

Home > Management & Governance

Setting up a cross-account federation between Amazon Connect and Azure AD using AWS SSO.

26 November 2021 - 6 min. read



In these times, delivering support using multiple communication channels is crucial for a business.

There are already big players in the contact center business, but Amazon Connect is an interesting option to evaluate. It's fully managed, easily scalable, and with an aggressive pricing placement on the market.

Embedded Artificial Intelligence and Machine Learning enable the business to perform sentiment analysis and gain valuable insights.

Every customer has different needs, sometimes leading to unexplored paths in system integration.

In this article, we'll describe a cross-account federation between Amazon Connect, and Azure AD using AWS SSO.

Scenario Overview

A customer wanted to configure an Amazon Connect instance federating their existing users on Office365 (using the underlying Azure Active Directory service) to keep centralized user management. Another requisite was to have a separate AWS account for the service, to let only some administrators manage services on the account. Amazon Connect can connect to Active Directory and use it for identity management, but you'll need to use AWS Directory Service. Sometimes it's better to leverage existing Identity providers.

AWS SSO was our service of choice because of the flexibility it offers in configuring SAML applications and account access. As a bonus, we also were able to grant different access levels to multiple AWS accounts using single-sign-on.

As you'll see in this article Amazon Connect doesn't have a native integration with AWS SSO, so we need to configure an application and use it as an identity provider in the destination account.

In this article, we will:

- Configure AWS SSO on the Organization master account to trust Azure Active Directory (used by Office365) to authenticate users
- Configure an Amazon Connect instance with SAML authentication into a different account belonging to the AWS organization (internal-services)
- Create and configure an AWS SSO SAML application for Amazon Connect
- Configure an Identity Provider on the internal-services account to trust the SAML application for cross-account authentication
- Add the required roles in the internal-service account to authenticate federated users
- Test the configuration

AWS SSO Setup

Log into the Azure Active Directory admin center

Select "Enterprise Applications"



Select "Create your own application" and give it a unique name

Dashboard > Enterprise applications >
Browse Azure AD Gallery
+ Create your own application ① Request new gallery app 🖗 Got feedback?
() You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience. $ o$
The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SS
Create your own application $\qquad \qquad \qquad$
☆ Got feedback?
If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.
What's the name of your app?
proud2becloud-article-sso
What are you looking to do with your application?
O Configure Application Proxy for secure remote access to an on-premises application
O Register an application to integrate with Azure AD (App you're developing)
Integrate any other application you don't find in the gallery (Non-gallery)

After a little while the application will be ready, we need to set-up **Single sign-on**, click on the menu and then select "**SAML**"

