

Azure Active Directory Integration with Amazon Cognito User Pools

Amazon Cognito lets us add user sign-up, sign-in, and access control to the web access within Data.all. Amazon Cognito supports sign-in with social identity providers via SAML 2.0.

We would like to integrate Azure AD with Cognito via authentication and redirection URLs/Tokens that will be entered into Azure AD. These are generated securely within Cognito before deployment to Azure AD.

To set up an AWS Cognito User Pool with an Azure AD identity provider and perform single sign-on (SSO) authentication with Azure AD account to access AWS services in the data.all serverless application, we need to follow these steps:

Get the ACS endpoint and the Entity ID from AWS Cognito

With the built-in hosted web UI, Amazon Cognito provides token handling and management for all authenticated users, so that Data.all backend systems can standardise on one set of user pool tokens.

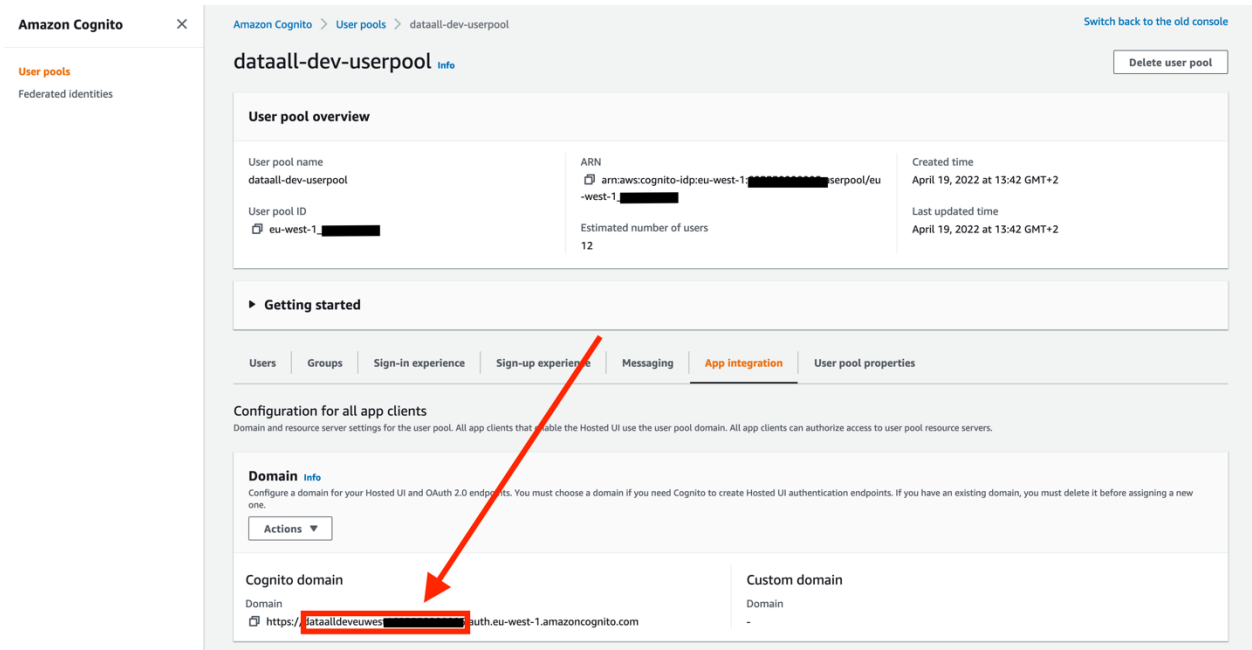


As part of its deployment, data.all already creates a Cognito User Pool, an App Client, and an Amazon Cognito domain. To build your Azure AD application that will integrate with the Cognito User Pool, you will need to provide two things:

- Assertion Consumer Service (ACS) endpoint - This corresponds to the location which the SSO tokens are sent. Configure this endpoint for SAML 2.0 POST binding in your SAML identity provider:

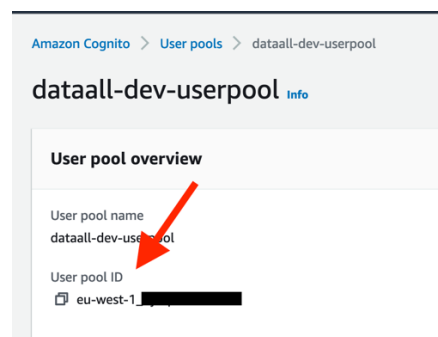
<https://<yourDomainPrefix>.auth.<region>.amazoncognito.com/saml2/idpresponse>

Use the region where data.all is deployed in this link. You can find your domain prefix for your user pool on the **App Integration** tab of the Amazon Cognito console.



- **Entity ID** - The globally-unique identifier for your Cognito User Pool. This ID has the following form: `urn:amazon:cognito:sp:<yourUserPoolID>`

You can find your **user pool ID** on Overview box in the Amazon Cognito console.

