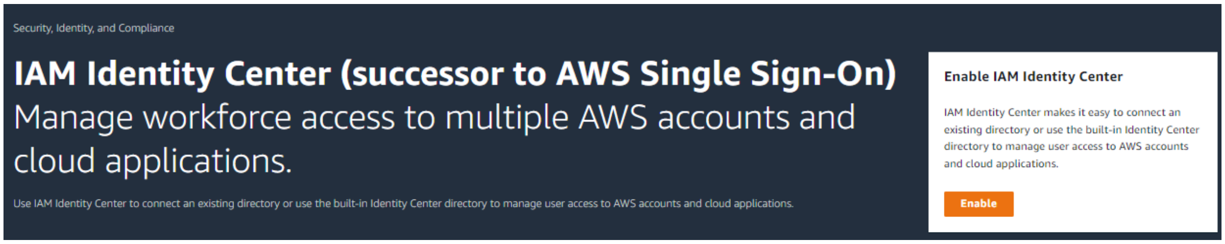
Step for Integration of AWS SSO with Azure AD

1. Enable AWS SSO:

Log in to the AWS Console with the AWS master account, then navigate to the AWS Single Sign-On console.

Verify the upper right corner of the AWS Management console to ensure that they are in the correct region.

If you access the Single Sign-On service for the first time in this region, you will be greeted with the welcome screen below. Select “Enable AWS SSO.”



Security, Identity, and Compliance

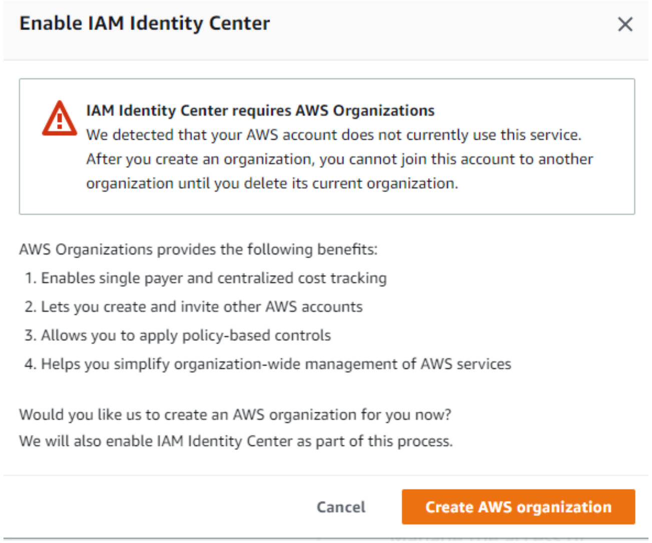
IAM Identity Center (successor to AWS Single Sign-On)

Manage workforce access to multiple AWS accounts and cloud applications.

Use IAM Identity Center to connect an existing directory or use the built-in Identity Center directory to manage user access to AWS accounts and cloud applications.

Enable IAM Identity Center

IAM Identity Center makes it easy to connect an existing directory or use the built-in Identity Center directory to manage user access to AWS accounts and cloud applications.



Enable IAM Identity Center

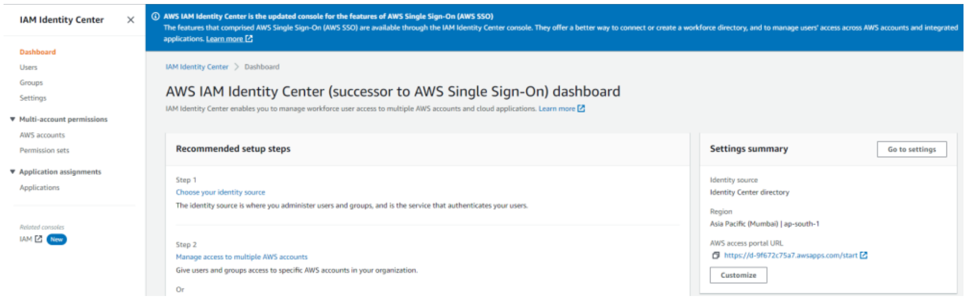
IAM Identity Center requires AWS Organizations

We detected that your AWS account does not currently use this service. After you create an organization, you cannot join this account to another organization until you delete its current organization.

AWS Organizations provides the following benefits:

1. Enables single payer and centralized cost tracking
2. Lets you create and invite other AWS accounts
3. Allows you to apply policy-based controls
4. Helps you simplify organization-wide management of AWS services

Would you like us to create an AWS organization for you now?
We will also enable IAM Identity Center as part of this process.



AWS IAM Identity Center is the updated console for the features of AWS Single Sign-On (AWS SSO)

The features that comprised AWS Single Sign-On (AWS SSO) are available through the IAM Identity Center console. They offer a better way to connect or create a workforce directory, and to manage users' access across AWS accounts and integrated applications. Learn more

AWS IAM Identity Center (successor to AWS Single Sign-On) dashboard

IAM Identity Center enables you to manage workforce user access to multiple AWS accounts and cloud applications. Learn more

Recommended setup steps

Step 1
Choose your identity source
The identity source is where you administer users and groups, and is the service that authenticates your users.

Step 2
Manage access to multiple AWS accounts
Give users and groups access to specific AWS accounts in your organization.

Or

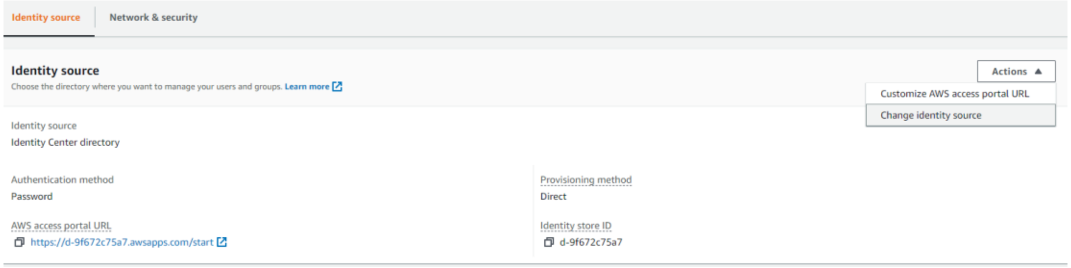
Settings summary

Identity source
Identity Center directory

Region
Asia Pacific (Mumbai) | ap-south-1

AWS access portal URL
https://d-9f672c75a7.awsapps.com/start

Once your SSO is enabled, click on “Change your Identity Source.” Navigate to Identity source and select action. Choose “Change identity source.”



