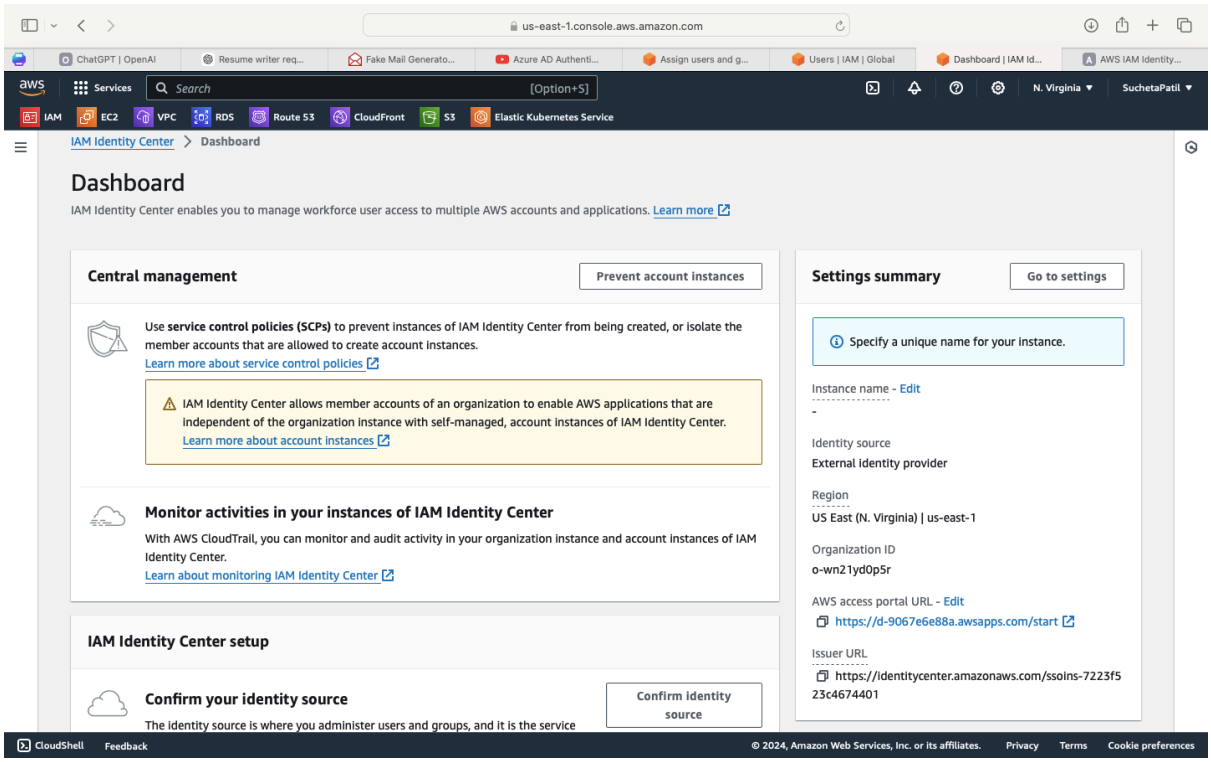
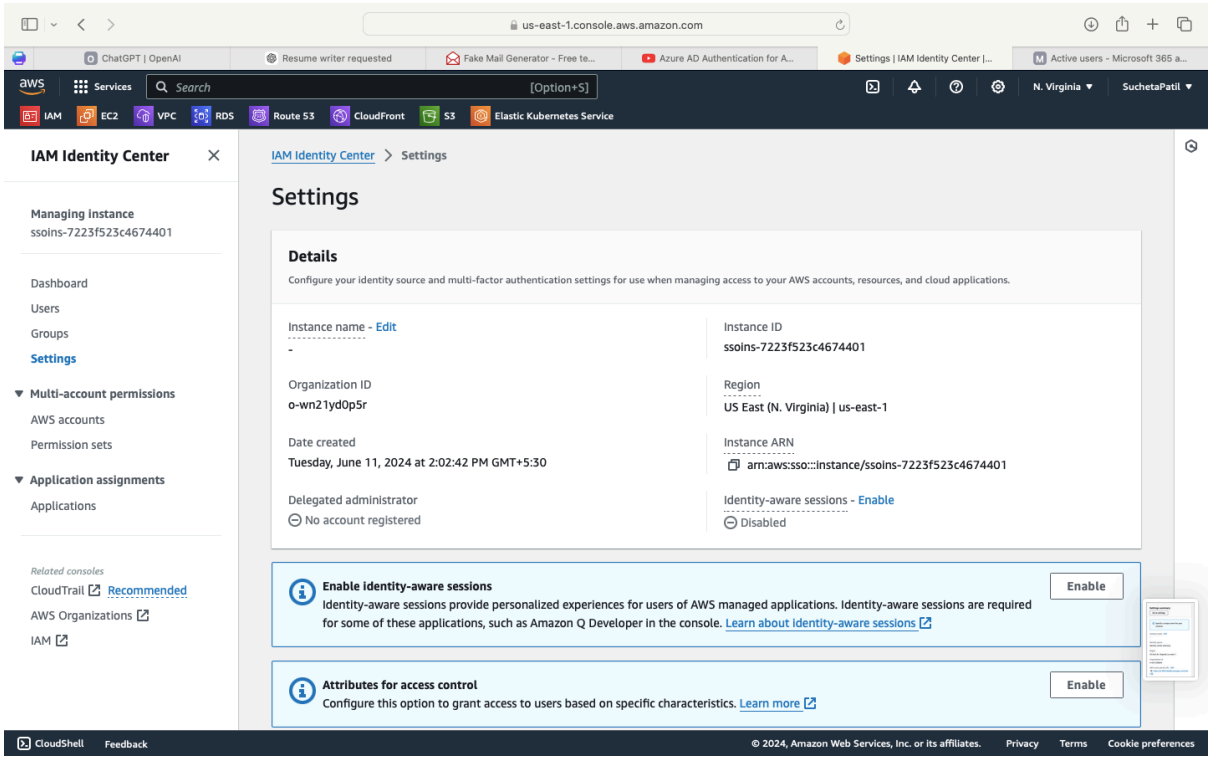
Tuesday, 11 June 2024

