

# 日々はOracle APEX

Oracle APEXを使った作業をしていて、気の付いたところを忘れないようにメモをとります。

2022年6月17日 金曜日

## Oracle IDCSを使ってAPEXアプリをSAMLで認証する

Oracle Identity Cloud Serviceを使って、Oracle APEXのアプリケーションをSAMLで認証させてみました。

最初に無料で利用できる範囲を確認します。IDCSのドキュメントの以下のセクションを参照します。

### About Oracle Identity Cloud Service Pricing Models

無償の範疇について、以下のように説明されています。

#### Understand the User Per Month Pricing Model

Learn about the pricing tiers for Oracle Identity Cloud Service for the User per Month pricing model and the features associated with each pricing tier.

For this pricing model, Oracle Identity Cloud Service has two pricing tiers:

- Oracle Identity Cloud Service Foundation: Oracle provides this free version of Oracle Identity Cloud Service for customers that subscribe to Oracle Software-as-a-Service (SaaS), Oracle Platform-as-a-Service (PaaS), and Oracle Cloud Infrastructure only.

A customer can use this version to provide basic identity management functions, including user management, group management, password management, and basic reporting. For additional features, as indicated in the table below, a subscription to Oracle Identity Cloud Service Standard is required.

A customer can't use this version to integrate with third-party SaaS, PaaS, custom web or mobile applications, programmatic clients or On-Premises applications, even if those applications are hosted on Oracle Cloud Infrastructure. Those use cases require Oracle Identity Cloud Service Standard.

日本語訳から抜粋します。

- Oracle Identity Cloud Service Foundation: Oracleは、Oracle Software-as-a-Service (SaaS)、Oracle Platform-as-a-Service (PaaS)およびOracle Cloud Infrastructureのみをサブスクライブするお客様に、この無料バージョンのOracle Identity Cloud Serviceを提供します。

顧客は、このバージョンを使用して、ユーザー管理、グループ管理、パスワード管理、基本的なレポートなどの基本的なアイデンティティ管理機能を提供できます。次の表に示すように、追加機能にはOracle Identity Cloud Service Standardのサブスクリプションが必要です。

サードパーティのSaaS、PaaS、カスタムWebまたはモバイル・アプリケーション、プログラムによるクライアントまたはオンプレミス・アプリケーションがOracle Cloud Infrastructureでホストされている場合でも、これらのアプリケーションとの統合にこのバージョンを使用することはできません。これらのユースケースでは、Oracle Identity Cloud Service Standardが必要です。

Oracle APEXではPaaSのAutonomous Databaseを利用している場合でも、SAML認証を使うにはORDSを別立てし独自ドメインを割り当てる必要があります。そのため、どのようにサードパーティの環

境とOracle Cloudの環境を見分けるのか、正直なところ分かりません。クライアントはブラウザですから、ネットワークとしてもOracle Cloudの外にあります。

技術的にどのような方法で範囲を限定するのか分かりませんが、ドキュメントの記述に依るとOracle CloudでOracle APEXを動かしている限り、Oracle Identity Cloud Service Foundationの範疇のようです。他のクラウドやオンプレミスで稼働しているOracle APEXの環境も（Oracle APEXはサードパーティの製品ではないため）、無償利用の範疇に入るようにも読めます。後者については、公式なパスを通して確認する必要があるかもしれません。

とりあえず、今回はOracle Cloudで稼働しているOracle APEXのインスタンスを使用するため、無償利用の範囲と判断して作業を行います。

**アップグレードしていないFree Tierアカウント**で、Oracle Identity Cloud Service側の作業を行います。

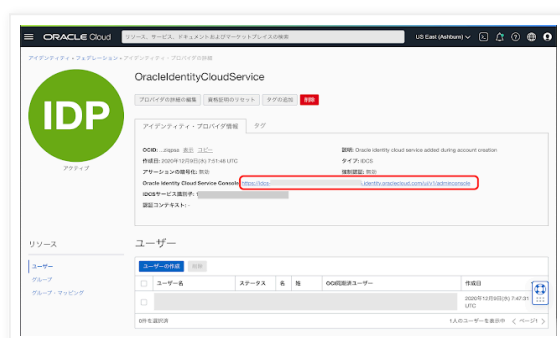
OCIコンソールより**アイデンティティとセキュリティのフェデレーション**を開きます。

