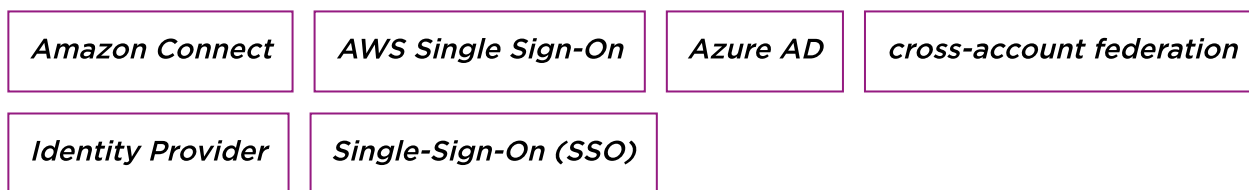


# Federazione cross-account tra Amazon Connect e Azure AD con AWS SSO

26 Novembre 2021 - 5 min. read



Per le aziende è diventato molto importante essere in grado di utilizzare differenti canali di comunicazione con i propri clienti, specialmente per fornire loro supporto.

Nel mercato dei servizi di contact center, in cui esistono già aziende affermate da tempo, Amazon Connect è una alternativa interessante da prendere in considerazione: è interamente gestito, facilmente scalabile e con un costo competitivo rispetto ai competitor sul mercato..

L'intelligenza artificiale abbinata agli algoritmi di machine learning rende possibile la sentiment analysis permettendo al business di ottenere informazioni di valore dai propri utenti.

Ogni cliente ha esigenze differenti che, a volte, ci portano a provare integrazioni tra servizi inusuali e non presenti nelle guide ufficiali.

In questo articolo descriveremo come siamo riusciti a configurazione una federazione cross-account fra Amazon Connect e Azure AD mediante l'uso di AWS SSO.

## Use Case

Per un nostro cliente è emersa l'esigenza di configurare Amazon Connect affinché fosse possibile per gli utenti esistenti su Office365, contenuti quindi in una istanza

Azure Active Directory, autenticarsi. L'altro requisito era di mantenere il servizio in un account AWS separato, per permettere ad un gruppo ristretto di utenti la gestione di Amazon Connect ed altri servizi.

Amazon Connect permette l'utilizzo di AWS Managed Microsoft AD ma, per realizzare la soluzione, abbiamo sfruttato gli Identity Provider aziendali già configurati.

La nostra scelta è ricaduta quindi su AWS SSO. Oltre ad essere molto flessibile nella configurazione di applicazioni SAML, offre la possibilità di implementare il single-sign-on sugli account AWS.

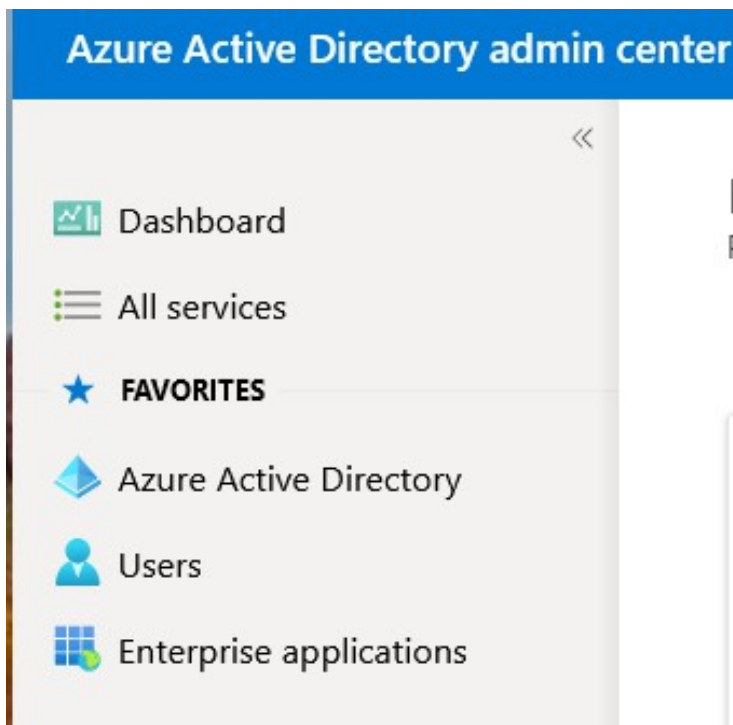
Come vedremo in questo articolo, Amazon Connect non consente di implementare direttamente l'integrazione nativa con AWS SSO. Dovremo quindi configurare un'applicazione SAML ed usarla come identity provider nell'account di destinazione.

