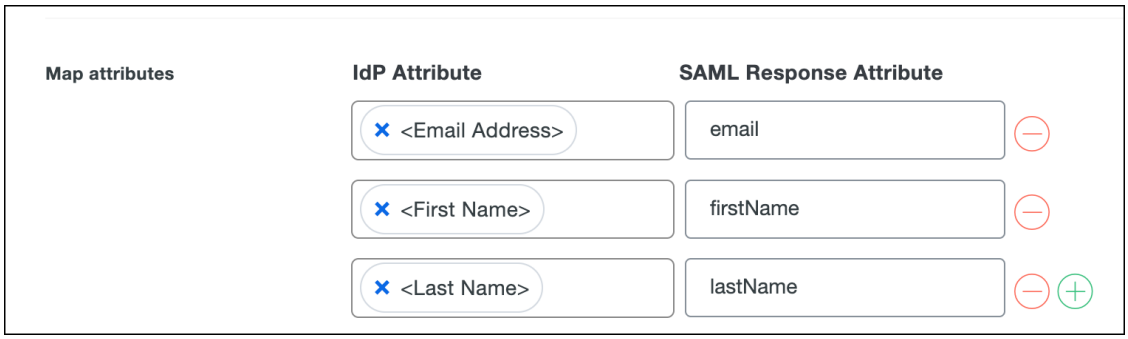
c) [保護タイプ（Protection Type）] が [DuoがホストするSSOによる2FA（2FA with SSO hosted by Duo）] の [汎用サービスプロバイダー（Generic Service Provider）] アプリケーションの横にある [保護（Protect）] をクリックします。汎用 SAML サービスプロバイダーの構成ページが開きます。

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) [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（urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified）] または [urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress（urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress）] を選択します。
- [NameID属性（NameID attribute）] で [<Email Address>（<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 ユーザー属性から SAML 応答属性へ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**



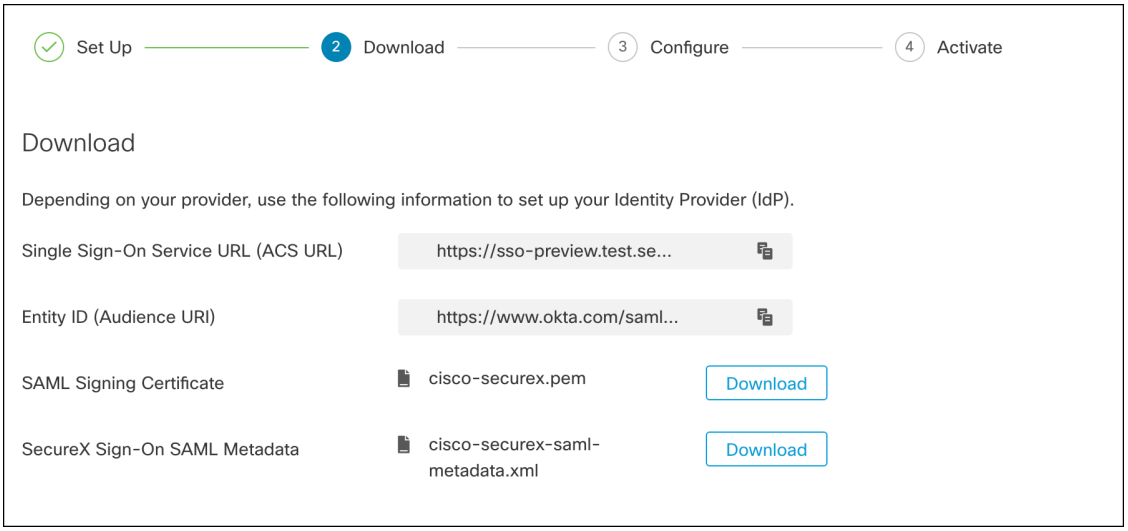
i) [設定（Settings）] セクションで、[名前（Name）] フィールドに「**Secure Cloud Sign On**」または他の値を入力します。

Duo の SAML 設定のブラウザウィンドウは開いたままにします。

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）] 画面の [セットアップ（Set Up）] ステップ（ステップ 3：SAML メタデータの交換 （11 ページ） を参照）が表示されます。

a) [IDプロバイダー名（Identity Provider Name）] フィールドに IdP の名前（例：**Duo SSO**）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、Duo からコピーした [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（Entity ID）] フィールドに、Duo からコピーした [エンティティID（Entity ID）] フィールドの値を入力します。

d) [ファイルの追加（Add File）] をクリックし、Duo からダウンロードした SAML 署名証明書を選択します。
e) 必要に応じて、Duo ベースの無料の MFA サービスからユーザーをオプトアウトします。
f) [次へ（Next）] をクリックして [ダウンロード（Download）] 画面に進みます。
g) 後で使用するために、[シングルサインオンサービスURL（ACS URL）（Single Sign-On Service URL (ACS URL)）] フィールドと [エンティティID（オーディエンスURI）（Entity ID (Audience URI)）] フィールドの値をコピーして保存します。
h) SAML 署名証明書（cisco-securex.pem）をダウンロードします。



