

チュートリアル: Azure Active Directory と Pega Systems の統合

2017年11月16日 共同作成者 

この記事の内容

[前提条件](#)

[シナリオの説明](#)

[ギャラリーからの Pega Systems の追加](#)

[Azure AD シングル サインオンの構成とテスト](#)

[その他のリソース](#)

このチュートリアルでは、Pega Systems と Azure Active Directory (Azure AD) を統合する方法について説明します。

Pega Systems と Azure AD の統合には、次の利点があります。

- Pega Systems にアクセスする Azure AD ユーザーを制御できます。
- ユーザーが自分の Azure AD アカウントで Pega Systems に自動的にサインオン (シングル サインオン) できるようにします。
- 1 つの中央サイト (Azure Portal) でアカウントを管理できます。

SaaS アプリと Azure AD の統合の詳細については、「[Azure Active Directory のアプリケーション アクセスとシングル サインオンとは](#)」をご覧ください。

前提条件

Pega Systems と Azure AD の統合を構成するには、以下が必要です。

- Azure AD サブスクリプション
- Pega Systems でのシングル サインオンが有効なサブスクリプション

① 注意

このチュートリアルの手順をテストする場合、運用環境を使用しないことをお勧めします。

このチュートリアルの手順をテストするには、次の推奨事項に従ってください。

- 必要な場合を除き、運用環境は使用しないでください。
- Azure AD の評価環境がない場合は、[1 か月の評価版を入手できます](#)。

シナリオの説明

このチュートリアルでは、テスト環境で Azure AD のシングル サインオンをテストします。このチュートリアルで説明するシナリオは、主に次の 2 つの要素で構成されています。

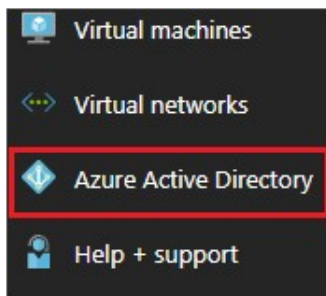
1. ギャラリーからの Pega Systems の追加
2. Azure AD シングル サインオンの構成とテスト

ギャラリーからの Pega Systems の追加

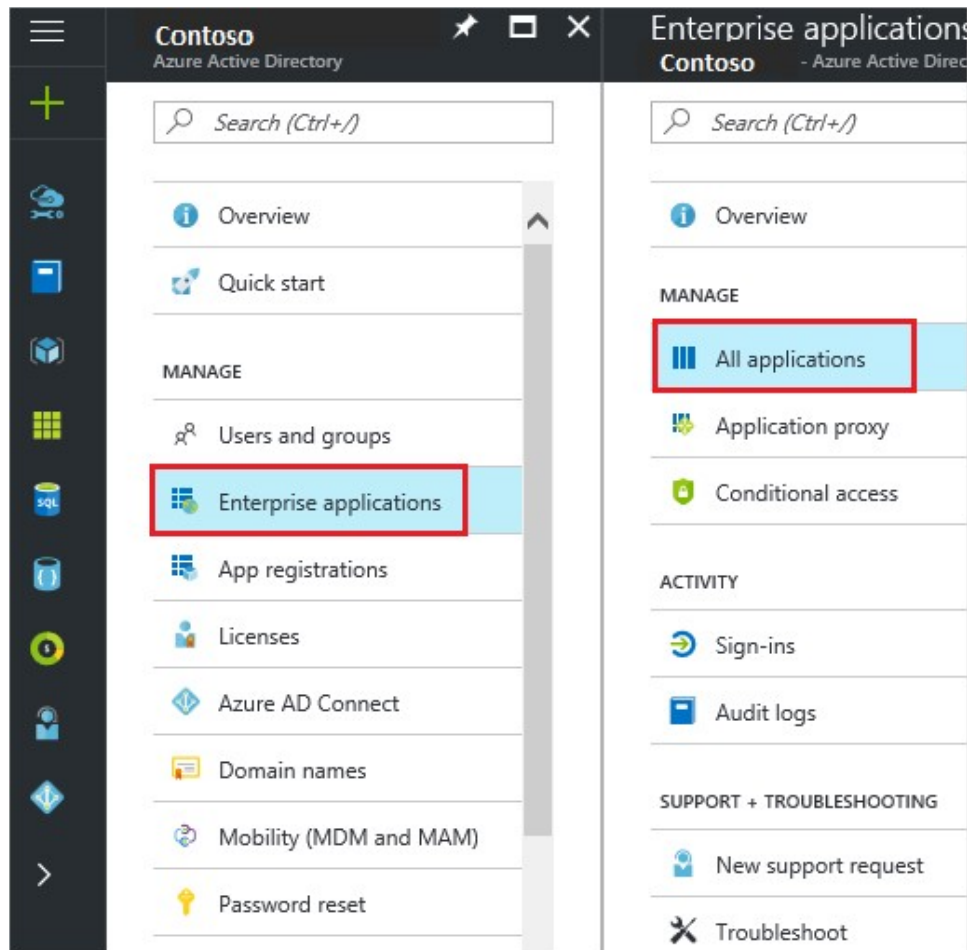
Azure AD への Pega Systems の統合を構成するには、ギャラリーから管理対象 SaaS アプリの一覧に Pega Systems を追加する必要があります。