In questo articolo ci occuperemo di:

- Configurare AWS SSO nell'account master dell'organizzazione per utilizzare Azure Active Directory (usato da Office365) ed autenticare gli utenti
- Attivare una istanza Amazon Connect con autenticazione SAML in un account differente nella stessa organizzazione (chiamato internal-services)
- Creare e configurare un'applicazione SAML per Amazon Connect
- Configurare un identity provider nell'account internal-services per autorizzare l'applicazione SAML ed occuparsi dell'autenticazione cross-account
- Aggiungere i ruoli richiesti all'account internal-services per autenticare gli utenti federati
- Collaudare la configurazione

## **Configurazione di AWS SSO**

Per prima cosa occorre effettuare il login all'[admin center di Azure Active Directory](#) e selezionare "Enterprise Applications". Fare click su "Create your own application" e assegnare un nome univoco



[Dashboard](#) > [Enterprise applications](#) >

## Browse Azure AD Gallery

[+](#) Create your own application | [🕒](#) Request new gallery app | [🗨️](#) Got feedback?

**i** You're in the new and improved app gallery experience. [Click here to switch back to the legacy app gallery experience.](#) →

The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO)

## Create your own application

[🗨️](#) 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.

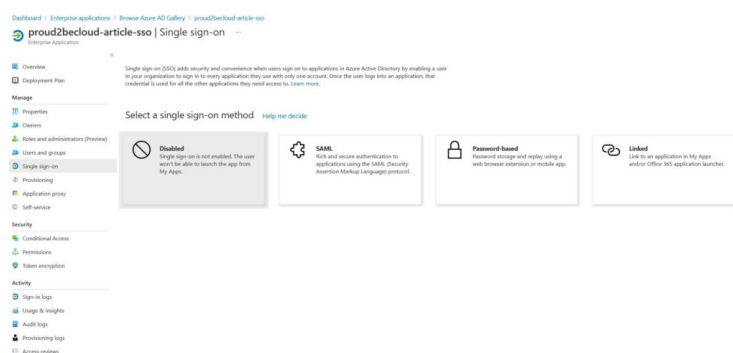
What's the name of your app?

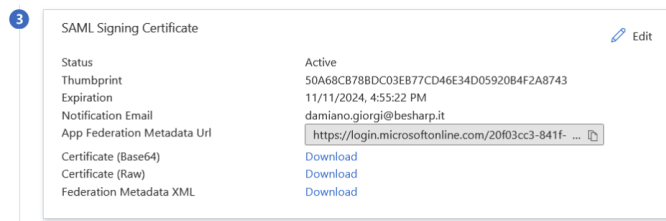
✓

What are you looking to do with your application?

- Configure Application Proxy for secure remote access to an on-premises application
- 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)

In breve tempo l'applicazione sarà disponibile. A quel punto sarà necessario impostare il **Single sign-on**: fare click sul menu e selezionare **“SAML”**

