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。

- 検証済みの電子メールドメイン
- 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。

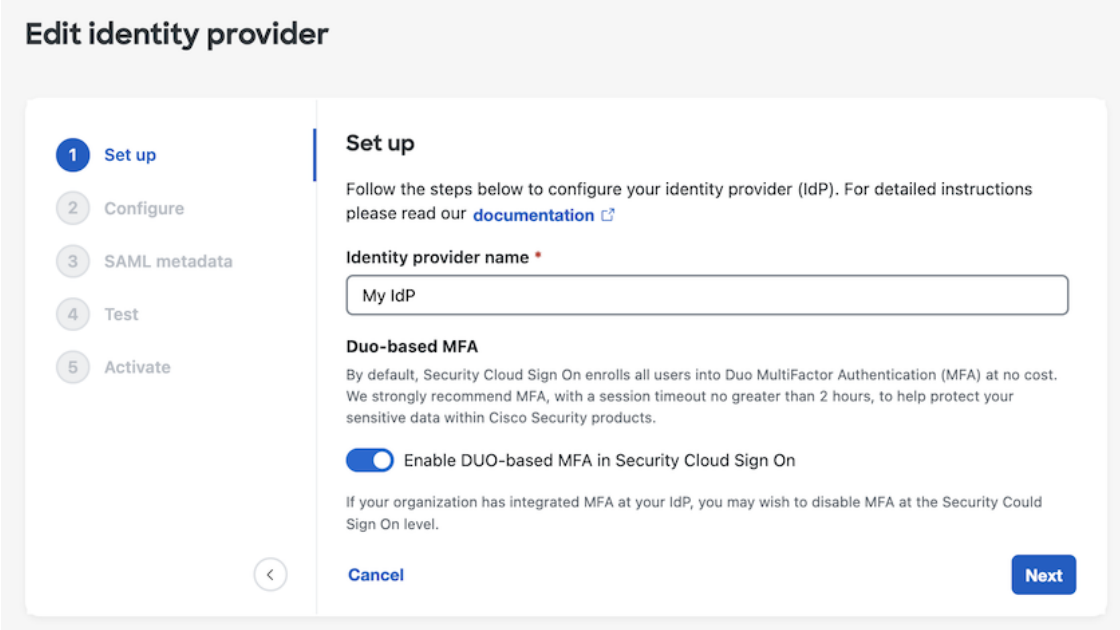
ステップ2 左側のナビゲーションから [IDプロバイダー（Identity Providers）] を選択します。

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、要求されたドメイン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。