ギャラリーから Pega Systems を追加するには、次の手順に従います。

1. [Azure Portal](#) の左側のナビゲーション ウィンドウで、[Azure Active Directory] アイコンをクリックします。



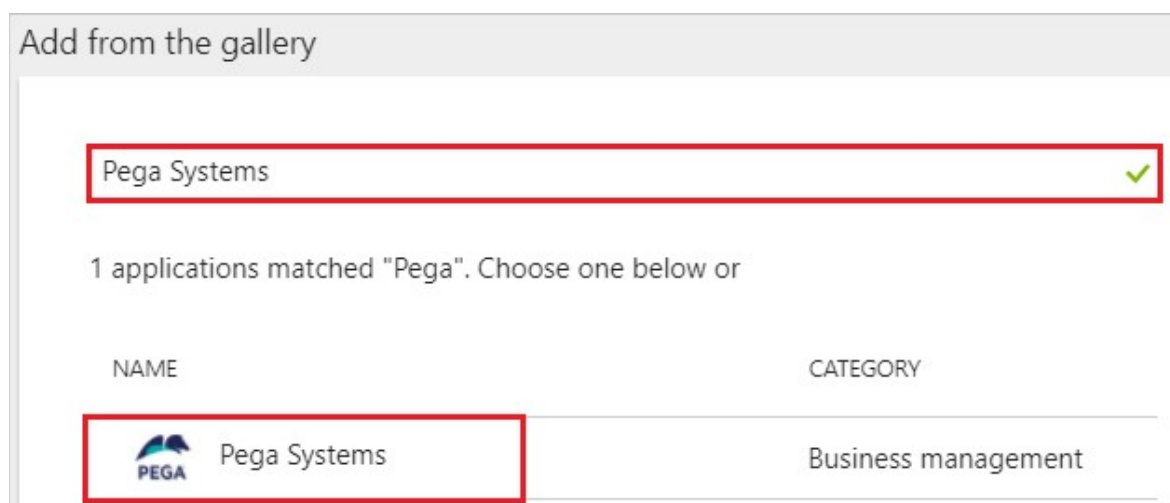
2. [エンタープライズ アプリケーション] に移動します。次に、[すべてのアプリケーション] に移動します。



3. 新しいアプリケーションを追加するには、ダイアログの上部にある **[新しいアプリケーション]** をクリックします。



4. 検索ボックスに「**Pega Systems**」と入力し、結果パネルで **Pega Systems** を選び、**[追加]** をクリックして、アプリケーションを追加します。



Azure AD シングル サインオンの構成とテスト

このセクションでは、"Britta Simon" というテスト ユーザーに基づいて、Pega Systems で Azure AD のシングル サインオンを構成し、テストします。

シングル サインオンが機能するには、Azure AD ユーザーに対応する Pega Systems ユーザーが Azure AD で認識されている必要があります。言い換えると、Azure AD ユーザーと Pega Systems の関連ユーザーの間で、リンク関係が確立されている必要があります。

Pega Systems で、Azure AD の **[ユーザー名]** の値を **[Username](ユーザー名)** の値として割り当ててリンク関係を確立します。

Pega Systems で Azure AD のシングル サインオンを構成してテストするには、次の構成要素を完了する必要があります。

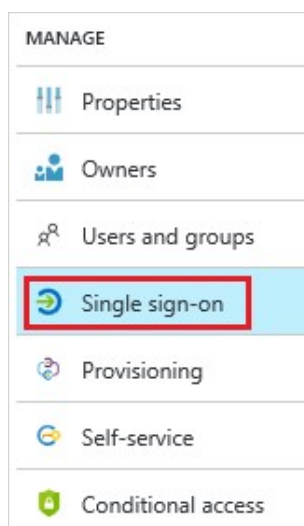
1. **Azure AD シングル サインオンの構成** - ユーザーがこの機能を使用できるようにします。
2. **Azure AD のテスト ユーザーの作成** - Britta Simon で Azure AD のシングル サインオンをテストします。
3. **Pega Systems テスト ユーザーの作成** - Pega Systems で Britta Simon に対応するユーザーを作成し、Azure AD の Britta Simon にリンクさせます。
4. **Azure AD テスト ユーザーの割り当て** - Britta Simon が Azure AD シングル サインオンを使用できるようにします。
5. **シングル サインオンのテスト** - 構成が機能するかどうかを確認します。

Azure AD シングル サインオンの構成

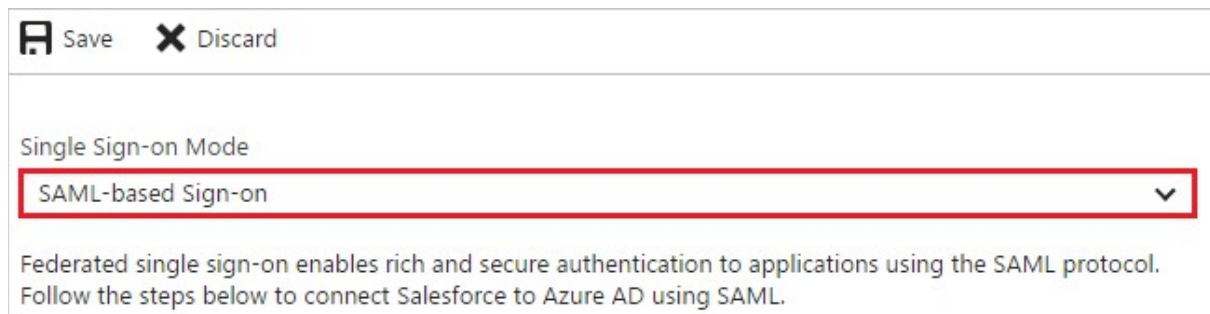
このセクションでは、Azure Portal で Azure AD のシングル サインオンを有効にして、Pega Systems アプリケーションでシングル サインオンを構成します。