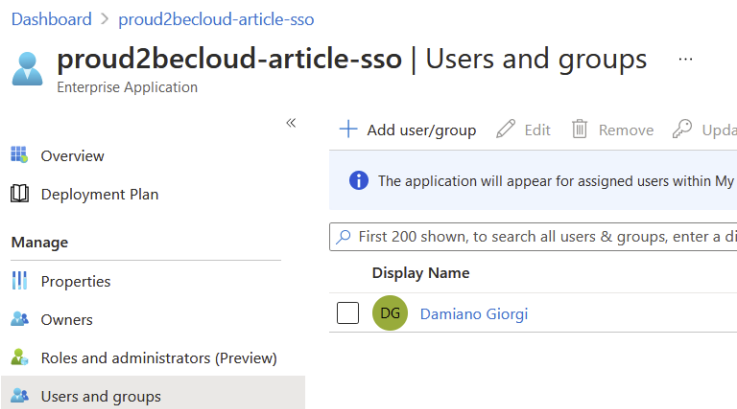




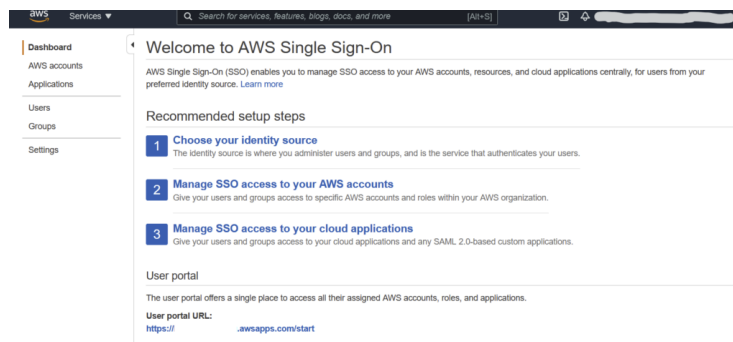
Fare click sul link **“Federation data XML”** e scaricare il file.

N.B.: il file non dovrà essere condiviso e andrà mantenuto al sicuro.

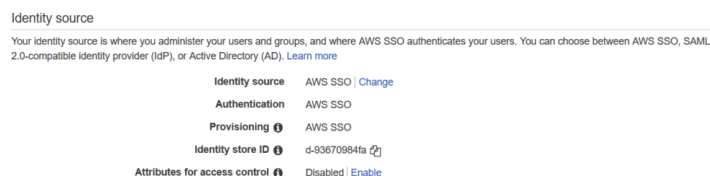
A questo punto è possibile assegnare gli utenti all’applicazione.



Terminata la configurazione dell’applicazione fare login sulla console AWS nell’account di management e selezionare il servizio **“Aws Single Sign on”**



Se AWS SSO è già stato configurato, è sempre possibile cambiare l’identity provider in uso sulla pagina **“Settings”**



## Choose where your identities are sourced

Your identity source is the place where you administer and authenticate identities. You use AWS SSO to manage permissions for identities from your identity source to access AWS accounts, roles, and applications. [Learn more](#)

- AWS SSO**  
You will administer all users, groups, credentials, and multi-factor authentication assignments in AWS SSO. Users sign in through the AWS SSO user portal.
- Active Directory**  
You will administer all users, groups, and credentials in AWS Managed Microsoft AD, or you can connect AWS SSO to your existing Active Directory using AWS Managed Microsoft AD or AD Connector. Users sign in through the AWS user portal.
- External identity provider**  
You will administer all users, groups, credentials, and multi-factor authentication in an external identity provider (IdP). Users sign in through your IdP sign-in page to access the AWS SSO user portal, assigned accounts, roles, and applications.

## Configure external identity provider

AWS SSO works as a SAML 2.0 compliant service provider to your external identity provider (IdP). To configure your IdP as your AWS SSO identity source, you must establish a SAML trust relationship by exchanging meta data between your IdP and AWS SSO. While AWS SSO will use your IdP to authenticate users, the users must first be provisioned into AWS SSO before you can assign permissions to AWS accounts and resources. You can either provision users manually from the Users page, or by using the automatic provisioning option in the Settings page after you complete this wizard. [Learn more](#)

## Service provider metadata

Your identity provider (IdP) requires the following AWS SSO certificate and metadata details to trust AWS SSO as a service provider. You may copy and paste, or type this information into your IdP's service provider configuration interface, or you may download the AWS SSO metadata file and upload it into your IdP.