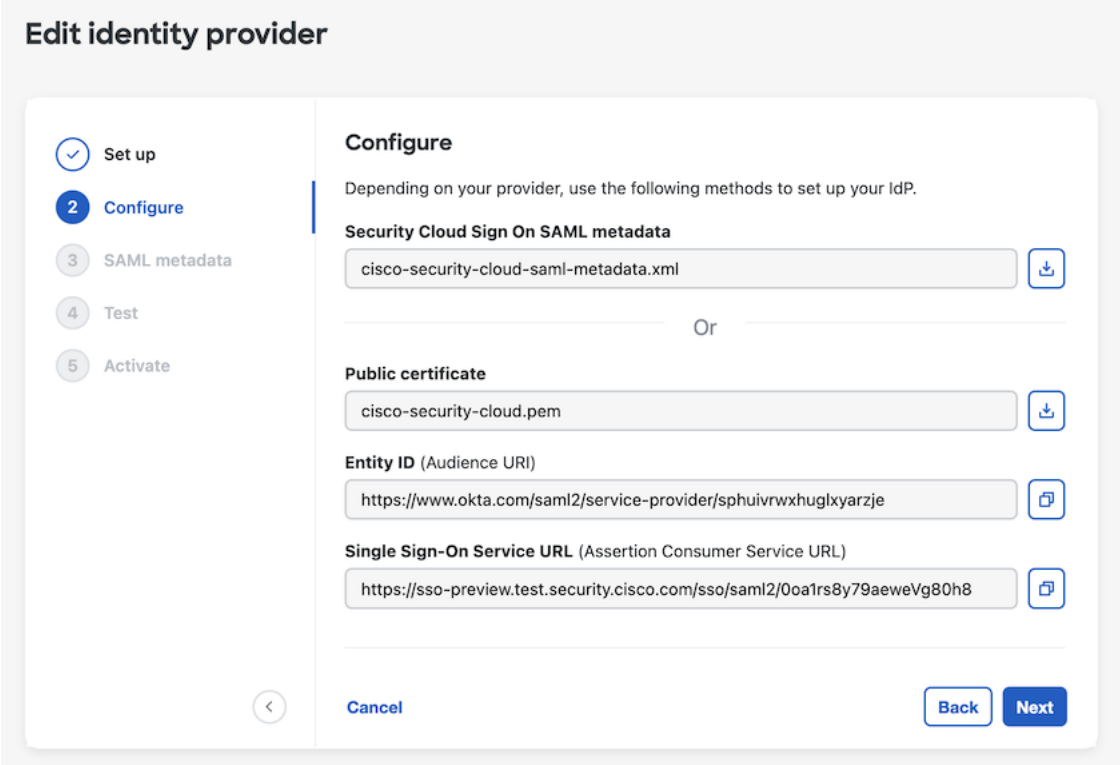
- **シングル サインオンサービス URL**：アサーション コンシューマ サービス（ACS）URL とも呼ばれます。これは、ID プロバイダーがユーザーの認証後に SAML 応答を送信する場所です。
- **エンティティ ID**：オーディエンス URI とも呼ばれます。ID プロバイダーを Security Cloud Sign On で一意に識別するための ID です。
- **署名証明書**：ID プロバイダーが認証要求で Security Cloud Sign On によって送信された署名を検証するために使用する X.509 署名証明書です。

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」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」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。

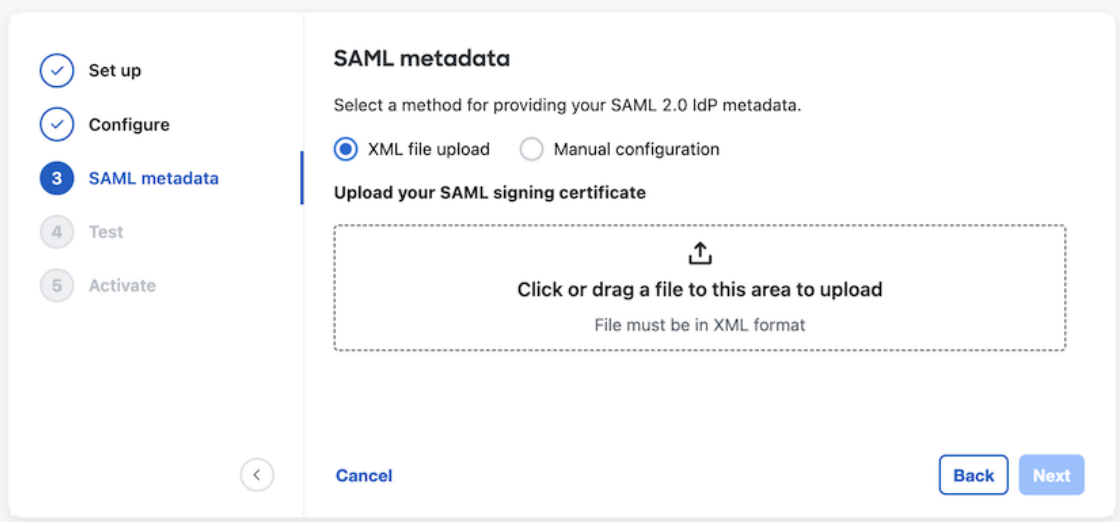
- シングルサインオンサービス URL
- エンティティ ID（オーディエンス URI）
- PEM 形式の署名証明書

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」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

