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 and Amazon Cognito domain. To build you Azure AD application that will integrate with the Cognito User Pool, you will need to provide two things:

• <u>Assertion Consumer Service (ACS) endpoint</u> - 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.

Amazon Cognito	×	Amazon Cognito > User pools > dataall-dev-userpool				Switch back to the old console
User pools Federated identities						Delete user pool
		User pool overview				
		User pool name dataall-dev-userpool User pool ID D eu-west-1	ARN arr:aws:cognito-idp:eu-west-1:	iserpool/eu	Created time April 19, 2022 at 13:42 GMT+2 Last updated time April 19, 2022 at 13:42 GMT+2	
		Getting started			~	
		Configuration for all app clients Domain and resource server settings for the user pool. All app clients that cable	the Hosted UI use the user pool domain. All app clients co	an authorize access to user	pool resource servers.	
		Domain Info Configure a domain for your Hosted UI and OAuth 2.0 endorsets. You must clone. Actions	oose a domain if you need Cognito to create Hosted UI au	uthentication endpoints. If y	you have an existing domain, you must de	lete it before assigning a new
		Cognito domain Domain D https://fataaildeveuwestanting.auth.eu-west-1.ama	Zoncognito.com -	domain		

• <u>Entity ID</u> - 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.

Amazon Cognito > User pools > dataall-dev-userpool dataall-dev-userpool info
User pool overview
User pool name dataall-dev-user fol User pool ID D eu-west-1

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 <u>next section of this guide</u>.



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

In Active Directory menu choose Enterprise applications:

«	Home > default directory - Overview			
+ Create a resource	default directory - Overview Azure Active Directory			* ×
i∃ All services	Search (Ctrl+/) «	Switch directory		
+ FAVORITES	Overview	gmail.onmicrosoft.com		
🧮 Dashboard	Getting started	Azure AD for Office 365		
All resources	MANAGE	Sign-ins	Your role	
Resource groups	🔮 Users	10	Global admini More info 3	istrator
Services	🔐 Groups	8	Find	
Function Apps	Roles and administrators	4	Users	~
👼 SQL databases	Enterprise applications	2	Search	
🥒 Azure Cosmos DB	Devices	0 Jun 24 July	Jul 8 Jul 15 Azure AD Co	onnect sync
Virtual machines	App registrations	What's new in Azure AD	Status Last sync	Not enabled Sync has never run
💠 Load balancers	Licenses	Stay up to date with the latest release notes and blog post-	s. Create	
Storage accounts	Azure AD Connect	43 entries since March 15, 2018. View archive C ²	Super User	er
• Virtual networks	Custom domain names	All services (43) New feature	Group	
Azure Active Directory	Ø Mobility (MDM and MAM)	B2B/B2C (6) May 20, 2018	Developer Experience Enterprise	stration
Monitor	Password reset	SSO (5) Monitoring & Reporting (4)	iraph API's for Other capab	bilities
💠 Advisor	Company branding	GoLocal (1) administrat	ive scenarios for TOU Identity Protect	ction
Security Center		3rd Party Integration (7)	Privileged Iden Tenant restric	tions

In opened section choose **New Application**:

Hide text labels	Home > default directory > Enterprise applicat Enterprise applications - All app default directory - Azure Active Directory	tions - All applications Dlications	_				* >
i≘ All services	Overview «	+ New application	E Columns				
	MANAGE	Application Type Enterprise Applicatio	ns 🗸	Applications status	Application visibility Any	~	Apply Reset
App Services	All applications	First 20 shown to se	arch all of your a	nolications enter a display r	name or the application ID		
Eurotion Apps	Application proxy	NAME	aren an or your o	HOMEPAGE URL	OBJECT ID		APPLICATION ID
	User settings				0010110		
SQL databases	SECURITY	10					
Azure Cosmos DB	Conditional access	-					
Virtual machines	ACTINITY	5					
💠 Load balancers	a Sign inc	2-					
Storage accounts	Audit loos	-					
Virtual networks	- Autorioga	14					
Azure Active Directory	TROUBLESHOOTING + SUPPORT						
Monitor	X Troubleshoot	100					
🔷 Advisor	New support request	2-					
Security Center		-					
Cost Management + Billing							
 Hala i sunnart 							

