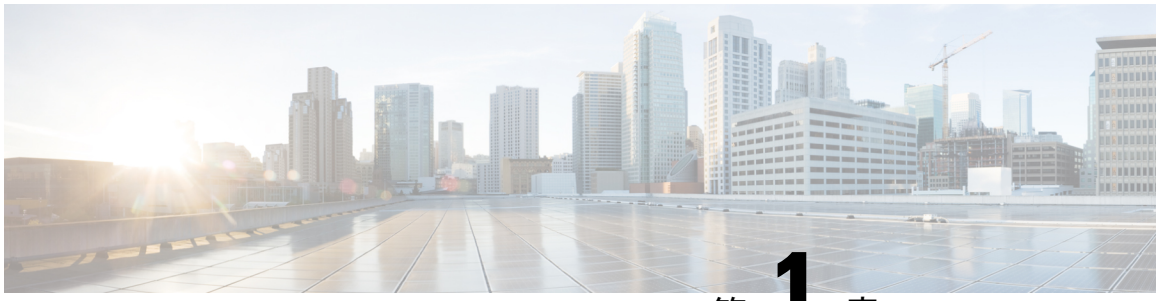
Cisco Security Cloud Control ユーザーガイド

初版：2023 年 4 月 16 日

最終更新：2023 年 10 月 6 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

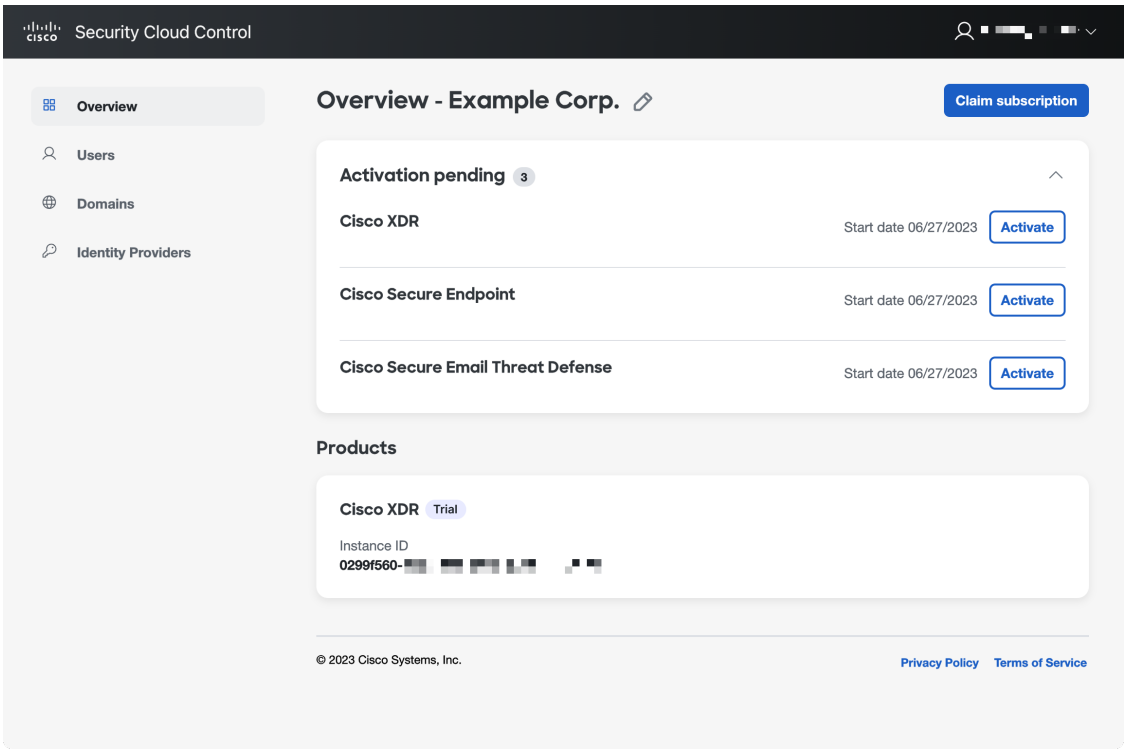
概要

Cisco Security Cloud Control の概要

Security Cloud Control は、Cisco Security Cloud 全体で Cisco Secure 製品のプロビジョニング、ユーザー アイデンティティ（ID）、およびユーザーアクセスを中央管理する Web アプリケーションです。Security Cloud Control の管理者は、新しい Security Cloud エンタープライズの作成、エンタープライズ内のユーザーの管理、ドメインの要求、組織の SSO ID プロバイダーの統合などのタスクを実行できます。

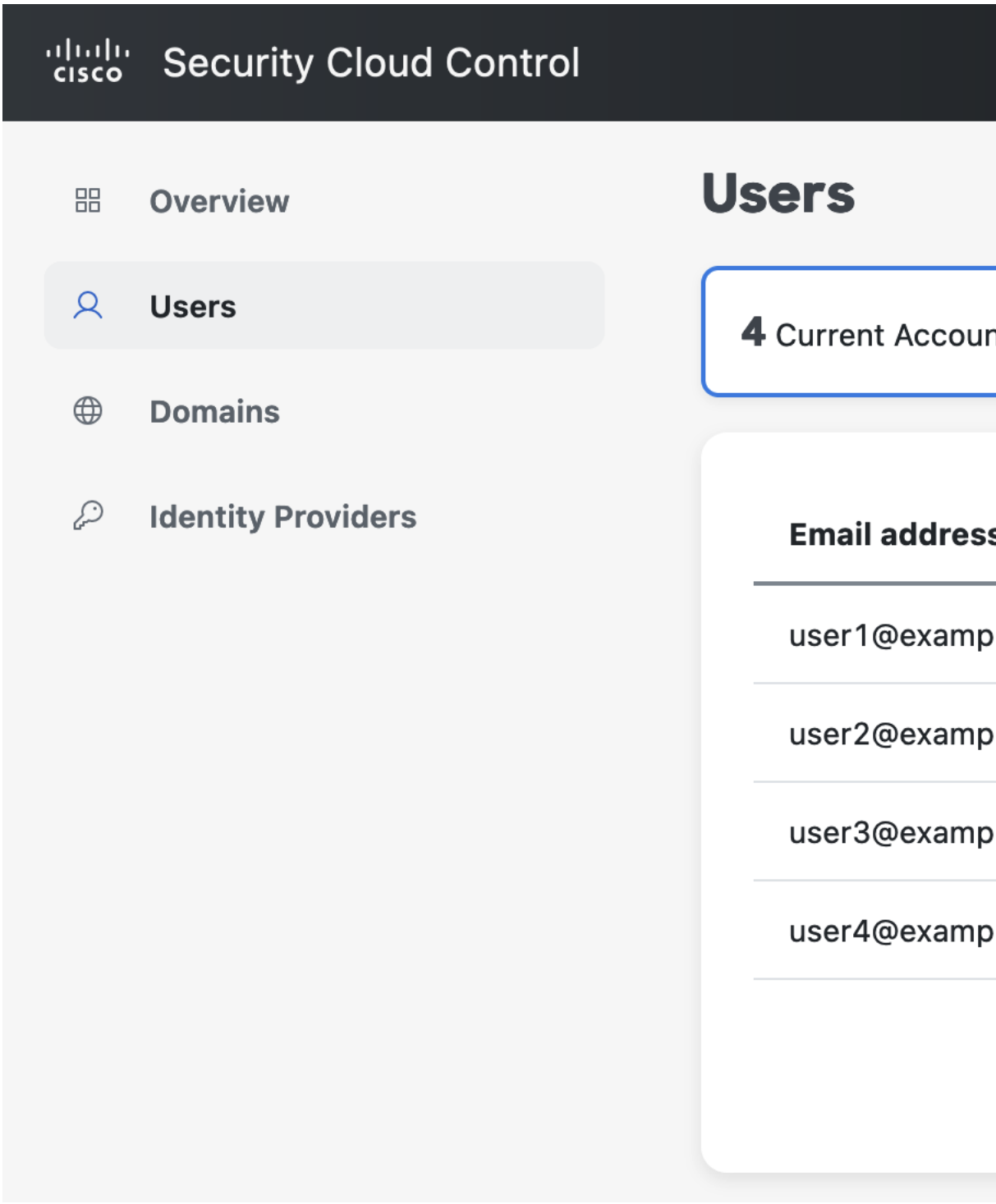
[概要（Overview）] タブ

[概要（Overview）] タブには、現在アクティブ化されているシスコ製品のインスタンスと、アクティブ化が保留中のシスコ製品のインスタンスが一覧表示されます。また、ここからサブスクリプションを要求したり、Security Cloud に外部製品を接続したりすることもできます。詳細については、製品およびサブスクリプションの管理 （7 ページ）を参照してください。



[ユーザー（Users）] タブ

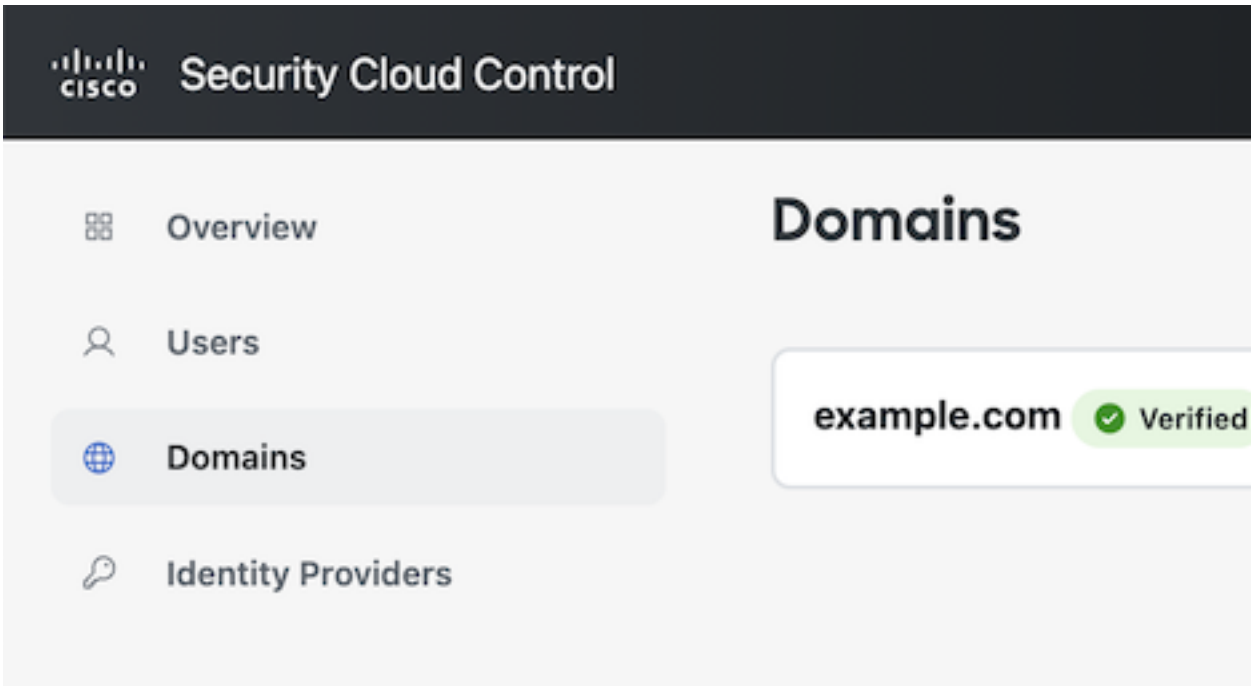
[ユーザー（Users）] タブには、管理者によってエンタープライズにユーザーの招待されたユーザーが一覧表示されます。管理者は、ユーザーパスワードと MFA 設定のリセット（ドメインの要求および検証のユーザーの場合）や、ユーザーアカウントの非アクティブ化もできます。詳細については、ユーザーの管理 （15 ページ）を参照してください。



[ドメイン（Domains）] タブ

[ドメイン（Domains）] タブには、エンタープライズに対して要求および検証された電子メールドメインが一覧表示されます。ID プロバイダーを Security Cloud Sign On と統合するには、

ドメインを検証する必要があります。また、管理者は、要求されたドメイン内のユーザーのパスワードまたは MFA 設定をリセットできます。詳細については、ドメインの管理 （19 ページ）を参照してください。