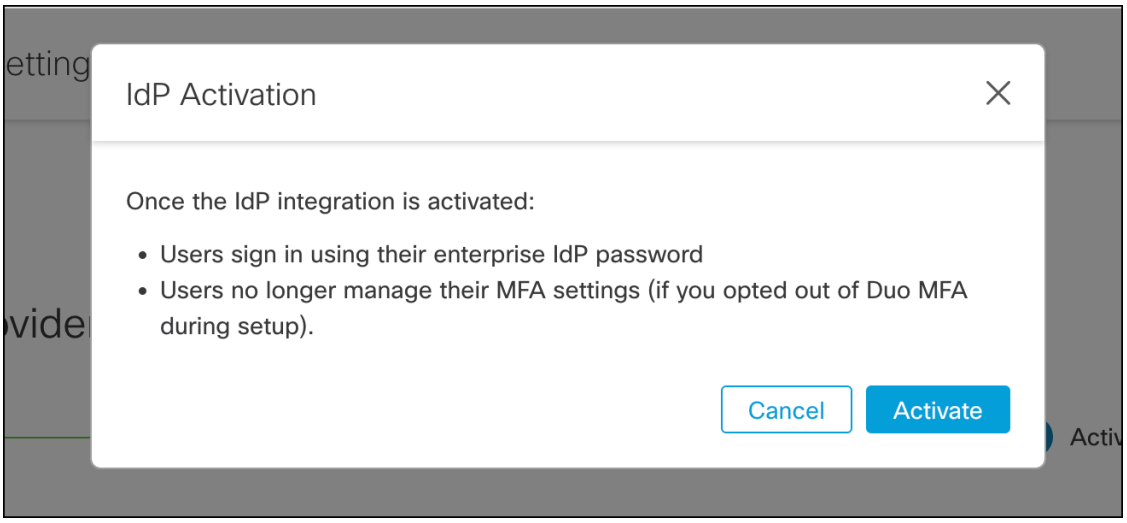
i) [次へ（Next）] をクリックして [構成（Configure）] 画面に進みます。

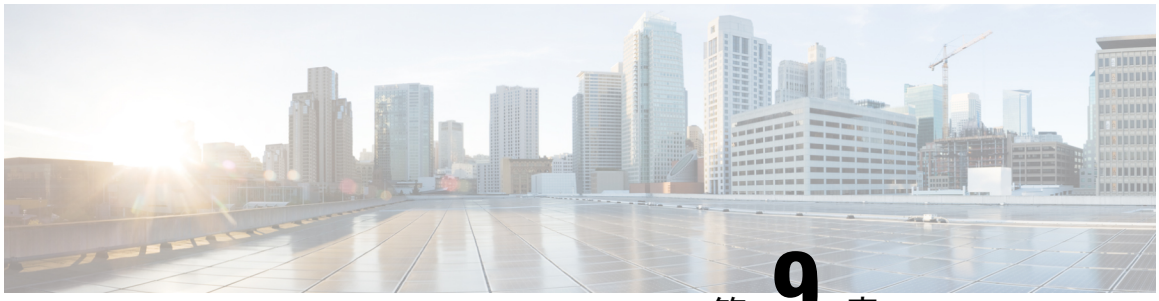
ステップ 3 Duo の SAML アプリケーション設定に戻り、次の手順を実行します。

a) [サービスプロバイダー（Service Provider）] セクションの [エンティティID（Entity ID）] フィールドに、前の手順で設定ウィザードによって提供された [エンティティID（オーディエンスURI）（Entity ID (Audience URI)）] フィールドの値を入力します。
b) [Assertion Consumer Service（ACS）URL（Assertion Consumer Service (ACS) URL）] に、前の手順で設定ウィザードによって提供された [シングルサインオンサービスURL（ACS URL）（Single Sign-On Service URL (ACS URL)）] フィールドの値を入力します。
c) 設定ページの下部で [保存（Save）] をクリックします。

ステップ 4 エンタープライズ設定ウィザードの [構成（Configure）] 画面に戻ります。

a) 表示された URL をコピーし、プライベート（シークレット）ブラウザウィンドウで開きます。
ブラウザが Duo SSO URL にリダイレクトされます。
b) ステップ 2：電子メールドメインの申請と検証と一致する電子メールアドレスで Duo にサインインします。
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。
c) 設定ウィザードで [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) ユーザーの統合をアクティブ化するには、[IdPをアクティブ化（Activate my IdP）] をクリックします。
e) ダイアログで選択内容を確認します。


IdP Activation
Once the IdP integration is activated:
Users sign in using their enterprise IdP password
Users no longer manage their MFA settings (if you opted out of Duo MFA during setup).
Cancel
Activate



第 9 章

Google

概要

ここでは、Google Workplace SAML アプリケーションを作成し、それを Security Cloud Sign On と統合する方法について説明します。

使用する前に

始める前に

- スーパー管理者権限を持つ Google Workspace アカウントが必要です。
- 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 （9 ページ） と ステップ 2：電子メールドメインの申請と検証 （10 ページ） が完了している必要があります。

ステップ 1 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。

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）] をクリックします。

e) [SSOのURL（SSO URL）] と [エンティティID（Entity ID）] をコピーし、証明書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エンタープライズ設定ウィザードを開きます。ステップ 3：SAML メタデータの交換 （11 ページ） の画面が表示されます。

a) [IDプロバイダー（IdP）名（Identity Provider (IdP) Name）] に「`Google SSO`」または他の値を入力します。

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、Google 管理コンソールからコピーした [SSOのURL（SSO URL）] 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、Google 管理コンソールからコピーした [エンティティID（Entity ID）] を入力します。

d) [ファイルの追加（Add File）] をクリックし、Google 管理コンソールからダウンロードした証明書を選択します。

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

f) [次へ（Next）] をクリックします。

g) [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)）] をコピーし、SAML 署名証明書をダウンロードします。

ステップ 3 Google 管理コンソールに戻ります。

a) [カスタムSAMLアプリの追加（Add custom SAML app）] ページで [続行（Continue）] をクリックします。

b) [ACSのURL（ACS URL）] フィールドに、エンタープライズ設定ウィザードから前にコピーした [シングルサインオンサービスURL（ACS URL）（Single Sign-On Service URL (ACS URL)）] を入力します。