Identity source

Choose the directory where you want to manage your users and groups. Learn more

Identity source
Identity Center directory

Authentication method
Password

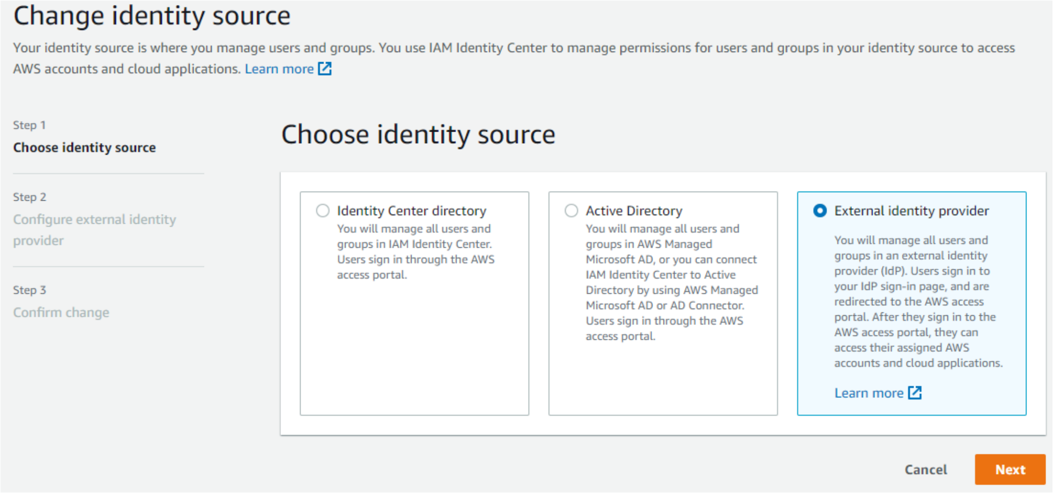
Provisioning method
Direct

AWS access portal URL
https://d-9f672c75a7.awsapps.com/start

Identity store ID
d-9f672c75a7

By default, the identity source in AWS SSO. We will change it to “External Identity provider” to integrate with Azure AD. Download the metadata from step 2 and now switch to the azure side.

Step:1



Change identity source

Your identity source is where you manage users and groups. You use IAM Identity Center to manage permissions for users and groups in your identity source to access AWS accounts and cloud applications. Learn more

Step 1
Choose identity source

Step 2
Configure external identity provider

Step 3
Confirm change

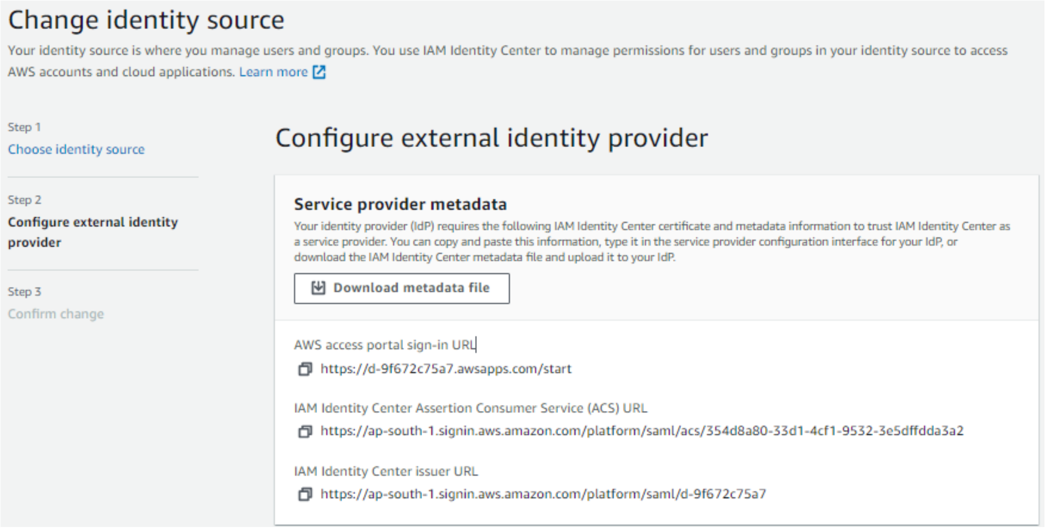
Choose identity source

○ Identity Center directory
You will manage all users and groups in IAM Identity Center. Users sign in through the AWS access portal.

○ Active Directory
You will manage all users and groups in AWS Managed Microsoft AD, or you can connect IAM Identity Center to Active Directory by using AWS Managed Microsoft AD or AD Connector. Users sign in through the AWS access portal.

● External identity provider
You will manage all users and groups in an external identity provider (IdP). Users sign in to your IdP sign-in page, and are redirected to the AWS access portal. After they sign in to the AWS access portal, they can access their assigned AWS accounts and cloud applications.
Learn more

Step:2



Change identity source

Your identity source is where you manage users and groups. You use IAM Identity Center to manage permissions for users and groups in your identity source to access AWS accounts and cloud applications. Learn more

Step 1
Choose identity source

Step 2
Configure external identity provider

Step 3
Confirm change

Configure external identity provider

Service provider metadata

Your identity provider (IdP) requires the following IAM Identity Center certificate and metadata information to trust IAM Identity Center as a service provider. You can copy and paste this information, type it in the service provider configuration interface for your IdP, or download the IAM Identity Center metadata file and upload it to your IdP.

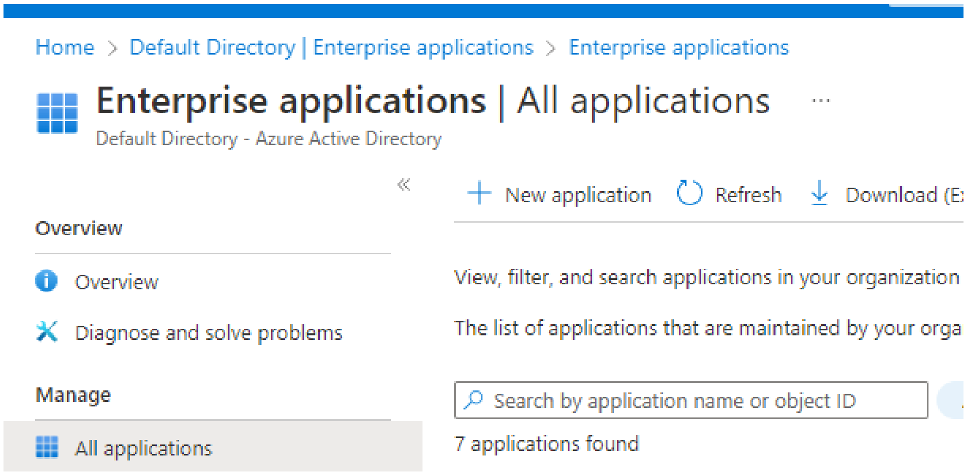
AWS access portal sign-in URL
https://d-9f672c75a7.awsapps.com/start