AWS SSO SAML metadata

Download metadata file

Show individual metadata values

## Identity provider metadata

AWS requires specific metadata provided by your identity provider (IdP) to establish trust. You may copy and paste from your IdP, type the metadata in manually, or upload a metadata exchange file that you download from your IdP.

IdP SAML metadata\*

proud2becloud-article-ssso.xml

Browse...

If you don't have a metadata file, you can manually type your metadata values

Selezionare **“External identity provider”**, scaricare il metadata file e, come fatto in precedenza, conservarlo in un luogo sicuro.

A questo punto occorre fare upload del file di metadati scaricato dalla console Azure. Sulla console Azure Active Directory Administration fare click su **“upload metadata file”** utilizzando il file scaricato dalla console AWS

Dashboard &gt; proud2becloud-article-ssso &gt;

## proud2becloud-article-ssso | SAML-based Sign-on

Enterprise Application



Upload metadata file

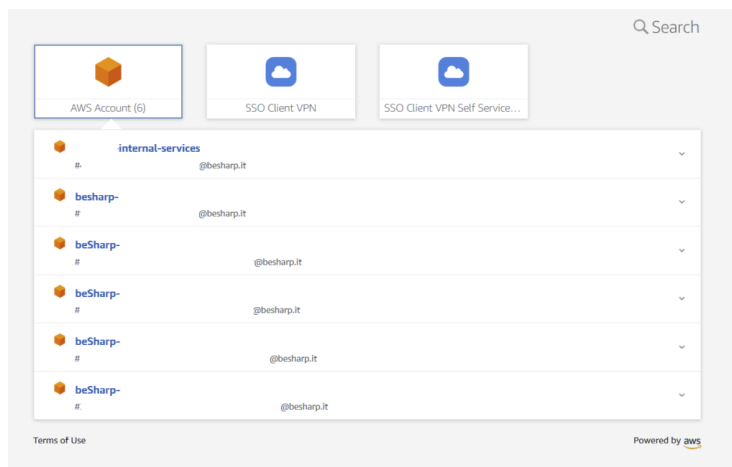


Change single sign-on mode

In questo modo, la configurazione della federazione fra Azure Active Directory e AWS SSO è stata portata a termine.

Sulla console Azure è possibile provare l'applicazione, simulando un login con le credenziali correnti.

Se sulla console AWS sono state già assegnate alcune applicazioni sarà possibile vederle ed utilizzarle.



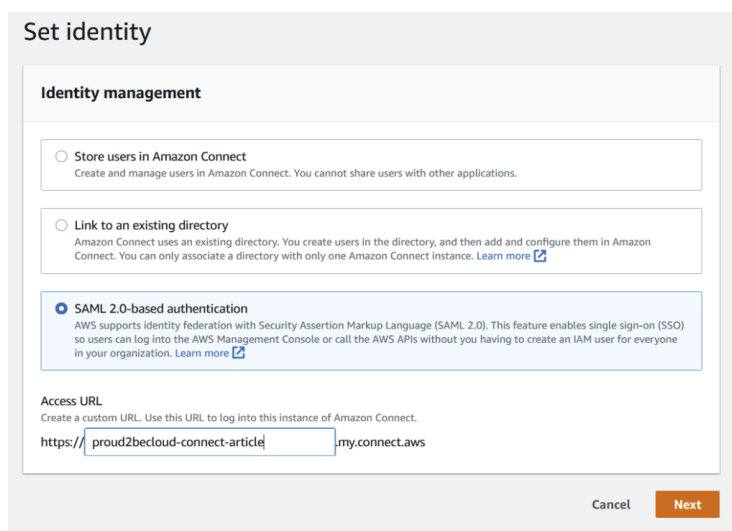
È possibile anche abilitare l'auto provisioning degli utenti ed assegnare gli utenti in modo che siano automaticamente importati su AWS SSO.