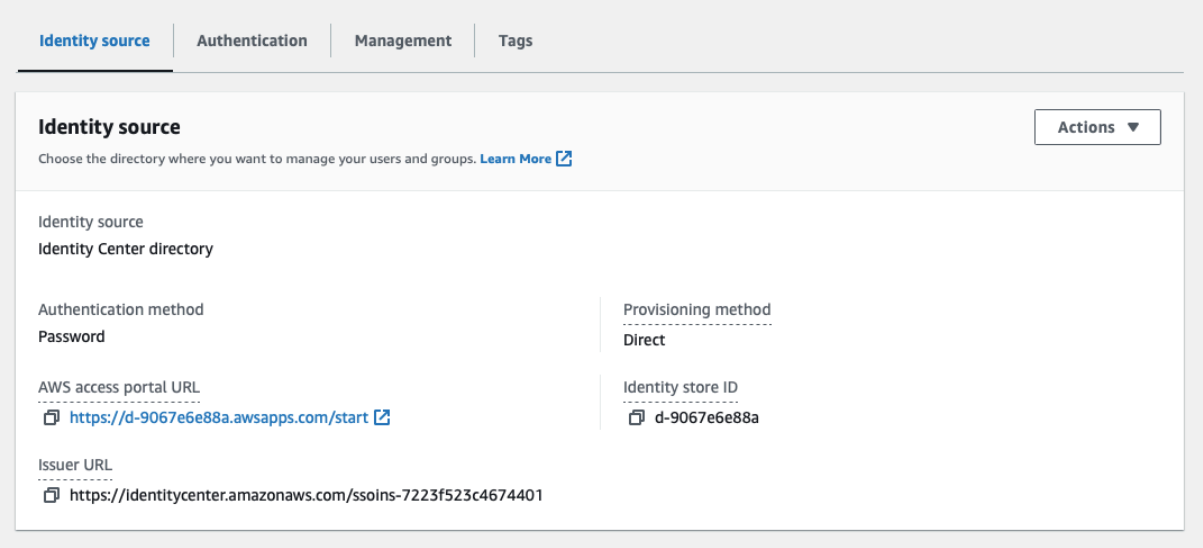
Accessing AWS Using Azure Active Directory

Go to AWS account and search for IAM Identity Center. Go to IAM Identity Center.

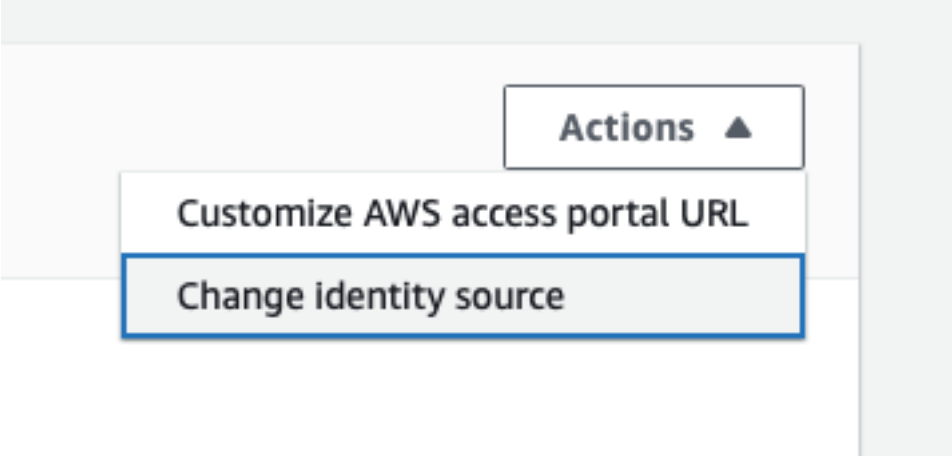


Scroll Down and go to Settings, Identity Source.