IAM Identity Center Assertion Consumer Service (ACS) URL
https://ap-south-1.signin.aws.amazon.com/platform/saml/acs/354d8a80-33d1-4cf1-9532-3e5dffdda3a2

IAM Identity Center issuer URL
https://ap-south-1.signin.aws.amazon.com/platform/saml/d-9f672c75a7

Configuring Azure AD as IdP

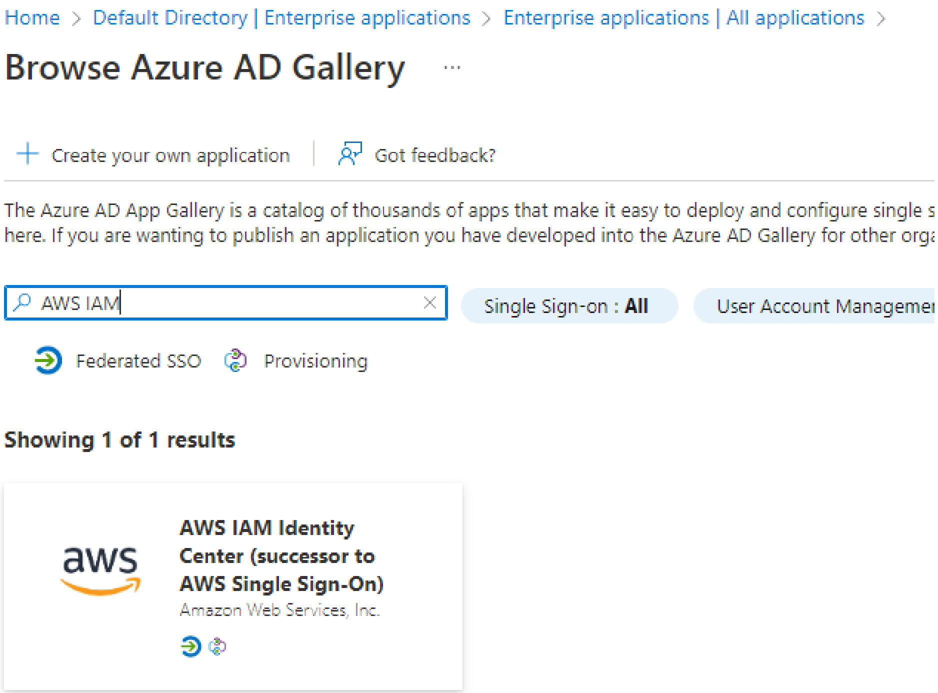
Login to your Azure account and navigate to Azure Active Directory. Select “**Enterprise Applications**” from the left panel and create a new application. Search for AWS SSO from the search bar then select AWS SSO as shown below:


Home > Default Directory | Enterprise applications > Enterprise applications
Enterprise applications | All applications ...
Default Directory - Azure Active Directory
«
+ New application
Refresh
Download (E
Overview
Overview
Diagnose and solve problems
Manage
All applications
Search by application name or object ID

View, filter, and search applications in your organization

The list of applications that are maintained by your orga

7 applications found


Home > Default Directory | Enterprise applications > Enterprise applications | All applications >
Browse Azure AD Gallery ...
+ Create your own application
Got feedback?
Single Sign-on : All
User Account Managemei
Federated SSO
Provisioning
aws

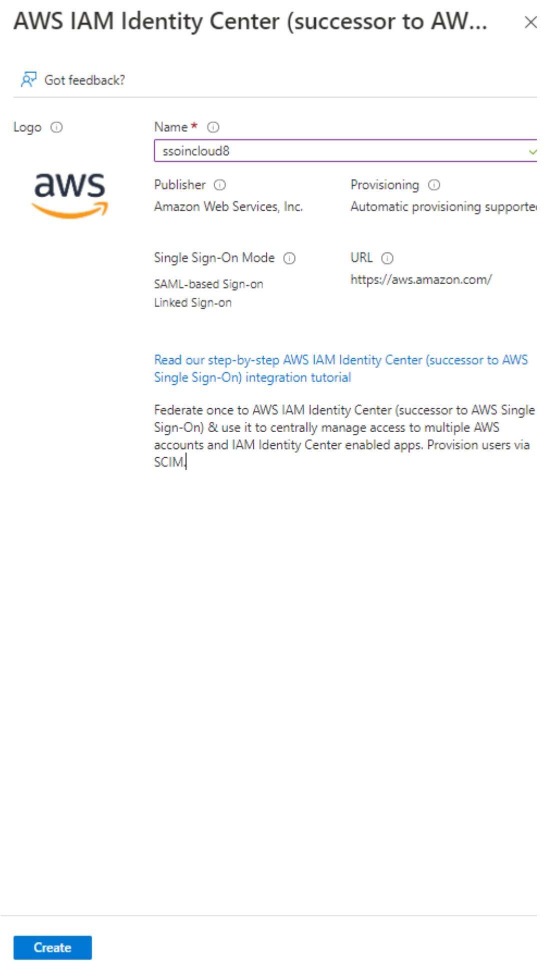
The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single s here. If you are wanting to publish an application you have developed into the Azure AD Gallery for other orga

AWS IAM

Showing 1 of 1 results

AWS IAM Identity Center (successor to AWS Single Sign-On)
Amazon Web Services, Inc.

After selecting AWS SSO, **Click on Create**.



AWS IAM Identity Center (successor to AW...

Logo

Name * ssoincloud8

Publisher: Amazon Web Services, Inc.

Provisioning: Automatic provisioning supporte

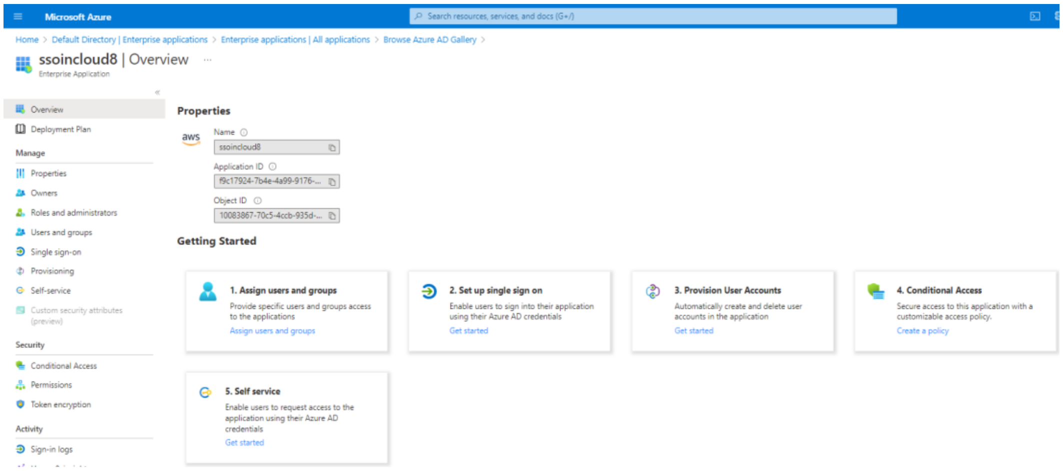
Single Sign-On Mode: SAML-based Sign-on, Linked Sign-on

URL: https://aws.amazon.com/

Read our step-by-step AWS IAM Identity Center (successor to AWS Single Sign-On) integration tutorial

Federate once to AWS IAM Identity Center (successor to AWS Single Sign-On) & use it to centrally manage access to multiple AWS accounts and IAM Identity Center enabled apps. Provision users via SCIM.