Assessment > Emerginse	apparations > trouse store so dately > productied on a rice so			
proud2bec	loud-article-sso Single sign-on			
Enterprise Application				
Cverview	Single sign on (SSO) adds security and convenience when	n users sign on to applications in Azure Active Directory by enabl	bling a user	
Deployment Plan	in your organization to sign in to every application they u credential is used for all the other applications they need	use with only one account. Once the user logs into an application I access to. Learn more.	n, that	
Aanage				
Properties	Select a single sign-on method	Help me decide		
Owners				
Roles and administrate	rs (Proview)	A		
Users and groups	Single sign-on is not enabled. The user	Rich and secure authentication to anninations using the SAMI. Genuity	Password storage and replay using a web trouger anternion or mobile ann	Link to an application in My Apps
Single sign-on	My Apps.	Assertion Markup Language) protocol.		
Application proxy				
Self-service				
iecurity				
Conditional Access				
Permissions				
Token encryption				
and a local sector of the				
a servery				
Sign-in logs				
 Sign-in logs Usage & insights 				
 Sign-in loga Usage & insights Audit logs 				
Sign-in logs Sign-in logs Sign-in logs Audit logs Provisioning logs Access reviews				
Sign-in loga Sign-in loga Usage & insights Audit loge Provisioning loga Access reviews				
Sign-in loga Sign-in loga Usage & Insights Audit logs Audit logs Action loga Access reviews	SAML Signing Certificate			/ Edit
 Sgin in logis Sgin in logis Utuge & ineights Audit logis Provisioning logis Receis reviews 	SAML Signing Certificate			🖉 Edit
Sign-in loga Sign-in loga 4 Audit loga 4 Audit loga 5 Throwisening loga 5 Access reviews	SAML Signing Certificate	Active		🖉 Edit
Spohlbar Spohlbar Barbing Audit Nay Providence Day Access reviews	SAML Signing Certificate Status Thumbprint	Active 50A68CB78BDC03	3EB77CD46E34D05920B4F2A87	🖉 Edit
Spinis loga Spinis loga Mark Singles Access releas 3	SAML Signing Certificate Status Thumbprint Expiration	Active 50A68CB78BDC03 11/11/2024,4:55:	3EB77CD46E34D05920B4F2A87 22 PM	🖉 Edit 43
Sport loga Sport loga 1 Usage & Insights 2 Audit Nogi Providening loga Access reviews 3	SAML Signing Certificate Status Thumbprint Expiration Notification Email	Active 50A68CB788DC0 11/11/2024, 4:55 damiano.giorgi@	3EB77CD46E34D05920B4F2A87 -22 PM besharp.it	🖉 Edit 43
g gan big i tage & mights i add tage i Add tage i Anderson i	SAML Signing Certificate Status Thumbprint Expiration Notification Email App Federation Metadata Url	Active 50A68CB78BDC0 11/11/2024, 4:55: damiano.giorij@ https://login.mik	3EB77CD46E34D05920B4F2A87 22 PM besharp.it crosoftonline.com/20f03cc3-84	 ✓ Edit 43 11
3 gran bag. i taga A maida A wala taga I - hadarang laga I - hadarang laga A cata stelens	SAML Signing Certificate Status Thumbprint Expiration Notification Email App Federation Metadata Url Certificate (Base64)	Active 50A68CB78BDC0: 11/11/2024, 4:55: damiano.giorgi@ https://login.mic Download	3EB77CD46E34D05920B4F2A87 22 PM besharp.it crosoftonline.com/20f03cc3-84	2 Edit 43 11 10
3 graph to bag is course for independent is course for independent is course for independent is course of independent	SAML Signing Certificate Status Thumbprint Expiration Notification Email App Federation Metadata Url Certificate (Base64) Certificate (Base64)	Active 50A68CB78BDC0 11/11/2024, 4:55: damiano.giorgi@ https://login.mic Download Download	3EB77CD46E34D05920B4F2A8; 22 PM besharp.it crosoftonline.com/20f03cc3-84	2 Edit 43 1F D
 Japa Is kaj, Lapa Kandara, Landaragi baja Anata Naja Nata Naja<!--</td--><td>SAML Signing Certificate Status Thumbprint Expiration Notification Email App Federation Metadata Url Certificate (Base64) Certificate (Raw) Evelopation Metadata XMI</td><td>Active 50A68CB78BDC0: 11/11/2024,4:55: damiano.giorgi@ https://login.mid Download Download</td><td>3EB77CD46E34D05920B4F2A87 22 PM besharp.it crosoftonline.com/20f03cc3-84</td><td>2 Edit 43 11 D</td>	SAML Signing Certificate Status Thumbprint Expiration Notification Email App Federation Metadata Url Certificate (Base64) Certificate (Raw) Evelopation Metadata XMI	Active 50A68CB78BDC0: 11/11/2024,4:55: damiano.giorgi@ https://login.mid Download Download	3EB77CD46E34D05920B4F2A87 22 PM besharp.it crosoftonline.com/20f03cc3-84	2 Edit 43 11 D

Click on the Download link for "**Federation Metadata XML**" and store the file in a secure place, don't share this file with anyone !