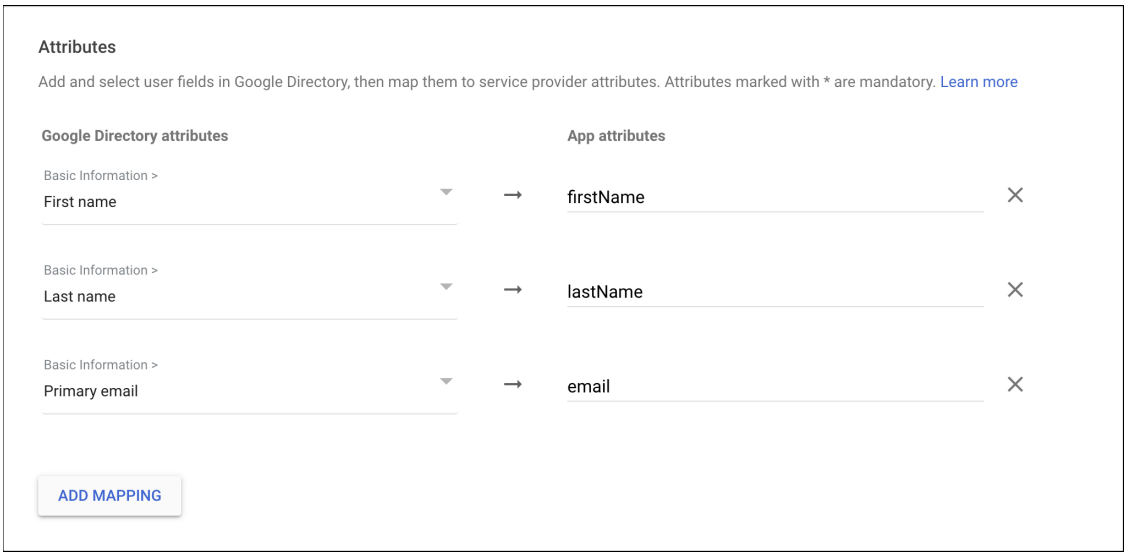
c) [名前IDの形式（Name ID format）] で [UNSPECIFIED（UNSPECIFIED）] または [EMAIL（EMAIL）] を選択します。

d) [名前ID（Name ID）] で [Basic Information > Primary email（Basic Information > Primary email）] を選択します。

e) [続行（Continue）] をクリックします。

f) [属性のマッピング（Attributes mapping）] ページで次の属性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
姓（Last name）	lastName
Primary email	email



ステップ 4 エンタープライズ設定ウィザードの [構成（Configure）] 画面に戻ります。

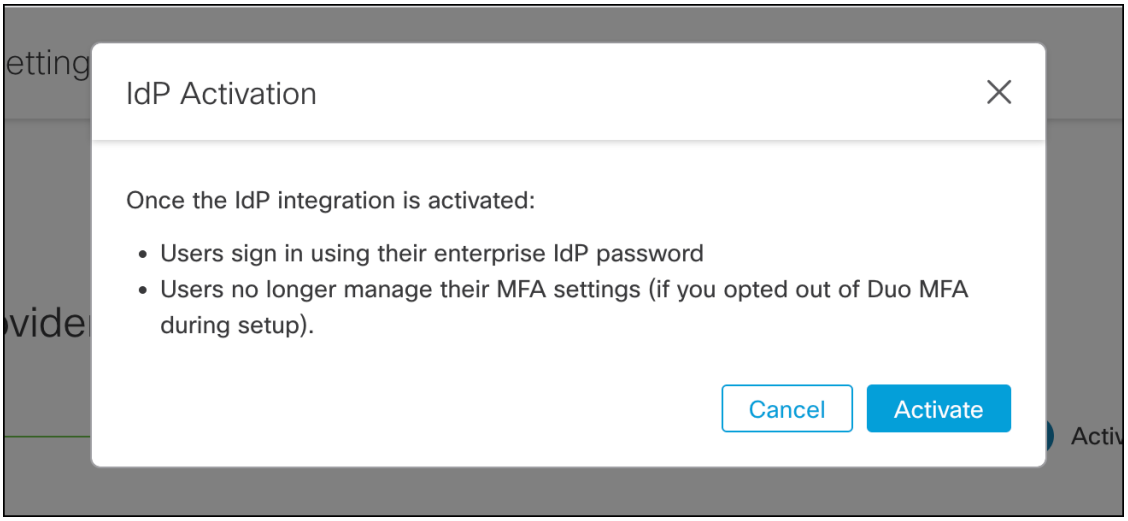
a) 表示された URL をコピーし、プライベート（シークレット）ブラウザウィンドウで開きます。
ブラウザが Google SSO URL にリダイレクトされます。

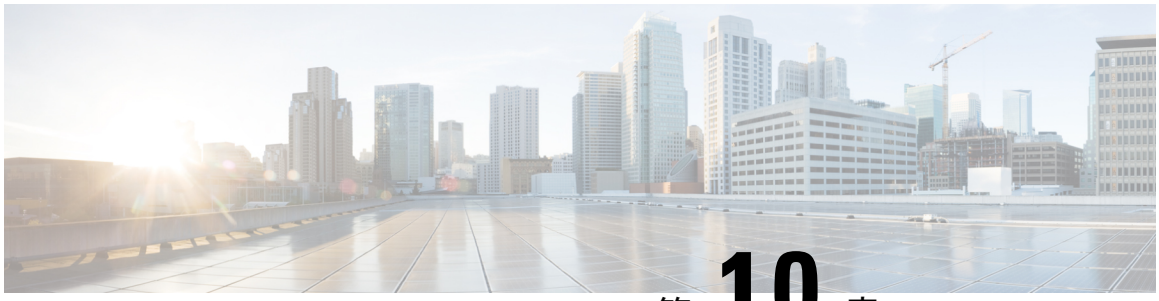
b) ステップ 2：電子メールドメインの申請と検証と一致する電子メールアドレスで Google にサインインします。
SecureX アプリケーションポータルに戻れば、テストは成功です。

c) 設定ウィザードで [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) ユーザーの統合をアクティブ化するには、[IdPをアクティブ化（Activate my IdP）] をクリックします。

e) ダイアログで選択内容を確認します。





第 10 章

Okta

概要

ここでは、Okta SAML アプリケーションを作成し、Security Cloud Sign On と統合する方法について説明します。

はじめに

始める前に

- 管理者権限で Okta ダッシュボード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 （9 ページ） と ステップ 2：電子メールドメインの申請と検証 （10 ページ） が完了している必要があります。

