CRESに対するMicrosoft Entra ID SSO外部認証の設定

内容

[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[背景説明](#)

[設定](#)

- [MicrosoftエントリID](#)
- [Cisco Eメール暗号化サービス](#)

[確認](#)

[トラブルシュート](#)

はじめに

このドキュメントでは、Cisco Secure Email Encryption Service(SEES)への認証用にMicrosoft Entry IDシングルサインオンを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Secure Email Encryption Service（登録済みエンベロープ）
- MicrosoftエントリID
- PEM形式の自己署名またはCA署名（オプション）X.509 SSL証明書

使用するコンポーネント

- Secure Email Encryption Service（登録済みエンベロープ）管理者アクセス
- Microsoft Entra ID管理センターの管理者アクセス

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

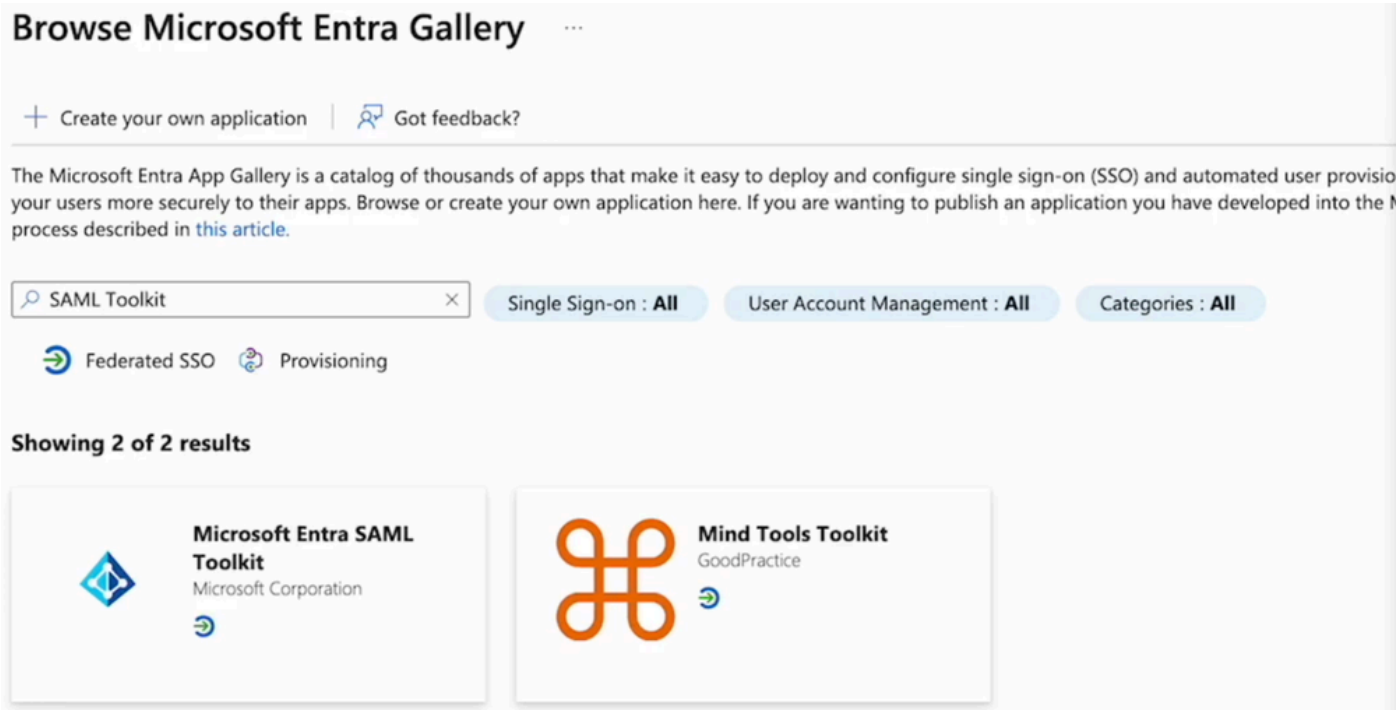
背景説明

- 登録済みエンベロープにより、SAMLを使用するエンドユーザのSSOログインが可能になります。
- Microsoft Entra SSOは、シングルサインオンを使用して、どこからでもSoftware as a Service(SaaS)アプリケーション、クラウドアプリケーション、またはオンプレミスアプリケーションへのアクセスを許可および制御します。
- 登録済みエンベロープは、パスワードのみの認証は安全ではなく、推奨もされないため、多要素認証を含む認証方法を使用してMicrosoft Entraに接続する管理対象IDアプリケーションとして設定できます。
- SAMLはXMLベースのオープンな標準データ形式であり、管理者は、アプリケーションの1つにサインインした後、定義された一連のアプリケーションにシームレスにアクセスできます。
- SAMLの詳細については、「SAMLとは」を参照してください。