Assign users to the SSO application to enable them



Log in into the **AWS Organizations management** account for and select "**AWS Single Sign On**"



If you previously configured AWS SSO you can change your identity source or configure a new one on the "Settings" page.

Identity source						
Your identity source is where you administer your 2.0-compatible identity provider (IdP), or Active D	r users and grou birectory (AD). Le	ps, and where AWS earn more	SSO authenticates y	vour users. You ca	n choose between A	WS SSO, SAML
Id	entity source	AWS SSO Chang	e			
A	uthentication	AWS SSO				
Pro	visioning 🚯	AWS SSO				
Identit	y store ID 🚯	d-93670984fa 🖧				
Attributes for acces	ss control 🚯	Disabled Enable				
Change identity source					1	2
Choose where your identities a	re source	h		Choos	e identity source	Review
Your identity source is the place where you admi source to access AWS accounts, roles, and appl	nister and authe ications. Learn I	enticate identities. Yo more	ou use AWS SSO to	o manage permis	sions for identities fr	om your identity
 AWS SSO You will administer all users, groups, credent 	ials, and multi-f	actor authentication	assignments in AW	/S SSO. Users si	gn in through the AV	VS SSO user portal.
Active Directory You will administer all users, groups, and cre AWS Managed Microsoft AD or AD Connect	dentials in AWS or. Users sign in	6 Managed Microsof h through the AWS u	AD, or you can co ser portal.	nnect AWS SSO	to your existing Activ	ve Directory using
 External identity provider You will administer all users, groups, credent page to access the AWS SSO user portal, as 	ials, and multi-f ssigned account	actor authentication ts, roles, and applica	in an external ident tions.	tity provider (IdP)	. Users sign in throu	gh your IdP sign-in
Configure external identity p	rovider					
AWS SSO works as a SAML 2.0 compliant s you must establish a SAML trust relationship users, the users must first be provisioned int manually from the Users page, or by using th Service provider metadata	ervice provider by exchanging o AWS SSO bet ne automatic pro	to your external ider meta data between fore you can assign ovisioning option in t	tity provider (IdP). your IdP and AWS permissions to AWS ne Settings page at	To configure your SSO. While AWS S accounts and re fter you complete	IdP as your AWS S SSO will use your esources. You can e this wizard. Learn n	SO identity source, IdP to authenticate ither provision users nore
Your identity provider (IdP) requires the follor paste, or type this information into your IdP's your IdP.	wing AWS SSO service provide	certificate and meta er configuration inter	data details to trust ace, or you may do	AWS SSO as a sownload the AWS	service provider. You SSO metadata file a	a may copy and and upload it into
AWS SSO SAML metadata	Download me	tadata file				
s	how individual r	netadata values				
Identity provider metadata						
AWS requires specific metadata provided by manually, or upload a metadata exchange file	your identity pre that you down	ovider (IdP) to estab load from your IdP.	lish trust. You may	copy and paste fi	rom your IdP, type th	ne metadata in
IdP SAML metadata*	proud2becloud	-article-sso.xml	Browse			
If	you don't have	a metadata file, you	can manually type	vour metadata va	alues	

Select "External identity provider", download the metadata file and, as previously,

store it in a secure place. Upload the metadata file you downloaded from the Azure SAML application page

Go back to the Azure Active Directory Administration Console and click on "**upload metadata file**"

Dashboard > proud2becloud-article-sso	>
proud2becloud-article-s	sso SAML-based Sign-on
	$\overline{\uparrow}$ Upload metadata file $~~$ Change single sign-on mode $~$ §

Select the file downloaded from the AWS Console and proceed.

We just exchanged the required configuration information to federate Azure Active Directory users with AWS SSO.

Back on the Azure Console you can try the application, you should now be able to login with your current Azure Active Directory credentials.