Oracle Cloudのアカウントを作成すると、**アイデンティティ・プロバイダ**として**OracleIdentityCloudService**があらかじめ作成されます。

このリンクをクリックして開きます。



**Oracle Identity Cloud Service Console**のリンクをクリックし、Oracle Identity Cloud Serviceのコンソールを開きます。

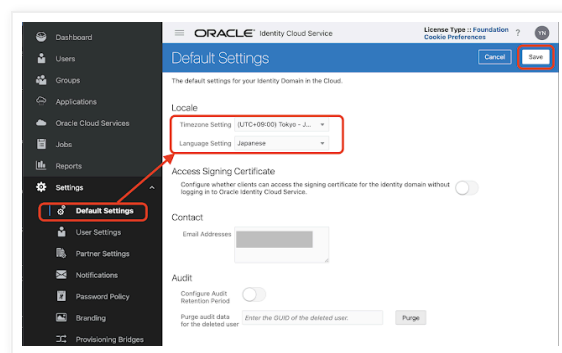


Identity Cloud Serviceのコンソールが開きます。



コンソールが英語で表示される場合は、ナビゲーション・メニューの**Settings**の**Default Settings**を開き、**Locale**の**Language Setting**を**Japanese**に変更します。また、**Timezone Setting**も**(UTC+09:00) Tokyo - Japan Time (JT)**に変更します。

設定を変更後、**Save**をクリックします。変更を反映させるために、サインインをし直します。



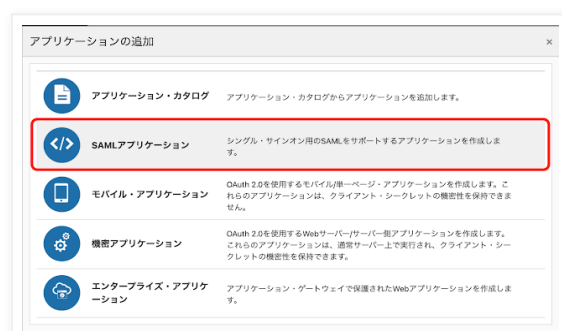
Oracle APEXの環境をアプリケーションとして登録します。

ナビゲーション・メニューの**アプリケーション**を開きます。

**追加**をクリックします。



ダイアログが開くので、**SAMLアプリケーション**を選択します。



**SAMLアプリケーションの追加**を行う画面が表示されます。**名前**は任意ですが、今回は**apex**とします。

それ以外はデフォルトのまま、**次**に進みます。

アプリケーション**apex**が**非アクティブ**の状態を追加されます。その後に開く画面にて、SAMLに関する構成を行います。

**一般のエンティティIDおよびアサーション・コンシューマのURL**は、双方ともAPEX側の**SAMLコールバックURL**を指定します。

以下のような形式のURLです。**apex\_authentication.saml\_callback**の部分は、どのインスタンスでも同じです。ベースとなるURLはOracle APEXが稼働している環境に合わせて変更します。

**[https://test.mydomain.dev/ords/xepdb1/apex\\_authentication.saml\\_callback](https://test.mydomain.dev/ords/xepdb1/apex_authentication.saml_callback)**

**[https://test.mydomain.dev/ords/apex\\_authentication.saml\\_callback](https://test.mydomain.dev/ords/apex_authentication.saml_callback)**

**NameID形式**と**NameID値**はそれぞれデフォルトの、**電子メール・アドレス**、**プライマリ電子メール**のままとします。ここで指定された値をOracle APEX側で読み取るために、**内部およびワークスペース・アプリケーション用のSAML: APEX属性の名前IDフォーマット**として、以下を指定します。**NameID形式**や**NameID値**をデフォルトから変更した場合、**APEX属性の名前IDフォーマット**も変更が必要です。

**urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**

**Autonomous DatabaseでのSAMLの設定には、名前IDフォーマットの指定がないため、この指定は不要です。**

opensslを使用して、アップロードする**署名証明書**を生成します。手順は**Oktaの記事**で紹介しています。実行するコマンドだけを以下に列記します。

```
openssl genrsa -out private.pem 2048
```

```
openssl req -new -key private.pem -out test.csr
```

```
openssl x509 -req -days 3650 -signkey private.pem -in test.csr -sha256 -extfile v3.ext -out cert-test.pem
```