[ID プロバイダー（Identity Providers）] タブ

[IDプロバイダー（Identity Providers）] タブには、現在のエンタープライズについて、SAML（Secure Assertion Markup Language）を使用して Security Cloud Sign On と統合されている ID プロバイダーが一覧表示されます。これにより、エンタープライズユーザーは、IDプロバイダーの SSO 認証情報を使用して Cisco Secure 製品にアクセスできます。詳細については、ID プロバイダー統合ガイド （21 ページ）を参照してください。

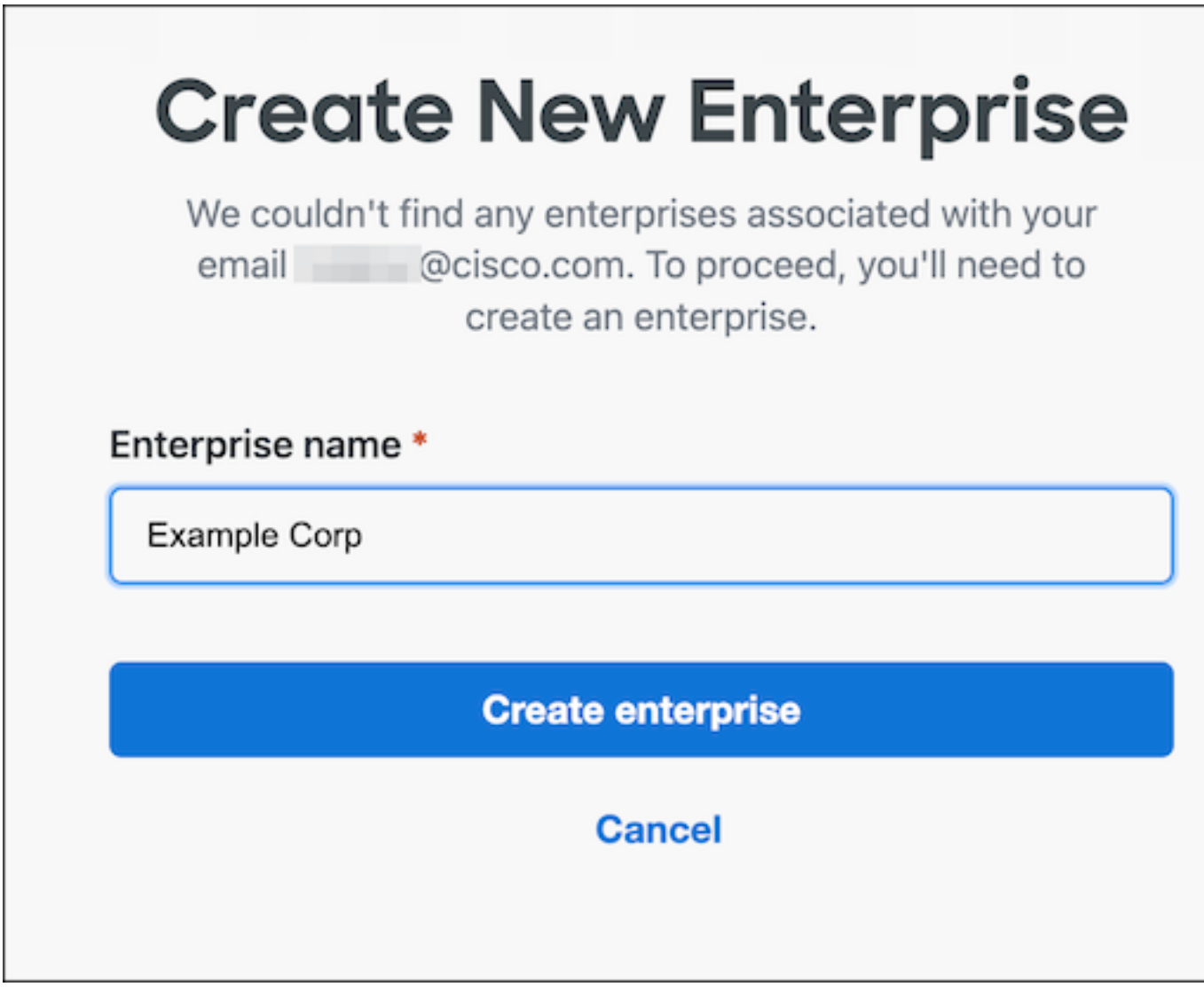
Security Cloud Control へのサインイン

Security Cloud Control にサインインするには、Cisco Security Cloud Sign On アカウントが必要です。アカウントをお持ちでない場合は、アカウントを作成できます。Security Cloud Sign On で認証を行ったら、Security Cloud エンタープライズも選択する必要があります。エンタープライズは、組織のユーザー、製品サブスクリプション、要求されたドメイン、その他の情報で構成されます。

ステップ 1 Security Cloud Control にサインインします。

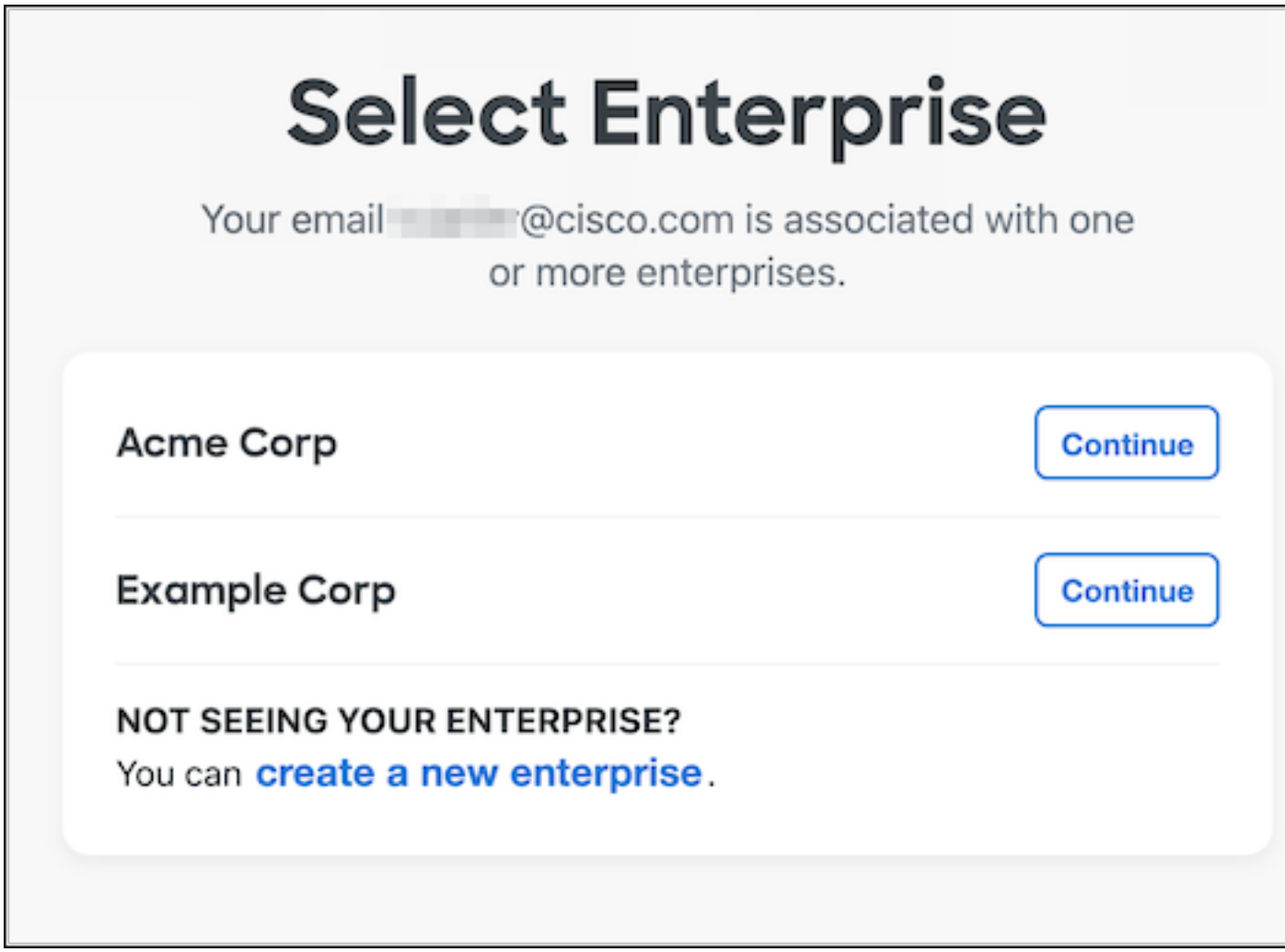
アカウントが Security Cloud エンタープライズに関連付けられていない場合、続行するにはエンタープライズを作成する必要があります。または、**ステップ 3** に進み、既存のエンタープライズでサインインします。

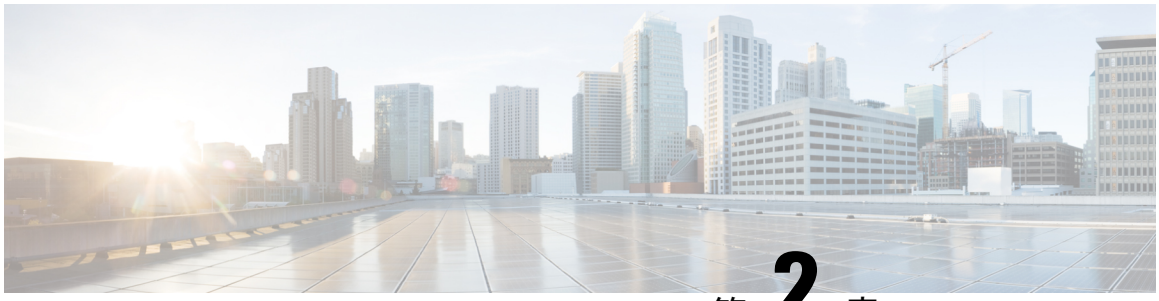
ステップ 2 エンタープライズ名を入力し、[エンタープライズの作成（Create enterprise）] をクリックします。



エンタープライズを作成すると、[エンタープライズの選択（Select Enterprise）] ページに戻ります。

ステップ 3 [続行（Continue）] をクリックして、サインインするエンタープライズを選択します。


Select Enterprise
Your email @cisco.com is associated with one or more enterprises.
Acme Corp
Continue
Example Corp
Continue
NOT SEEING YOUR ENTERPRISE?
You can create a new enterprise.



第 2 章

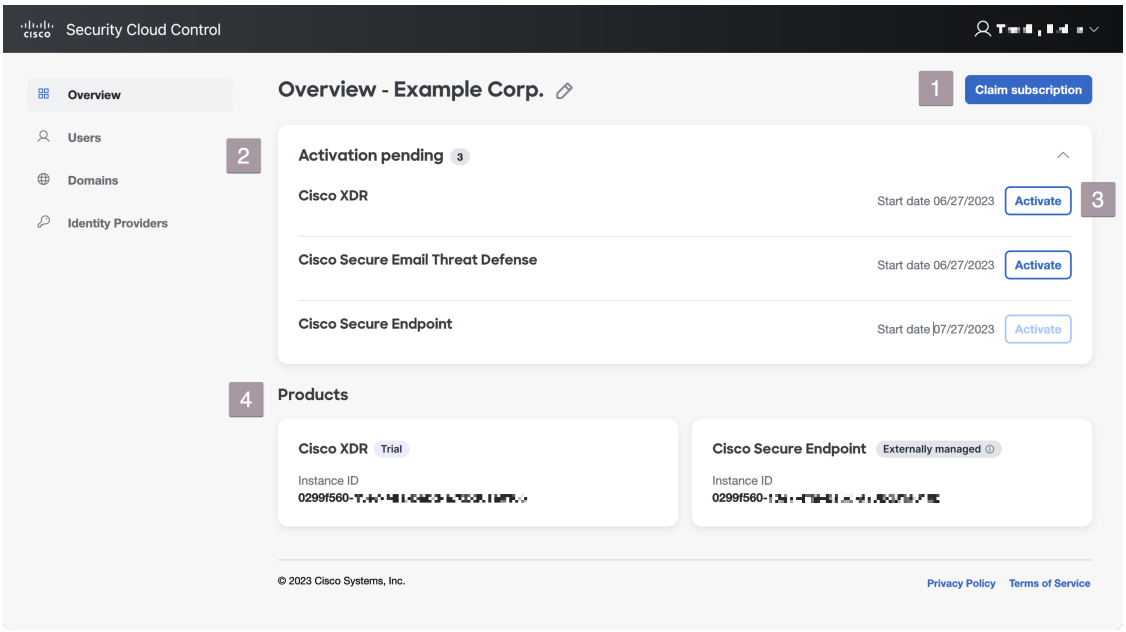
製品およびサブスクリプションの管理

概要

新しいサブスクリプションをシスコから購入すると、購入プロセス中に指定された最初のプロビジョニング連絡先にサブスクリプション要求コードが電子メールで送信されます。Security Cloudエンタープライズ管理者は、要求コードを受信したら、[サブスクリプションの要求（Claim subscription）]（**1**）をクリックして、現在のエンタープライズのサブスクリプションの要求します。

