



## ID プロバイダーの統合

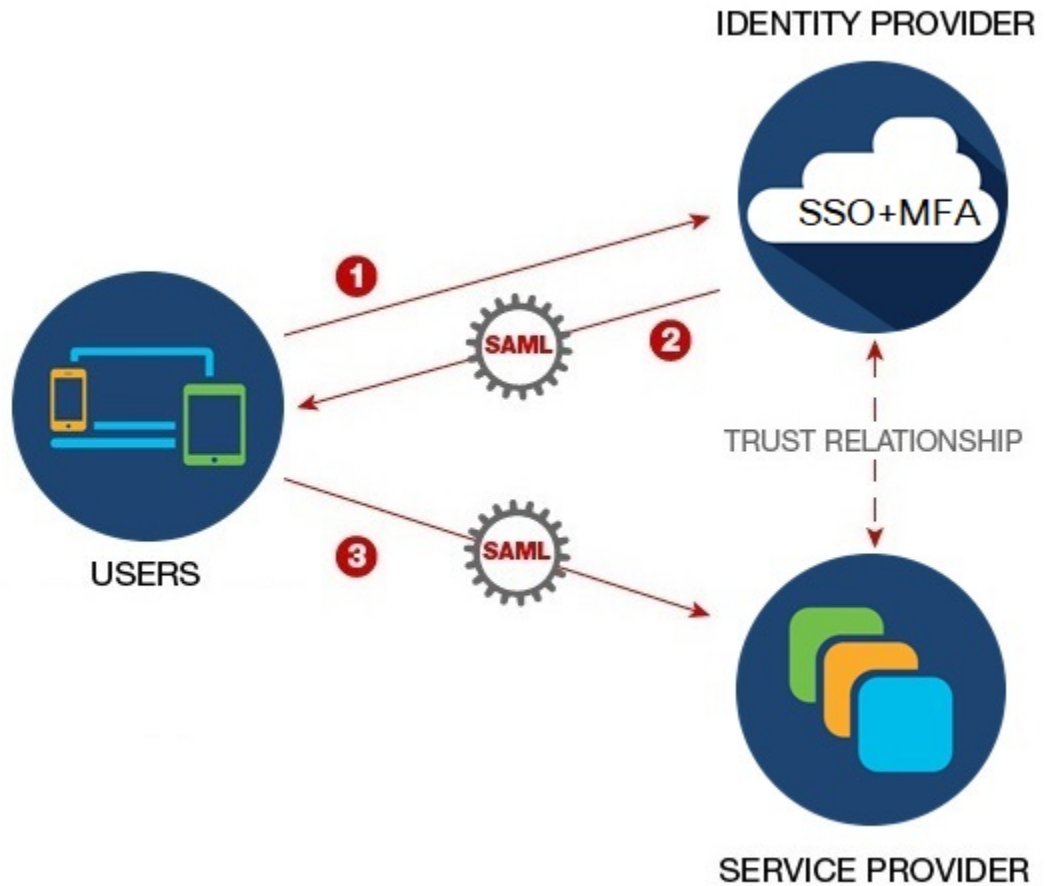
---

- [概要 \(1 ページ\)](#)
- [エンタープライズ設定ウィザード \(2 ページ\)](#)
- [ステップ 1 : エンタープライズの作成 \(3 ページ\)](#)
- [ステップ 2 : 電子メールアドレスの申請と検証 \(4 ページ\)](#)
- [ステップ 3 : SAML メタデータの交換 \(5 ページ\)](#)
- [ステップ 4 : SSO 統合のテスト \(7 ページ\)](#)
- [ステップ 5 : IdP 統合のアクティブ化 \(8 ページ\)](#)