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

"	Home > default directory > Enterprise applications - All ap	pplications > Categories > Add an app	olication	
+ Create a resource	Categories ×	Add an application		* = >
i Ξ All services	All (2983)	Add your own app		
- 🛨 FAVORITES	Business management (313)	Application	On-premises	Non-gallery
Resource groups	Collaboration (408)	you're developing	application	application
App Services	Construction (8)	Register an app you're	Configure Azure AD Application Proxy to	Integrate any other application that you don't
🤣 Function Apps	Consumer (38)	working on to integrate it with Azure AD	enable secure remote access	find in the gallery
📓 SQL databases	Content management (133)			
🬌 Azure Cosmos DB	CRM (145)	Add from the gallery		
Virtual machines	Data services (139)			
Load balancers	Developer services (98)	Enter a name		
	E-commerce (73)	Featured applications		
Storage accounts	Education (126)	Burney		
Virtual networks	ERP (68)	box	C • C	DS
Azure Active Directory	Finance (247)			
Monitor	Health (59)	Box Con	cur Cornerstone On	Docusign
🗬 Advisor	Human resources (259)			
Security Center	IT infrastructure (163)		Q ()	22
Ost Management + Billing	it-infrastructure (1)		0	
Help + support	Mail (32)	Dropbox for Busi G Su	uite GitHub.com	GoToMeeting
A State of	management (1)			

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**:

Overview	·····
Getting started Deployment Plan Manage	Disabled User must manually enter their username and password. SAML Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.
 Properties Owners Users and groups 	
Single sign-on	
 Provisioning Application proxy Self-service 	Password-based Password-based browser extension or mobile app. Password storage and replay using a web browser extension or mobile app. Password password password Directory Access Panel and/or Office 365 application launcher.
Security	
 Conditional access Permissions 	

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>
- <u>Reply URL</u>: This is the link from where your Azure AD application expects to receive the authentication link token. This is your Cogntio ACS https://<yourDomainPrefix>.auth.<region>.amazoncognito.com/saml2/idpresponse

· · · · · · · · · · · · · · · · · · ·	Enterprise Application	
= All services	«	E Save X Discard C Change single sign-on modes 5 Try out our new experience
- 🗙 FAVORITES	u Overview	
🔤 Dashboard	Getting started	Check out the new experience to help you easily configure and manage SAML based apps.
All resources	Deployment Plan	
📦 Resource groups	Малала	1. How to configure AWS_Tutorial_app with Azure AD
Services		We highly recommend reviewing the following document to reduce configuration errors. How to configure single sign-on between Azure AD and AWS_Tutorial_app.
Function Apps	· Owner	
📓 SQL databases	Users and groups	2. AWS_Tutorial_app Domain and URLs
🬌 Azure Cosmos DB	Single sign-on	Values for the fields below are provided by AWS_Tutorial_app. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by AWS_Tutorial_app. Upload metadata file.
Virtual machines	Provisioning	
🚸 Load balancers	Application provy	
Storage accounts	Self-senice	* Reply URL (Assertion Consumer Service URL) https://example-setup-app.auth.us-east-1.amazonco
💮 Virtual networks	o Sen-Service	Show advanced URL settings
Azure Active Directory	Security	Create a resource Test SAML Settings
Monitor	Conditional access	Please Save the values to test the settings.
🐢 Advisor	A Permissions	3. User Attributes Learn more
Security Center	Activity	Edit the user information sent in the SAML token when user signs in to AWS_Tutorial_app.
0 Cost Management + Billing	Sign-ins	Itea Identifiar A userusemininalname
Help + support	Audit logs	View and with all allow user statilization
	Troubleshooting + Support	view and contait oper atmostes
	X Troubleshoot	4. SAML Signing Certificate Learn more
	New support request	Manage the certificate used by Azure AD to sign SAML tokens issued to AWS_Tutorial_app.