Pega Systems で Azure AD シングル サインオンを構成するには、次の手順に従います。

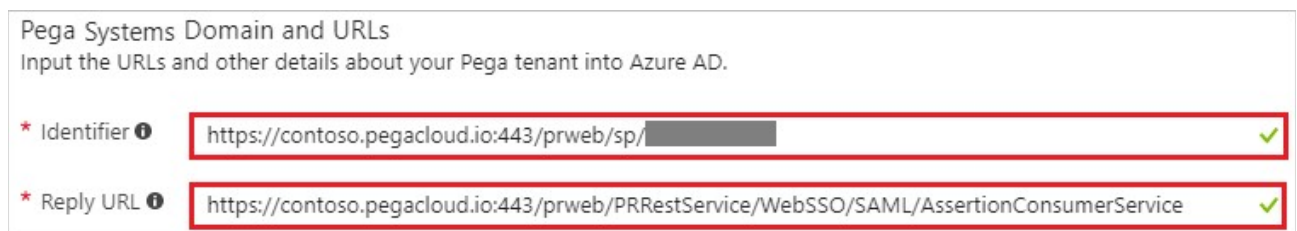
1. Azure Portal の Pega Systems アプリケーション統合ページで、**[シングル サインオン]** をクリックします。



2. **[シングル サインオン]** ダイアログで、**[モード]** として **[SAML ベースのサインオン]** を選択し、シングル サインオンを有効にします。



3. **[Pega Systems のドメインと URL]** セクションで、IDP 開始モードでアプリケーションを構成する場合は、次の手順に従います。



a. **[識別子]** ボックスに、`https://<CUSTOMERNAME>.pegacloud.io:443/prweb/sp/<INSTANCEID>` の形式で URL を入力します。

b. **[応答 URL]** ボックスに、`https://<CUSTOMERNAME>.pegacloud.io:443/prweb/PRRestService/WebSSO/SAML/AssertionConsumerService` のパターンを使用して URL を入力します。

4. アプリケーションを SP 開始モードで構成する場合は、**[詳細な URL 設定の表示]** チェックボックスをオンにして次の手順を実行します。



[リレー状態] ボックスに、`https://<CUSTOMERNAME>.pegacloud.io/prweb/sso` のパターンで URL を入力します。



ⓘ 注意

これらは実際の値ではありません。実際の識別子、応答 URL、およびリレー状態 URL でこれらの値を更新します。このチュートリアルの後半で説明する Pega アプリケーションで、識別子と応答 URL の値を見つけることができます。リレー状態については、[Pega Systems のクライアント サポート チーム](#)に連絡して値を取得してください。

5. Pega Systems アプリケーションでは、特定の形式の SAML アサーションを使用するため、カスタム属性マッピングを SAML トークン属性の構成に追加する必要があります。これらの要求はお客様に固有であり、お客様の要件によって異なります。次のオプションの要求は、アプリケーションで構成できる単なる例です。この属性の値は、アプリケーション統合ページの **[User Attributer]** セクションで管理できます。










User Attributes [Learn more](#)

Edit the user information sent in the SAML token when user sign in to Pega Systems

User Identifier  

☒ View and edit all other user attributes

SAML Token Attributes

NAME	VALUE	NAMESPACE
givenname	user.givenname	http://schemas.xmlsoap.org/ws/2005/05/identi... ..
surname	user.surname	http://schemas.xmlsoap.org/ws/2005/05/identi... ..
emailaddress	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identi... ..
name	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identi... ..
uid		...
cn		...
mail		...
accessgroup		...
organization		...
orgdivision		...
orgunit		...
workgroup		...
Phone		...

6. **[Single sign-on](シングル サインオン)** ダイアログの **[User Attributes](ユーザー属性)** セクションで、上記の図に示すように SAML トークン属性を構成し、次の手順を実行します。

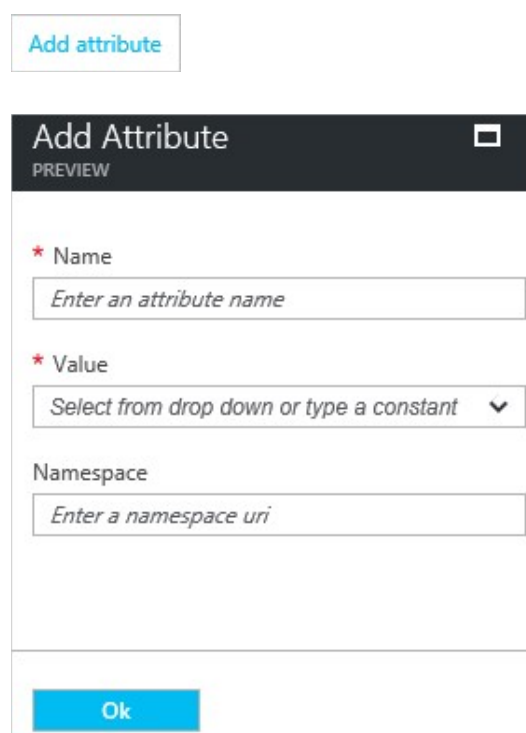
属性名	属性値
uid	*****
cn	*****
mail	*****
accessgroup	*****
organization	*****