Now navigate to the application that you just created and select "Set up single sign-on" as shown below.



ssoincloud8 | Overview

Enterprise Application

Properties

Name: ssoincloud8

Application ID: f9c17924-7b4e-4a99-9176-...

Object ID: 10083867-70c5-4ccb-935d-...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

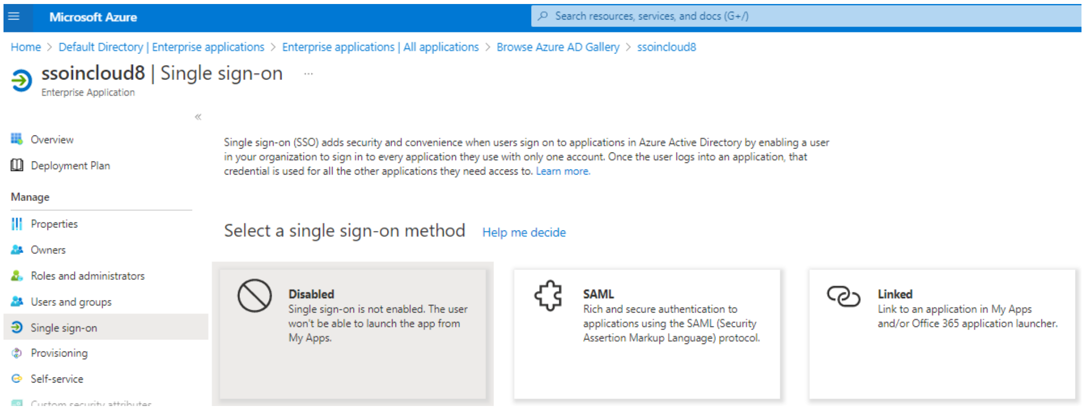
2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

Select SAML


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Default Directory | Enterprise applications > Enterprise applications | All applications > Browse Azure AD Gallery > ssoincloud8
ssoincloud8 | Single sign-on
Enterprise Application
Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Self-service
Custom security attributes
Select a single sign-on method
Help me decide
Disabled
SAML
Linked

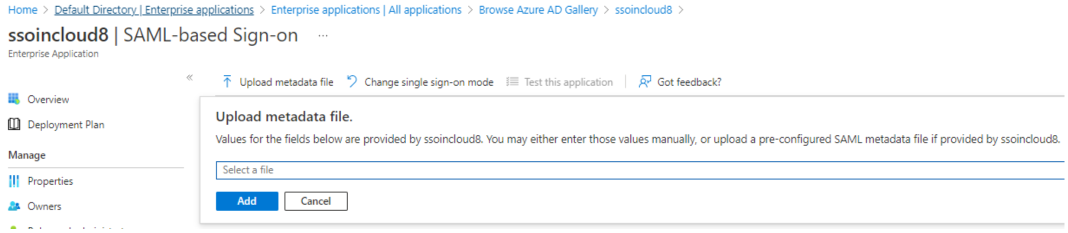
Single sign-on (SSO) adds security and convenience when users sign on to applications in Azure Active Directory by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

Disabled: Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML: Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Linked: Link to an application in My Apps and/or Office 365 application launcher.

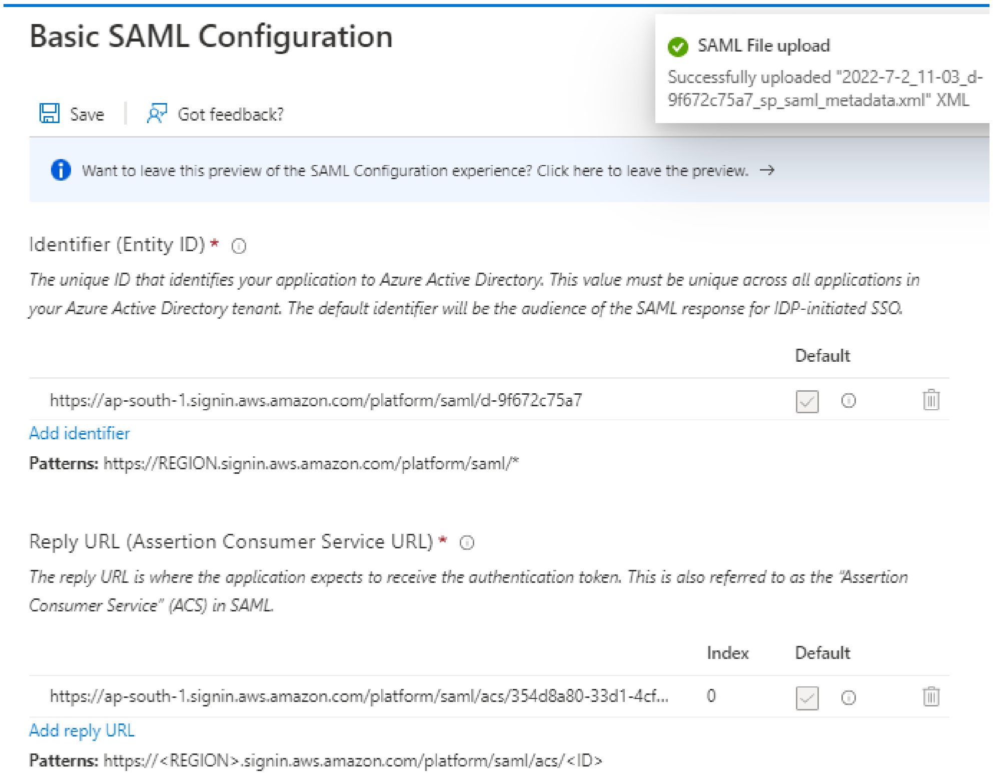
Upload the metadata data you downloaded from AWS SSO.


Home > Default Directory | Enterprise applications > Enterprise applications | All applications > Browse Azure AD Gallery > ssoincloud8 >
ssoincloud8 | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
Got feedback?
Overview
Deployment Plan
Manage
Properties
Owners
Select a file
Add
Cancel

Upload metadata file.