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

Microsoft Azure		🔎 Search resources, services, and docs 🛛 🗴 🗳 ڬ 🔞 😨 🕢 🕀	0
+ Create a resource	me > default directory > Enterprise applicatio xampleCognitoAzureApp - Sing terprise Application	ns - All applications > Categories > Add an application > ExampleCognitoAzureApp - Single sign-on le sign-on 2	• >
i∃ All services	Getting started «	F Save X Discard	
★ FAVORITES (۹₽) Resource groups	MANAGE	Add attribute 4. SAML Signing Certificate Learn more	
🔇 App Services	Properties	Manage the certificate used by Azure AD to sign SAML tokens issued to ExampleCognitoAzureApp.	
Function Apps	DeploymentPlan	App Federation Metadata Url https://login.microsoftonline.com/	
SQL databases	R ^Q Users and groups	STATUS EXPIRATION THUMBPRINT DOWNLOAD	
🦉 Azure Cosmos DB	Single sign-on	Active 7/17/2021 Certificate (Raw)	
Virtual machines	Provisioning	Create new certificate	
🚸 Load balancers	Application proxy	Your SAMI file	
Storage accounts	G Self-service	Show advanced certificate signing settings Learn more	
↔ Virtual networks st	ECURITY	* Notification Email 0	
Azure Active Directory	Conditional access	5 ExampleCognitoAzureApp Configuration	
Monitor	Rermissions	ExampleCognitoRatureApp must be configured to use Azure AD as a SAML identity provider. Click below to view instructions on how to do this.	
🗣 Advisor 🛛	CTIVITY		
Security Center	Sign-ins	Configure ExampleCognitoAzureApp	
O Cost Management + Billing	Audit logs		

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**.

*	Home > default directory > Enterprise applicat	ions - All applications > Categories > Add an application > ExampleCognitoAzureApp - Users and groups	
+ Create a resource	ExampleCognitoAzureApp - Use Enterprise Application	*	×
i≣ All services	😴 Getting started «	+ Add user Add user I Call X Remove II Update Credentials	
+ FAVORITES	MANAGE	The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →	
🔇 App Services	Properties	DISPLAY NAME SUCCESSIONED	
Function Apps	E DeploymentPlan	No application assignments found	
SQL databases	Owners		
🥒 Azure Cosmos DB	 Osers and groups Single sign-on 		
Virtual machines	Provisioning		
🚸 Load balancers	B Application proxy		
Storage accounts	G Self-service		
↔ >> Virtual networks	SECURITY		
Azure Active Directory	O Conditional access		
Monitor	A Permissions		
🜪 Advisor	ΑCTIVITY		
Security Center	∋ Sign-ins		
Ocost Management + Billing	Audit logs		

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**.

**************************************	Home > default directory > Enterprise	applications - All a		tion > ExampleCogn	oAzureApp - Users and gro	oups > Add Assignment >	Users and groups
+ Create a resource	Add Assignment	×	Users and groups	□ ×			
i∃ All services	Users and groups		🕂 Invite				
- * FAVORITES	None Selected	>	Select ① Search by name or email address	~			
Resource groups	Select Role User	>					
Services	200000		Name Test				
Sunction Apps							
SQL databases							
🬌 Azure Cosmos DB							
Virtual machines							
💠 Load balancers							
Storage accounts							
💮 Virtual networks							
Azure Active Directory							
Monitor							
🐢 Advisor			Selected Name Test	>			
Security Center							
Ost Management + Billing	Assign		Select				

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

- <u>SAML file with XML format</u>
- 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

Id identity provide zon Cognito supports federation wit	Г Info h OAuth 2.0, SAML 2.0, and OpenID Conne	ect (OIDC) identity providers.
dentity provider		
ederated sign-in options Info hoose the third-party identity providers the	at you would like to configure. You can add or rer	nove federation providers at any time.
Facebook Allow sign-in with a Facebook account.	 Google Allow sign-in with a Google account. 	 Login with Amazon Allow sign-in with an Amazon account.
 Sign in with Apple Allow sign-in with an Apple ID. 	 SAML Configure trust between Cognito and a SAML 2.0-compatible identity provider, such as Okta or Active Directory Federation Services. 	OpenID Connect (OIDC) Configure trust between Cognito and an OIDC identity provider, such as PayPal or Salesforce.