サブスクリプションを要求すると、[概要（Overview）] タブの [アクティベーション保留中（Activation pending）]（**2**）の下にその製品名と対応する開始日が表示されます。製品サブスクリプションの開始日になると、[アクティブ化（Activate）] ボタン（**3**）が有効になり、エンタープライズ管理者は製品を概要できます。アクティブ化された製品は、[製品（Products）] セクション（**4**）に表示されます。

トライアル製品には Trial ラベルが付きます。外部管理対象製品インスタンスの接続されている外部管理製品インスタンスには、 Externally managed ⓘ ラベルが付きます。



サブスクリプションの要求

Cisco Secure 製品のサブスクリプションを購入すると、最初のプロビジョニング連絡先として指定されたユーザーにサブスクリプション要求コードが電子メールで送信されます。この連絡先は、サブスクリプションを管理する Security Cloud Control 管理者であるとは限りません。Security Cloud Control 管理者は、要求コードを使用してエンタープライズのサブスクリプションを要求します。要求されると、サブスクリプションの製品は [アクティベーション保留（Activation pending）] リストに追加され、サブスクリプションの開始日に達すると製品インスタンスのアクティブ化できます。

始める前に

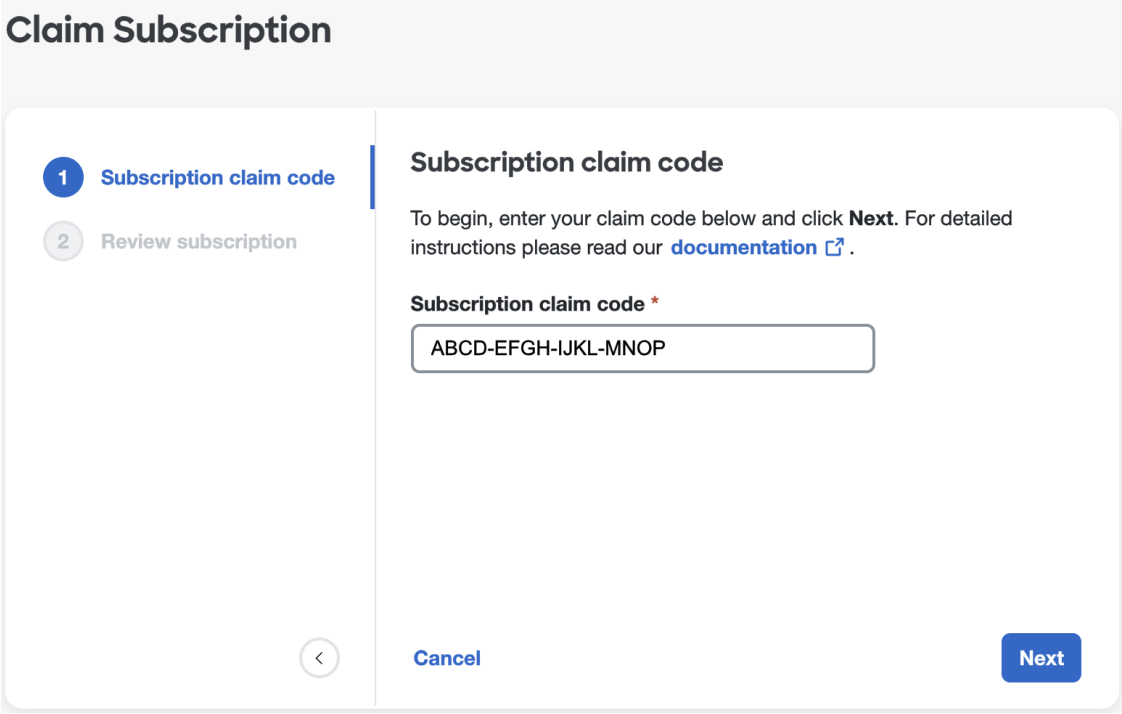
これらの手順を完了するには、サブスクリプション要求コードが必要です。

ステップ 1 Security Cloud Control にサインインします。

ステップ 2 プロンプトが表示されたら、サブスクリプション内の製品を要求してアクティブ化するエンタープライズを選択するか、新しいエンタープライズを作成します。

ステップ 3 右上隅にある [サブスクリプションの要求（Claim subscription）] をクリックします。

ステップ 4 要求コードを入力し、[次へ（Next）] をクリックします。



ステップ 5 サブスクリプション内の製品のリストを確認し、[サブスクリプションの要求（Claim subscription）] をクリックします。

サブスクリプション内の製品が、[概要（Overview）] タブの [アクティベーション保留中（Activation pending）] リストに追加されます。

次のタスク

サブスクリプションの開始日に達した製品インスタンスのアクティブ化を開始できます。

製品インスタンスのアクティブ化

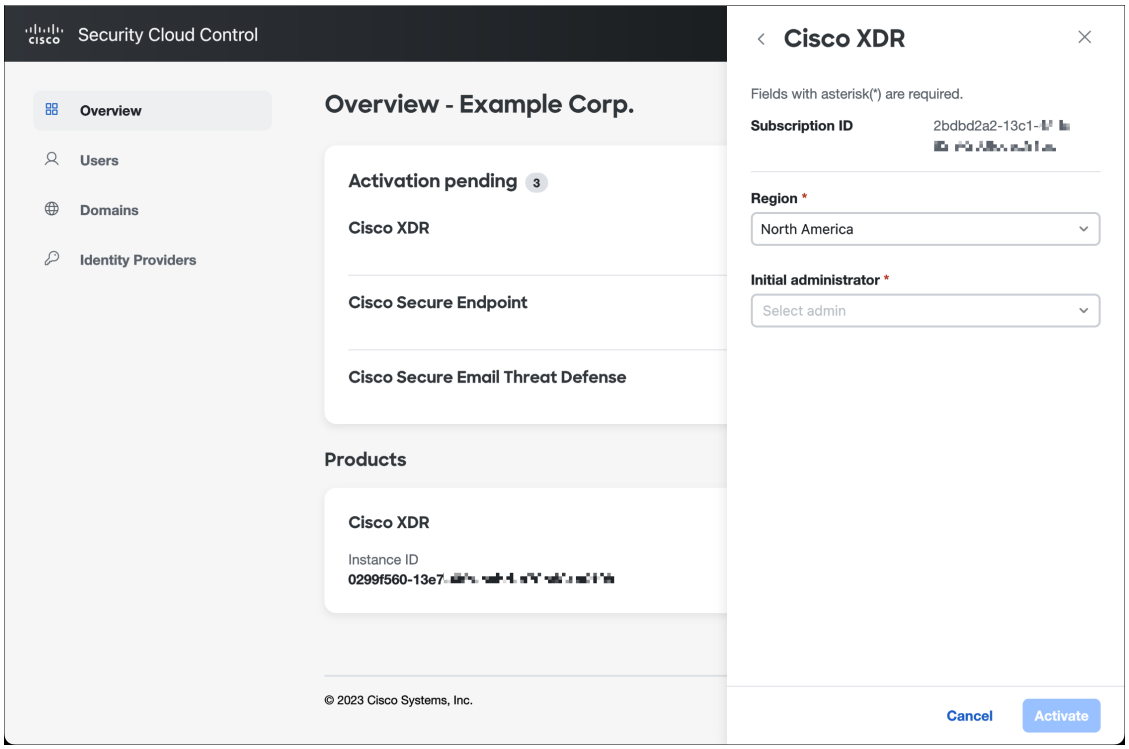
サブスクリプションがサブスクリプションの要求され、その開始日に達すると、サブスクリプションの製品をアクティブ化できます。現在のエンタープライズでアクティブ化された既存の製品インスタンスがある場合は、新しい製品ライセンスを既存のインスタンスに適用するか、新しいインスタンスをアクティブ化するかを選択できます。新しいインスタンスをアクティブ化する場合は、アクティブ化するリージョンと、最初の管理者になるユーザーの電子メールを指定します。

ステップ 1 Security Cloud Control にサインインします。

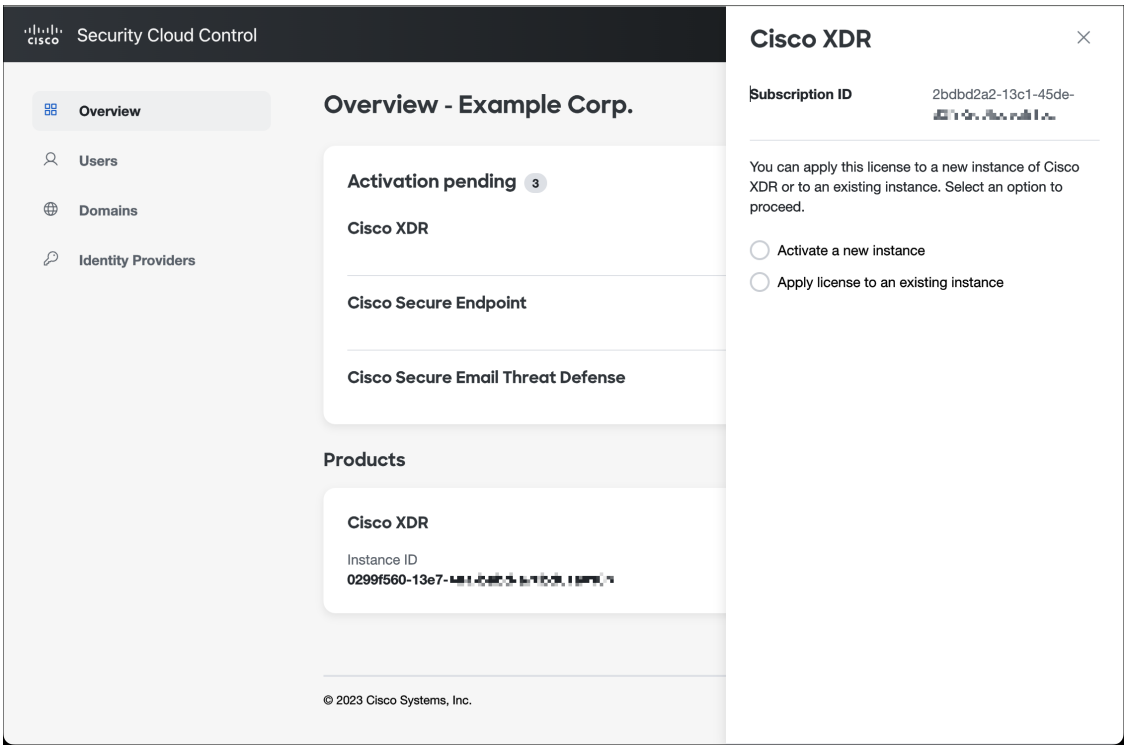
ステップ 2 エンタープライズを選択するように求められたら、関連する製品サブスクリプションのサブスクリプションの要求に使用したのと同じエンタープライズを選択します。

ステップ 3 [アクティベーション保留中（Activation pending）] リストで、アクティブ化する製品の [アクティブ化（Activate）] をクリックします。