属性名	属性値
orgdivision	*****
orgunit	*****
workgroup	*****
電話	*****

ⓘ 注意

これらは、お客様に固有な値です。適切な値を指定してください。

- a. **[属性の追加]** をクリックして **[属性の追加]** ダイアログを開きます。

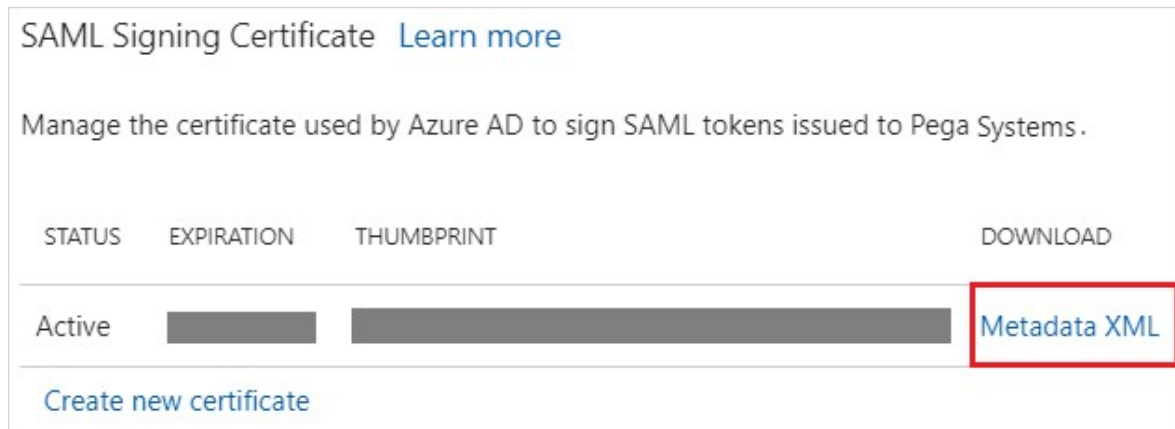


- b. **[名前]** ボックスに、その行に対して表示される属性名を入力します。

- c. **[値]** 一覧から、その行に対して表示される値を入力します。

- d. **[OK]** をクリックします。

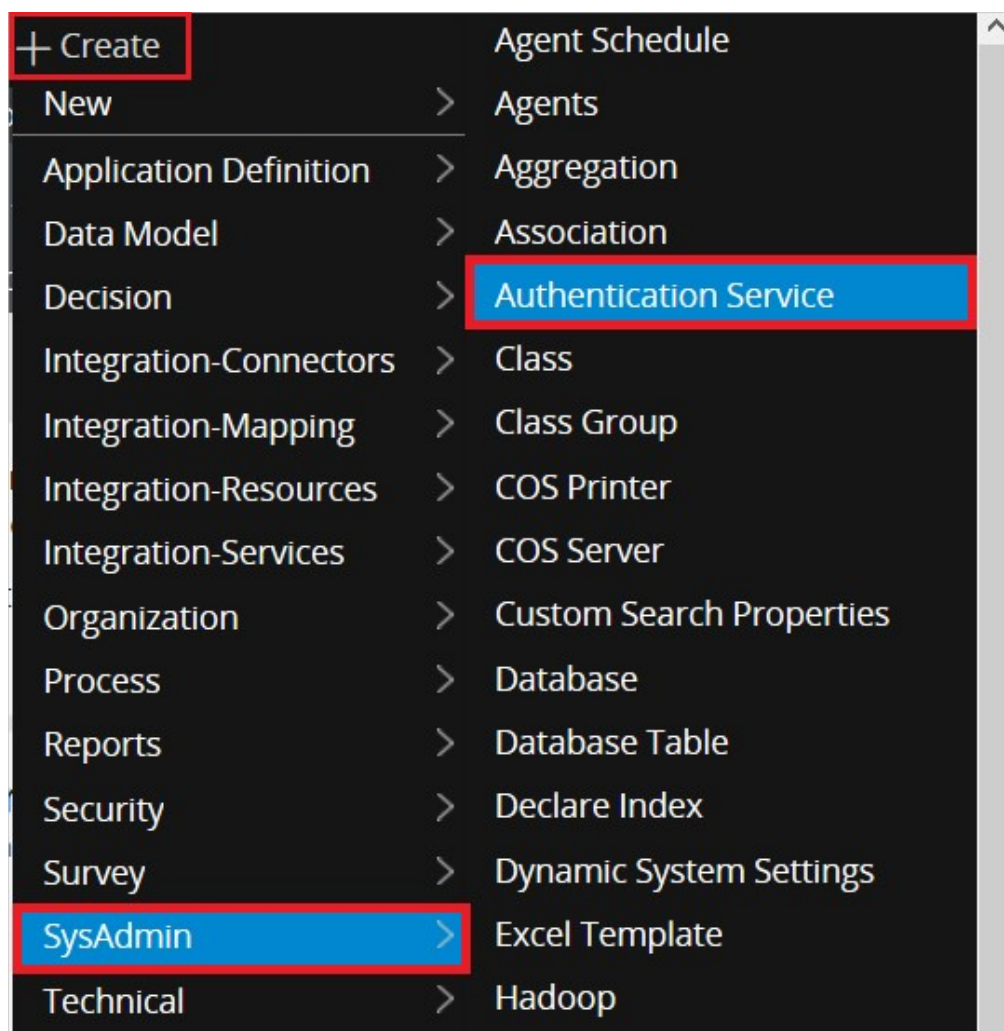
7. **[SAML 署名証明書]** セクションで、**[Metadata XML (メタデータ XML)]** をクリックし、コンピューターにメタデータ ファイルを保存します。