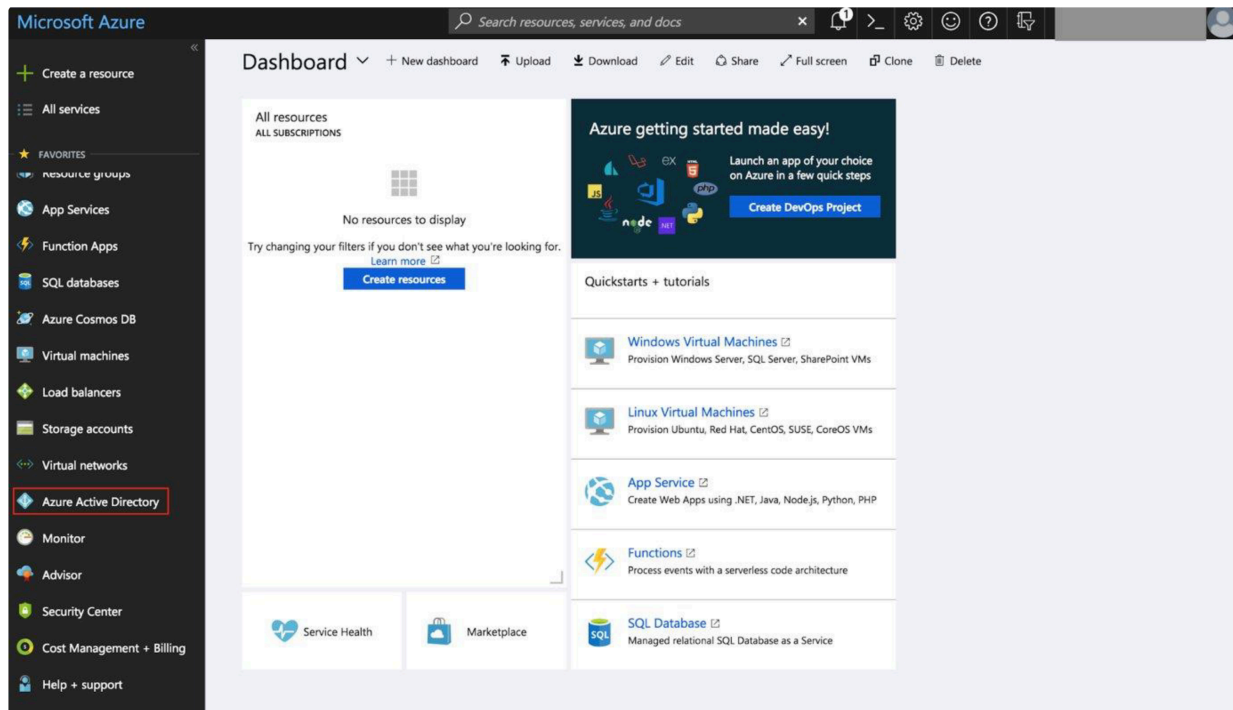


Store your ACS endpoint and your Entity ID somewhere as they will be required when creating the SAML application in Azure AD.

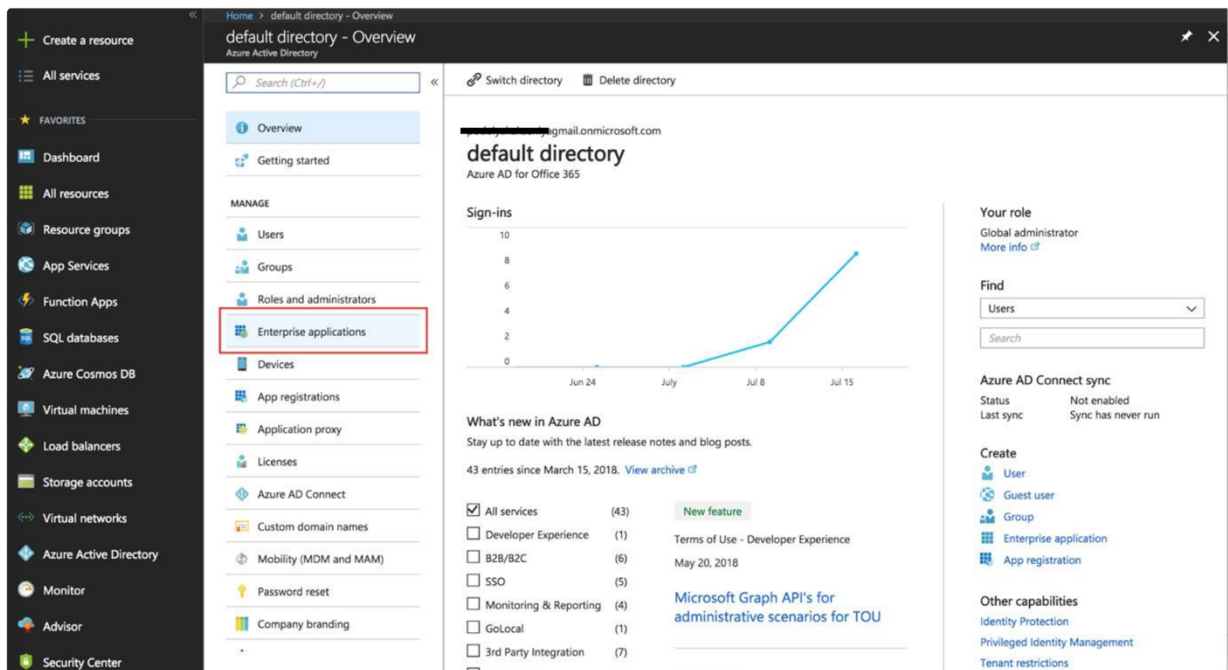
Create an Azure AD enterprise application and set up Azure AD identity provider to the Cognito User Pool