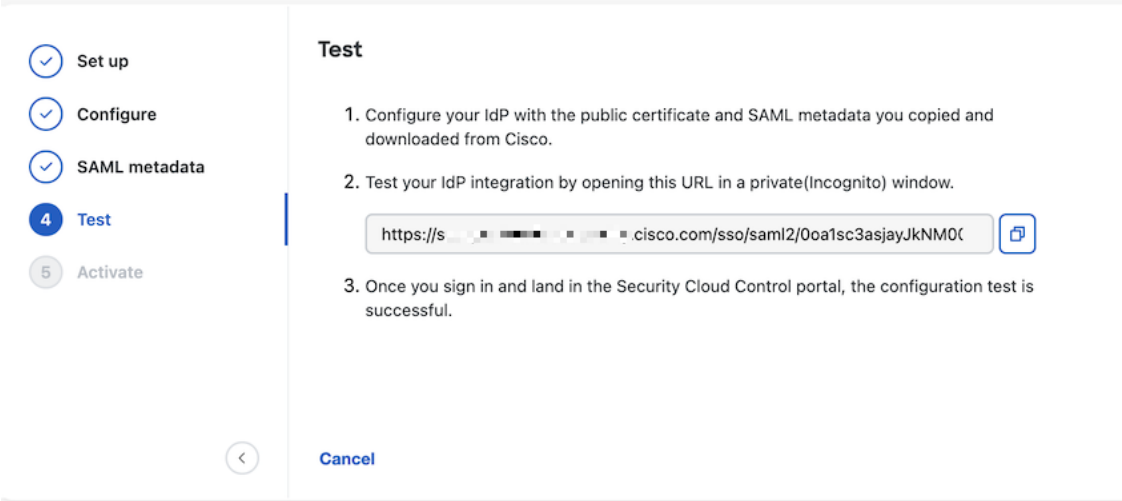
次に、Security Cloud Control から ID プロバイダーへの SSO を開始して、ステップ 4：SAML 統合のテスト。

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 （10 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

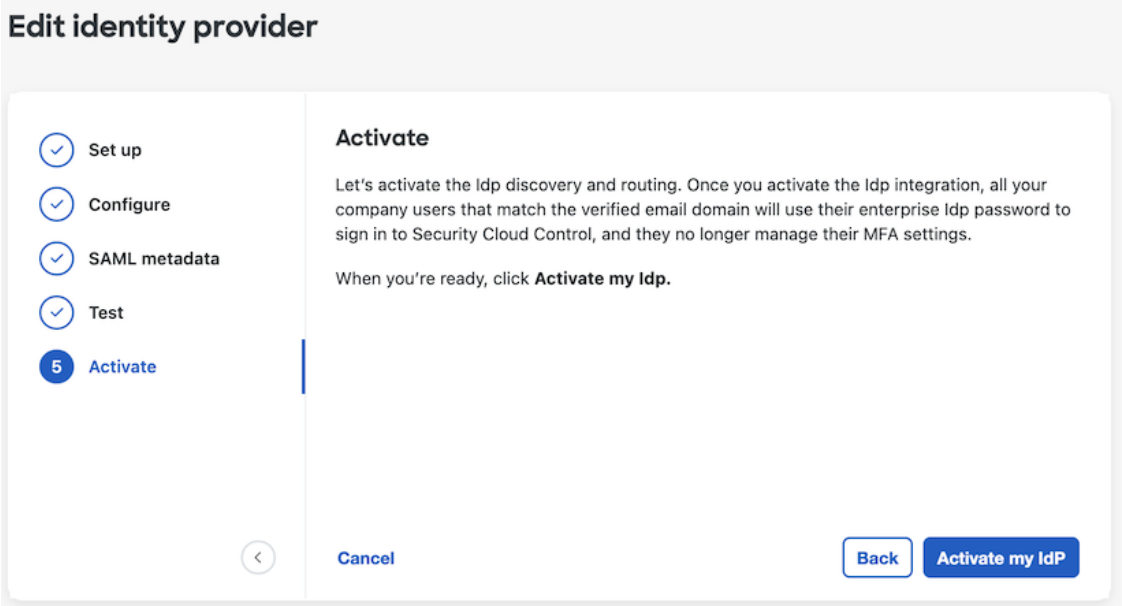
ステップ 4：SAML 統合のテストしたら、アクティブ化できます。統合をアクティブにすると、次のような影響があります。

- 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。
- 要求されたドメイン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要求されたドメイン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 2」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 2」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。

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。