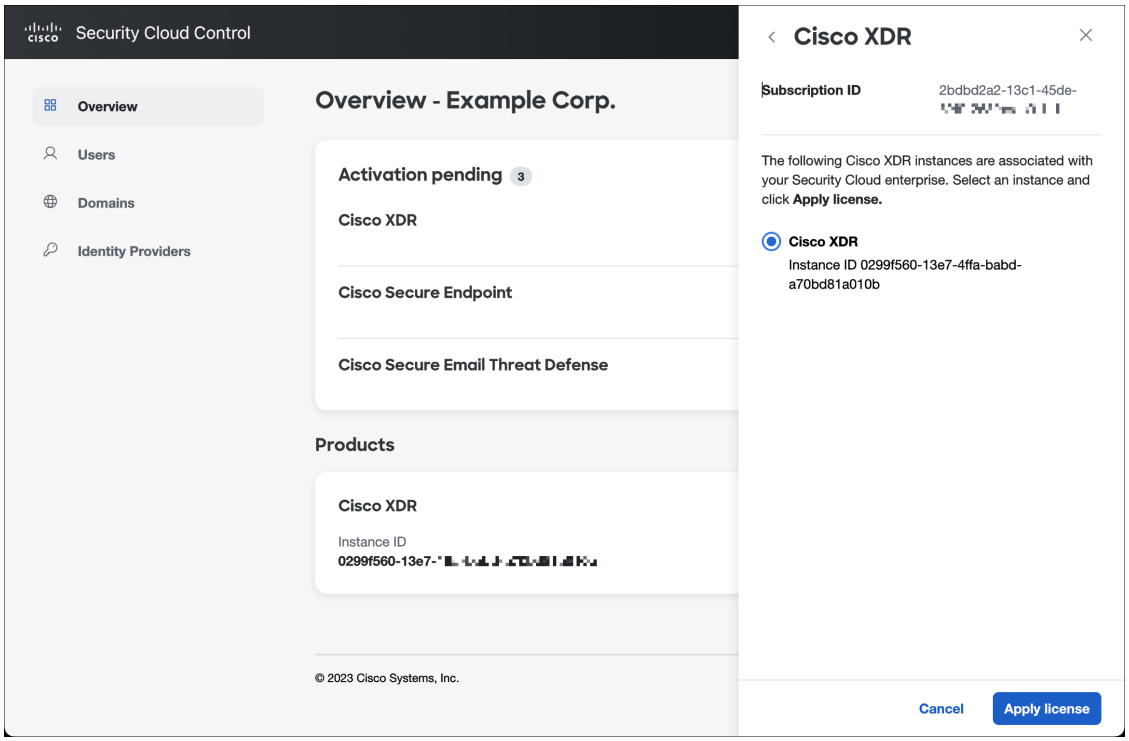
- 既存のアクティブ化された製品インスタンスがない場合は、製品をアクティブ化するリージョンと最初の管理者の電子メールを選択します。準備ができたら、[アクティブ化（Activate）] をクリックします。



- 同じ製品の既存のアクティブ化されたインスタンスがある場合は、新しいインスタンスをアクティブ化するか、既存のインスタンスにライセンスを適用するかを尋ねられます。



- 新しいインスタンスをアクティブ化するには、[新しいインスタンスのアクティブ化（Activate a new instance）] を選択し、上記と同じ手順に従います。既存のインスタンスにライセンスを適用するには、[既存のインスタンスにライセンスを適用（Apply license to an existing instance）] を選択し、目的のインスタンスを選択して、[ライセンスの適用（Apply license）] をクリックします。



製品が [製品（Products）] テーブルに追加されます。

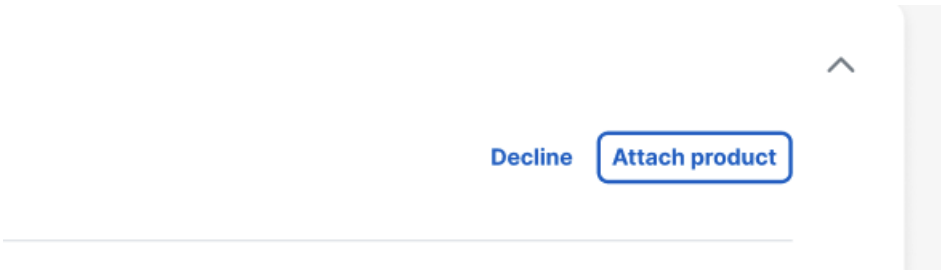
外部管理対象製品インスタンスの接続

Security Cloud Control の外部で管理されているシスコ製品インスタンスがある場合は、必要に応じて Security Cloud エンタープライズに接続できます。シスコは、Security Cloud Control 管理者のリストに、インスタンスを Security Cloud に接続するよう招待する電子メールを送信することで、このプロセスを開始します。管理者はサインインして、外部インスタンスを Security Cloud に接続できます。Security Cloud に接続されている製品インスタンスには、製品名の横に [外部管理（Externally managed）] ラベルが付いています。

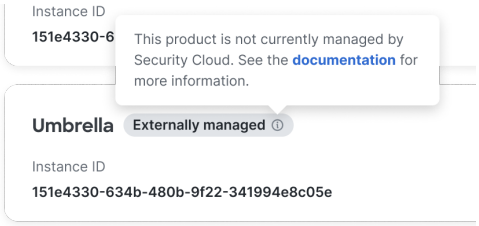
ステップ 1 Security Cloud Control にサインインします。

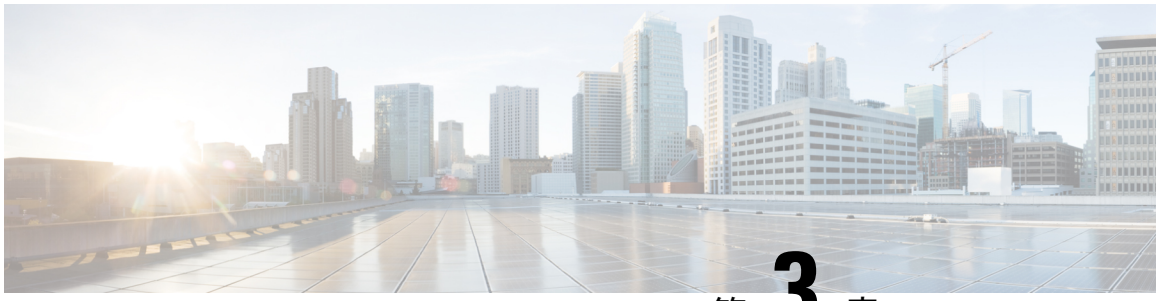
ステップ 2 エンタープライズを選択するように求められたら、外部管理製品インスタンスを接続するエンタープライズを選択します。

ステップ 3 接続する製品の横にある [製品の接続（Attach product）] をクリックします。



接続された製品は、製品のリストに外部管理ラベル付きで表示されます。





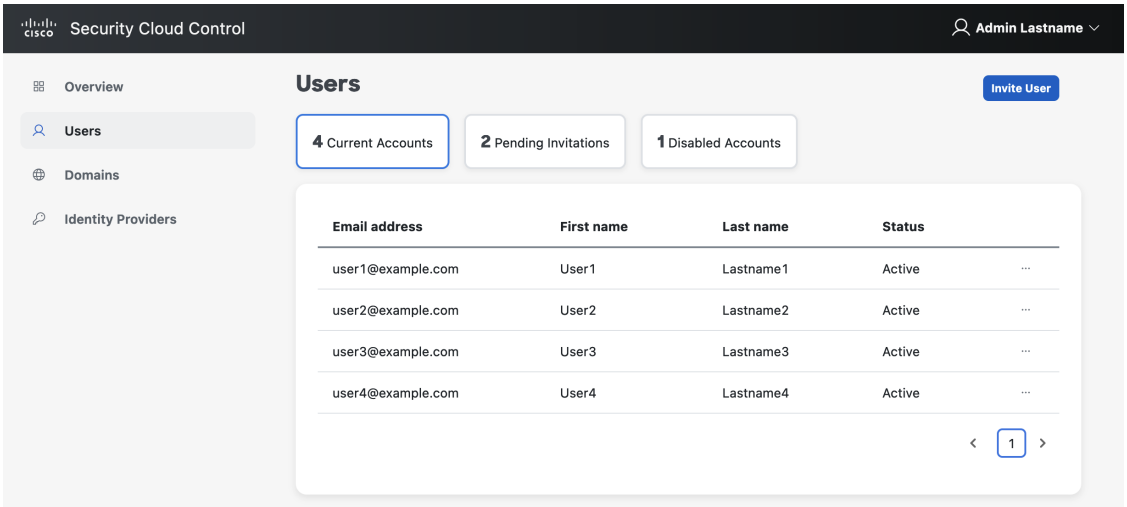
第 3 章

ユーザーの管理

ユーザーの一覧表示

[ユーザー（Users）] ページには、ユーザーアカウントの次のビューが表示されます。

- [現在のアカウント（Current Accounts）] には、エンタープライズにユーザーの招待されているエンタープライズ内のユーザーが一覧表示されます。
- [保留中の招待（Pending Invitations）] には、エンタープライズへの参加にユーザーの招待されているが、まだアカウントをアクティブ化していないユーザーが一覧表示されます。
- [無効なアカウント（Disabled Accounts）] には、アカウントがユーザーアカウントの削除または無効化になっているユーザーが一覧表示されます。



ユーザーの招待

エンタープライズ管理者は、ユーザーをエンタープライズに招待できます。

ステップ 1 [ユーザー（User）] タブを選択します。

ステップ 2 [Invite User] をクリックします。

ステップ 3 ユーザーの名、姓、電子メールを入力します。

ステップ 4 [招待（Invite）] をクリックします。

招待されたユーザーには、1 時間で期限切れになるアクティベーションリンクが記載された電子メールが送信されます。まだアクティブ化されていない招待は、[保留中の招待（Pending Invitations）] で表示できます（「ユーザーの一覧表示 （15 ページ）」を参照）。

（注） アカウントアクティベーションの電子メールは、IDプロバイダー統合ガイドしているエンタープライズ内のユーザーには送信されません。

ユーザーの編集

エンタープライズ管理者は、ユーザーの姓名を編集できます。ユーザーの電子メールアドレスは変更できません。

ステップ 1 左側のナビゲーションで [ユーザー（Users）] をクリックし、[現在のユーザー（Current Users）] をクリックします。

ステップ 2 メニューアイコン … をクリックし、[編集（Edit）] を選択します。

ステップ 3 ユーザーの名または姓を編集します。

ステップ 4 **[更新（Update）]**をクリックします。

ユーザーパスワードまたは MFA 設定のリセット

エンタープライズ管理者は、ドメインの要求および検証に属するユーザーのパスワードと MFA ログイン情報をリセットできます。

ステップ 1 [ユーザー（User）] タブを選択します。

ステップ 2 [現在のアカウント（Current Accounts）] で、パスワードまたは MFA 設定をリセットするユーザーを見つけ、アイコンメニュー をクリックします。

a) ユーザーのパスワードをリセットするには、[パスワードのリセット（Reset password）] を選択します。

b) ユーザーの MFA 設定をリセットするには、[MFAのリセット（Reset MFA）] を選択します。

ユーザーが次回サインオンすると、パスワードをリセットするか、Duo MFA 認証解除要素を設定するように求められます。

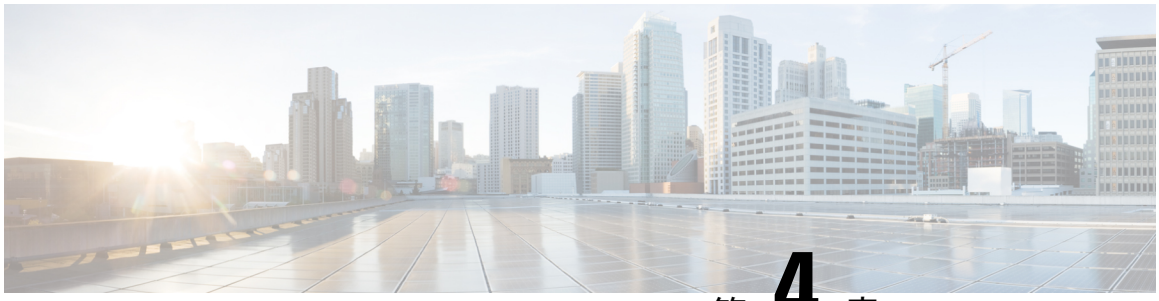
ユーザーアカウントの削除または無効化

ステップ 1 [ユーザー（User）] タブを選択します。

ステップ 2 [現在のアカウント（Current Accounts）] で、削除または無効にするユーザーアカウントを見つけ、アイコンメニュー をクリックします。

a) エンタープライズからユーザーを削除するには、[削除（Remove）] を選択します。

b) ユーザーのアカウントを無効にするには、[無効化（Disable）] を選択します。



第 4 章

ドメインの管理

Security Cloud Control でエンタープライズのドメインの要求および検証できます。これは、IDプロバイダー統合ガイドための前提条件です。また、エンタープライズ管理者が要求されたドメインでユーザーのパスワードまたは MFA 設定をリセットできるようにするためにも必要です。

ドメインの要求および検証

- 作成した DNS レコードは、Security Cloud Control がドメインを検証したら削除できます。
- 現在、Security Cloud Control を使用して単一のドメインを検証できます。複数のドメインを検証する必要がある場合、Cisco Technical Assistance Center（TAC）でケースを開いてください。