If you don't have access to Azure AD, you can skip this section and raise a ticket to team responsible for your Identity Provider. They will ask you the **Entity ID** and the **ACS endpoint** you recovered from the previous steps. When they send you the XML file, go to the [next section of this guide](#).

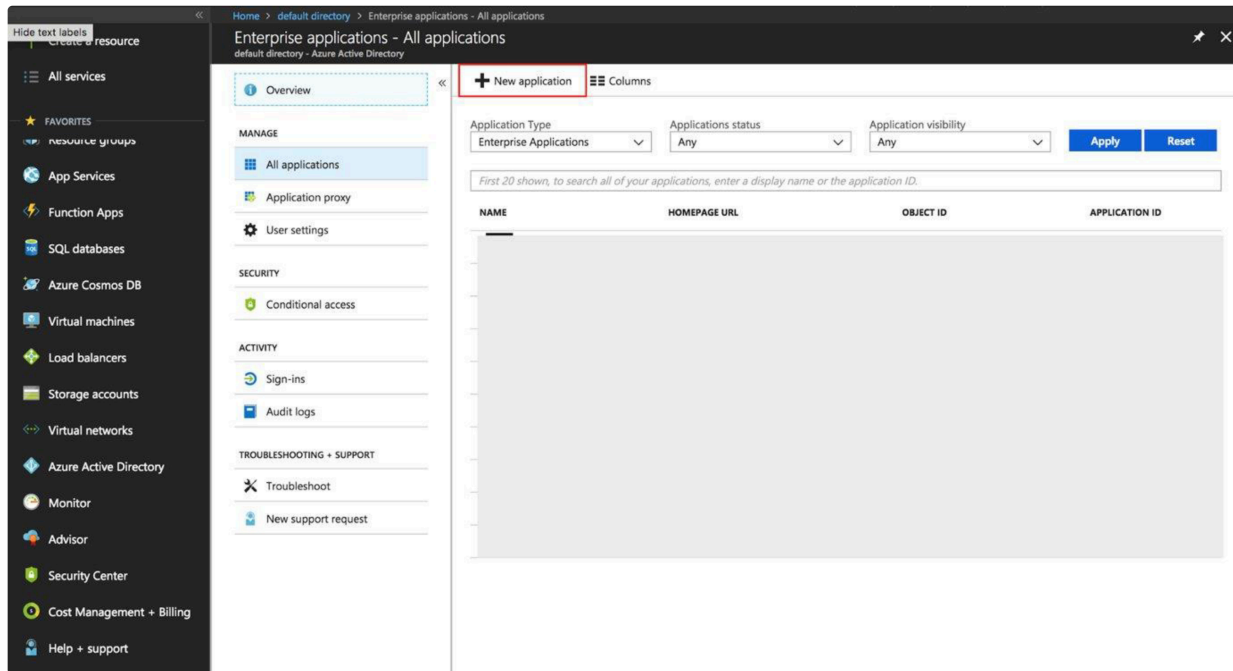
Open Azure Portal, on the right side menu choose **Azure Active Directory**.