ステップ 1 Okta 管理コンソールにサインインして、次の手順を実行します。

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) [Next] をクリックします。

f) [SAMLの設定（Configure SAML）] タブを選択します。

g) [シングルサインオンURL（Single sign on URL）] フィールドに一時的な値（例：**`https://example.com/sso`**）を入力します。これは後で Security Cloud Sign On の実際の ACS URL に置き換えます。

h) [オーディエンスURI（Audience URI）] フィールドに一時的な値（例：`https://example.com/audience`）を入力します。これは後で Security Cloud Sign On の実際のオーディエンス ID URI に置き換えます。

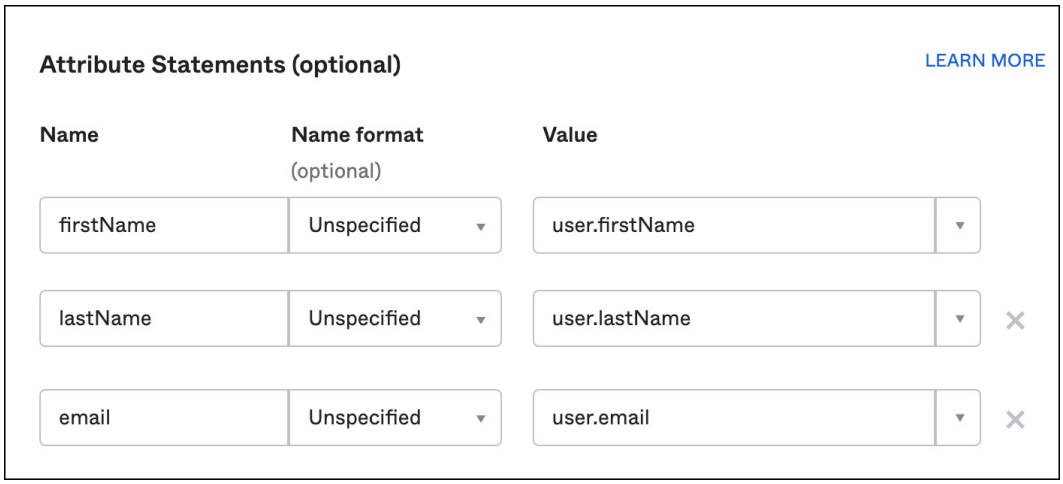
i) [名前IDの形式（Name ID Format）] で [指定なし（Unspecified）] または [EmailAddress（EmailAddress）] を選択します。

j) [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。

k) [属性ステートメント（オプション）（Attribute Statements (optional)）] セクションで、次の属性マッピングを追加します。

[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.email

図 *1*: 属性を追加する例



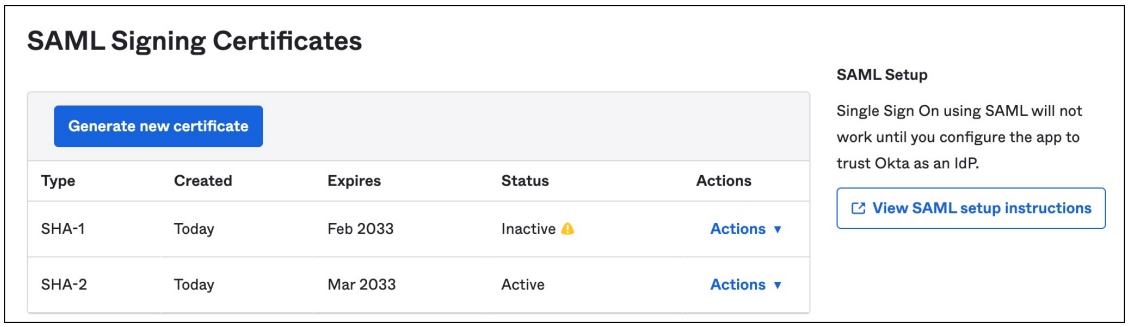
l) [Next] をクリックします。

m) Okta にフィードバックを送信し、[完了（Finish）] をクリックします。

n) ユーザーのグループにアプリケーションを割り当てます。

o) [サインオン（Sign On）] タブを選択します。

p) 下にスクロールして、[SAMLセットアップ手順を表示（View SAML Setup Instructions）] をクリックします。



q) 開いたページで [IDプロバイダーのシングルサインオンURL（Identity Provider Single Sign-On URL）] と [IDプロバイダー発行元（Identity Provider Issuer）] をコピーし、X.509 証明書をダウンロードします。
次に、エンタープライズ設定ウィザードで Security Cloud Sign Onとの SAML アプリケーションの統合を開始します。