## Setup di Amazon Connect

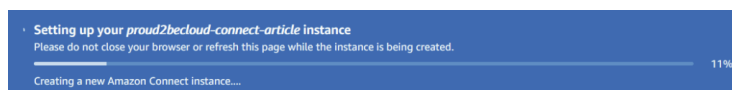
Utilizzeremo un account AWS differente (**internal-services**) per configurare Amazon Connect. Utilizzando AWS SSO e Organization saremo in grado di assegnare permessi molto granulari a differenti utenti e ruoli.

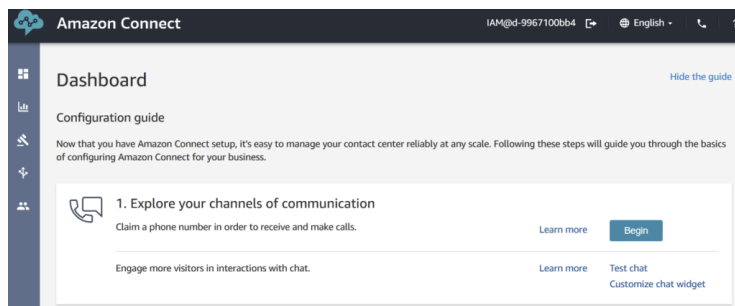
Sull'account internal-service alla sezione "Amazon Connect", fare click su "Create new instance".

Alla sezione "identity management", selezionare "**SAML 2.0-based authentication**". Una volta selezionato il tipo di autenticazione non sarà più possibile modificarlo.



A questo punto, nel wizard di configurazione, è possibile selezionare le opzioni preferite e procedere con la creazione. Il servizio dopo pochi minuti sarà pronto:





**Attenzione:** Amazon Connect non supporta il provisioning automatico degli utenti: è necessario creare un utente con lo stesso username definito in Azure Active Directory

## Integrazione Con SSO

Sulla console SSO dell'account di management fare click su "Applications" "Add a new Application", ricercando l'applicazione "**Amazon Connect**".

Configure Proud2beCloud Amazon Connect

AWS SSO works as an identity provider (IdP) for any SAML 2.0-compliant cloud applications. To configure this application for SSO access, you must establish a trust relationship between AWS SSO and your cloud application (service provider) through a SAML metadata exchange. You can view instructions on this page and find metadata details for your provider.

[View instructions](#)

Details

Display name\* Proud2beCloud Amazon Connect ⓘ

Description Proud2beCloud Amazon Connect Application

The description you type here does not appear in the user portal. However, it will be visible in the AWS SSO console and when using the AWS SSO APIs.

AWS SSO metadata

Your cloud application may require the following certificate and metadata details to recognize AWS SSO as the identity provider.

AWS SSO SAML metadata file	<input type="text" value="https://portal.sso.eu-west-1.amazonaws.com/saml"/>	<a href="#">Copy URL</a>	<a href="#">Download</a>
AWS SSO sign-in URL	<input type="text" value="https://portal.sso.eu-west-1.amazonaws.com/saml"/>	<a href="#">Copy URL</a>	
AWS SSO sign-out URL	<input type="text" value="https://portal.sso.eu-west-1.amazonaws.com/saml"/>	<a href="#">Copy URL</a>	
AWS SSO issuer URL	<input type="text" value="https://portal.sso.eu-west-1.amazonaws.com/saml"/>	<a href="#">Copy URL</a>	
AWS SSO certificate	<a href="#">Download certificate</a>		

Application properties

Your cloud application may optionally take additional settings to configure your user experience. [Learn more](#)

Application start URL

Relay state

Session duration\* 1 hour

Application metadata

AWS SSO requires specific metadata about your cloud application before it can trust this application. You can type this metadata manually or upload a metadata exchange file.

Application ACS URL\*

Application SAML audience\*

If you have a metadata file, you can upload it now instead.