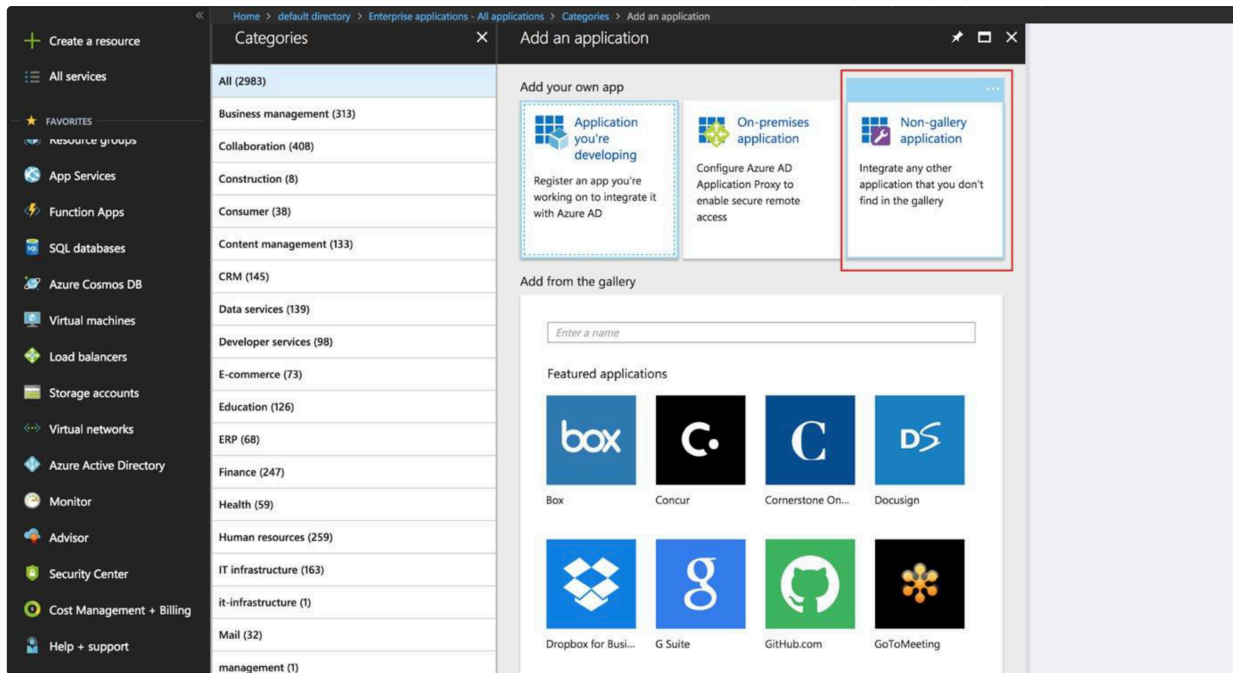
In Active Directory menu choose **Enterprise applications**:



In opened section choose **New Application**:

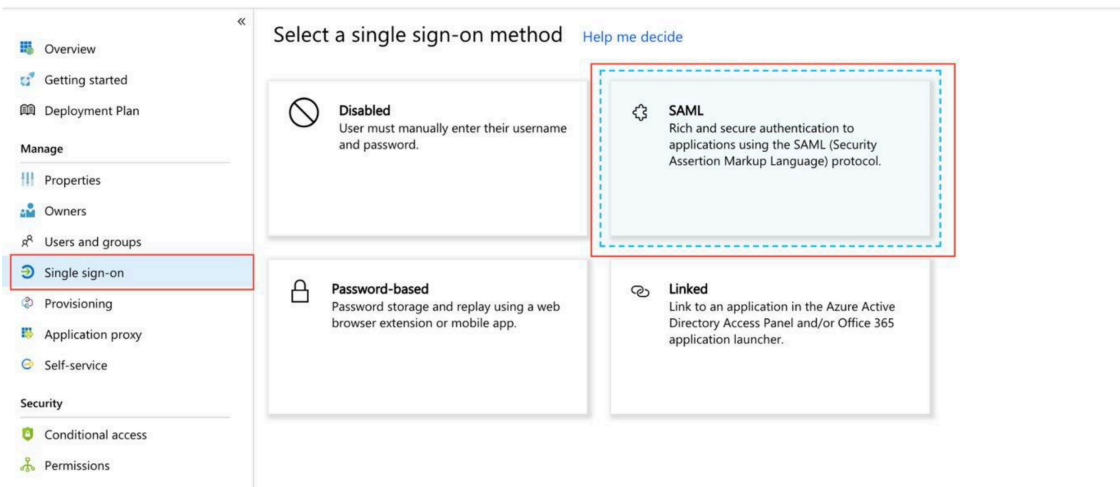


Pick **Non-gallery application** type for your application:



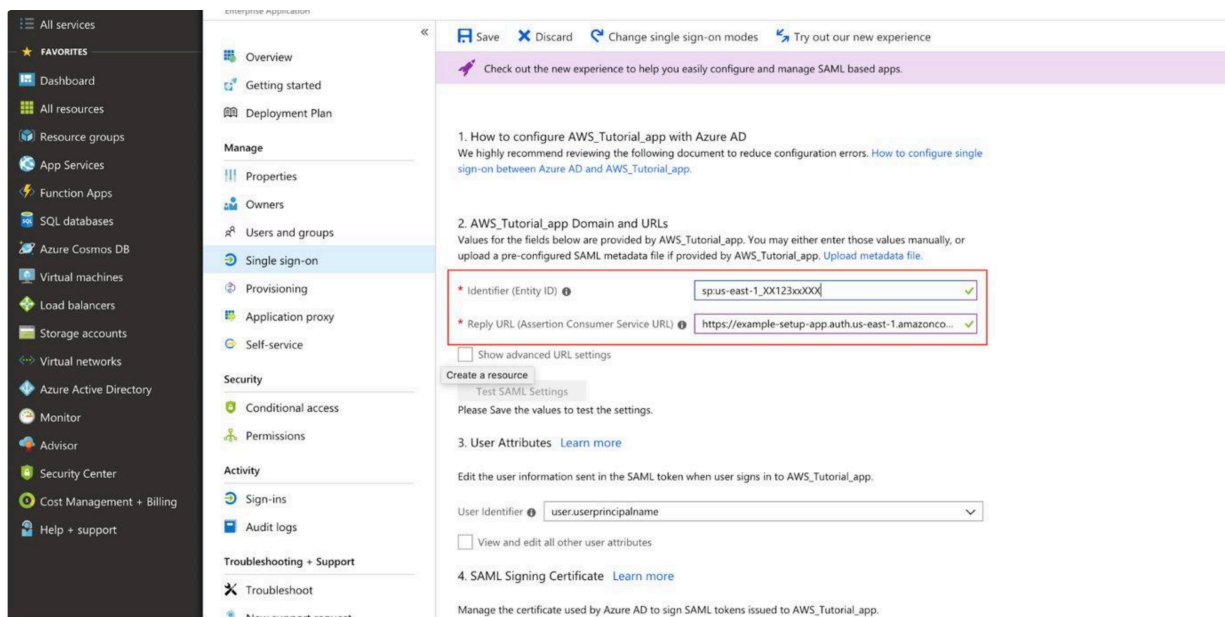
Type the name of your application and press **Add**. Now your application is created and it is time to connect it to AWS User Pool.