始める前に

このタスクを完了するには、ドメインのレジストラサービスで DNS レコードを作成できる必要があります。

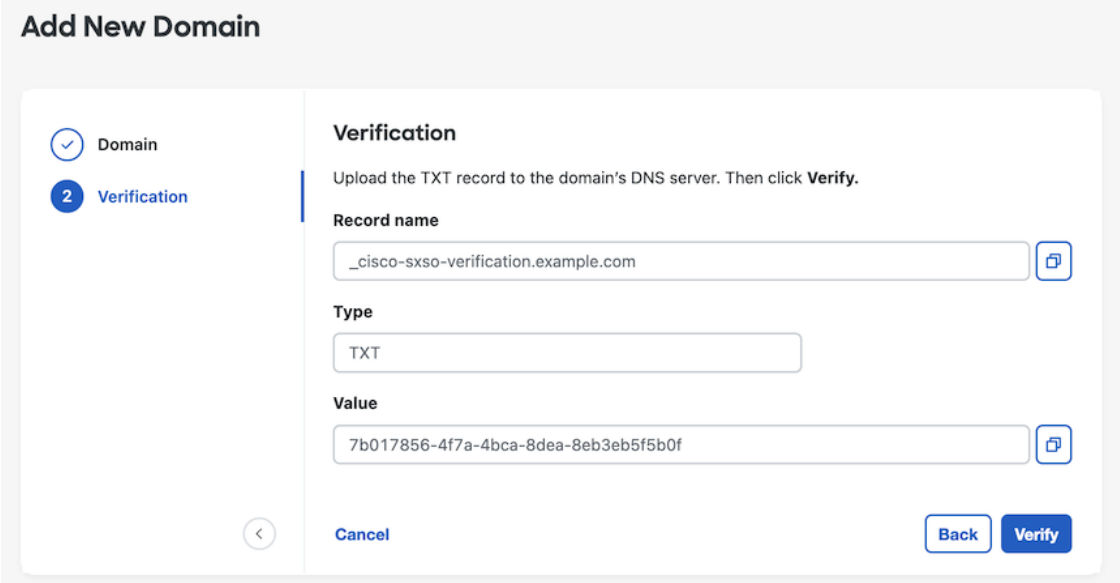
[ドメイン（Domains）] タブには、ドメインの要求および検証または検証中のドメインが一覧表示されます。ドメインを要求済みでない場合は、代わりに[+ドメインの追加（+Add Domain）] ボタンが表示されます。

ステップ 1 [ドメイン（Domains）] タブを選択します。

ステップ 2 [+ドメインの追加（+ Add Domain）] をクリックします。

ステップ 3 [新しいドメインの追加（Add New Domain）] 画面で、要求するドメイン名を入力し、[次へ（Next）] をクリックします。

[検証（Verification）] ページには、ドメインレジストラで作成する必要がある TXT レコードの**レコード名**と**値**が表示されます。



ステップ 4 新しいブラウザタブで、ドメイン名レジストラサービスにサインインします。

ステップ 5 指定された**レコード名**と Security Cloud Control から提供された**値**を使用して、新しい TXT レコードを作成します。

ステップ 6 変更を保存し、DNS レコードが反映されるまで待ちます。

ステップ 7 [新しいドメインの追加（Add New Domain）] に戻り、[検証（Verify）] をクリックします。

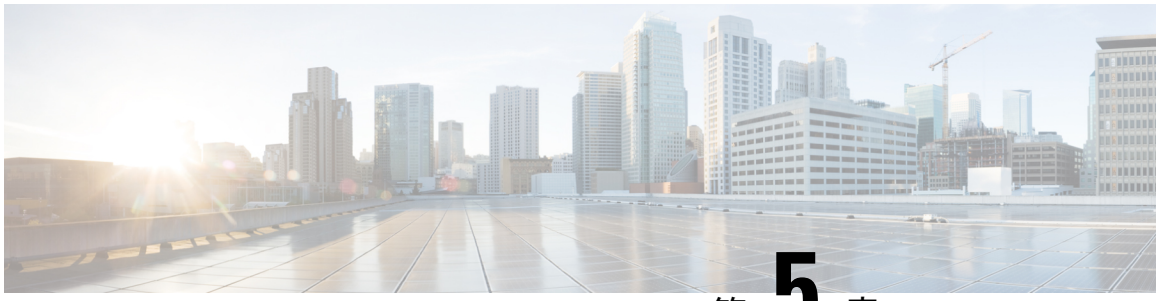
検証が失敗したかどうかを示すメッセージが表示されます。検証に失敗した場合は、次の手順を試してください。

- DNS レコードが反映されるまでしばらく待ちます。
- ドメインレジストラで作成した DNS レコードのタイプ、名前、値が Security Cloud Control で生成された値と一致することを検証します。

次のタスク

電子メールドメインを検証したら、次の操作を実行できます。

- Security Cloud Sign On と ID プロバイダー統合ガイド
- 要求されたドメイン内のユーザーのユーザーパスワードまたは MFA 設定のリセットします。



第 5 章

ID プロバイダー統合ガイド

セキュリティ アサーション マークアップ言語（SAML）を使用してアイデンティティ（ID）プロバイダーを Security Cloud Sign On と統合し、エンタープライズのユーザーに SSO を提供できます。デフォルトでは、Security Cloud Sign On はすべてのユーザーを Duo 多要素認証（MFA）に追加費用なしで登録します。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。

特定の ID サービス プロバイダーと統合する手順については、次のガイドを参照してください。

- Auth0 社
- Azure AD
- Duo
- Google ID
- Okta
- ping

（注） ID プロバイダーの統合後、ドメイン内のユーザーの認証には、シスコや Microsoft のソーシャルログインなどではなく、統合した ID プロバイダーを使用する必要があります。

前提条件

ID プロバイダーを Security Cloud Sign On と統合するには、次のものが必要です。

- ドメインの要求および検証
- ID プロバイダーの管理ポータルで SAML アプリケーションを作成および構成する機能

SAML 応答の要件

Security Cloud Sign On からの SAML 認証要求への応答として、ID プロバイダーは SAML 応答を送信します。ユーザーが正常に認証された場合、応答には `NameID` 属性とその他のユーザー属性を含む SAML アサーションが含まれます。SAML 応答は、以下で説明する特定の基準を満たす必要があります。

SHA-256 署名付き応答

ID プロバイダーからの応答の SAML アサーションには、次の属性名を含める必要があります。これらの名前は、IdP のユーザープロファイルの対応する属性にマッピングする必要があります。IdP ユーザープロファイル属性名はベンダーによって異なります。

SAML アサーション属性

ID プロバイダーからの応答の SAML アサーションには、次の属性名を含める必要があります。これらの名前は、IdP のユーザープロファイルの対応する属性にマッピングする必要があります。IdP ユーザープロファイル属性名はベンダーによって異なります。

SAML アサーション属性名	ID プロバイダーのユーザー属性
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>** 要素と一致させる必要があります（以下参照）。

<NameID> 要素フォーマット

SAML 応答の `<NameID>` 要素の値は有効な電子メールアドレスにする必要があり、アサーションの `email` 属性の値と一致させる必要があります。`<NameID>` 要素のフォーマット属性を次のいずれかに設定する必要があります。

- `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
- `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`

SAML アサーションの例

次の XML は、ID プロバイダーから Security Cloud Sign On ACL URL への SAML 応答の例です。**jsmith@example.com** は `<NameID>` 要素であり、また `email` SAML 応答属性です。

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion ID="id95383894959750298492624 25" IssueInstant="2023-08-02T01:13:04.861Z"
 Version="2.0"
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"/>
    <saml2:Subject>
        <saml2:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">jsmith@example.com</saml2:NameID>

        <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml2:SubjectConfirmationData NotOnOrAfter="2023-08-02T01:18:05.160Z"
Recipient="https://sso.security.cisco.com/sso/saml2/0oa1rs8y79aeweVg80h8"/>
        </saml2:SubjectConfirmation>
    </saml2:Subject>
    <saml2:Conditions NotBefore="2023-08-02T01:08:05.160Z"
NotOnOrAfter="2023-08-02T01:18:05.160Z">
        <saml2:AudienceRestriction>

<saml2:Audience>https://www.okta.com/saml2/service-provider/12345678890</saml2:Audience>

        </saml2:AudienceRestriction>
    </saml2:Conditions>
    <saml2:AuthnStatement AuthnInstant="2023-08-02T01:13:04.861Z">
        <saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>