\* Required fields

[Cancel](#) [Save changes](#)

Dopo aver assegnato un nome all'applicazione, fare click su "Download" alla sezione "AWS SSO SAML metadata file".

Nell'account **internal-services** selezionare il servizio IAM e, alla sezione "**Identity Providers**", fare click su "Add provider" e fare l'upload del metadata file appena caricato

## 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.

 OpenID Connect

Establish trust between your AWS account and Identity Provider services, such as Google or Salesforce.

## 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.

Choose file

File needs to be a valid UTF-8 XML document.

Amazon Connect\_ins-2393b1763b136ed4.xml

## 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

## Impostazione dei ruoli

Una volta creato l'identity provider è necessario creare i ruoli e le policy per fare in modo che gli utenti SSO riescano ad accedere al servizio. Nella console IAM dell'account internal-services fare click su Roles e "Create a new Role". Selezionare "SAML 2.0 federation" come tipo di trusted identity e selezionare l'identity provider appena creato.

## Create role

1 2 3 4

## Select type of trusted entity

AWS service  
EC2, Lambda and others
  Another AWS account  
Belonging to you or 3rd party
  Web identity  
Cognito or any OpenID provider
  SAML 2.0 federation  
Your corporate directory

Allows users that are federated with SAML 2.0 to assume 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 Attribute and then type a Value to include in the role. This restricts access to users with the specified attributes.

SAML provider: Proud2beCloudAmazonConnect

[Create new provider](#) [Refresh](#)

Allow programmatic access only  
 Allow programmatic and AWS Management Console access

Attribute: SAML:aud

Value\*: https://signin.aws.amazon.com/saml

Condition: [Add condition \(optional\)](#)

Creare una nuova policy per permettere al ruolo di ottenere un "Federation Token" dall'istanza Amazon Connect, utilizzando questo template json:

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

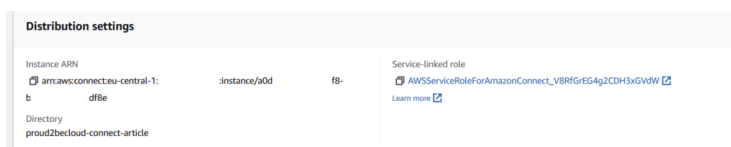


```

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

```

È possibile trovare il valore di “amazonconnectinstanceid” facendo click sull’istanza Connect e copiando l’ultima parte del campo “ARN” per **region:Account-id** utilizzare invece la region e l’id dell’account internal-service.



Terminata la creazione occorre tornare sulla console AWS SSO sull’account di management e modificare l’applicazione Connect per concludere la configurazione. Selezionare “Edit configuration” e lasciare vuoto il campo “**Application start URL**”. Per il campo “**Relay state**” utilizzare:

<https://region.console.aws.amazon.com/connect/federate/amazonconnectid>  
 inserendo i valori utilizzati in precedenza.

### Configure Proud2beCloud Amazon Connect

Details

**Display name\*** Proud2beCloud Amazon Connect ⓘ

**Description** Proud2beCloud Amazon Connect Application

The description you type here does not appear in the user portal. However, it will be visible in the AWS SSO console and when using the AWS SSO APIs.

---

**AWS SSO metadata**

Your cloud application may require the following certificate and metadata details to recognize AWS SSO as the identity provider.

**AWS SSO SAML metadata file** <https://portal.sso.eu-west-1.amazonaws.com/saml> [Copy URL](#) [Download](#)

**AWS SSO sign-in URL** <https://portal.sso.eu-west-1.amazonaws.com/saml> [Copy URL](#)

**AWS SSO sign-out URL** <https://portal.sso.eu-west-1.amazonaws.com/saml> [Copy URL](#)

**AWS SSO issuer URL** <https://portal.sso.eu-west-1.amazonaws.com/saml> [Copy URL](#)

**AWS SSO certificate** [Download certificate](#)

---

**Application properties**

Your cloud application may optionally take additional settings to configure your user experience. [Learn more](#)

**Application start URL** ⓘ

**Relay state** <https://eu-central-1.console.aws.amazon.com/cor>

**Session duration\*** 12 hours ▼

---

**Application metadata**

AWS SSO requires specific metadata about your cloud application before it can trust this application. You can type this metadata manually or upload a metadata exchange file.