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。ステップ 3：SAML メタデータの交換 （11 ページ） の画面が表示されます。

a) [IDプロバイダー名（Identity Provider Name）] フィールドに IdP の名前（例：**`Okta SSO`**）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、Okta からコピーした [IDプロバイダーのシングルサインオンURL（Identity Provider Single Sign-On URL）] の値を入力します。
c) [エンティティID（Entity ID）] フィールドに、Okta からコピーした [IDプロバイダー発行元（Identity Provider Issuer）] フィールドの値を入力します。
d) [ファイルの追加（Add File）] をクリックし、Okta からダウンロードした SAML 署名証明書を選択します。
e) 必要に応じて、Duo ベースの無料の MFA サービスからユーザーをオプトアウトします。
f) [次へ（Next）] をクリックして [ダウンロード（Download）] 画面に進みます。
g) 次の手順で使用するために、[シングルサインオンサービスURL（ACS URL）（Single Sign-On Service URL (ACS URL)）] フィールドと [エンティティID（オーディエンスURI）（Entity ID (Audience URI)）] フィールドの値をコピーして保存します。
h) 次の手順で使用するために、SAML 署名証明書（cisco-securex.pem）をダウンロードします。

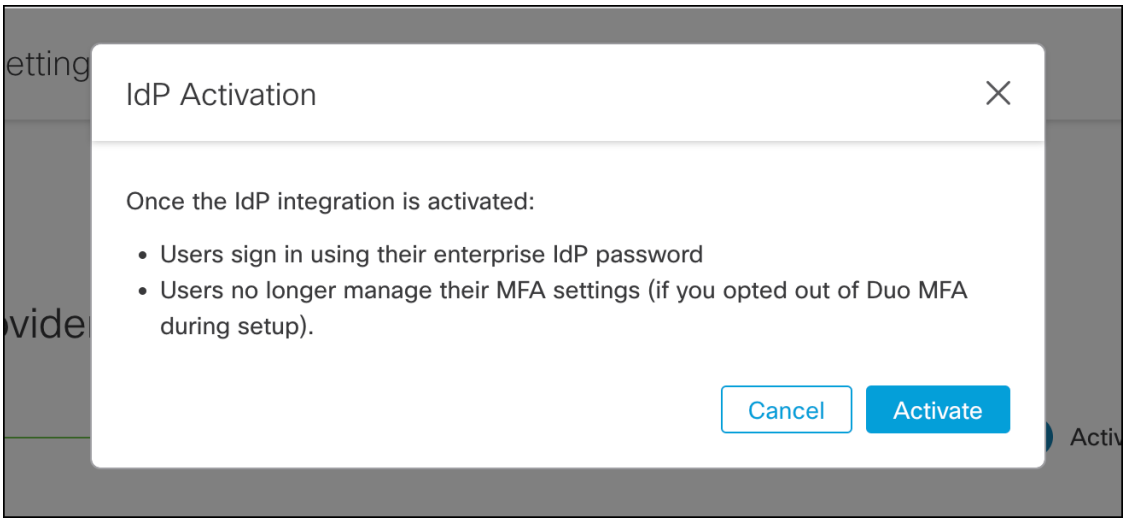
ステップ 3 Okta の SAML アプリケーション設定に戻ります。

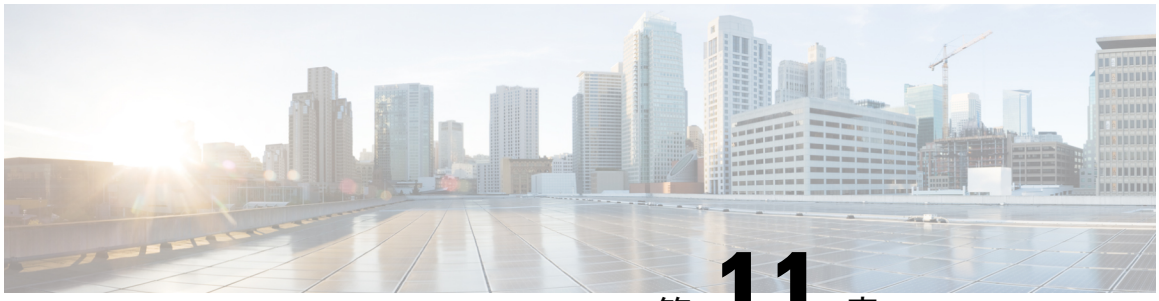
a) [全般（General）] タブをクリックします。
b) [SAML設定（SAML Settings）] セクションで [編集（Edit）] をクリックします。
c) [次へ（Next）] をクリックします。
d) [シングルサインオンURL（Single sign-on URL）] の値を、エンタープライズ設定ウィザードで提供された [シングルサインオンサービスURL（ACS URL）（Single Sign-On Service URL (ACS URL)）] フィールドの値に置き換えます。
e) [オーディエンスURI（SPエンティティID）（Audience URI (SP Entity ID)）] の値を、エンタープライズ設定ウィザードで提供された [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。

f) [詳細設定を表示（Show Advanced Settings）] をクリックし、[署名証明書（Signature Certificate）] フィールドを見つけます。
g) [ファイルの参照（Browse files）] をクリックし、前にダウンロードしたシスコの SAML 署名証明書を見つけます。
h) [Next] をクリックします。
i) [終了（Finish）] をクリックして変更を保存します。

ステップ 4 エンタープライズ設定ウィザードの [構成（Configure）] 画面に戻ります。

a) 表示された URL をコピーし、プライベート（シークレット）ブラウザウィンドウで開きます。
ブラウザが Okta SSO URL にリダイレクトされます。
b) ステップ 2：電子メールドメインの申請と検証と一致する電子メールアドレスで Duo にサインインします。
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。
c) 設定ウィザードで [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) ユーザーの統合をアクティブ化するには、[IdPをアクティブ化（Activate my IdP）] をクリックします。
e) ダイアログで選択内容を確認します。





第 11 章

Ping ID

概要

ここでは、Ping Identity で SAML アプリケーションを作成し、それを Security Cloud Sign On と統合する方法について説明します。