### 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。

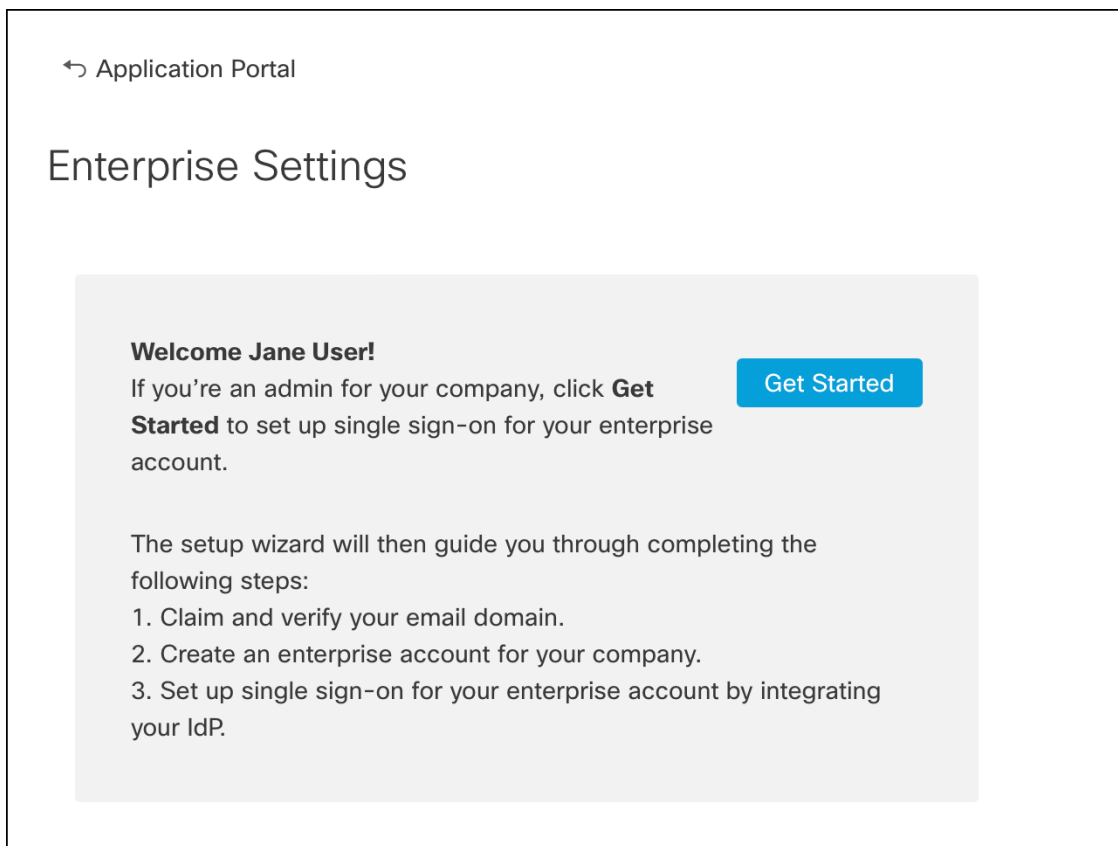


デフォルトでは、Security Cloud Sign On はすべての IdP のユーザーを [Duo 多要素認証 \(MFA\)](#) に無料で登録します。組織ですでに MFA が IdP と統合されている場合、統合プロセス中に必要に応じて Duo ベースの MFA を無効にすることができます。

## 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ィー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つの電子メールアドレスを申請し、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
- 複数の電子メールアドレスを申請する必要がある
- **ステップ2: 電子メールアドレスの申請と検証**の後に組織名や電子メールアドレスを変更する