Values for the fields below are provided by ssoincloud8. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by ssoincloud8.

After the upload is complete click **“Save”** and then close the Basic SAML Configuration pane.



Basic SAML Configuration

SAML File upload

Successfully uploaded "2022-7-2_11-03_d-9f672c75a7_sp_saml_metadata.xml" XML

Want to leave this preview of the SAML Configuration experience? Click here to leave the preview. →

Identifier (Entity ID) *

The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
https://ap-south-1.signin.aws.amazon.com/platform/saml/d-9f672c75a7	☑

Add identifier

Patterns: https://REGION.signin.aws.amazon.com/platform/saml/*

Reply URL (Assertion Consumer Service URL) *

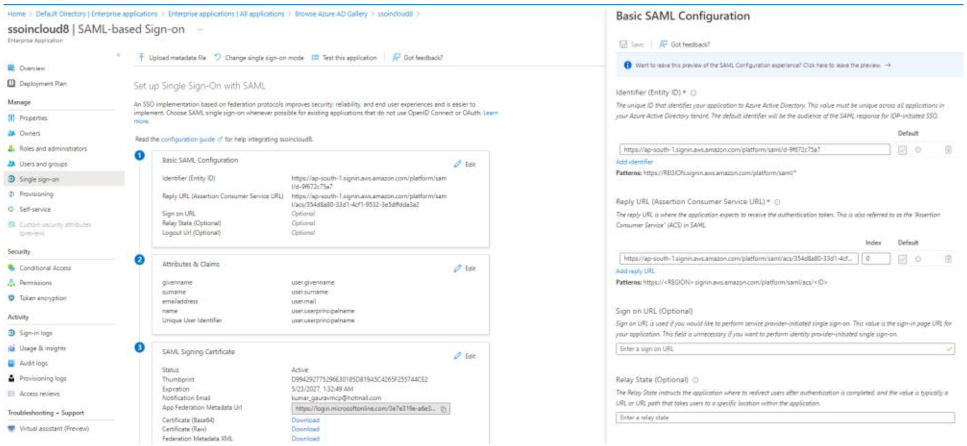
The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://ap-south-1.signin.aws.amazon.com/platform/saml/acs/354d8a80-33d1-4cf...	0	☑

Add reply URL

Patterns: https://<REGION>.signin.aws.amazon.com/platform/saml/acs/<ID>

Now download the Azure Federation Metadata XML as shown below.



ssoincloud8 | SAML-based Sign-on

Enterprise Application

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating ssoincloud8.

1 Basic SAML Configuration

Identifier (Entity ID)	https://ap-south-1.signin.aws.amazon.com/platform/saml/d-9f672c75a7
Reply URL (Assertion Consumer Service URL)	https://ap-south-1.signin.aws.amazon.com/platform/saml/acs/354d8a80-33d1-4cf1-9532-3e5dffdda3a2
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

2 Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Signing Certificate

Status	Active
Thumbprint	D994292775296E30185D819A5C4265F255744CE2
Expiration	5/23/2027, 1:32:49 AM
Notification Email	kumar_gauravmcp@hotmail.com
App Federation Metadata Url	https://login.microsoftonline.com/3e7e319e-a6e3...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Basic SAML Configuration

Want to leave this preview of the SAML Configuration experience? Click here to leave the preview. →

Identifier (Entity ID) *

The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
https://ap-south-1.signin.aws.amazon.com/platform/saml/d-9f672c75a7	☑

Add identifier

Patterns: https://REGION.signin.aws.amazon.com/platform/saml/*

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://ap-south-1.signin.aws.amazon.com/platform/saml/acs/354d8a80-33d1-4cf...	0	☑

Add reply URL

Patterns: https://<REGION>.signin.aws.amazon.com/platform/saml/acs/<ID>

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

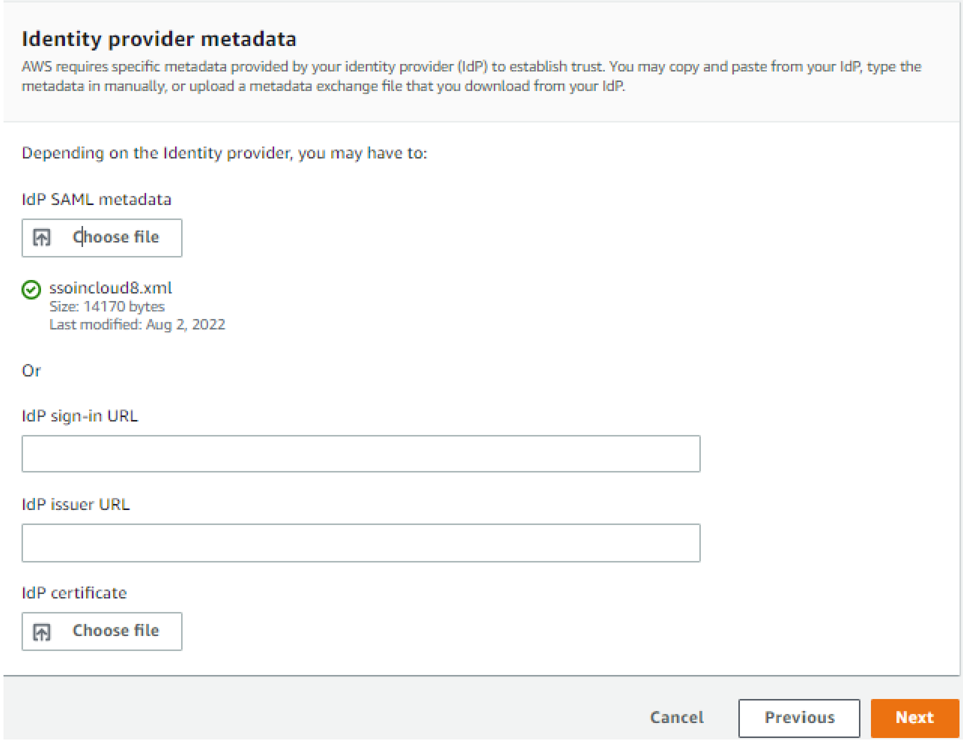
Enter a sign on URL

Relay State (Optional)

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Enter a relay state

Once downloaded the metadata file, go back to the AWS console and upload the downloaded metadata as shown below then click on Next.



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.