使用する前に

始める前に

- 管理者権限で Ping Idendity 管理コンソー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 （9 ページ） と ステップ 2：電子メールドメインの申請と検証 （10 ページ） が完了している必要があります。

ステップ 1 Ping Idendity コンソールで次の手順を実行します。

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

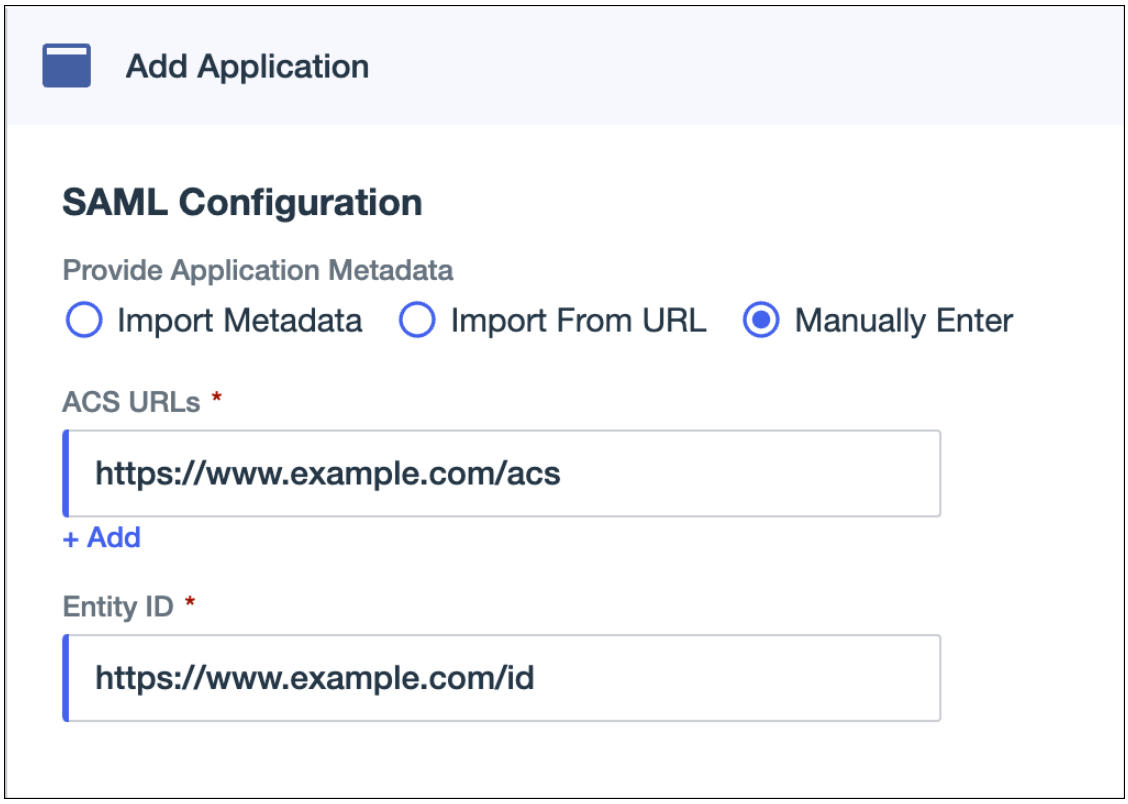
b) [+] ボタンをクリックして [アプリケーションの追加（Add Application）] ダイアログを開きます。

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。

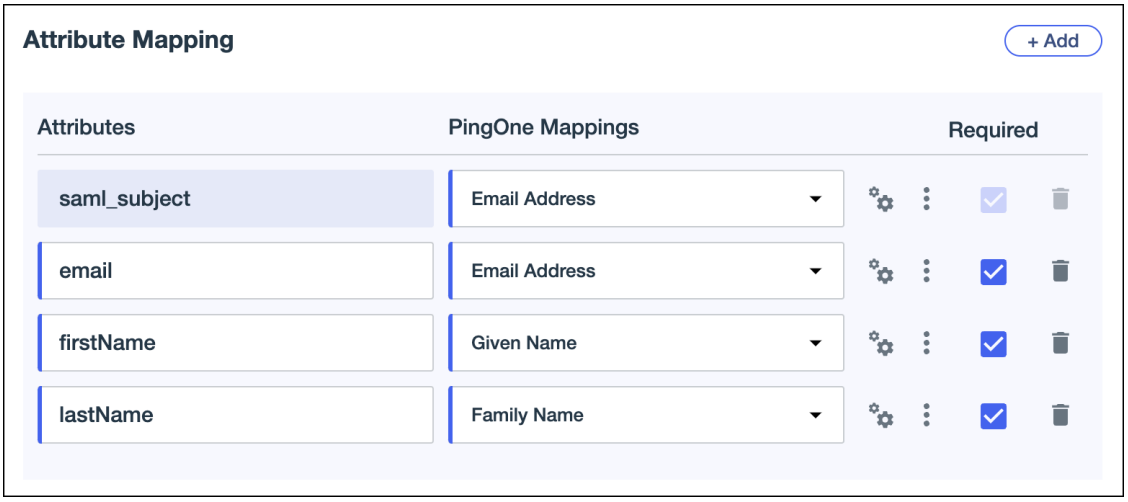
f) [SAML設定（SAML Configuration）] ダイアログで、SAML メタデータを手動で入力するオプションを選択し、[ACS URL（ACS URL）] と [エンティティID（Entity ID）] に一時的な URL を入力します。これらは後で実際の URL に置き換えます。



g) [保存（Save）] をクリックします。
h) [設定（Configuration）] タブをクリックします。
i) [署名証明書のダウンロード（Download Signing Certificate）] をクリックします。
j) 次の手順で使用するために、[発行元ID（Issuer ID）] プロパティと [シングルサインオンサービス（Single Signon Service）] プロパティの値をコピーします。
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	名
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。