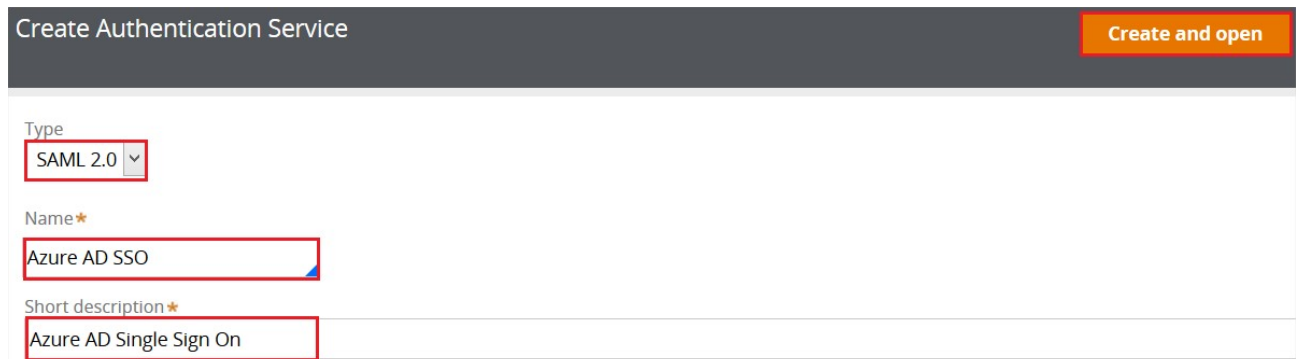
8. **[保存]** ボタンをクリックします。



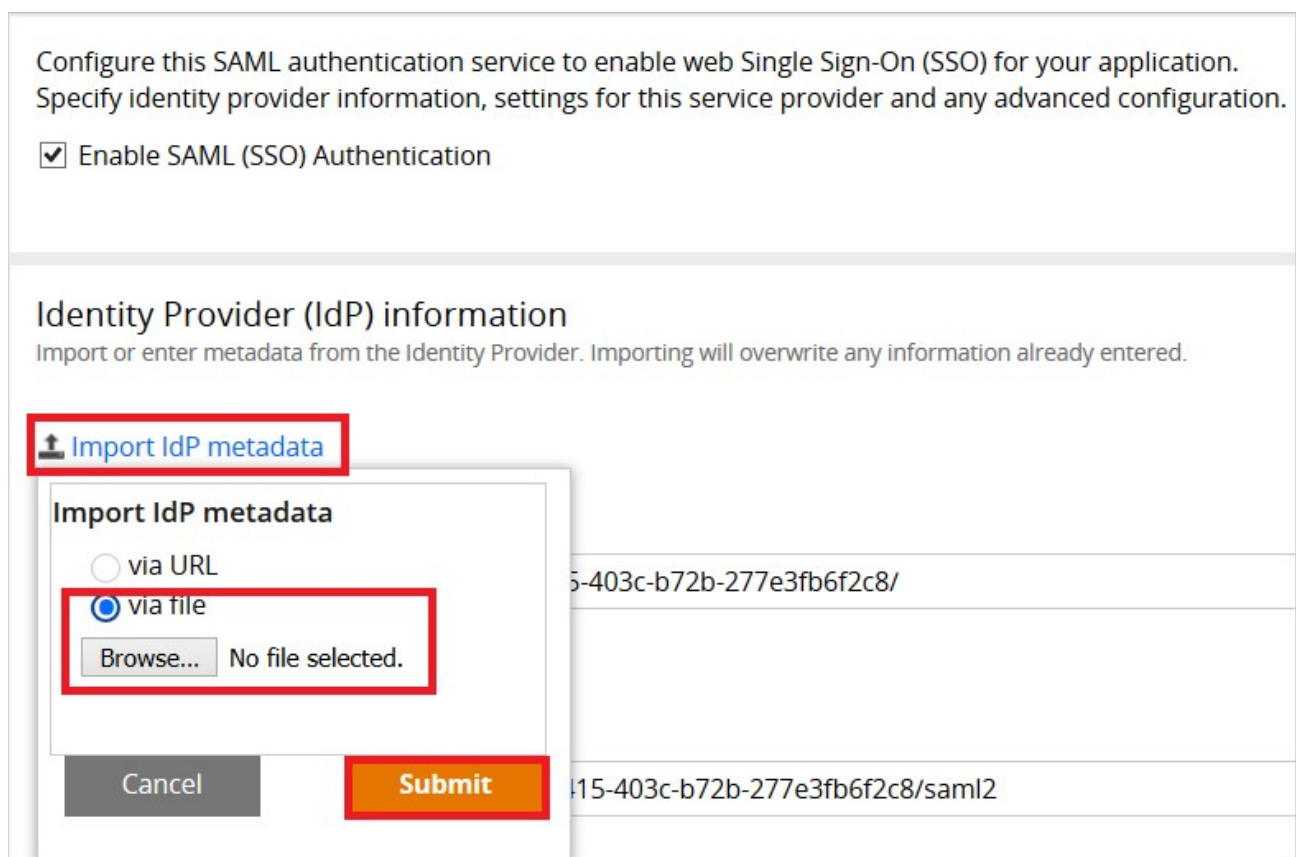
9. Pega Systems 側でシングル サインオンを構成するには、別のブラウザー ウィンドウで管理者アカウントを使って Pega **ポータル**を開きます。
10. **[Create](作成)** -> **[SysAdmin]** -> **[Authentication Service](認証サービス)** の順に選択します。