Dashboard > proud2becloud-article-sso			Test single sign-on with proud2becloud-article-sso
proud2becloud-article- Enterprise Application	sso SAML-based Sign-on –		R Got fredback?
~	🕴 Upload metadata file 🌱 Change single sign-on	node 📕 Test this application	
 Overview Deployment Plan 	Set up Single Sign-On with SAML		Monotone control to the second sec
Manage	An SSO implementation based on federation protocols in	nproves security, reliability, and end u	
Properties	implement. Choose SAML single sign on whenever possi more.	ble for existing applications that do n	Testing sign in
A Owners	Read the configuration guide of for help integrating pro	ud2becloud-article-sso.	Test the single sign-on configuration for proud/2becloud-article-sso by signing in here. Ensure that you have configured both the Azure Active Directory configuration and proud/2becloud-article-sso itself.
Roles and administrators (Preview)	0		
Users and groups	Basic SAML Configuration		Select a way to test sign in Sion in as current user
Single sign-on	Identifier (Entity ID)	https://eu-west-1.signin.aws.amazon 4.025700844	Sign in as someone else (requires browser extension)
Provisioning	Reply URL (Assertion Consumer Service URL)	https://eu-west-1.signin.aws.amazon	Test sign in
Application proxy	Sign on URL	acs/dbb006d1-2f7d-4079-b66d-621a Optional	

If you assign AWS accounts and different applications to your users you should be able to see them

			Q Search
AWS Account (6)	SSO Client VPN	SSO Client VPN Self Service	
internal-services #.	abesharo.it		~
besharp- # @	besharp.it		~
# besnarp-	@besharp.it		~
e besharn-			
#	@besharp.it		~
esharp-			
#	@besharp.it		Ý
📦 beSharp-			č
#.	@besharp.it		
ms of Lisa			Rowarad by an

You can also enable **auto-provisioning** for users and enable selected groups to access your AWS accounts.

Amazon Connect Setup

We'll use a different AWS account (**internal-services**) to configure Amazon Connect. With SSO and Organizations we can enable fine-grained access to different teams and isolate duties.

On the internal-service account search for "Amazon Connect" and click on "Create new instance".

Select "**SAML 2.0-based authentication**" for identity management and assign a name to your instance.

Once you set an authentication mechanism in Amazon Connect you can't change it.

iei	tity management
0	Store users in Amazon Connect
	Create and manage users in Amazon Connect. You cannot share users with other applications.
0	Link to an existing directory
	Amazon Connect uses an existing directory. You create users in the directory, and then add and configure them in Amazon Connect. You can only associate a directory with only one Amazon Connect Instance. Learn more 📝
0	SAML 2.0-based authentication
	AWS supports identity federation with Security Assertion Markup Language (SAML 2.0). This feature enables single sign-on (SSO) so users can log into the AWS Management Console or call the AWS APIs without you having to create an IAM user for everyone in your organization. Learn more 🖸
res	s (IR)
eate	a custom URL. Use this URL to log into this instance of Amazon Connect.
	the second block and second seco

Continue with the configuration wizard steps with your preferences.

In a matter of minutes, your amazon connect instance should be ready.



Please note: since Connect doesn't support user auto-provisioning you'll need to create a user with the same username you defined in Azure Active Directory

SSO Integration Setup

On the management account go back on the AWS SSO Console click on "Applications" and "Add a new Application", search for "**Amazon Connect**"