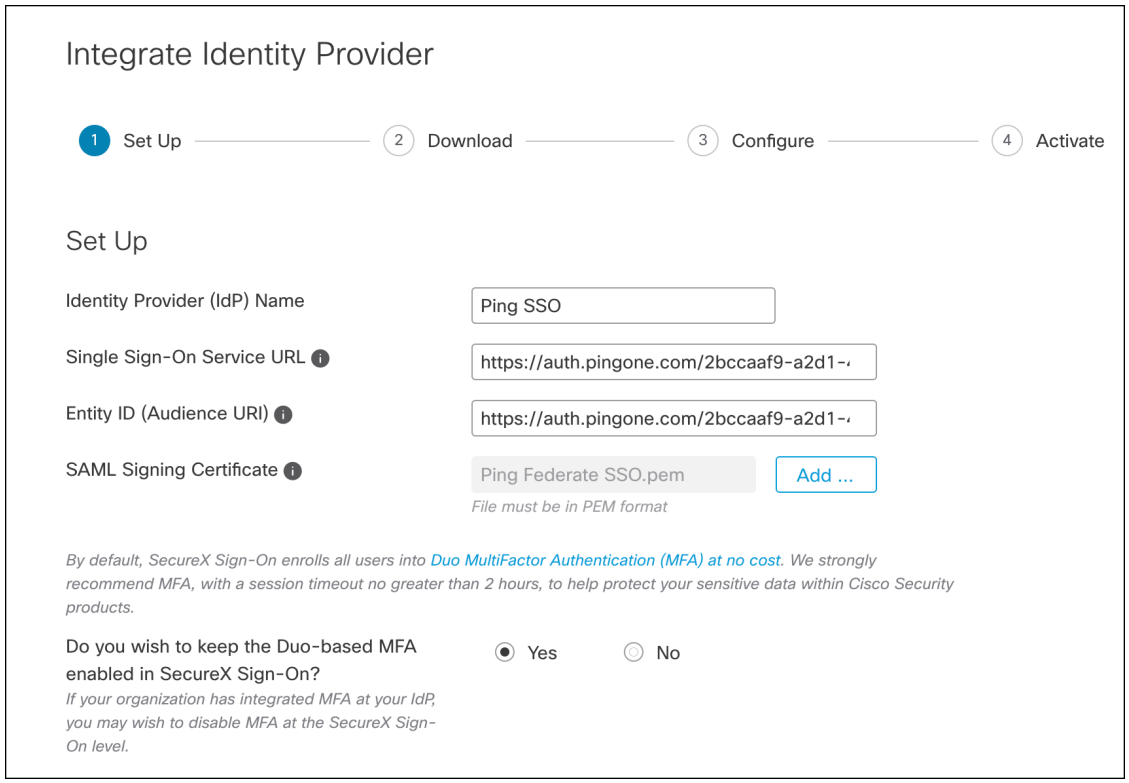
ステップ 2 新しいブラウザタブでエンタープライズ設定ウィザードを開きます。[IDプロバイダーの統合（Integrate Identity Provider）] 画面の [セットアップ（Set Up）] ステップ（ステップ 3：SAML メタデータの交換 （11 ページ））が表示されます。

a) [IDプロバイダー（IdP）名（Identity Provider (IdP) Name）] フィールドに統合の名前（例：**`Ping SSO`**）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、Ping SAML アプリケーションからコピーした [発行元ID（Issuer ID）] の値を入力します。

c) [追加...（Add...）] をクリックし、前にダウンロードした Ping 署名証明書を選択します。

d) 必要に応じて、無料の Duo 多要素認証からユーザーをオプトアウトします。



e) [次へ（Next）] をクリックして [ダウンロード（Download）] 画面に進みます。

f) [ダウンロード（Download）] 画面で、[シングルサインオンサービスURL（ACS URL）（Single Sign-On Service URL (ACS URL)）] プロパティと [エンティティID（オーディエンスURI）（Entity ID (Audience URI)）] プロパティの値をコピーし、[ダウンロード（Download）] をクリックして署名証明書をダウンロードします。

ステップ 3 Ping Idendity コンソールに戻り、次の手順を実行します。

a) [構成（Configuration）] タブで、編集（鉛筆）アイコンをクリックします。

b) [ACS URL（ACS URLs）] フィールドで、一時的な URL を前の手順でコピーした [シングルサインオンサービスURL（ACS URL）（Single Sign-On Service URL (ACS URL)）] に置き換えます。

c) [エンティティID（Entity ID）] フィールドで、一時的な URL を前の手順でコピーした [エンティティID（オーディエンスURI）（Entity ID (Audience URI)）] に置き換えます。

d) [検証証明書（Verification Certificate）] フィールドで、[インポート（Import）] オプションを選択し、[ファイルの選択（Choose File）] をクリックします。