        </saml2:AuthnContext>
    </saml2:AuthnStatement>
    <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">Joe
            </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">Smith
            </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">jsmith@example.com
            </saml2:AttributeValue>
        </saml2:Attribute>
    </saml2:AttributeStatement>
</saml2:Assertion>
```

ステップ1：初期設定

始める前に

まず、Secure Cloud エンタープライズの名前を指定し、無料の Duo 多要素認証（MFA）にユーザーを登録するか、独自の MFA ソリューションを使用するかを決定する必要があります。

すべての統合について、シスコのセキュリティ製品内の機密データを保護するために、セッションタイムアウトを 2 時間以下に設定して MFA を実装することを強く推奨します。

ステップ1 Security Cloud Control にサインインします。

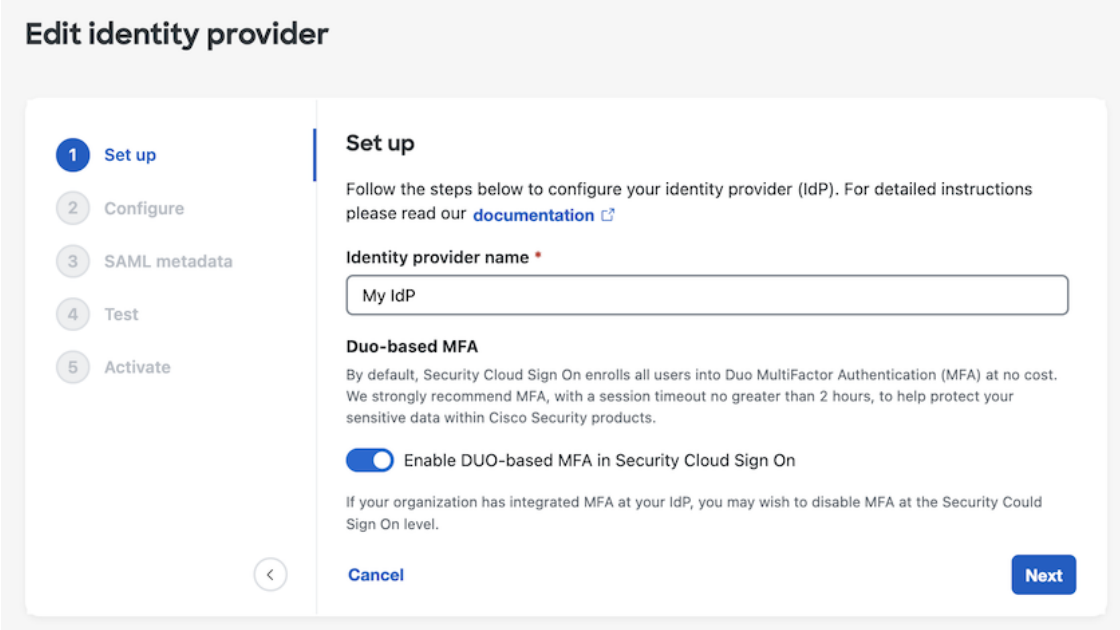
ステップ2 左側のナビゲーションから [IDプロバイダー（Identity Providers）] を選択します。

ステップ3 [+ IDプロバイダーの追加（+ Add Identity Provider）] をクリックします。

（注） ドメインをまだ要求していない場合は、代わりに [+ドメインの追加（+ Add Domain）] ボタンが表示されます。そのボタンをクリックして、ドメインの要求および検証を開始します。

ステップ4 [セットアップ（Set Up）] 画面で ID プロバイダー名を入力します。

ステップ5 必要に応じて、ドメインの要求および検証のユーザーに対して Duo MFA をオプトアウトします。



ステップ6 [次へ（Next）] をクリックして [構成（Configure）] 画面に進みます。

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

この手順では、Security Cloud Control から提供される SAML メタデータと署名証明書を使用して、ID プロバイダーの SAML アプリケーションを構成します。これには、次の事項が含まれます。

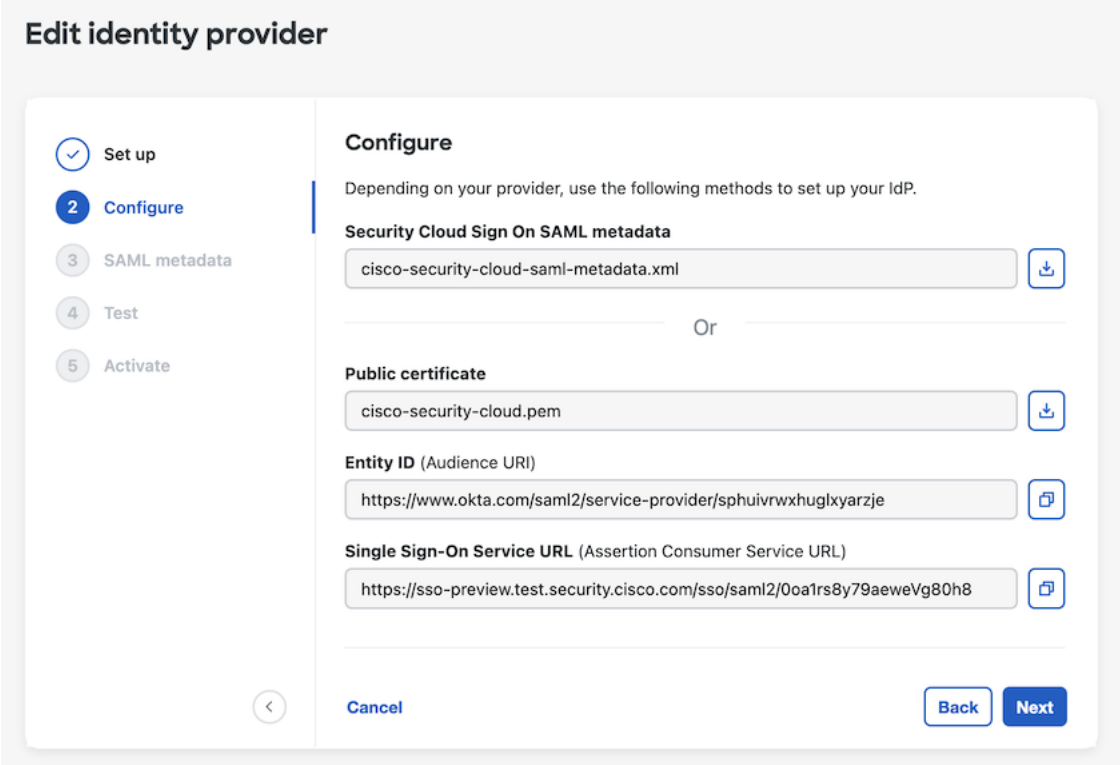
- **シングル サインオンサービス URL**：アサーション コンシューマ サービス（ACS）URL とも呼ばれます。これは、ID プロバイダーがユーザーの認証後に SAML 応答を送信する場所です。
- **エンティティ ID**：オーディエンス URI とも呼ばれます。ID プロバイダーを Security Cloud Sign On で一意に識別するための ID です。
- **署名証明書**：ID プロバイダーが認証要求で Security Cloud Sign On によって送信された署名を検証するために使用する X.509 署名証明書です。

Security Cloud は、ID プロバイダーにアップロードできる単一の SAML メタデータファイルでこの情報を提供し（サポートされている場合）、個々の値としてコピーして貼り付けることができます。市販の ID サービス プロバイダーに固有の手順については、「ID サービスプロバイダーの手順 （31 ページ）」を参照してください。

ステップ 1 ID プロバイダーにより SAML メタデータファイルがサポートされている場合は、それを [設定（Configure）] ページでダウンロードします。サポートされていない場合は、[シングルサインオンサービス（Single Sign-On Service）] と [エンティティ ID（Entity ID）] の値をコピーし、**パブリック証明書**をダウンロードします。

ステップ 2 ID プロバイダーで、Security Cloud Sign On と統合する SAML アプリケーションを開きます。

ステップ 3 プロバイダーにより SAML メタデータファイルがサポートされている場合は、それをアップロードします。サポートされていない場合は、必要な Security Cloud Sign On SAML URI をコピーして SAML アプリケーションの設定フィールドに貼り付け、Security Cloud Sign On 公開署名証明書をアップロードします。



ステップ 4 前の手順で取得した Security Cloud Sign On SAML メタデータを使用して SAML アプリケーションを設定します。これには、XML メタデータファイルをインポートするか、SSO サービス URL とエンティティ ID の値を手動で入力し、公開署名証明書をアップロードします。

ステップ 5 Security Cloud Control に戻り、[**次へ（Next）**] をクリックします。

次のタスク

次に、ID プロバイダーの SAML アプリケーションに対応するメタデータを Security Cloud Control に提供します。

ステップ 3：IdP から Security Cloud に SAML メタデータを提供する

Security Cloud Control からの SAML メタデータを使用して 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 したら、次の手順では、対応するメタデータを SAML アプリケーションから Security Cloud Controlに提供します。市販の ID サービス プロバイダーに固有の手順については、「ID サービスプロバイダーの手順 （31 ページ）」を参照してください。

始める前に

この手順を完了するには、ID プロバイダーの SAML アプリケーションに次のメタデータが必要です。

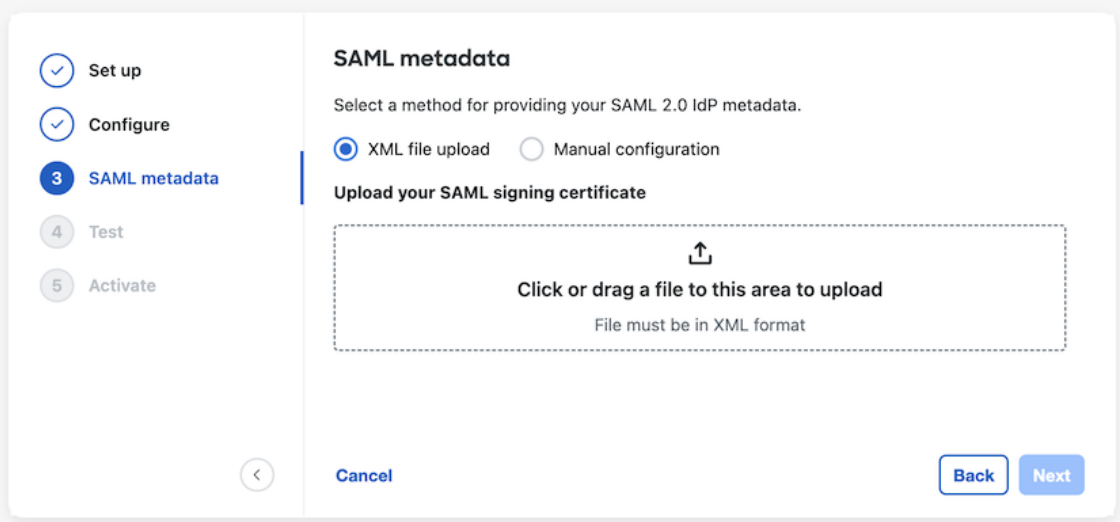
- シングルサインオンサービス URL
- エンティティ ID（オーディエンス URI）
- PEM 形式の署名証明書

ID プロバイダーに応じて、上記の情報をすべて含むメタデータ XML ファイルをアップロードするか、個々の SAML URI を手動で入力（コピーして貼り付け）して署名証明書をアップロードできます。市販の ID サービス プロバイダーに固有の手順については、「ID サービスプロバイダーの手順 （31 ページ）」を参照してください。

ステップ 1 Security Cloud Controlでブラウザタブを開きます。

ステップ 2 [SAMLメタデータ（SAML metadata）] ステップで、次のいずれかを実行します。

- IDプロバイダーからのXMLメタデータファイルがある場合は、[XMLファイルのアップロード（XML file upload）] を選択し、XML ファイルをアップロードします。
