DMP用のMicrosoft Entry ID SSO外部認証の設定

内容

はじめに

このドキュメントでは、Cisco Domain Protection(CDNS)ポータルで認証するために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推奨されます。

- Ciscoドメイン保護
- 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

- Cisco Domain Protection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

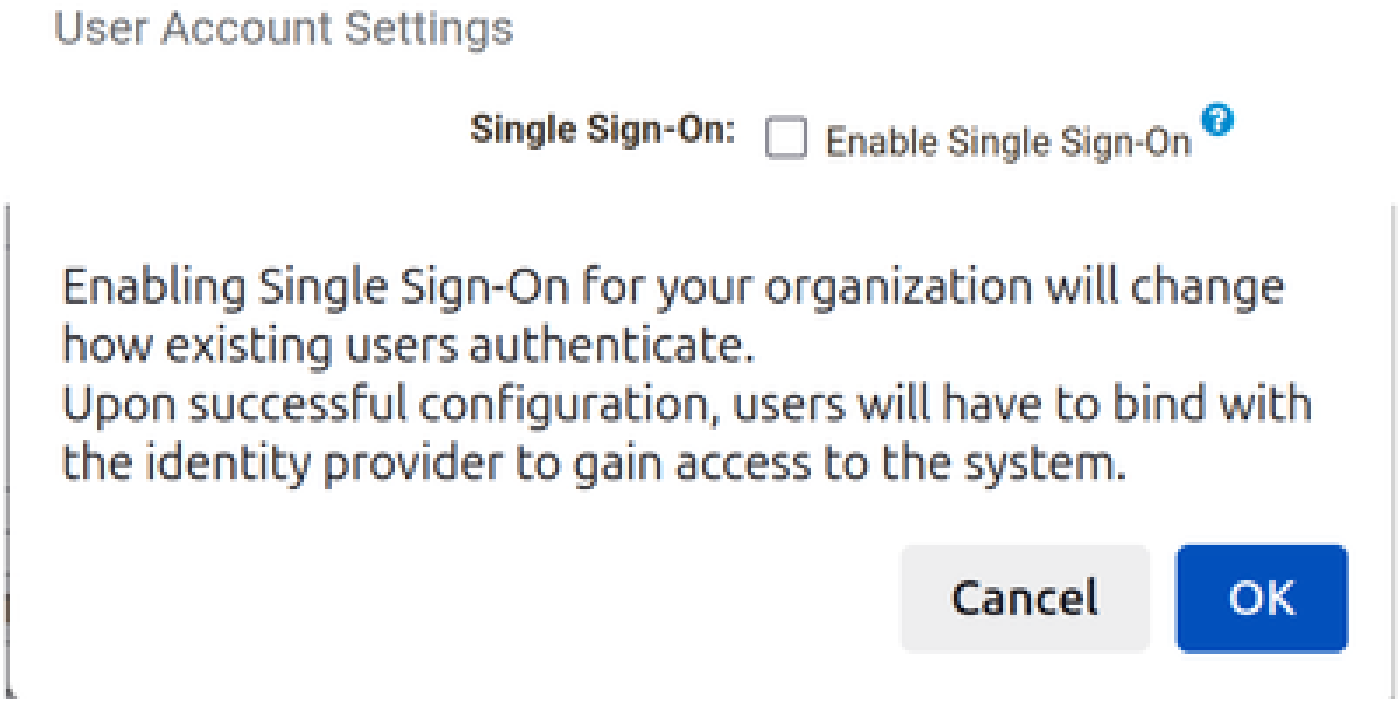
- Cisco Domain Protectionでは、SAML 2.0プロトコルを介してエンドユーザのSSOログインが可能です。
- Microsoft Entra SSOは、シングルサインオンを使用して、どこからでもSoftware as a Service(SaaS)アプリケーション、クラウドアプリケーション、またはオンプレミスアプリケーションへのアクセスを許可および制御します。
- Cisco Domain Protectionは、パスワードのみの認証は安全ではなく推奨もされないため、多要素認証を含む認証方式を使用してMicrosoft Entraに接続する、管理対象のアイデンティティ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

Cisco Domain Protection（パート1）

1. Cisco Domain Protection管理ポータルにログインし、Admin > Organizationに移動します。 図に示すように、組織の詳細の編集ボタンをクリックします。

2. [ユーザーアカウント設定]セクションに移動し、[シングルサインオンを有効にする]チェックボックスをオンにします。次の図に示すようなメッセージが表示されます。