You can view instructions on this page and five the second	nd metadata details for your provider.	
etails		
Display name*	Proud2beCloud Amazon Connect	0
Description	Proud2beCloud Amazon Connect Application	e
	The description you type here does not appear in the SSO console and when using the AWS SSO APIs.	///. e user portal. However, it will be visible in the AWS
WS SSO metadata		
our cloud application may require the following certi	ficate and metadata details to recognize AWS SSO as	s the identity provider.
AWS SSO SAML metadata file	https://portal.sso.eu-west-1.amazonaws.com/san	Copy URL Download
AWS SSO sign-in URL	https://portal.sso.eu-west-1.amazonaws.com/san	Copy URL
AWS SSO sign-out URL	https://portal.sso.eu-west-1.amazonaws.com/san	Copy URL
AWS SSO issuer URL	https://portal.sso.eu-west-1.amazonaws.com/san	Copy URL
AWS SSO certificate	Download certificate	
pplication properties		
our cloud application may optionally take additional	settings to configure your user experience. Learn more	e
Application start URL		0
Relay state		
Session duration ^e	1 hour 👻	
pplication metadata		
WS SSO requires specific metadata about your clou schange file.	ad application before it can trust this application. You o	can type this metadata manually or upload a metada
Application ACS URL*	https://signin.aws.amazon.com/saml	θ
Application SAML audience*	um:amazon:webservices	
	If you have a metadata file, you can upload it now in	stead.

Give your application a name and, once again, download the metadata file. On the **internal-services** account, go to IAM and go in the "**Identity Providers**" section, click on "Add provider" and upload the metadata file

Add an Identity provider		
Configure provider		
Provider type		
SAML Establish trust between your AWS account and a SAML 2.0 compatible identity Provider such as Shibboleth or Active Directory Federation Services.		
Provider name Enter a meaningful name to identify this provider		
Proud2beCloudAmazonConnect		
Maximum 128 characters. Use alphanumeric or '' characters.		
Metadata document This document is issued by your IdP.		
Add tags (Optional) Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.		
No tags associated with the resource.		
Add tag You can add up to 50 more tags		
	Cancel	Add provider

IAM > Identity providers > Create Identity Provider

Setup roles

Once the identity provider has been created we'll need to setup the necessary roles and policies to let SSO users access the service

On the internal-services account go to IAM -> Roles and create a new Role. Select

"**SAML 2.0 federation**" for the type of trusted identity and choose the identity provider you have just created.

Create role		1 2 3 4
Select type of trusted entity		
AWS service EC2, Lambda and others	Inother AWS account Cognito or any OpenID Cognito or any OpenID provider	SAML 2.0 federation Your corporate directory
Allows users that are federated with SAML 2.0 to a	ssume this role to perform actions in your account. Learn more	
Choose a SAML 2.0 provider		
If you're creating a role for API access, choose an a attributes.	Attribute and then type a Value to include in the role. This restricts a	access to users with the specified
SAML provider	Proud2beCloudAmazonConnect	
	Create new provider C Refresh	
	Allow programmatic access only	
	 Allow programmatic and AWS Management Console access 	1
Attribute	SAML:aud 🔻	
Value*	https://signin.aws.amazon.com/saml	
Condition	Add condition (optional)	

Create a new policy to let the role get a "Federation Token" from the Amazon Connect instance, use this json template:

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
```

```
"Sid": "Statement1",
    "Effect": "Allow",
    "Action": "connect:GetFederationToken",
    "Resource": [
    "arn:aws:connect:region:Account-id:instance/amazoncon
nectintanceid/user/${aws:userid}"
    ]
    }
}
```

You can find the instance id by clicking on the connect instance and copying the last part of the "**Instance ARN"** field, use the internal-services accountid and the connect region for the remaining fields:

Distribution settings			
Instance ARN arraws:connect:eu-central-1: b df8e Directory proud2becloud-connect-article	instance/a0d	f8-	Service-linked role MWSServiceRoleForAmazonConnect_VBRfGrEG4g2CDH5aGVdW [2] Laam more [2]

Once the appropriate role and policy have been created we can go back to the AWS SSO Console on the management account to modify the Connect application to finish the configuration.

Edit the configuration, leave the "**Application start UR**L" field blank, for "**Relay state**" use:

https://region.console.aws.amazon.com/connect/federate/amazonconnectid

Details		
Display name*	Proud2beCloud Amazon Connect	0
Description	Proud2beCloud Amazon Connect Application	
	The description you type here does not appear in the SSO console and when using the AWS SSO APIs.	/// user portal. However, it will be visible in the AWS
AWS SSO metadata		
/our cloud application may require the following certi	ficate and metadata details to recognize AWS SSO as	the identity provider.
AWS SSO SAML metadata file	https://portal.sso.eu-west-1.amazonaws.com/san	Copy URL Download
AWS SSO sign-in URL	https://portal.sso.eu-west-1.amazonaws.com/san	Copy URL
AWS SSO sign-out URL	https://portal.sso.eu-west-1.amazonaws.com/sam	Copy URL
AWS SSO issuer URL	https://portal.sso.eu-west-1.amazonaws.com/sam	Copy URL
AWS SSO certificate	Download certificate	
Application properties		
our cloud application may optionally take additional	settings to configure your user experience. Learn mon	8
Application start URL		0
Relay state	https://eu-central-1.console.aws.amazon.com/cor	
Session duration*	12 hours 👻	
WS SSO requires specific metadata about your clou exchange file.	ud application before it can trust this application. You c	an type this metadata manually or upload a metada
Application ACS URL*	https://signin.aws.amazon.com/saml	0
Application SAML audience*	um:amazon:webservices	
	If you have a metadata file, you can upload it now ins	tead.

Go to "Attribute Mappings" and add a new mapping:

Set https://aws.amazon.com/SAML/Attributes/Role as "User attribute in the application" field and

arn:aws:iam::internal-services-account-id:saml-provider/saml-provider-

name,arn:aws:iam::internal-services-account-id:role/amazon-connect-federation-role

for the "Maps to this string value or user attribute in AWS SSO" field.

Assigned users SAML assertions successfully updated. tributes you map here become part of the SAML assertion that is sent to the application. You can choose which user attributes in your applications are attributes in your connected directory. Learn more User attribute in the application Maps to this string value or user attribute in AWS SSO Format	tion map
SAML assertions successfully updated. Inducts you map here become part of the SAML assertion that is sent to the application. You can choose which user attributes in your applica rresponding user attributes in your connected directory. Learn more User attribute in the application Maps to this string value or user attribute in AWS SSO Format	: ation man
tributes you map here become part of the SAML assertion that is sent to the application. You can choose which user attributes in your application greeponding user attributes in your connected directory. Learn more ser attribute in the application Maps to this string value or user attribute in AWS SSO Format	ation map
Subject \$(user.email) persistent	•
https://aws.amazon.com/SAMU/A \$(user.email) unspecified	•
https://aws.amazon.com/SAMU/A am.aws.iam:::sami-provider/Proud2beCloudAmazonConn unspecified	•

Save changes and on the "Assigned users"tab assign users to the Proud2beCloud Amazon Connect application

Testing

Go to your SSO start url (usually https://youdefinedname.awsapps.com/start/)and login with your Azure AD/Office365 credentials, you'll find the Amazon Connect Application.



Clicking on it will take you to the Amazon Connect dashboard with your credentials.

\$	Amazon Connect	damiano.giorgi@besharp.it	G•	🖨 English 🛛	r.	?
::	Dashboard			Hide	the gui	ide
ш	Configuration guide					

That's it! Your Amazon Connect instance now uses Azure AD to validate user credentials

A cross-account scenario isn't always easy to troubleshoot but with this tutorial, you should be able to get it running in a couple of minutes

Now you can configure Amazon Connect, if you are not able to access your instance using SSO check the IDP provider, configured role, policies, and mappings.

Have you faced any particular use case? Feel free to leave your thoughts in the comments!

And see you again in 14 days on Proud2beCloud!



Damiano Giorgi

Ex on-prem systems engineer, lazy and prone to automating boring tasks. In constant search of technological innovations and new exciting things to experience. And that's why I love Cloud Computing! At this moment, the only "hardware" I regularly dedicate myself to is that my bass; if you can't find me in the office or in the band room try at the pub or at some airport, then!

Copyright © 2011-2021 by beSharp srl - P.IVA IT02415160189