11. **[Create Authentication Service](認証サービスの作成)** 画面で次の操作を実行します。



- a. [Type](種類) で [SAML 2.0] を選択します
 - b. [Name](名前) ボックスに名前を入力します (例: Azure AD SSO)
 - c. [Short Description](簡単な説明) ボックスに、任意の説明を入力します
 - d. [Create and open](作成して開く) をクリックします
12. [Identity Provider (IdP) information](ID プロバイダー (IdP) 情報) セクションで [Import IdP metadata](IdP メタデータのインポート) をクリックし、Azure Portal からダウンロードしたメタデータ ファイルを参照します。 [Submit](送信) をクリックして、メタデータを読み込みます。



13. 次のように、IdP データが設定されます。

 [Import IdP metadata](#)

Entity Identification (Issuer)

Login (SSO) protocol binding

HTTP POST

Login location



Logout (SLO) protocol binding

HTTP Redirect

Logout location

Artifact Resolution Service (ARS) location

Verification certificate

 Alias: CN= Expiry date: 

14. [Service Provider (SP) settings](サービスプロバイダー (SP) 設定) セクションで、以下の操作を行います。

Service Provider (SP) settings

These settings are dynamically generated and can be edited or reset to new values. Complete this section and provide necessary certificates; then do

Entity Identification

<https://.pegacloud.io:443/prweb/sp/>

Login (SSO) protocol binding

HTTP POST

When selecting "HTTP Artifact" for SP login binding, ensure that an ARS location is specified in the IdP information section above.

Assertion Consumer Service (ACS) location

<https://.pegacloud.io:443/prweb/PRRestService/WebSSO/SAML/AssertionConsumerService>

Redirect logout location

<https://.pegacloud.io:443/prweb/PRRestService/WebSSO/SAML/Logout>

SOAP logout location

<https://.pegacloud.io:443/prweb/PRSOAPServlet/SOAP/WebSSO/SAML/Logout>

Artifact Resolution Service (ARS) location

<https://.pegacloud.io:443/prweb/PRSOAPServlet/SOAP/WebSSO/SAML/ArtifactResolutionService>

[Reset](#)

☒ Disable request signing

- a. [Entity Identification](エンティティの識別) の値をコピーし、Azure Portal の [識別子] ボックスに貼り付けます。
- b. [Assertion Consumer Service (ACS) location](Assertion Consumer Service (ACS) の場所) の値をコピーし、Azure Portal の [応答 URL] ボックスに貼り付けます。

c. [Disable request signing](要求署名を無効にする) をオンにします。


15. [保存]

💡 ヒント

アプリのセットアップ中、[Azure Portal](#) 内で上記の手順の簡易版を確認できるようになりました。[Active Directory] の [エンタープライズ アプリケーション] セクションからこのアプリを追加した後、[シングル サインオン] タブをクリックし、一番下の [構成] セクションから組み込みドキュメントにアクセスするだけです。埋め込みドキュメント機能の詳細については、[Azure AD の埋め込みドキュメント](#)に関するページを参照してください。

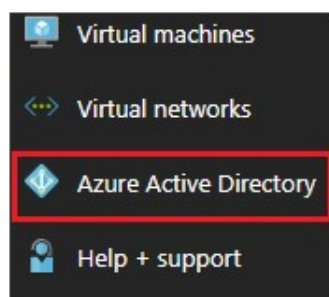
Azure AD のテスト ユーザーの作成

このセクションの目的は、Azure Portal で Britta Simon というテスト ユーザーを作成することです。

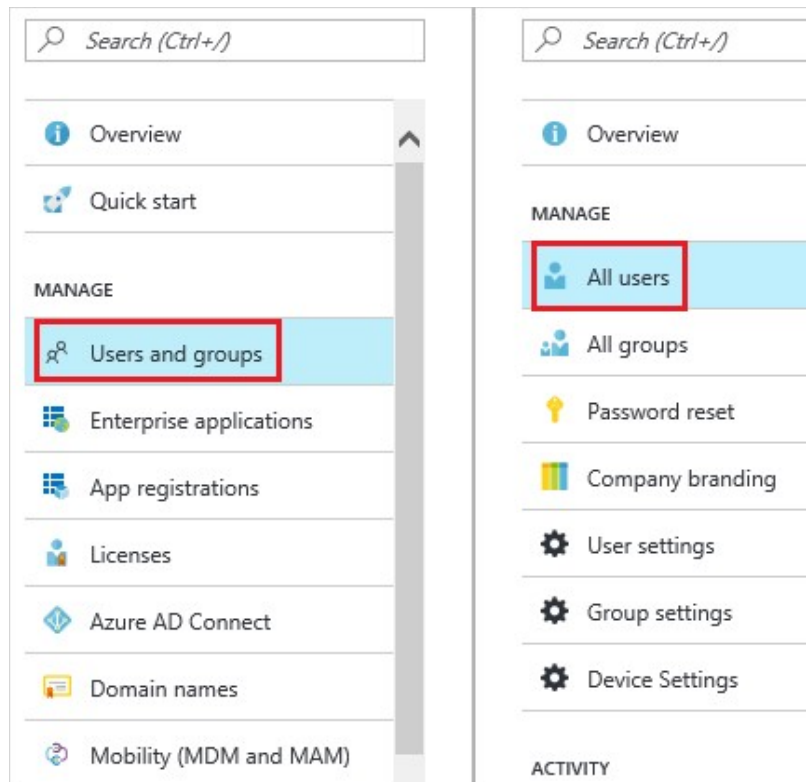
NAME	USER NAME
 Britta Simon	BrittaSimon@contoso.com ...