In your Azure AD enterprise application choose section **Single sign-on**, in dropdown list choose **SAML-based Sign-on**:



In section **Domain and URLs**, set the following information (refer to previous section of this document) :

- **Identifier** : This is your Cognito Entity ID - urn:amazon:cognito:sp:<yourUserPoolID>
- **Reply URL** : This is the link from where your Azure AD application expects to receive the authentication link token. This is your Cognito ACS - https://<yourDomainPrefix>.auth.<region>.amazoncognito.com/saml2/idpresponse



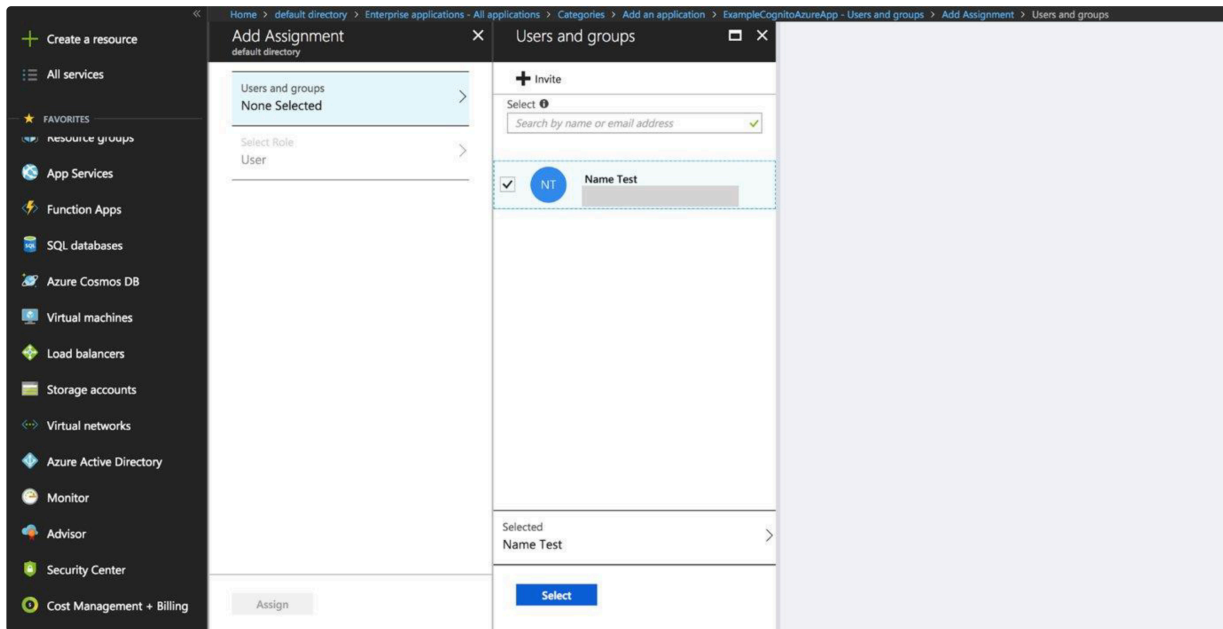
Save your changes and **download SAML File**:

The screenshot shows the Azure portal interface for configuring an application. The left sidebar contains various service categories, with 'Single sign-on' highlighted in red. The main content area shows the configuration for 'ExampleCognitoAzureApp - Single sign-on'. Under the '4. SAML Signing Certificate' section, there is a table with columns for STATUS, EXPIRATION, THUMBPRINT, and DOWNLOAD. The 'DOWNLOAD' column contains three links: 'Certificate (Base64)', 'Certificate (Raw)', and 'Metadata XML'. The 'Metadata XML' link is circled in red, and a red arrow points to it with the text 'Your SAML file'. Below the table, there is a 'Create new certificate' section and a 'Notification Email' field.

For later tests, you can start adding Users to your application. In Azure AD select **Enterprise applications** and choose your application. Select **Users and groups**, then **Add user**.