- ファイルがない場合は、[手動構成（Manual configuration）] をクリックし、シングルサインオンサービス URL のエンドポイントとエンティティ ID を入力し、ID プロバイダーから提供された公開署名証明書をアップロードします。



ステップ 3 [次へ（Next）] をクリックします。

次のタスク

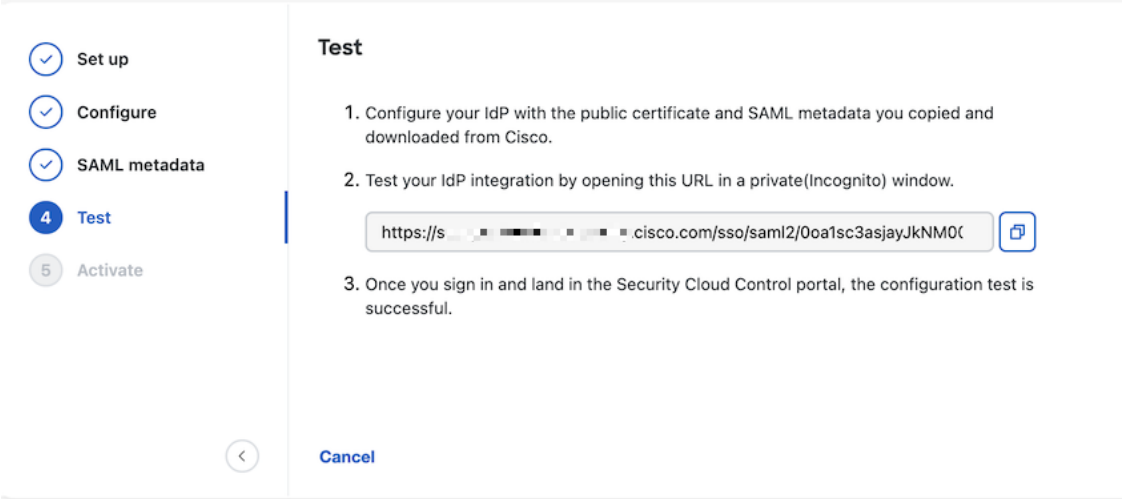
次に、Security Cloud Control から ID プロバイダーへの SSO を開始して、ステップ 4：SAML 統合のテスト。

ステップ 4：SAML 統合のテスト

SAML アプリケーションと Security Cloud Sign On の間で SAML メタデータを交換したら、統合をテストできます。Security Cloud Sign On は、ID プロバイダーの SSO URL に SAML 要求を送信します。ID プロバイダーがユーザーを正常に認証すると、ユーザーは SecureX Application Portal にリダイレクトされ、自動的にサインインします。

重要：Security Cloud Control で SAML 統合を作成したときに使用したものとは別の SSO ユーザーアカウントでテストしてください。たとえば、admin@example.com を使用して統合を作成した場合は、別の SSO ユーザー（jsmith@example.com など）でテストします。

ステップ 1 Security Cloud Control で、[テスト（Test）] ページに表示されるサインイン 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 2 ID プロバイダーにサインインします。

IdP で認証された後、SecureX Application Portal にサインインしている場合、テストは成功です。エラーが表示された場合は、「SAML エラーのトラブルシューティング （30 ページ）」を参照してください。

[次へ（Next）] をクリックして [アクティブ化（Activate）] ステップに進みます。

ステップ 5：統合のアクティブ化

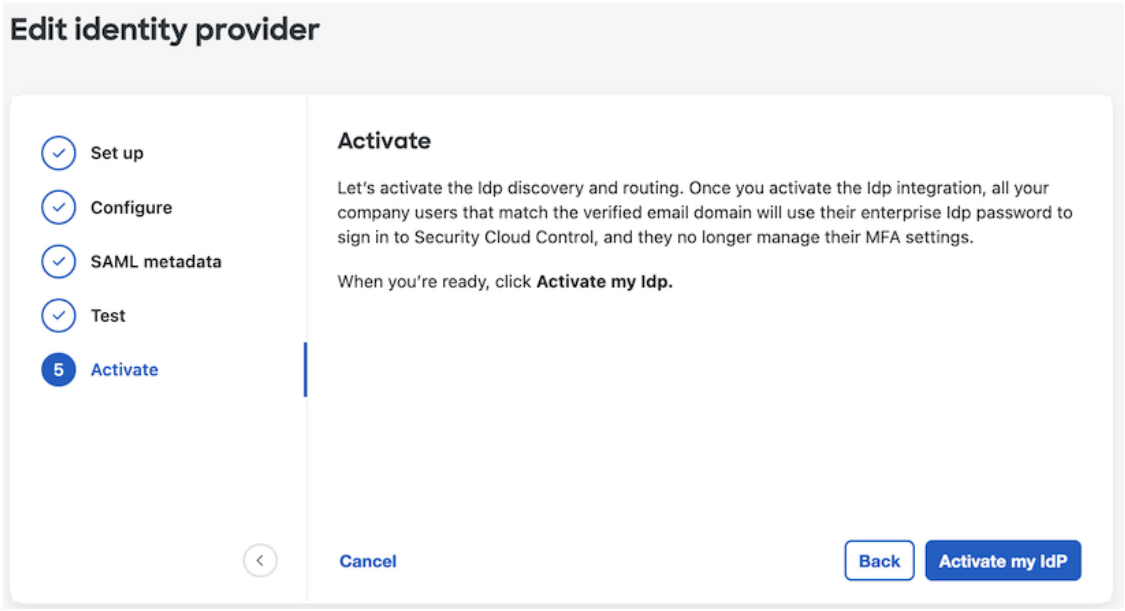
ステップ 4：SAML 統合のテストしたら、アクティブ化できます。統合をアクティブにすると、次のような影響があります。

- 検証済みドメインのユーザーは、統合した ID プロバイダーを使用して認証する**必要があります**。ユーザーがシスコや Microsoft のソーシャル サインオン オプションを使用してサインオンしようとすると、400 エラーが発生します。
- ドメインの要求および検証と一致する電子メールドメインを使用して Security Cloud Sign On にサインインするユーザーは、認証のために ID プロバイダーにリダイレクトされます。
- Duo MFA にオプトインした場合、要求されたドメインのユーザーは MFA 設定を管理できなくなります。

注意 統合をアクティブ化する前に、必ずステップ 4：SAML 統合のテスト。

統合をアクティブにすると、次のような影響があります。

ステップ 1 アクティブ化ステップで、[IdPをアクティブ化（Activate my IdP）] をクリックします。



ステップ 2 ダイアログで [アクティブ化（Activate）] をクリックしてアクションを確認します。

SAML エラーのトラブルシューティング

ステップ 4：SAML 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要求され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ドメインの要求および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。

ユーザーが ID プロバイダーを使用してサインインしていることを確認する

ユーザーは統合 ID プロバイダーを使用して認証する必要があります。ユーザーがシスコや Microsoft ソーシャル サインイン オプションを使用してサインインするか、Okta から直接サインインしようとすると、HTTP 400 エラーが返されます。

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

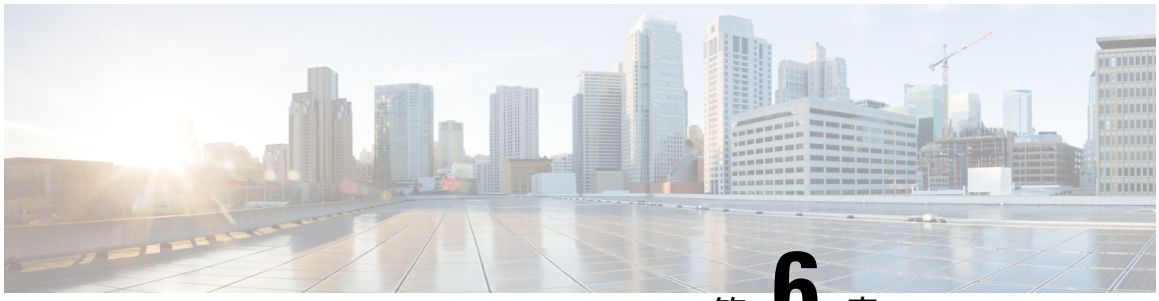
SAML 応答の `<NameId>` 要素の値は電子メールアドレスでなければなりません。電子メールアドレスは、ユーザーの SAML 属性で指定された **email** と一致する必要があります。詳細については、「SAML 応答の要件, on page 22」を参照してください。

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, on page 22」を参照してください。

IdP からの SAML 応答が SHA-256 で署名されていることを確認する

ID プロバイダーからの SAML 応答は、SHA-256 署名アルゴリズムで署名する必要があります。Security Cloud Sign On は、署名されていないアサーションまたは別のアルゴリズムで署名されたアサーションを拒否します。



第 6 章

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 （21 ページ）」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 （25 ページ）」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 （26 ページ）」について、Auth0 SAML 統合に固有の詳細を補足します。

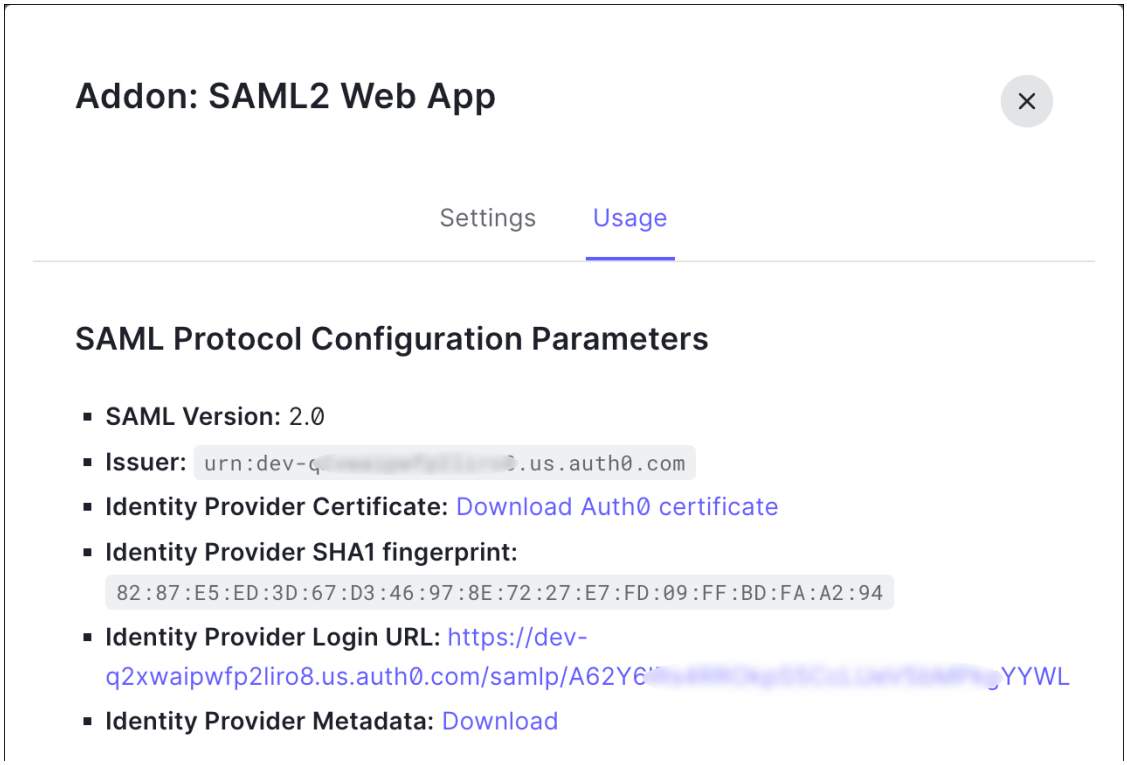
ステップ 1 Auth0 と統合するエンタープライズで Security Cloud Control にサインインします。

a) 「ステップ 1：初期設定 （24 ページ）」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 （25 ページ）」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 Cloud Control] ブラウザタブは開いたままにしておきます。

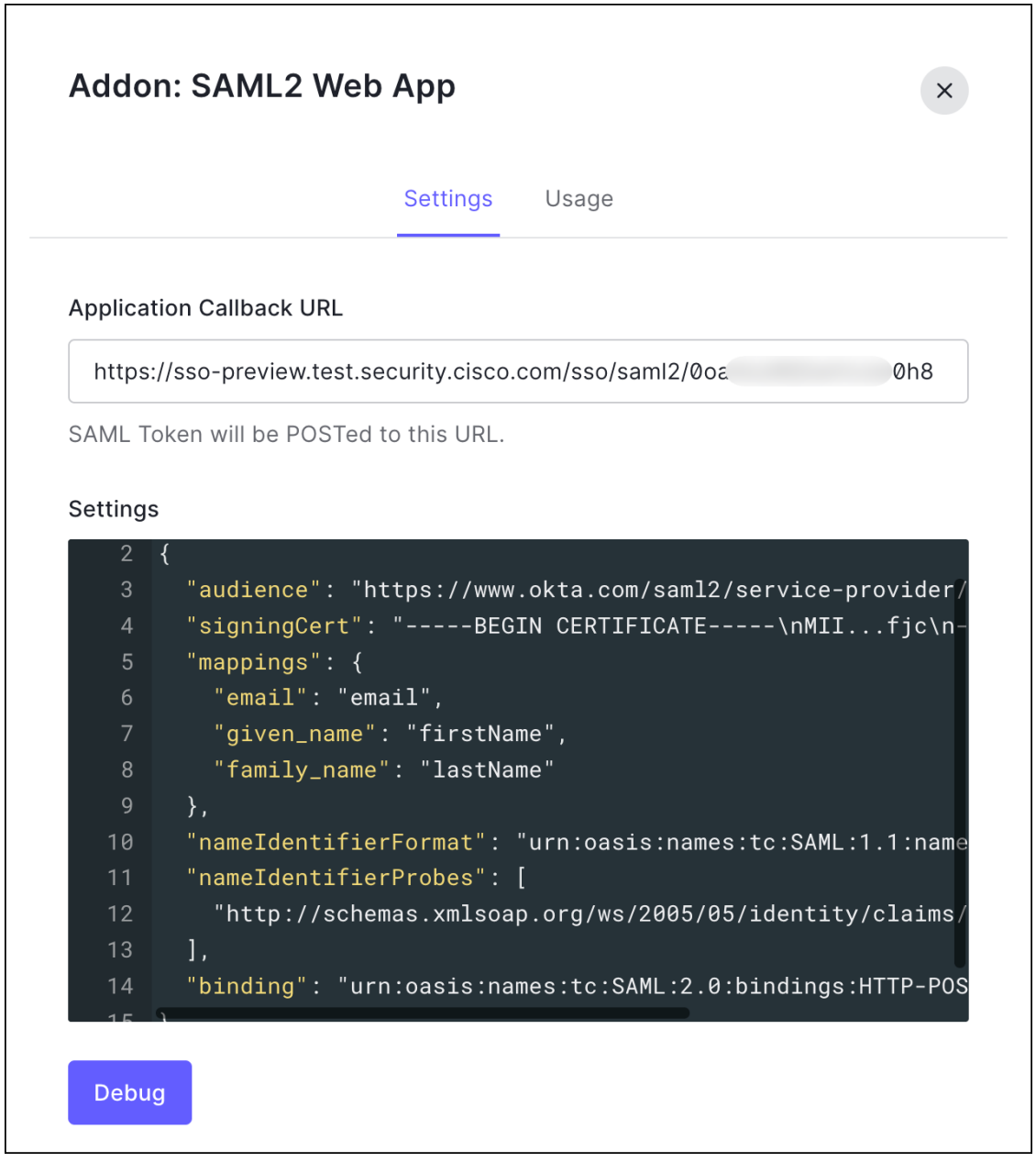
a) [アプリケーション（Applications）] メニューから [アプリケーション（Applications）] を選択します。
b) [アプリケーションの作成（Create Application）] をクリックします。
c) [名前（Name）] フィールドに「**Secure Cloud Sign On**」または他の名前を入力します。
d) アプリケーションタイプとして [通常のWebアプリケーション（Regular Web Applications）] を選択し、[作成（Create）] をクリックします。
e) [アドオン（Addons）] タブをクリックします。
f) [SAML2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