設定

MicrosoftエントリID

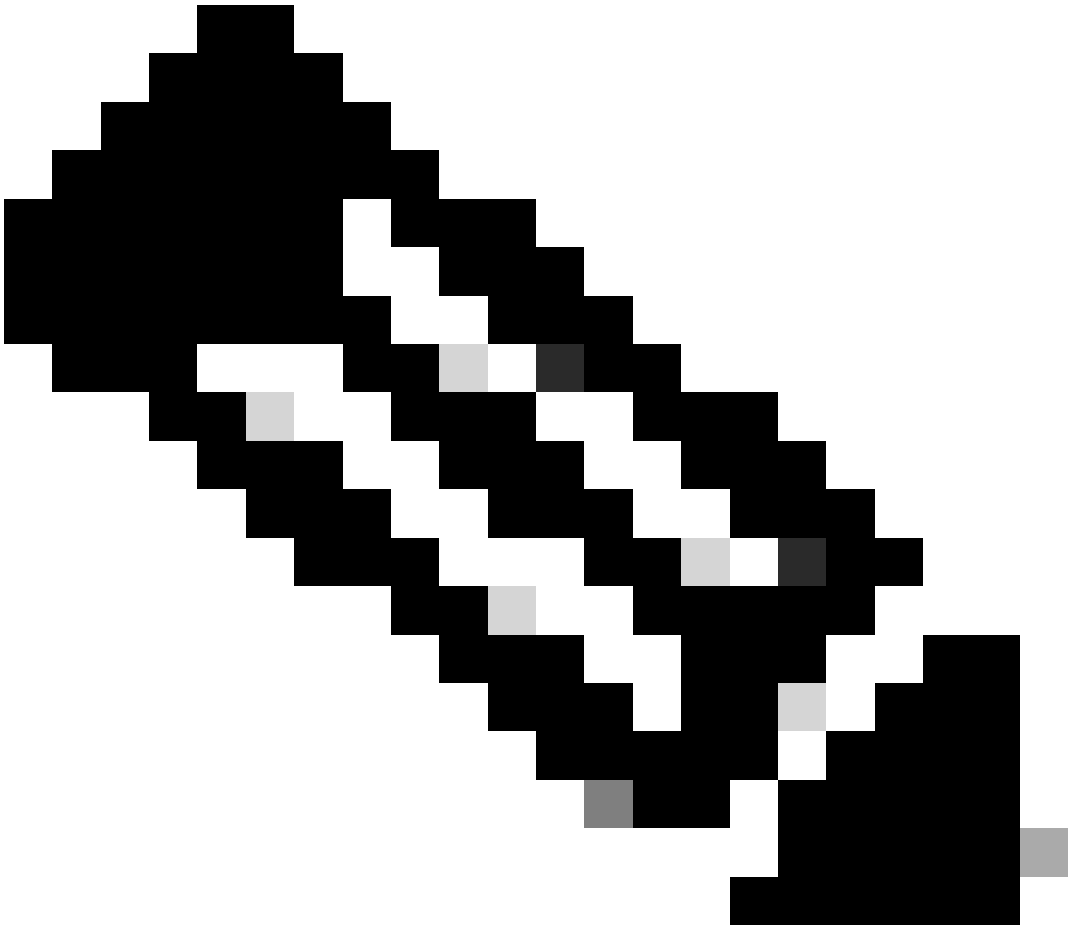
1. Microsoft Entra ID admin centerに移動し、Addボタンをクリックします。図に示すように、Enterprise Applicationを選択し、Microsoft Entra SAML Toolkitを検索します。



Microsoft Entra Galleryの参照

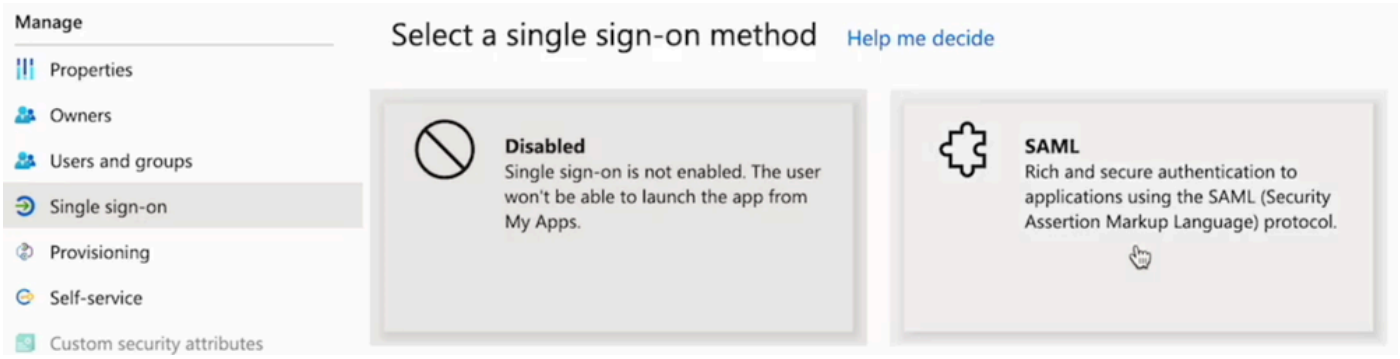
2. 意味のある値で名前を付けて、Createをクリックします。たとえば、CRESシングルサインオ