The screenshot shows the Azure portal interface for adding users to an application. The left sidebar contains various service categories, with 'Users and groups' highlighted in red. The main content area shows the configuration for 'ExampleCognitoAzureApp - Users and groups'. At the top, there is a '+ Add user' button highlighted in red, along with 'Edit', 'Remove', and 'Update Credentials' options. Below this, there is a search bar and a table with columns for DISPLAY NAME, OBJECT TYPE, and ROLE ASSIGNED. The table currently shows 'No application assignments found'.

Invite new users or select from existing. These users will be able to login with this Azure AD account to your application. When you'll finish adding a user select **Assign**.

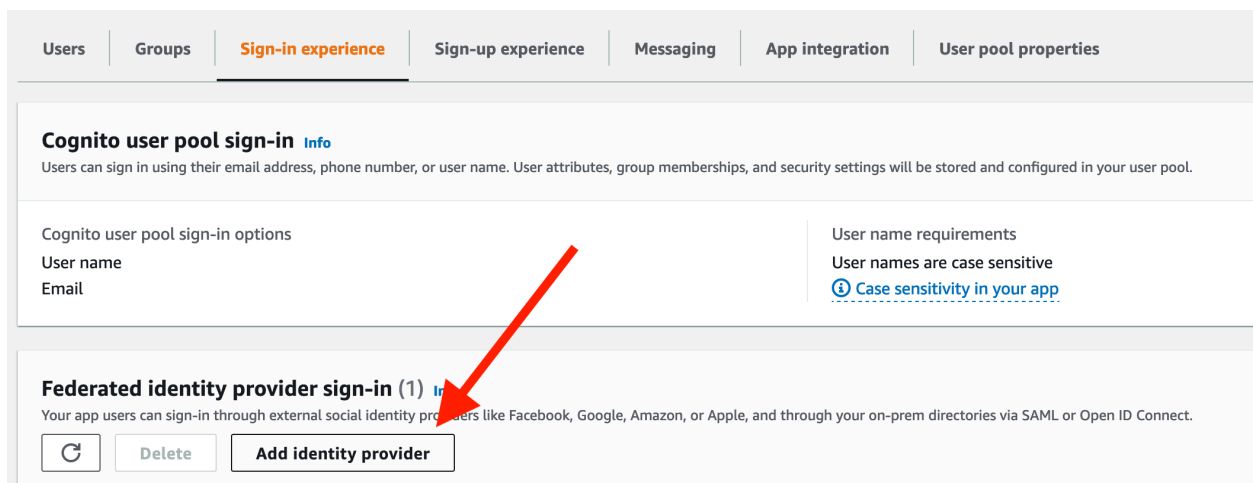


This is all settings in the Azure portal. At the end of this section you should have:

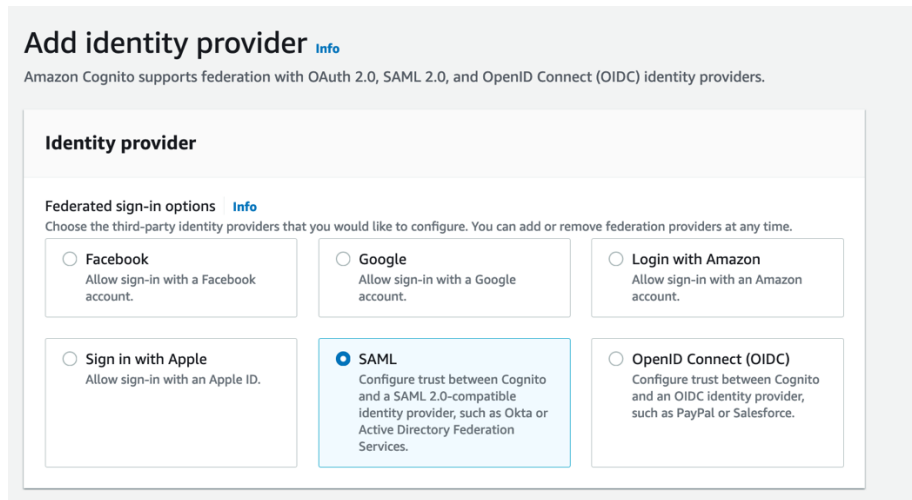
- SAML file with XML format
- user(s) to login

Configure federation in Amazon Cognito

We will now integrate Azure AD with Cognito. To enable federation from Amazon Cognito side, go to the **Sign-in Experience** tab in the Amazon Cognito console and select **Add Identity Providers**.