Azure AD でテスト ユーザーを作成するには、次の手順に従います。

1. Azure Portal の左側のウィンドウで、Azure Active Directory のボタンをクリックします。



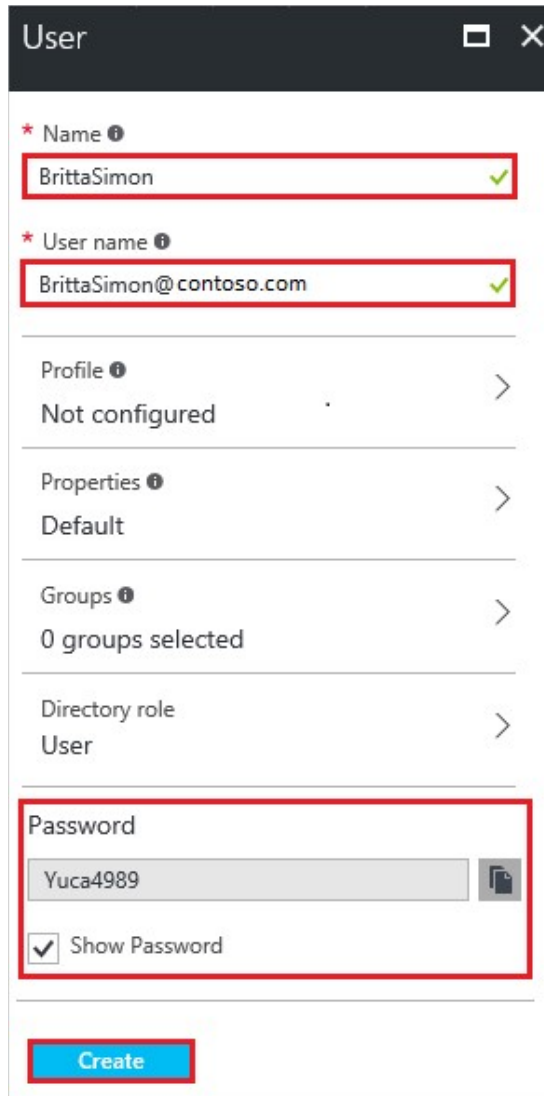
2. ユーザーの一覧を表示するには、[ユーザーとグループ] に移動し、[すべてのユーザー] をクリックします。



3. [ユーザー] ダイアログ ボックスを開くには、[すべてのユーザー] ダイアログ ボックスの上部にある [追加] をクリックしてきます。



4. [ユーザー] ダイアログ ボックスで、次の手順に従います。



User

* Name ⓘ
BrittaSimon ✓


* User name ⓘ
BrittaSimon@contoso.com ✓

Profile ⓘ
Not configured >

Properties ⓘ
Default >

Groups ⓘ
0 groups selected >

Directory role
User >

Password
Yuca4989 
☒ Show Password

Create

- [名前] ボックスに「BrittaSimon」と入力します。
- [ユーザー名] ボックスに、ユーザーである Britta Simon の電子メール アドレスを入力します。
- [パスワードを表示] チェック ボックスをオンにし、[パスワード] ボックスに表示された値を書き留めます。
- Create をクリックしてください。

Pega Systems テスト ユーザーの作成

このセクションの目的は、Pega Systems で Britta Simon というユーザーを作成することです。Pega Sysyems でユーザーを作成するには、[Pega Systems クライアント サポート チーム](#)と協力してください。

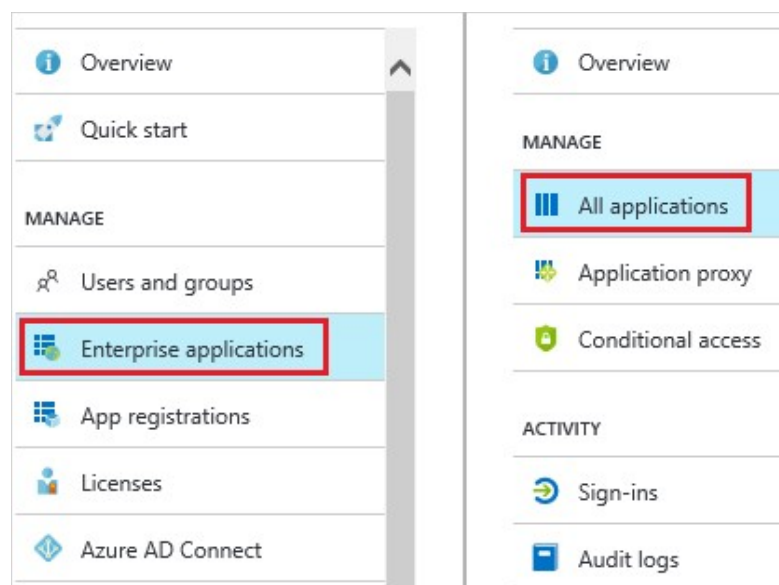
Azure AD テスト ユーザーの割り当て

このセクションでは、Britta Simon に Pega Systems へのアクセスを許可することで、このユーザーが Azure シングル サインオンを使用できるようにします。