Depending on the Identity provider, you may have to:

IdP SAML metadata

✓ ssoincloud8.xml
Size: 14170 bytes
Last modified: Aug 2, 2022

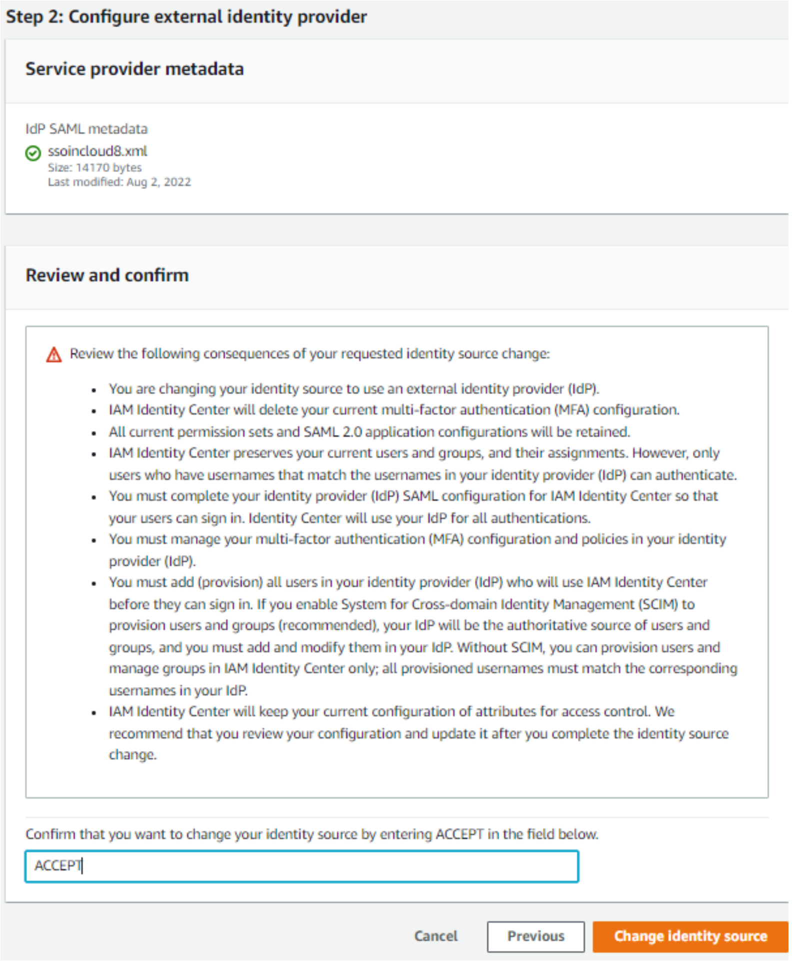
Or

IdP sign-in URL

IdP issuer URL

IdP certificate

In the next step, acknowledge and change the identity source as shown.



Step 2: Configure external identity provider

Service provider metadata

IdP SAML metadata

✓ ssoincloud8.xml
Size: 14170 bytes
Last modified: Aug 2, 2022

Review and confirm

⚠ Review the following consequences of your requested identity source change:

- You are changing your identity source to use an external identity provider (IdP).
- IAM Identity Center will delete your current multi-factor authentication (MFA) configuration.
- All current permission sets and SAML 2.0 application configurations will be retained.
- IAM Identity Center preserves your current users and groups, and their assignments. However, only users who have usernames that match the usernames in your identity provider (IdP) can authenticate.
- You must complete your identity provider (IdP) SAML configuration for IAM Identity Center so that your users can sign in. Identity Center will use your IdP for all authentications.
- You must manage your multi-factor authentication (MFA) configuration and policies in your identity provider (IdP).
- You must add (provision) all users in your identity provider (IdP) who will use IAM Identity Center before they can sign in. If you enable System for Cross-domain Identity Management (SCIM) to provision users and groups (recommended), your IdP will be the authoritative source of users and groups, and you must add and modify them in your IdP. Without SCIM, you can provision users and manage groups in IAM Identity Center only; all provisioned usernames must match the corresponding usernames in your IdP.
- IAM Identity Center will keep your current configuration of attributes for access control. We recommend that you review your configuration and update it after you complete the identity source change.

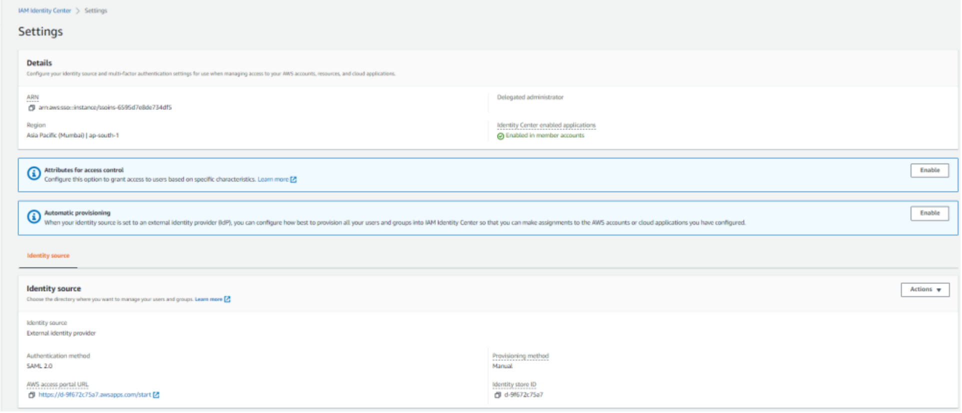
Confirm that you want to change your identity source by entering ACCEPT in the field below.

ACCEPT

The basic configuration is completed.

Automatic provisioning of Users and groups

Enable the provisioning to Automatic and copy "SCIM endpoint" and "token" to the notepad.



Settings

Details

Configure your identity source and multi-factor authentication settings for use when managing access to your AWS accounts, resources, and cloud applications.

ARN
arn:aws:sso:::instance/ssoins-6595d7e8de734df5

Region
Asia Pacific (Mumbai) | ap-south-1

Delegated administrator

Identity Center enabled applications
✓ Enabled in member accounts

Attributes for access control
Configure this option to grant access to users based on specific characteristics. Learn more

Automatic provisioning
When your identity source is set to an external identity provider (IdP), you can configure how best to provision all your users and groups into IAM Identity Center so that you can make assignments to the AWS accounts or cloud applications you have configured.