e) 前の手順でダウンロードした Security Cloud Sign On 署名証明書を選択します。

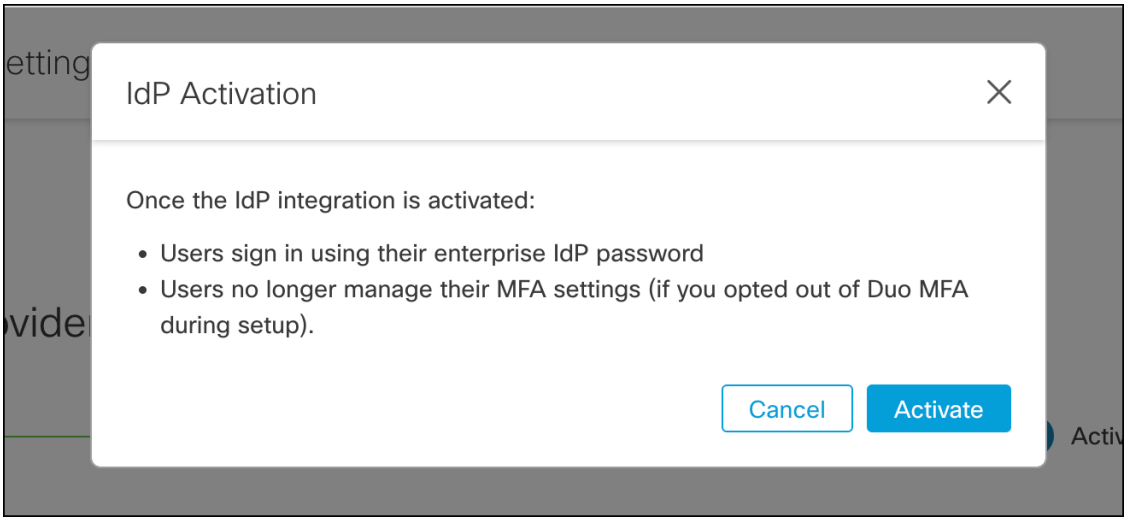
f) [保存（Save）] をクリックします。

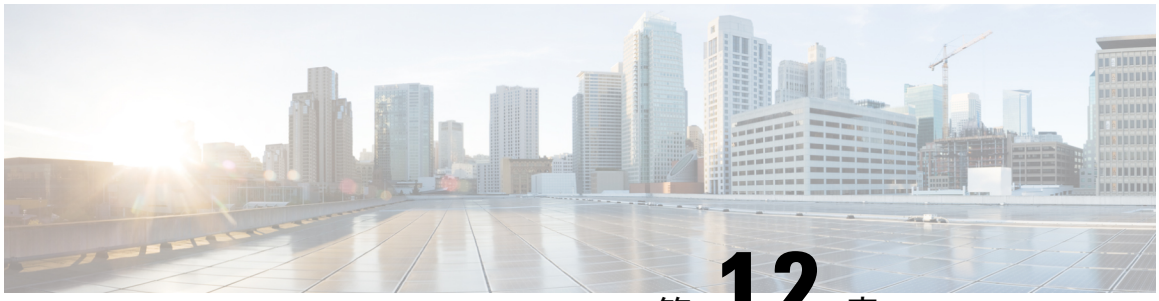
g) アプリケーション設定パネルの上部にあるトグルをクリックして、アプリケーションへのユーザーアクセスを有効にします。

ステップ 4 エンタープライズ設定ウィザードの [構成（Configure）] 画面に戻ります。

a) 表示された URL をコピーし、プライベート（シークレット）ブラウザウィンドウで開きます。ブラウザが Ping Idendity SSO ページにリダイレクトされます。

b) ステップ 2：電子メールドメインの申請と検証と一致する電子メールアドレスで Ping Idendity にサインインします。
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。
c) 設定ウィザードで [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) ユーザーの統合をアクティブ化するには、[IdPをアクティブ化（Activate my IdP）] をクリックします。
e) ダイアログで選択内容を確認します。





第 12 章

一般的な IdP の手順

一般的な IdP の手順

特定の ID プロバイダー用の SAML アプリケーションを作成する手順がここに記載されていない場合は、IdP が提供する手順に従ってください。SAML 応答は、適切な <NameID> 値と属性名のマッピングで構成する必要があります。また、Security Cloud Sign On に SAML アプリのシングルサインオン URL とエンティティ ID を提供する必要があります。

SAML 応答の要件

SAML 応答の属性

IdP によって送信される SAML 応答のアサーションには、次の属性名が含まれている必要があり、IdP の対応する属性にマッピングされている必要があります。

SAML アサーション属性名	IdP ユーザー属性
firstName	ユーザーの名。
lastName	ユーザーの姓。
email	ユーザーの電子メール。これは、SAML 応答の **<NameID>** 要素と一致する必要があります。

たとえば、次の XML スニペットは、Security Cloud Sign On ACL URL への SAML 応答に含まれる **<AttributeStatement>** 要素の例です。

```
<saml2:AttributeStatement>
  <saml2:Attribute Name="firstName"
```

```
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml2:AttributeValue
          xmlns:xs="http://www.w3.org/2001/XMLSchema"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">John

      </saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="lastName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml2:AttributeValue
          xmlns:xs="http://www.w3.org/2001/XMLSchema"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Doe

      </saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml2:AttributeValue
          xmlns:xs="http://www.w3.org/2001/XMLSchema"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">jdoe@example.com
      </saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

NameID 要素

IdP からの SAML 応答の **<NameID>** 要素には、その値として有効な電子メールアドレスが含まれている必要があり、電子メールは SAML 応答の属性 （51 ページ） の **email** 属性の値と一致する必要があります。

<NameID> の **Format** 属性は、**urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified** または **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress** に設定されている必要があります。

`<NameID>` 要素の例を次に示します。

```
<saml2:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">jdoe@example.com</saml2:NameID>
```

SAML メタデータの要件

Security Cloud Sign On と統合するには、IdP の SAML アプリケーションの次のメタデータが必要です。

- **シングルサインオンサービスの初期 URL** – これは「SSO URL」または「ログイン URL」と呼ばれることもあります。この URL を使用して、IdP から Security Cloud Sign On への認証を開始できます。
- **エンティティ ID URI** – IdP のグローバルな一意の名前。これは「発行元」と呼ばれることもあります。
- **X.509 署名証明書** – IdP が SAML アサーションに署名するために使用する公開キー/秘密キーのペアの公開キー。

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。