```
{
  "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 Cloud Control] 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 （26 ページ） 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 （28 ページ）」および「ステップ 5：統合のアクティブ化 （29 ページ）」の手順に従って、統合をテストしてアクティブ化します。

Azure AD の Security Cloud Sign On との統合

このガイドでは、Azure AD を Security Cloud Control 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 （21 ページ）」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 （25 ページ）」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 （26 ページ）」について、Azure AD SAML 統合に固有の詳細を補足します。

ステップ 1 Azure AD と統合するエンタープライズで Security Cloud Control にサインインします。

a) 「ステップ 1：初期設定 （24 ページ）」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 （25 ページ）」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 Cloud Control] 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 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「**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 Cloud Control 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 Cloud Control 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。

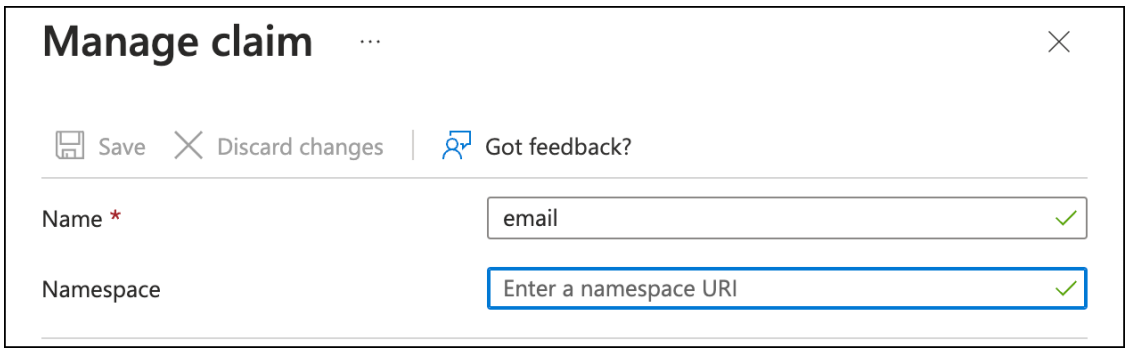
i) [属性と要求（Attributes & Claims）] パネルで、[編集（Edit）] をクリックします。

- [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、Azure AD ユーザープロパティと SAML 属性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 [Azure AD識別子（Azure AD Identifier）] の値をコピーします。

ステップ 3 [Security Cloud Control] 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 （26 ページ） 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、Azure AD から提供された [Azure AD識別子（Azure AD 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。

ステップ 4 [Security Cloud Control] 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 （28 ページ）」および「ステップ 5：統合のアクティブ化 （29 ページ）」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 （21 ページ）」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 （25 ページ）」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 （26 ページ）」について、Duo SAML 統合に固有の詳細を補足します。

ステップ 1 Duo と統合するエンタープライズで Security Cloud Control にサインインします。

a) 「ステップ 1：初期設定 （24 ページ）」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 （25 ページ）」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 Cloud Control] タブは開いたままにしておきます。

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。

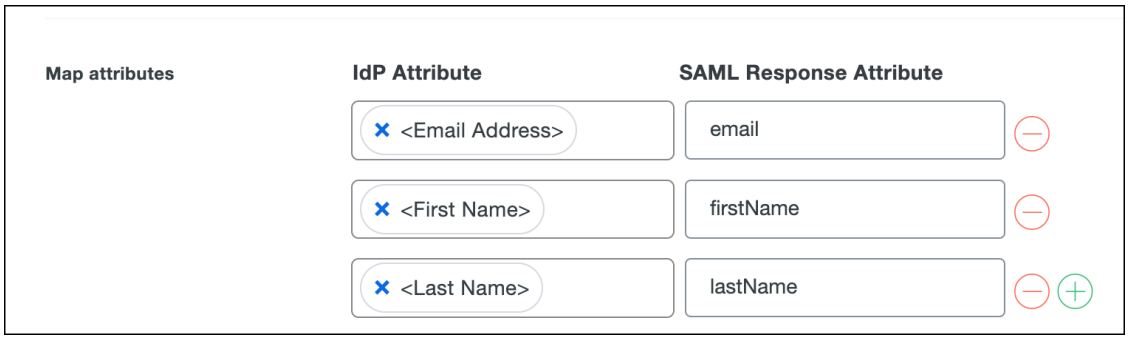
f) [シングルサインオンURL（Single Sign-On URL）] の値をコピーし、後で使用するために保存します。

g) 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（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）] セクションで、[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 Cloud Control] 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 （26 ページ） 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 （28 ページ）」および「ステップ 5：統合のアクティブ化 （29 ページ）」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 （21 ページ）」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 （25 ページ）」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 （26 ページ）」について、Google ID 統合に固有の詳細を補足します。

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

a) 「ステップ 1：初期設定 （24 ページ）」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 （25 ページ）」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 Cloud Control] タブを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] フィールドに、Security Cloud Control 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 Cloud Control 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。

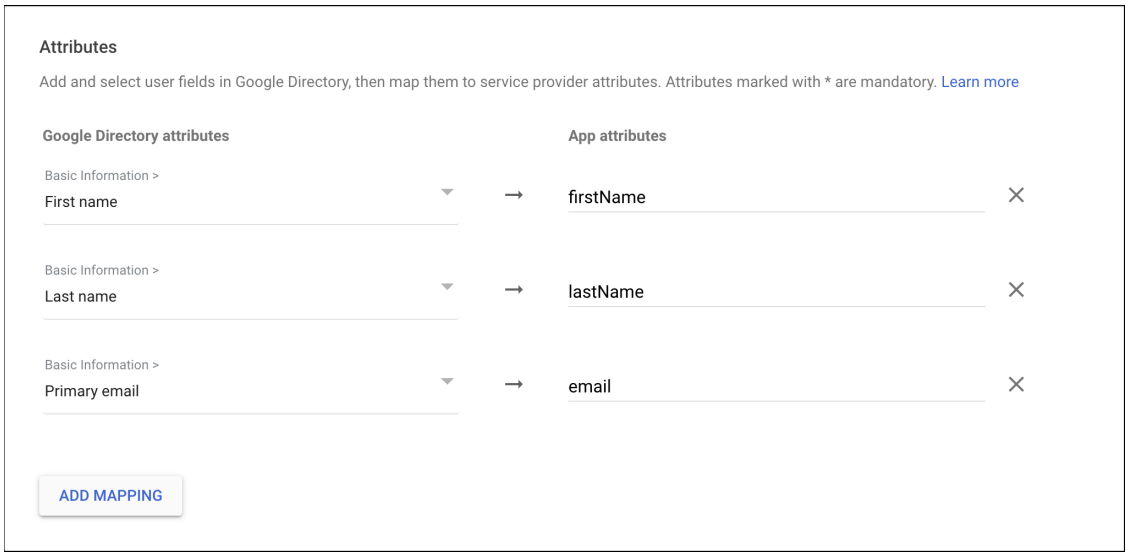
j) [名前IDの形式（Name ID Format）] で [UNSPECIFIED（UNSPECIFIED）] または [EMAIL（EMAIL）] を選択します。

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
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 Cloud Control] 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 （26 ページ） 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 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 （28 ページ）」および「ステップ 5：統合のアクティブ化 （29 ページ）」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 Cloud Control 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 （21 ページ）」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 （25 ページ）」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 （26 ページ）」について、Okta SAML 統合に固有の詳細を補足します。

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

a) 「ステップ 1：初期設定 （24 ページ）」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 （25 ページ）」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 Cloud Control] 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）] 画面に進みます。

f) [シングルサインオンURL（Single sign-on URL）] フィールドに、Security Cloud Control 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 Cloud Control 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.email

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 Cloud Control 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 Cloud Control に提供します。

ステップ 3 [Security Cloud Control] 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 （26 ページ） 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 （28 ページ）」および「ステップ 5：統合のアクティブ化 （29 ページ）」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、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 （21 ページ）」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 （25 ページ）」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 （26 ページ）」について、Google ID 統合に固有の詳細を補足します。

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

a) 「ステップ 1：初期設定 （24 ページ）」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 （25 ページ）」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 Cloud Control] 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。

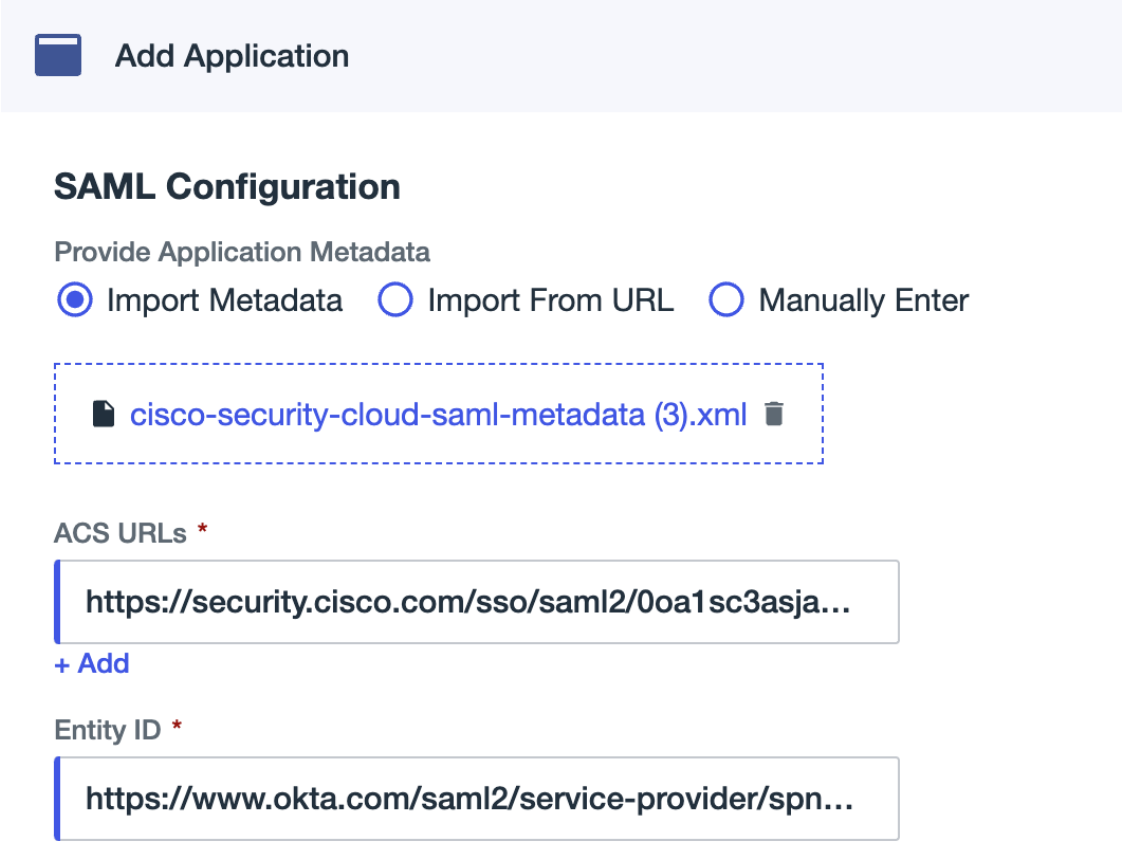
c) [アプリケーション名（Application Name）] フィールドに「**`Secure Cloud Sign On`**」または他の名前を入力します。

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 Cloud Control 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 Cloud Control 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。

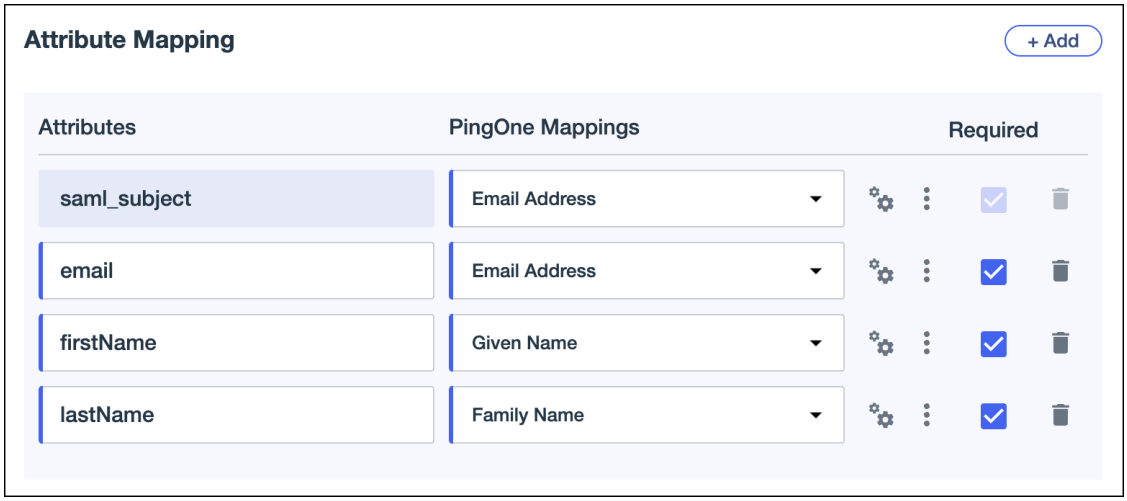
l) [編集（Edit）]（鉛筆アイコン）をクリックします。

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	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 3 [Security Cloud Control] 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 （26 ページ） 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 （28 ページ）」および「ステップ 5：統合のアクティブ化 （29 ページ）」 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。