Identity source

Choose the directory where you want to manage your users and groups. Learn more

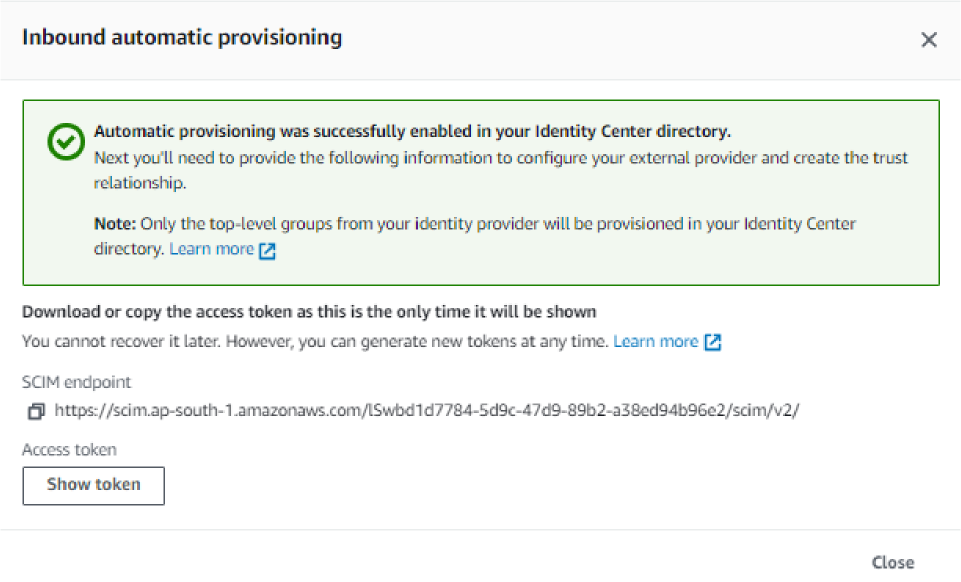
Identity source
External identity provider

Authentication method
SAML 2.0

Provisioning method
Manual

AWS access portal URL
https://d-9f672c75a7.awsapps.com/start

Identity store ID
d-9f672c75a7



Inbound automatic provisioning

Automatic provisioning was successfully enabled in your Identity Center directory.
Next you'll need to provide the following information to configure your external provider and create the trust relationship.

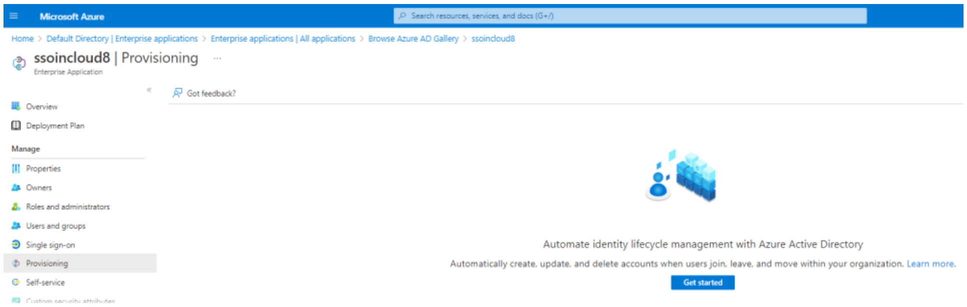
Note: Only the top-level groups from your identity provider will be provisioned in your Identity Center directory. Learn more

Download or copy the access token as this is the only time it will be shown
You cannot recover it later. However, you can generate new tokens at any time. Learn more

SCIM endpoint
https://scim.ap-south-1.amazonaws.com/lSwbd1d7784-5d9c-47d9-89b2-a38ed94b96e2/scim/v2/

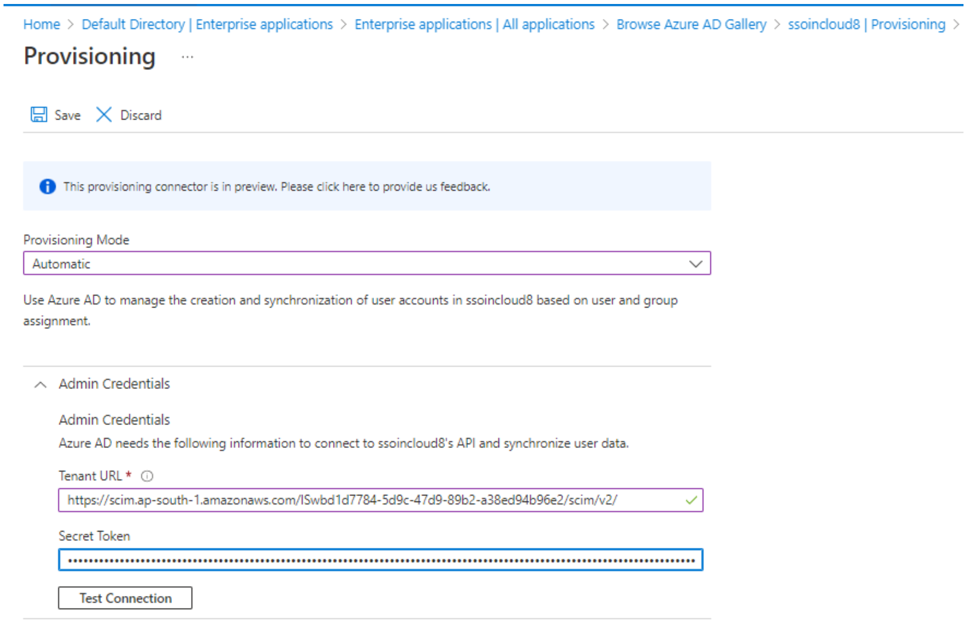
Access token

Now, back to Azure. Navigate to “Provisioning” from the left panel in the application and click on Get Started. Change the provisioning mode to **automatic** and paste the copied SCIM endpoint and token that you copied from the AWS console. Click on Save.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Default Directory | Enterprise applications > Enterprise applications | All applications > Browse Azure AD Gallery > ssoincloud8
ssoincloud8 | Provisioning
Enterprise Application
Got feedback?
Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Self-service
Custom security attributes

Automate identity lifecycle management with Azure Active Directory
Automatically create, update, and delete accounts when users join, leave, and move within your organization. Learn more.



Home > Default Directory | Enterprise applications > Enterprise applications | All applications > Browse Azure AD Gallery > ssoincloud8 | Provisioning >
Provisioning
Save
Discard

This provisioning connector is in preview. Please click here to provide us feedback.

Provisioning Mode
Automatic

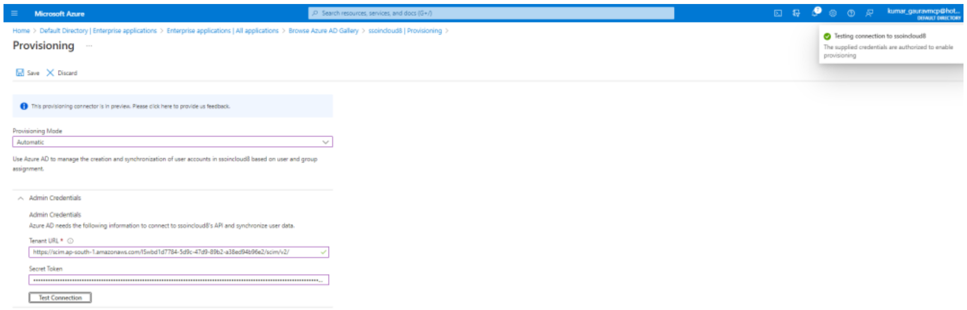
Use Azure AD to manage the creation and synchronization of user accounts in ssoincloud8 based on user and group assignment.