Select SAML



Under Metadata document, select the **metadata xml file that you got** at the end of the previous section. Next add **Provider Name - "ADTest"** for example

The screenshot shows the 'Set up SAML federation with this user pool' page in Amazon Cognito. The page title is 'Set up SAML federation with this user pool'. Below the title, there are several sections:

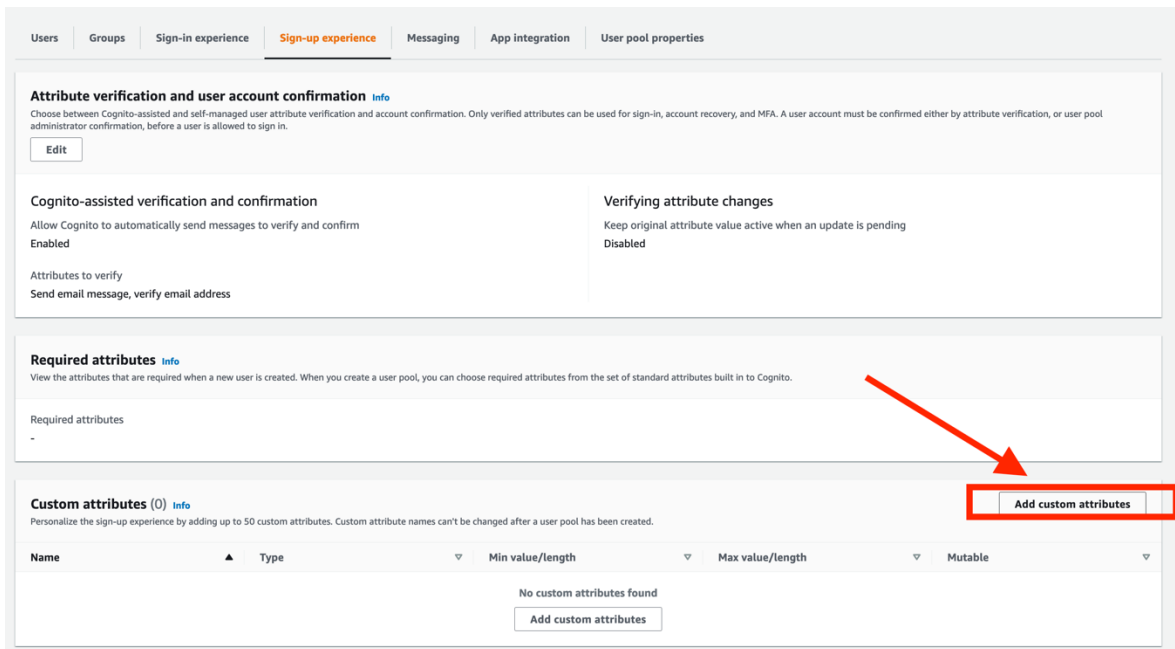
- Provider name** (Info): Enter a friendly name for your SAML 2.0 identity provider. The input field contains 'ADTest'.
- Identifiers - optional** (Info): Enter identifiers for this provider. Identifiers can be used to redirect users to the correct IdP in multitenant apps. The input field is empty and contains the placeholder text 'Enter identifiers'.
- Sign-out flow** (Info): Add sign-out flow. Enable simultaneous sign-out from the SAML provider and Cognito.
- Metadata document source** (Info): Provide a SAML metadata document. This document is issued by your SAML provider. It includes the issuer's name, expiration information, and keys that can be used to validate the response from the identity provider. Upload metadata document. Enter metadata document endpoint URL.
- Metadata document** (Info): . Must be an XML document using a UTF-8 character set.
- Map attributes between your SAML provider and your user pool** (Info): Your required attributes are mapped to the equivalent SAML attributes. Each attribute you add must be mapped to a SAML attribute. No mappings available.

Attribute Mapping - mapping identity provider attributes to user pool attributes

In order to collect the right user information from federated users, you need to map user attributes from external identity providers to the corresponding attributes for Cognito User Pools.

Step 1: Add "groups" custom attribute in you Amazon Cognito User Pool

We first need to create a new custom attribute to capture **Groups** from Azure AD. Under **Sign-up experience**, select **Add custom attributes**



The screenshot shows the Amazon Cognito console interface. The 'Sign-up experience' tab is selected. The 'Custom attributes' section is highlighted with a red box, and a red arrow points to the 'Add custom attributes' button. The console shows the following sections:

- Attribute verification and user account confirmation**: Includes an 'Edit' button and a description of verification options.
- Cognito-assisted verification and confirmation**: Includes a description and a toggle for 'Enabled'.
- Verifying attribute changes**: Includes a description and a toggle for 'Disabled'.
- Required attributes**: Includes a description and a list of required attributes.
- Custom attributes (0)**: Includes a description and a table with columns for Name, Type, Min value/length, Max value/length, and Mutable. The table is currently empty, and there is an 'Add custom attributes' button below it.

Name the new custom attributes "groups" with minimum length 1 and maximum length 2048 (should set to highest as this is immutable later on), check mutable and save.

Custom attributes

Personalize the sign-up experience by adding up to 50 custom attributes. Custom attribute names can't be changed after a user pool has been created.

Name	Type	Min - optional	Max - optional	Mutable
groups	String	1	2048	<input checked="" type="checkbox"/>

Name must be 20 characters or fewer.

Length must be 2048 bytes or fewer.

Length must be 2048 bytes or fewer.

[Add another](#)

You can add 49 more custom attributes

⚠ Custom attributes can't be renamed or deleted after you create them. Amazon Cognito prepends "custom:" to custom attribute names.