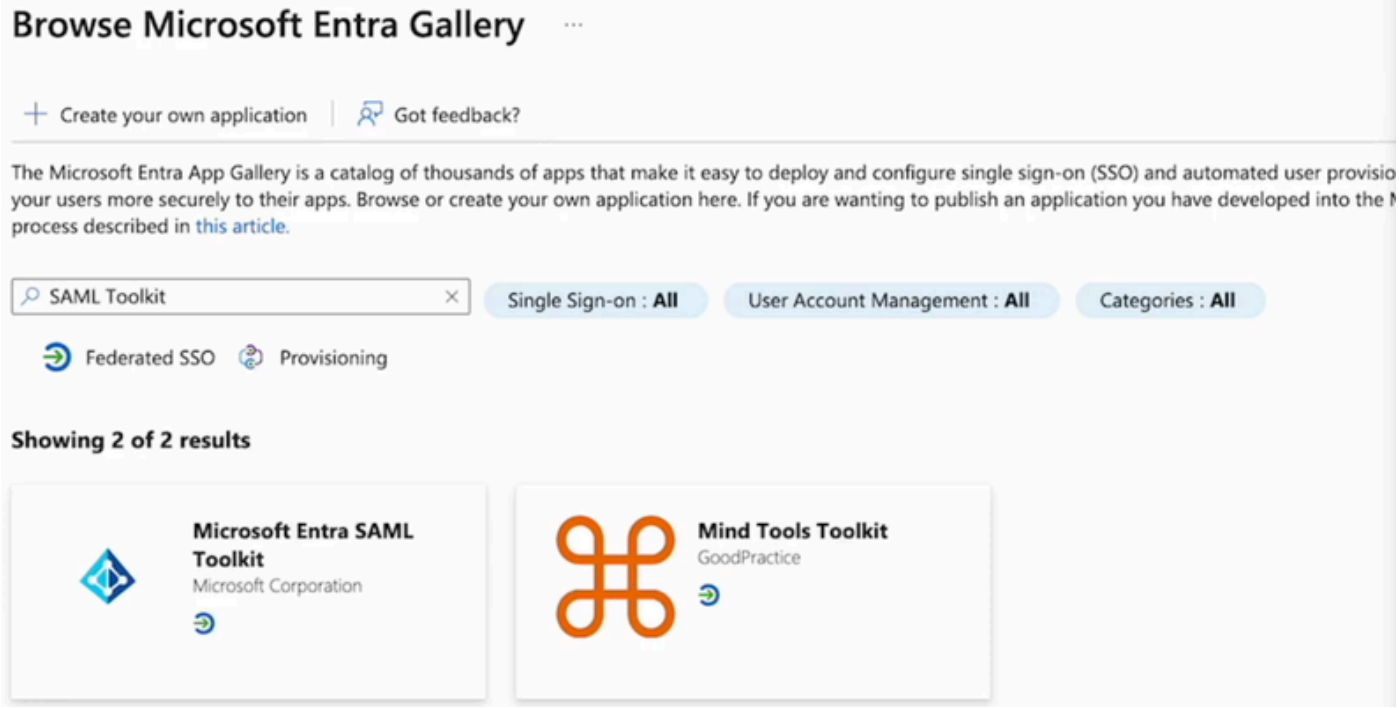


3. OKボタンをクリックして、Entity ID(AID)およびAssertion Consumer Service(ACS)URLパラメータをコピーします。これらのパラメータは、Microsoft Entry ID Basic SAML認証で使用する必要があります。Name Identifier Format、SAML 2.0 Endpoint、およびPublic Certificateの各パラメータの設定については、後で戻ってください。

- エンティティID:dmp.cisco.com
- アサーションコンシューマサービスURL:https://<dmp_id>.dmp.cisco.com/auth/saml/callback

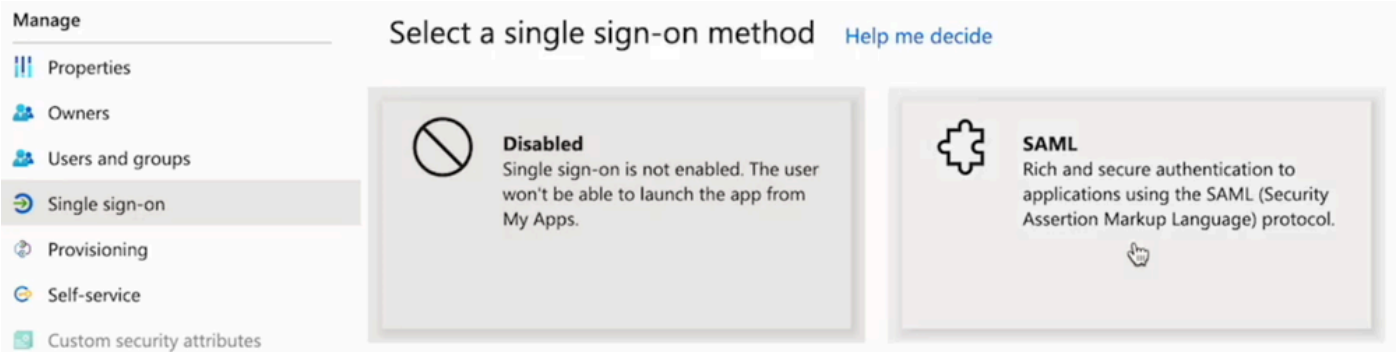
MicrosoftエントリID

1. Microsoft Entra ID管理センターに移動し、[追加]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。



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、ドメイン保護のサインオンです。

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



4. Basic SAML ConfigurationパネルでEditをクリックし、次のパラメータを入力します。

- 識別子（エンティティID）:dmp.cisco.com
- 返信URL（アサーションコンシューマサービスURL）:https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- サインオンURL:https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- [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。