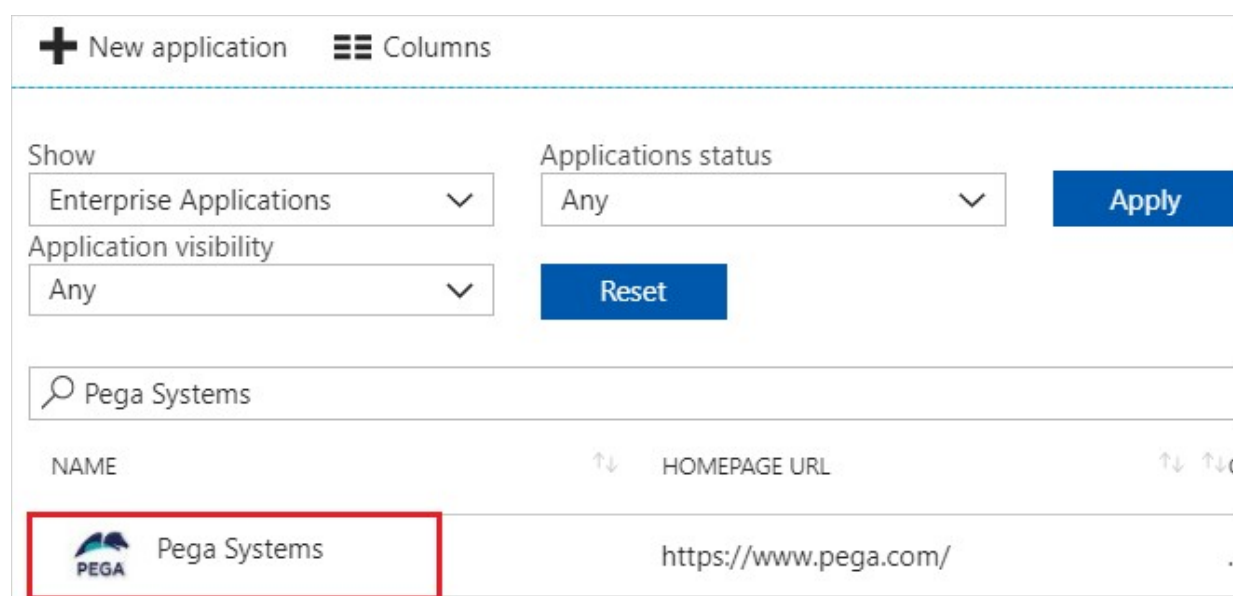
DISPLAY NAME	OBJECT TYPE	ROLE
Britta Simon	User	Default Access

Pega Systems に Britta Simon を割り当てるには、次の手順に従います。

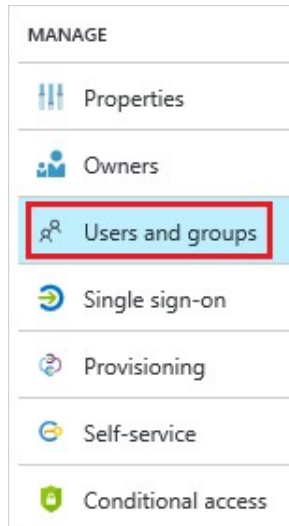
1. Azure Portal でアプリケーション ビューを開き、ディレクトリ ビューに移動します。次に、[エンタープライズ アプリケーション] に移動し、[すべてのアプリケーション] をクリックします。



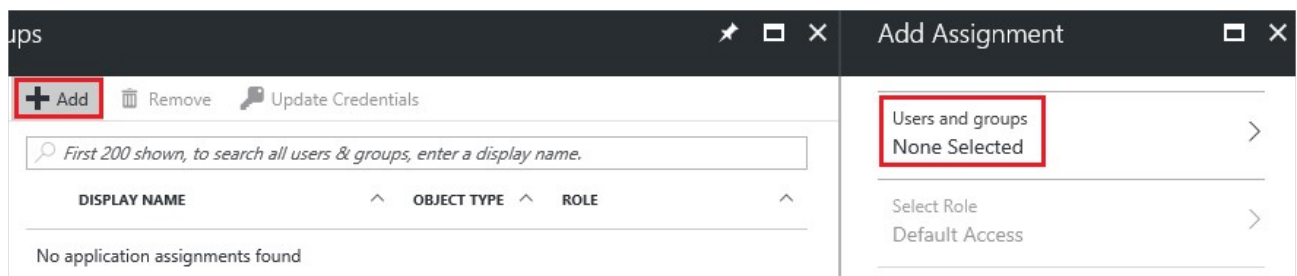
2. アプリケーションの一覧で [Pega Systems] を選択します。



3. 左側のメニューで [ユーザーとグループ] をクリックします。



4. [追加] ボタンをクリックします。次に、[割り当ての追加] ダイアログで [ユーザーとグループ] を選択します。



5. [ユーザーとグループ] ダイアログで、ユーザーの一覧から [Britta Simon] を選択します。
6. [ユーザーとグループ] ダイアログで [選択] をクリックします。
7. [割り当ての追加] ダイアログで [割り当て] ボタンをクリックします。

シングル サインオンのテスト

このセクションでは、アクセス パネルを使用して Azure AD のシングル サインオン構成をテストします。

アクセス パネルで Pega Systems のタイルをクリックすると、Pega Systems アプリケーションに自動的にサインオンします。アクセス パネルの詳細については、[アクセス パネルの概要](#)に関するページを参照してください。

その他のリソース

- [SaaS アプリと Azure Active Directory を統合する方法に関するチュートリアルの一覧](#)
- [Azure Active Directory のアプリケーション アクセスとシングル サインオンとは](#)