X.509バージョン3の拡張を指定するファイルv3.extの内容は以下になります。

**keyUsage = digitalSignature,keyEncipherment**

```
% openssl genrsa -out private.pem 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
% openssl req -new -key private.pem -out test.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, fully qualified host name) []: test.mydomain.dev
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
% openssl x509 -req -days 3650 -signkey private.pem -in test.csr -sha256 -extfile
v3.ext -out cert-test.pem
Signature ok
subject=/CN=test.apexugj.dev
Getting Private key
%
```

上記の手順で生成された**cert-test.pem**を、**署名証明書**として選択します。

続いて、**署名証明書のダウンロード**と**アイデンティティ・プロバイダ・メタデータのダウンロード**を実行します。先ほどアップロードした署名証明書はサービス・プロバイダ（APEX側）のもので、こちらの署名証明書はアイデンティティ・プロバイダのものになります。

署名署名書は**IDCSCertificate.pem**、**アイデンティティ・プロバイダ・メタデータ**は**IDCSMetadata.xml**としてダウンロードされます。

詳細設定を開きます。

署名付きSSOとして、**アサーションおよびレスポンス**を選択します。署名に署名証明書を含めるはチェックします。署名ハッシュ・アルゴリズムはSHA-256です。

シングル・ログアウトの有効化を**チェック**します。

ログアウト・バインドに**POST**を選択します。**シングル・ログアウトURL**、**ログアウト・レスポンスURL**共に、APEXの**SAMLコールバックURL**を設定します。

アサーションの暗号化は**チェック**しません。



現時点では、**シングル・サインアウト**の正常な動作は確認できていません。

**属性構成**を開いて、アサーションに含めるユーザー情報を指定します。

**属性**の**+**をクリックしてユーザー情報を追加します。**形式**は**基本**、**タイプ**は**ユーザー属性**とします。

**名前**を**groups**として、**グループ・メンバーシップ**を送信します。**条件**は**すべてのグループ**です。サインインしたユーザーが所属しているグループがアサーションに含まれます。グループ情報は、APEX側の認可処理に使用できます。**firstName**として**名**、**lastName**として**姓**の情報も含めます。



**認証と認可の権限付与を認可として実施**は、デフォルトで**チェック**が入っているのでそのままにします。必要な設定なのか、確認はできていません。

以上の設定を行い、**終了**をクリックします。

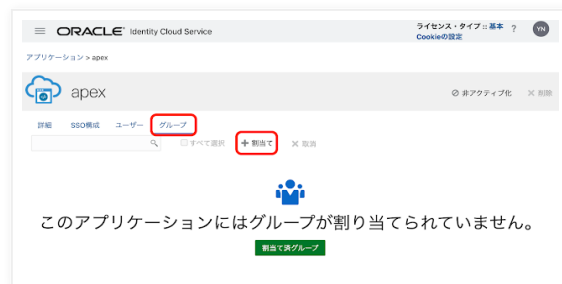


SAMLによるSSO構成が行われます。

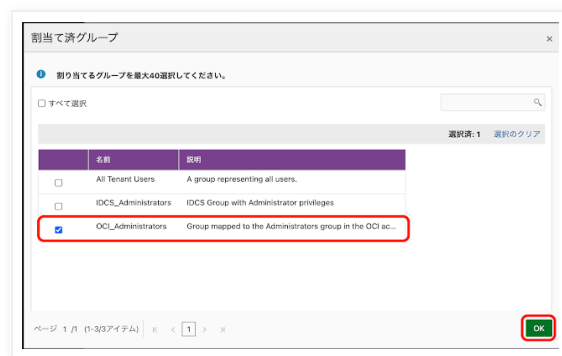
アプリケーションを**アクティブ化**します。確認のダイアログがポップアップするので、**OK**をクリックします。



このアプリケーションでサインインできるユーザーを割り当てます。今回はユーザーを割り当てる代わりに、**グループ**を割り当てます。**グループ**タブを開き、**+ 割り当て**をクリックします。



**OCI\_Administrators**にチェックを入れ、**OK**をクリックします。



グループとしてOCI\_Administratorsが割り当たります。少なくとも、現在Oracle CloudにサインインしてIdentity Cloud Serviceの設定を行なっているユーザーは、このアプリケーションapexにサインインできるようになりました。