Cancel [Save changes](#)

Step 2: Map identity provider attributes to user pool attributes

Under the **Sign-In** tab in the Amazon Cognito console, select the ADTests identity provider and go to the **Attribute Mapping** section.

You will now define the mapping between attributes of the user pool and those from the SAML response received from the customer side.

Select your Identity Provider Name, and map the following attributes: <http://schemas.microsoft.com/ws/2008/06/identity/claims/groups>

SAML Attribute	User pool attribute
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	email
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	custom:groups

Attribute mapping (2) [Info](#) Edit

View, add, and edit attribute mappings between SAML and your user pool.

< 1 > ⚙

User pool attribute	SAML attribute
custom:groups	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
email	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Metadata document [Info](#)

View and update your SAML metadata. This document is issued by your SAML provider. It includes the issuer's name, expiration information, and keys that can be used to validate the response from the identity provider.

[Replace metadata](#) [Summary](#) [XML](#)

Metadata document source [Upload metadata document](#)

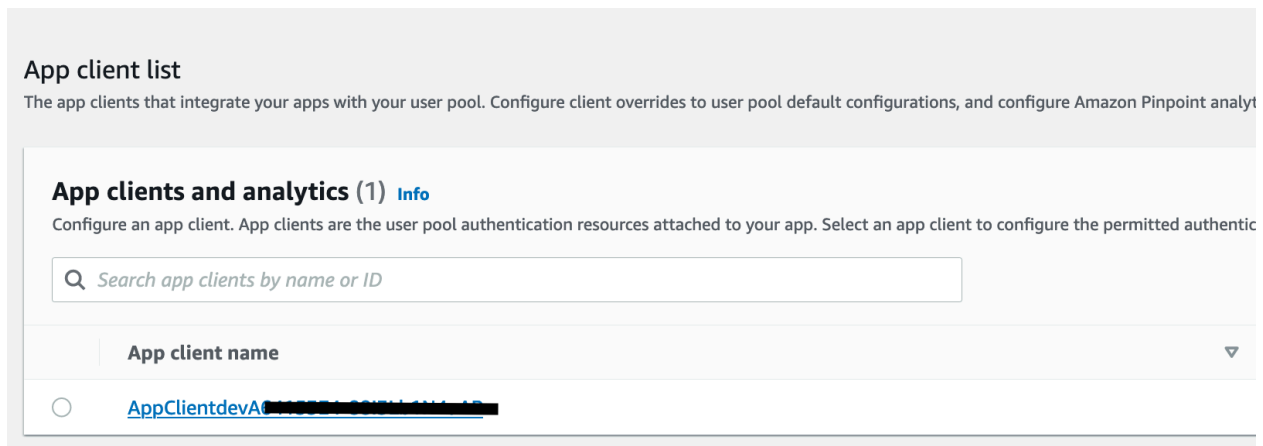
Metadata document [metadata.xml](#)

You can map other attributes if required. You will find each available **SAML Attribute** in the XML file.

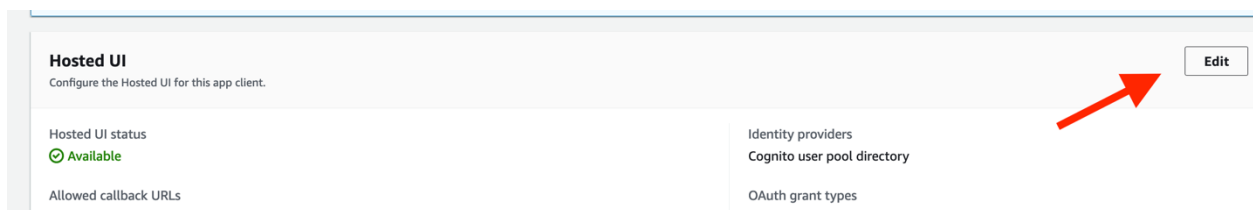
Register the identity Provider in you App Client Settings

During its deployment, data.all already creates an app client in your Cognito User Pool. Each of your app clients can use different identity providers and OAuth 2.0 settings. You must enable at least one identity provider for each app client. By default, the app client created by data.all uses Cognito User Pool to authenticate. This has to be changed to Azure AD federation.

Go to the **Application Integration** tab in the Amazon Cognito console and in the **App client settings** section, click in the hyperlink of the app client.



Under **Hosted UI**, click on Edit.



In the Identity providers section, **uncheck Cognito User Pool** and **check the Identity Provider Name** (ADTest in our example) you have created in this guide.

That's all settings which you should do in AWS console and Azure portal. You can now test your set-up.

Testing your setup

You can easily test your setup when opening data.all. On the login page, you should see the name of Identity Provider you created. Click on it to login.

If you do not already have an active session opened in your browser, this redirects you to an authentication portal. Use your usual credentials to connect to Data.all.

Inside data.all, create a new organization to check that attribute mapping worked as expected. This is what you need to verify:

- **Email address** : displayed when clicking your initial at the top right of the screen
- **Groups** : When creating an Organization in data.all, you can indicate a group. Check that you can select any group you are part of in your Azure AD environment.