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

Enter a friendly name fo	r your SAML 2.0 identity provider.
ADTest	
Identifiers - optional Enter identifiers for this	Info provider. Identifiers can be used to redirect users to the correct IdP in multitenant apps.
Enter identifiers	
Separate each identifier	by a comma
Sign-out flow Info	
Add sign-out flow	v
Enable simultaneou	sign-out from the SAML provider and Cognito.
Enable simultaneou Metadata document Provide a SAML metada and keys that can be use	s sign-out from the SAML provider and Cognito. source Info ta document. This document is issued by your SAML provider. It includes the issuer's name, expiration information, d to validate the response from the identity provider.
Enable simultaneou Metadata document Provide a SAML metada and keys that can be use O Upload metadata	s sign-out from the SAML provider and Cognito. source Info ta document. This document is issued by your SAML provider. It includes the issuer's name, expiration information, ed to validate the response from the identity provider. I document
Enable simultaneou Metadata document Provide a SAML metada and keys that can be use Upload metadata Enter metadata c	s sign-out from the SAML provider and Cognito. source Info ta document. This document is issued by your SAML provider. It includes the issuer's name, expiration information, ed to validate the response from the identity provider. document locument URL
Enable simultaneou Metadata document Provide a SAML metada and keys that can be use Upload metadata Enter metadata c Metadata document	s sign-out from the SAML provider and Cognito. source Info ta document. This document is issued by your SAML provider. It includes the issuer's name, expiration information, ed to validate the response from the identity provider. I document locument endpoint URL Info
Enable simultaneou Metadata document Provide a SAML metada and keys that can be uss O Upload metadata Enter metadata c Metadata document Choose file	s sign-out from the SAML provider and Cognito. source Info ta document. This document is issued by your SAML provider. It includes the issuer's name, expiration information, d to validate the response from the identity provider. document locument Info Info

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 "saml.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**

Users Groups S	Sign-in experience	Messaging App integration User pool properties		
Attribute verification and user account confirmation info Choose between Copito-assisted and self-managed user attribute verification and account confirmation. Only verified attributes can be used for sign-in, account recovery, and MFA. A user account must be confirmed either by attribute verification, or user pool administrator confirmation, before a user is allowed to sign in. Edit				
Cognito-assisted veri Allow Cognito to automatic Enabled Attributes to verify Send email message, verify	fication and confirmation tally send messages to verify and confirm remail address	Verifying attribute changes Keep original attribute value active when an update is pending Disabled		
Required attributes View the attributes that are required attributes	Info ulired when a new user is created. When you create a r	user pool, you can choose required attributes from the set of standard attributes built in to Cognito.		
Custom attributes (0 Personalize the sign-up experier) Info nce by adding up to 50 custom attributes. Custom att	ribute names can't be changed after a user pool has been created.	stom attributes	
Name	▲ Туре	v min value/length v Max value/length v Mutable No custom attributes found Add custom attributes	~	

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

Personalize the sign- peen created.	JUTES -up experience by add	ling up to 50 custom attr	ributes. Custom attribu	te names can't be changed after a user pool has
lame	Туре	Min - optional	Max - optional	Mutable
saml.groups	String 🔻	1	2048	
Name must be 20 characters or ewer.		Length must be 2048 bytes or fewer.	Length must be 2048 bytes or fewer.	
Add another	e custom attributes			
Custom at	tributes can't be re attribute names.	enamed or deleted af	ter you create them	. Amazon Cognito prepends "custom:"

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:<u>http://schemas.microsoft.com/ws/2008/06/identity/claims/groups</u>

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 View, add, and edit attribute mappings between SAML and your u	ser pool.	Edit	
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 단		

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.

App client list The app clients that integrate your apps with your user pool. Configure client overrides to user pool default configurations,	and configure Amazon Pinpoint analyt
App clients and analytics (1) Info Configure an app client. App clients are the user pool authentication resources attached to your app. Select an app client Q Search app clients by name or ID	nt to configure the permitted authentic
App client name	∇

Under Hosted UI, click on Edit.

Hosted UI Configure the Hosted UI for this app client.	Edit
Hosted UI status	Identity providers Cognito user pool directory
Allowed callback URLs	OAuth grant types

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 you 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.