**Application ACS URL\*** <https://signin.aws.amazon.com/saml> ⓘ

**Application SAML audience\*** urn:amazon:webservices

If you have a metadata file, you can upload it now instead.

---

\* Required fields [Cancel](#) [Save changes](#)

A questo punto alla sezione **“Attribute Mappings”** aggiungere un nuovo mapping, impostando <https://aws.amazon.com/SAML/Attributes/Role> come valore per il campo **User attribute in the application** e `arn:aws:iam::internal-services-account-id:saml-provider/saml-provider-name,arn:aws:iam::internal-services-account-id:role/amazon-connect-federation-role` come valore per il campo **“Maps to this string value or user attribute in AWS SSO”**

### Proud2beCloud Amazon Connect

Configuration for Proud2beCloud Amazon Connect has been saved. You can now review attribute mappings for this application.

Configuration | **Attribute mappings** | Assigned users

SAML assertions successfully updated.

Attributes you map here become part of the SAML assertion that is sent to the application. You can choose which user attributes in your application map to corresponding 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
Subject	\$(user.email)	persistent ▼
<a href="https://aws.amazon.com/SAML/A">https://aws.amazon.com/SAML/A</a>	\$(user.email)	unspecified ▼ ⓘ
<a href="https://aws.amazon.com/SAML/A">https://aws.amazon.com/SAML/A</a>	arn:aws:iam:: :saml-provider:Proud2beCloudAmazonConn	unspecified ▼ ⓘ

[Add new attribute mapping](#) [Save changes](#)

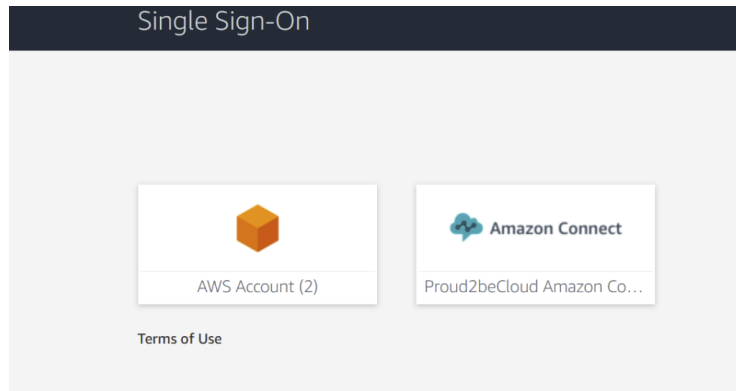
Una volta salvati i cambiamenti assegnare gli utenti utilizzando il tab **“Assigned users”**.

## Testing

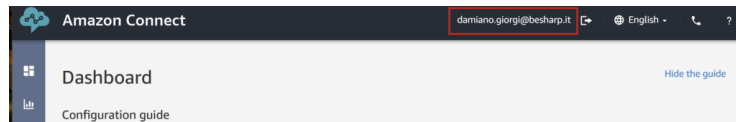
Utilizzare lo “start url” definito in amazon sso (solitamente <https://nomeimpostato.awsapps.com/start/> ) e fare login con le credenziali Azure

AD/Office365.

A questo punto l'applicazione Amazon Connect sarà disponibile.



Facendo click sull'applicazione sarà possibile utilizzare la dashboard di Amazon Connect con le credenziali corrette:



## Damiano Giorgi

Ex sistemista on-prem, pigro e incline all'automazione di task noiosi. Alla ricerca costante di novità tecnologiche e quindi passato al cloud per trovare nuovi stimoli. L'unico hardware a cui mi dedico ora è quello del mio basso; se non mi trovate in ufficio o in sala prove provate al pub o in qualche aeroporto!