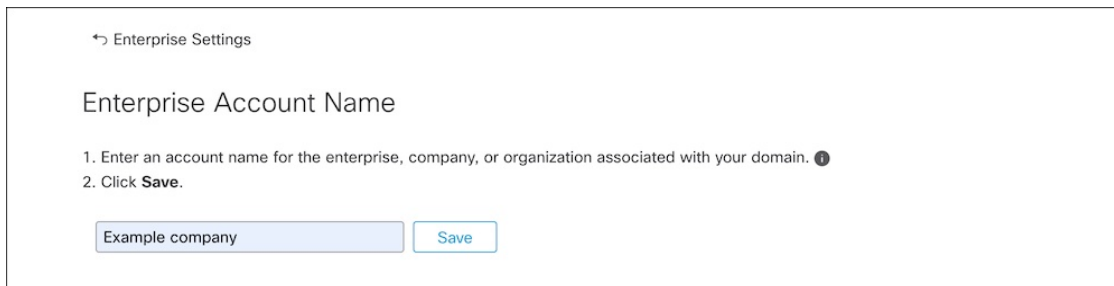
(注) エンタープライズ設定ウィザードで作成されていない既存のIdP統合がある場合、その統合をウィザードを使用して変更することはできません。詳細については、[既存のIdP統合を使用しているお客様](#)を参照してください。

## 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 2: 電子メールアドレスの申請と検証

- 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。



↩ Enterprise Settings

Enterprise Account Name

1. Enter an account name for the enterprise, company, or organization associated with your domain. ①

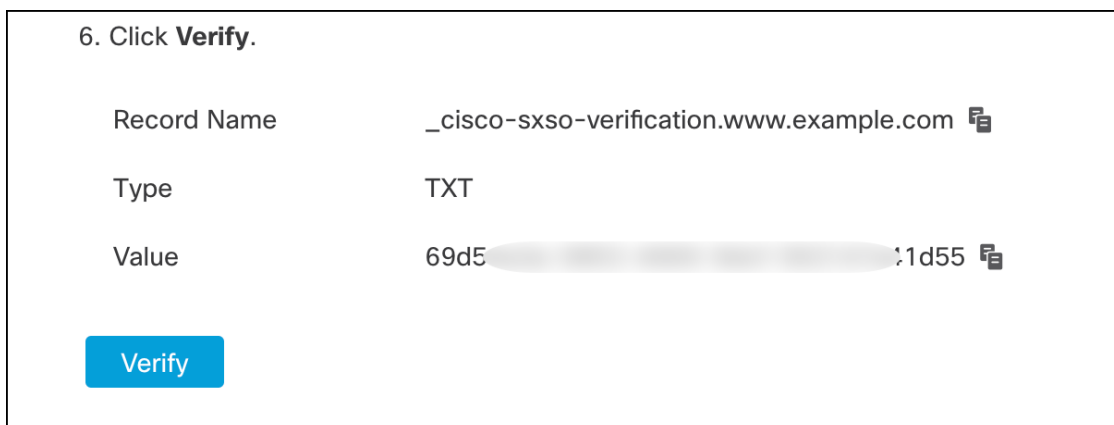
2. Click **Save**.

Example company Save

## ステップ 2: 電子メールアドレスの申請と検証

次に、エンタープライズの電子メールアドレス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。



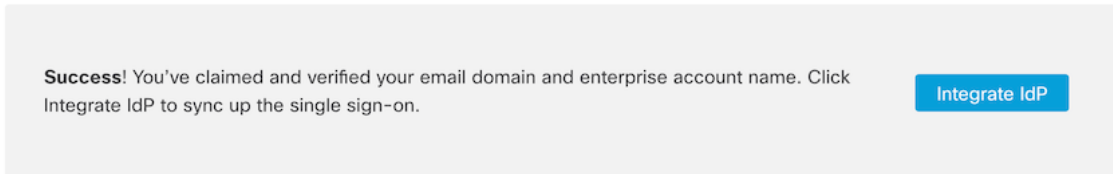
6. Click **Verify**.