ンなどです。



注：すべてのユーザがCRESポータルにサインインできるようにするには、CRES Sign On (SAML toolkit) プロパティでRequired Assignmentを手動で無効にし、Assignment RequiredにはNoを選択する必要があります。

3.左側のパネルに移動し、Manageセクションの下で、Single sign-onをクリックして、SAMLを選択します。



4. Basic SAML Configurationパネルで**Edit**をクリックし、次のように属性を入力します。

- 識別子（エンティティID）:https://res.cisco.com/
- 返信URL（アサーションコンシューマサービスURL）:https://res.cisco.com/websafe/ssourl
- サインオンURL:https://res.cisco.com/websafe/ssourl
- [Save] をクリックします。

5.「属性および要求」パネルで、「編集」をクリックします。

[必須の要求]で、一意のユーザー識別子（名前ID）要求をクリックして編集します。

- 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であることを前提としています。そうでない場合は、Sourceをuser.primaryauthoritativeemailに設定します。
- Additional ClaimsパネルでEditをクリックし、Microsoft Entra IDユーザプロパティとSAML属性間のマッピングを作成します。

[名前(Name)]	名前空間	ソース属性
電子メールアドレス	値なし	ユーザー.userprincipalname
名	値なし	ユーザー.givenname
姓	値なし	ユーザ。姓

次に示すように、各クレームのNamespaceフィールドを必ずクリアしてください。

6. 属性セクションと要求セクションに入力すると、最後のセクションのSAML署名証明書にデータが入力されます。CRESポータルで必要に応じて、次の値を保存します。

- ログインURLを保存します。

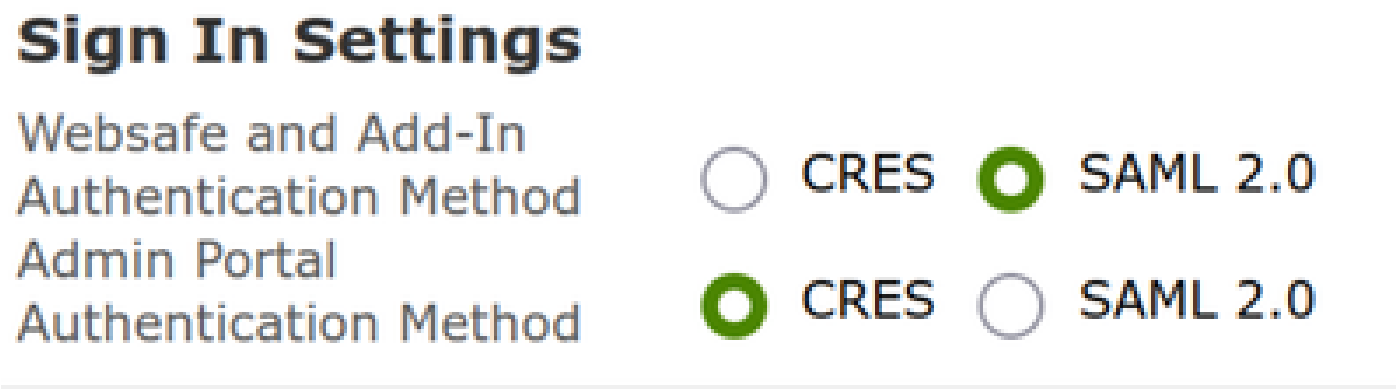
- Certificate (Base64) Downloadリンクを選択します。

Cisco Eメール暗号化サービス

1. 管理者としてSecure Email Encryption Service(SEES)組織ポータルにログインします。

2. 「アカウント」タブで、「アカウントの管理」タブを選択し、「アカウント番号」をクリックします。

3. Detailsタブで、Authentication Methodまでスクロールし、SAML 2.0を選択します。



4. – 属性を次のように入力します。

- SSO代替電子メール属性名：emailaddress
- SSOサービスプロバイダーエンティティID*:https://res.cisco.com/
- SSOカスタマーサービスURL*:このリンクは、
- SSOログアウトURL:空白のままにします

5.- Activate SAMLをクリックします。

確認

ログインに成功した後、SAML認証が有効になったことを確認する新しいウィンドウが表示されます。 [Next] をクリックします。 IDプロバイダーのログインページにリダイレクトされます。 SSOクレデンシャルを使用してログインします。 ログインに成功したら、ウィンドウを閉じることができます。[Save] をクリックします。

トラブルシュート

ウィンドウでIDプロバイダーのログインページにリダイレクトされなかった場合は、エラーを示すトレースバックが返されます。 属性と要求を確認し、CRES認証方式セクションと同じ名前で設定されていることを確認します。 SAMLログインで使用するユーザ電子メールアドレスは、CRESの電子メールアドレスと一致している必要があります。 エイリアスは使用しないでください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。