以上で、Oracle Identity Cloud Serviceの準備は完了です。

Oracle APEX側の設定を行います。

Oracle APEXの**管理サービス**にサインインし、**SAML**の構成画面を開きます。(ナビゲーション・パスは**インスタンスの管理**>**セキュリティ**>**認証制御**>**SAML**です。スクリーンショットは[Oktaの記事](#)を参照してください。)

内部およびワークスペース・アプリケーション用の**SAML: APEX属性のアプリケーションのSAML有効化をON**にします。名前IDフォーマットはOracle Identity Cloud Serviceの設定に合わせて、以下を設定します。**Autonomous Databaseにこの指定はありません。**

**urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**

**証明書と秘密キー**は、opensslを使って生成したものを貼り付けます。



内部およびワークスペース・アプリケーション用のSAML: アイデンティティ・プロバイダ属性を設定します。

発行者はIDCSMetadata.xmlよりentityIDを取り出して設定します。署名証明書はIdentity Cloud Serviceからダウンロードした証明書、IDCSCertificate.pemの内容を貼り付けます。サインインURLはXMLMetadata.xmlのSingleSignOnService要素のLocation属性の値を設定します。

```
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://idcs-*****.identity.oraclecloud.com/fed/v1/idp/sso"/>
```

サインアウトURLとしてSingleLogoutService要素のLocation属性の値を設定します。(正常動作が確認できてから設定するのが望ましいです。)

```
<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://idcs-*****.identity.oraclecloud.com/fed/v1/idp/slo"
ResponseLocation="https://idcs-*****.identity.oraclecloud.com/fed/v1/idp/slo"/>
```

Binding属性がHTTP-RedirectとHTTP-POSTのどちらでもLocationは同じようです。もし異なっている場合は、どちらか動く方を確認して選択します。

以上で変更の適用をします。

ORDSのCORS設定で、アクセスを許可するOriginはhttps://idcs-\*\*\*\*\*.identity.oraclecloud.comでした。IDCSMetadata.xmlのentityIDやシングル・サインインURLのホスト部分になるので、それらの値から伏せ字の部分を補完してください。

ORDS 22.1では以下のコマンドを実行します。ordsコマンドのパスや構成ファイルの位置は、それぞれのインストールで異なります。

```
/usr/local/bin/ords --config /etc/ords/config config set
security.externalSessionTrustedOrigins https://idcs-*****.identity.oraclecloud.com
```



ORDS 21.xでは以下のコマンドを実行します。

```
java -jar ords.war set-property security.externalSessionTrustedOrigins https://idcs-
*****.identity.oraclecloud.com
```

変更を反映するには、ORDSの再起動が必要です。

以上でOracle APEX側の設定は完了です。

SAMLによるサインインを確認するために作成したアプリケーションにアクセスし、設定を確認します。

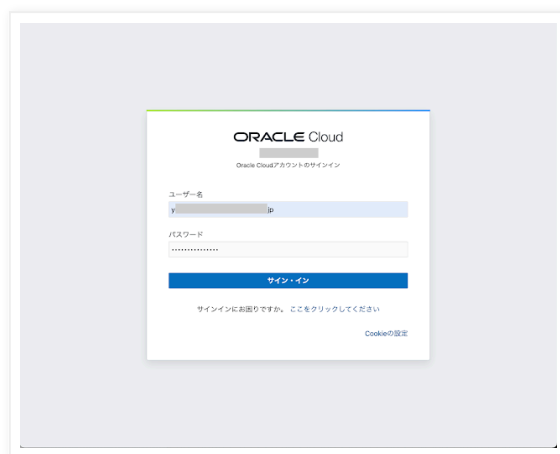
**https://ホスト名/ords/PDB名/r/ワークスペース名/samltest/home**

今回の例では、以下のURLにアクセスします。

**https://test.mydomain.dev/ords/xepdb1/r/apexdev/samltest/home**

Oracle Cloudのサインイン画面が表示されます。

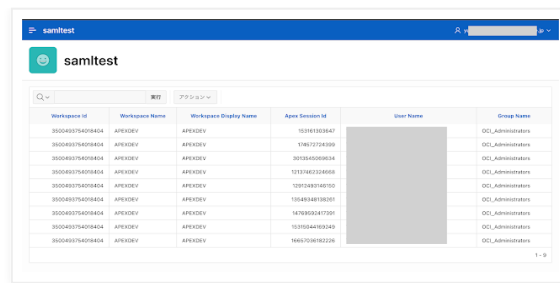
**ユーザー名**と**パスワード**を入力し、**サイン・イン**を実行します。