Admin Credentials

Admin Credentials
Azure AD needs the following information to connect to ssoincloud8's API and synchronize user data.

Tenant URL *
https://scim.ap-south-1.amazonaws.com/lSwbd1d7784-5d9c-47d9-89b2-a38ed94b96e2/scim/v2/

Secret Token
••


Microsoft Azure
Search resources, services, and docs (G+/)
kumar_gauravmcp@hot...
DEFAULT DIRECTORY
Home > Default Directory | Enterprise applications > Enterprise applications | All applications > Browse Azure AD Gallery > ssoincloud8 | Provisioning >
Save
Discard
Test Connection

Provisioning

Testing connection to ssoincloud8

The supplied credentials are authorized to enable provisioning

This provisioning connector is in preview. Please click here to provide us feedback.

Provisioning Mode: Automatic

Use Azure AD to manage the creation and synchronization of user accounts in ssoincloud8 based on user and group assignment.

Admin Credentials

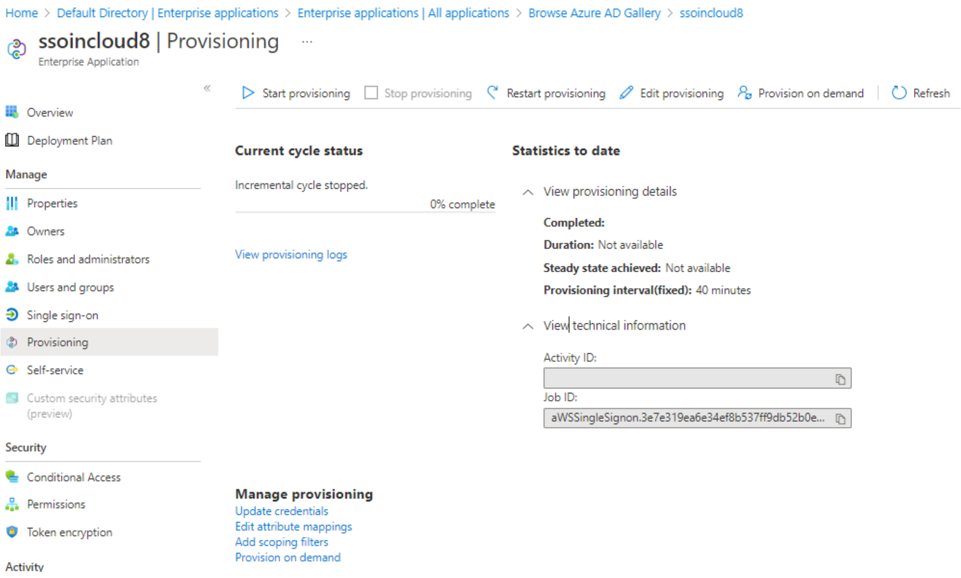
Admin Credentials

Azure AD needs the following information to connect to ssoincloud8's API and synchronize user data.

Tenant URL *: https://scim.ap-south-1.amazonaws.com/15wbd1d7784-5d9c-47d9-89b2-a38ed94b96e2/scim/v2/

Secret Token: ••...

Back in the "Provisioning" section and start the provisioning.
The default provisioning setups as below.



ssoincloud8 | Provisioning

Enterprise Application

Current cycle status

Incremental cycle stopped.

0% complete

View provisioning logs

Statistics to date

View provisioning details

Completed:

Duration: Not available

Steady state achieved: Not available

Provisioning interval(fixed): 40 minutes

View technical information

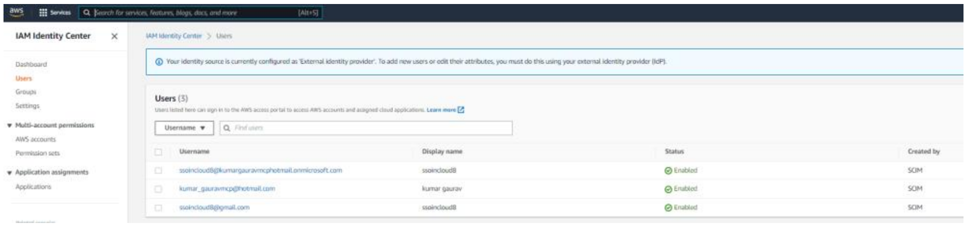
Activity ID:

Job ID: aWSSingleSignon.3e7e319ea6e34ef8b537ff9db52b0e...

Manage provisioning

Update credentials
Edit attribute mappings
Add scoping filters
Provision on demand

Once successfully provisioned. It should be visible in the AWS SSO console



Your identity source is currently configured as 'External identity provider'. To add new users or edit their attributes, you must do this using your external identity provider (IdP).

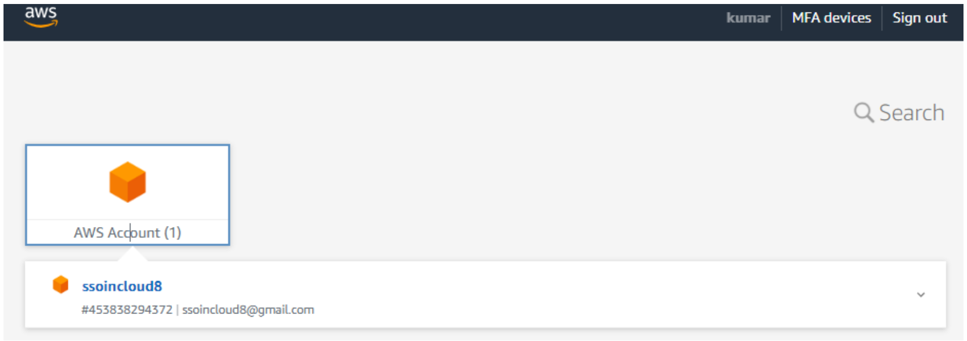
Users (3)

Users listed here can sign in to the AWS access portal to access AWS accounts and assigned cloud applications. Learn more

Username	Display name	Status	Created by
ssoincloud8@kumargauravmcphotmail.onmicrosoft.com	ssoincloud8	Enabled	SCIM
kumar_gauravmcp@hotmail.com	kumar gaurav	Enabled	SCIM
ssoincloud8@gmail.com	ssoincloud8	Enabled	SCIM

As the next step, we can assign permissions to the users and access AWS accounts as Azure AD users.

SSO logging as below for Azure AD user.



ssoincloud8

#453838294372 | ssoincloud8@gmail.com