



ADFS

- [概要 \(1 ページ\)](#)
- [使用する前に \(1 ページ\)](#)

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](#) と [ステップ 2 : 電子メールドメインの申請と検証](#) 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** の画面が表示されます。

a)

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。