APEXアプリケーションの画面が開きます。

Oracle Identity Cloud ServiceのSAMLを構成するときに、**属性構成**としてアサーションに名前 **groups**として、サインインしたユーザーが所属しているグループを渡すように設定しています。groupsという名称はOktaのときと同じ名前なので、[こちらの記事](#)で行ったダイナミック・グループの構成をそのままOracle Identity Cloud Serviceでも使用できます。

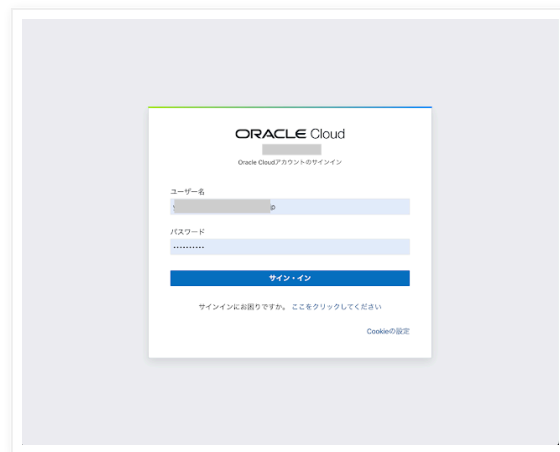
今回の作業では、ダイナミック・グループとしてOCI\_Administratorsがサインインしたユーザーに割り当てられていることが確認できます。



Workspace ID	Workspace Name	Workspace Display Name	Apex Session Id	User Name	Group Name
300493174078424	AFEXDEV	AFEXDEV	101815133847		OCI Administrators
300493174078424	AFEXDEV	AFEXDEV	1186171714399		OCI Administrators
300493174078424	AFEXDEV	AFEXDEV	301244668024		OCI Administrators
300493174078424	AFEXDEV	AFEXDEV	12119412124668		OCI Administrators
300493174078424	AFEXDEV	AFEXDEV	130148190100		OCI Administrators
300493174078424	AFEXDEV	AFEXDEV	11548948198101		OCI Administrators
300493174078424	AFEXDEV	AFEXDEV	1478953417391		OCI Administrators
300493174078424	AFEXDEV	AFEXDEV	1010144193149		OCI Administrators
300493174078424	AFEXDEV	AFEXDEV	16617146182226		OCI Administrators

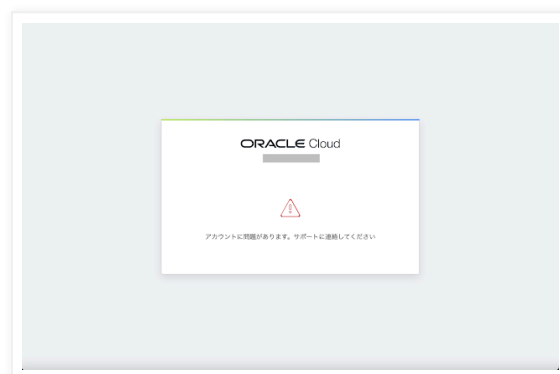
シングル・サインアウトの動作を確認します。

アプリケーションからサインアウトすると、Oracle Cloudのサインイン画面に戻ります。



以下のようなエラーが発生する場合があります。Autonomous Databaseでは、必ず発生します。

今回の検証作業はAlways Freeのインスタンスで行っており、Customer Managed ORDSを使う要件であるプライベート・エンドポイントを使っていません。公式にはサポートされない構成での検証になります。



シングル・サインアウトが動いているAPEXのバージョンは22.1、Autonomous Databaseは21.2なので、その違いもあるかもしれません。近日中にADBも22.1へアップグレードされるので、その後に再度確認しようと思います。

すべての動作が確認できなかったのは残念ですが、以上で、Oracle Identity Cloud Serviceを使ってAPEXアプリをSAMLで認証するための作業は終了です。

完

Yuji N. 時刻: 17:55

共有

---

<

ホーム

>

[ウェブ バージョンを表示](#)

## 自己紹介

**Yuji N.**

日本オラクル株式会社に勤務していて、Oracle APEXのGroundbreaker Advocateを拝命しました。  
こちらの記事につきましては、免責事項の参照をお願いいたします。

[詳細プロフィールを表示](#)

Powered by Blogger.

---