Record Name	_cisco-sxso-verification.www.example.com
Type	TXT
Value	69d5...:1d55

Verify

- 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 [SAML 統合](#) 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 : 電子メールアドレスの申請と検証](#) 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 3 : SAML メタデータの交換

### Integrate Identity Provider

1 Set Up ————— 2 Download ————— 3 Configure —————

#### Set Up

Identity Provider (IdP) Name

Single Sign-On Service URL (Assertion Consumer Service URL) ⓘ

Entity ID (Audience URI) ⓘ

SAML Signing Certificate ⓘ  [Add File](#)  
File must be in PEM format

*By default, SecureX Sign-On enrolls all users into Duo MultiFactor Authentication (MFA) at no cost. We strongly recommend MFA, with a session timeout no greater than 2 hours, to help protect your sensitive data within Cisco Security products.*

Do you wish to keep the Duo-based MFA enabled in SecureX Sign-On?  Yes  No  
If your organization has integrated MFA at your IdP, you may wish to disable MFA at the SecureX Sign-On level.

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。

### Integrate Identity Provider

✓ Set Up ————— 2 Download ————— 3 Configure ————— 4 Activate

#### Download

Depending on your provider, use the following information to set up your Identity Provider (IdP).

Single Sign-On Service URL (ACS URL)  [📄](#)

Entity ID (Audience URI)  [📄](#)

SAML Signing Certificate  [Download](#)

SecureX Sign-On SAML Metadata  [Download](#)

ステップ 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 (Auth0 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アドレスは、前に申請した [ステップ 2 : 電子メールアドレスの申請と検証](#) 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。

Configure

1. Configure your IdP with the public certificate and SAML metadata you copied and downloaded from Cisco.
2. Test your IdP integration by opening this URL in a private (incognito) window.  

<https://sso.security.cisco.com/sso/saml2/Ooa...>
3. Once you sign in and land in the SecureX application portal, the configuration test is successful.

**ステップ 3** ID プロバイダーにサインインします。

## ステップ 5 : IdP 統合のアクティブ化

- サインインに使用する電子メールアドレスは、前に申請した[ステップ 2 : 電子メールアドレスの申請と検証](#)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。

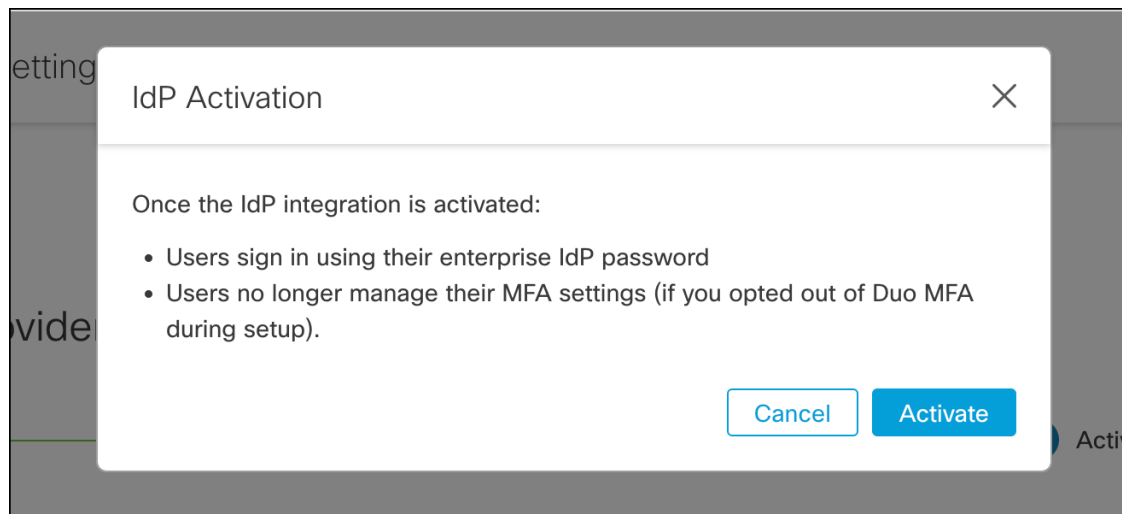
SecureX アプリケーションポータルが表示されれば、構成のテストは成功です。SSO プロセスでエラーが発生する場合は、[トラブルシューティング](#)を参照してください。

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なら、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。





## 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。