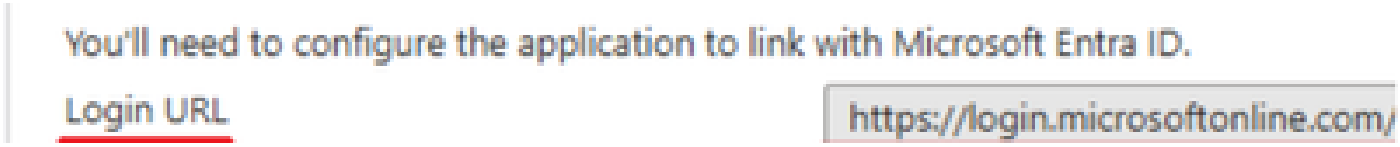
- Additional ClaimsパネルでEditをクリックし、Microsoft Entra IDユーザプロパティとSAML属性間のマッピングを作成します。

[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。

- ログインURLを保存します。

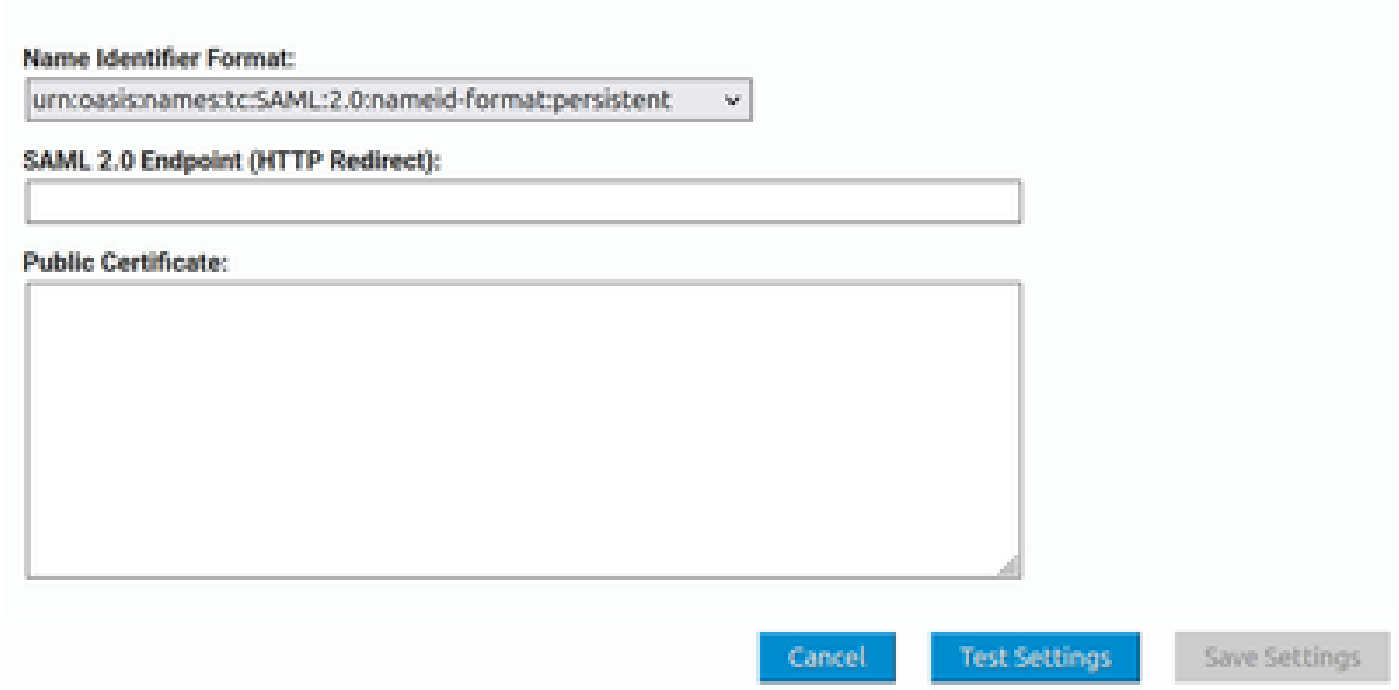


- 証明書(Base64)を保存します。

Cisco Domain Protection（パート2）

Cisco Domain Protection > Enable Single Sign-Onの順に選択します。

- 名前識別子の形式： urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- SAML 2.0エンドポイント（HTTPリダイレクト）:Microsoft Entra IDによって提供されるログインURL
- 公開証明書:Microsoft Entra IDによって提供される証明書(Base64)



確認

Test Settings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 Settingsをクリックします。

トラブルシュート

```
Error - Error parsing X509 certificate
```

- 証明書がBase64にあることを確認します。

```
Error - Please enter a valid URL
```

- Microsoft Entra IDで指定されたログインURLが正しいことを確認します。

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。