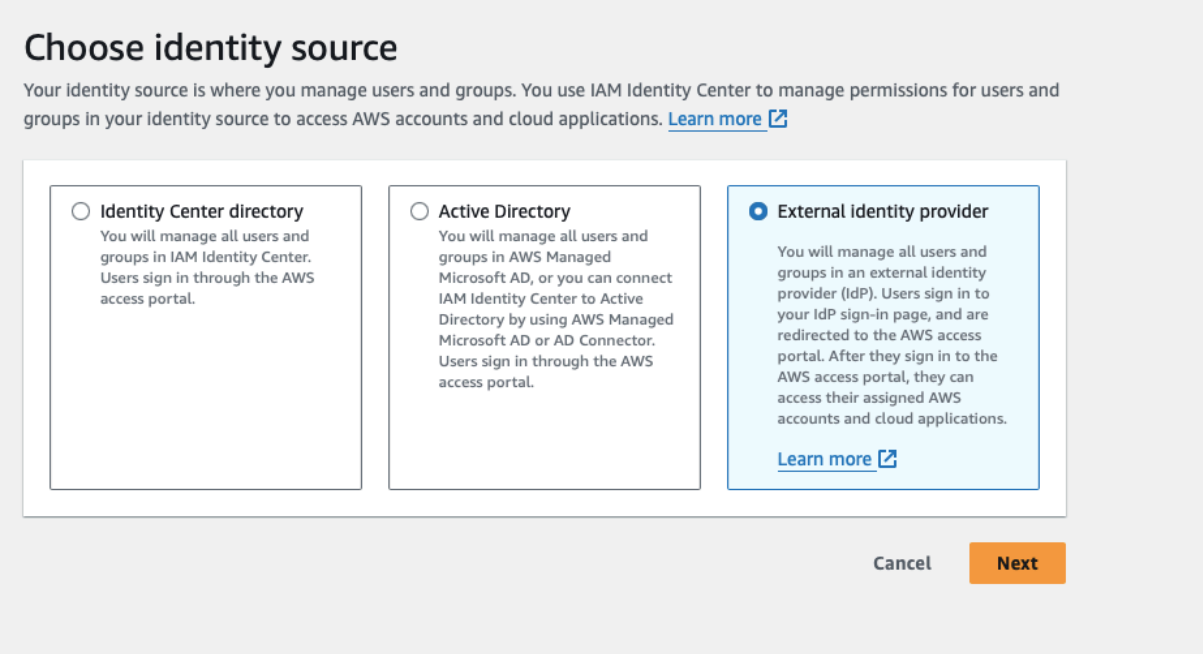




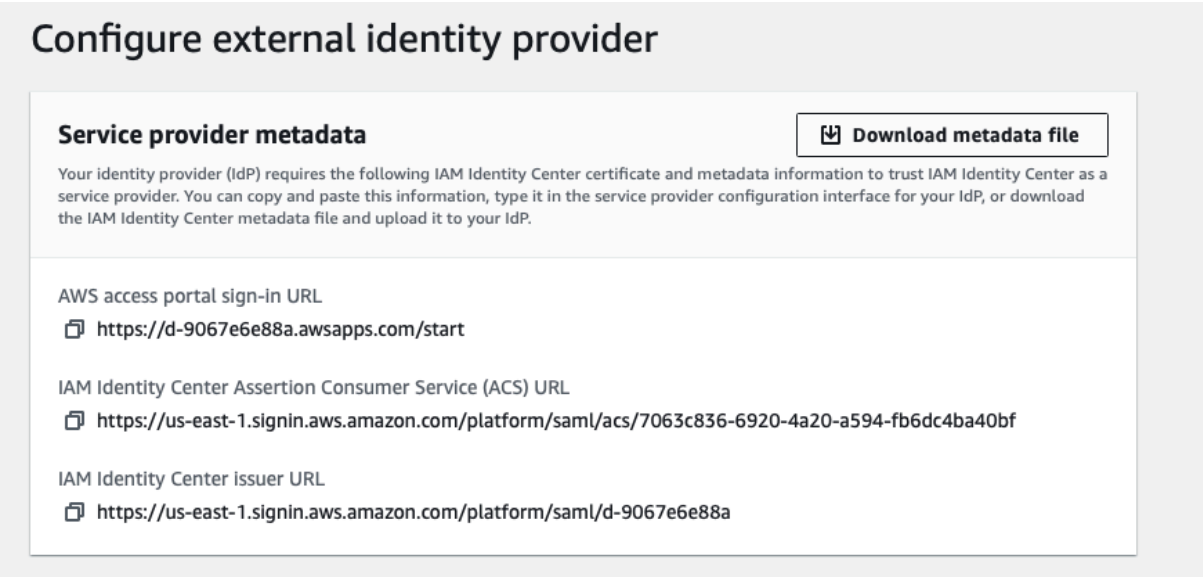
Here we need to Change identity source, Go to Actions tab and select Change identity source.

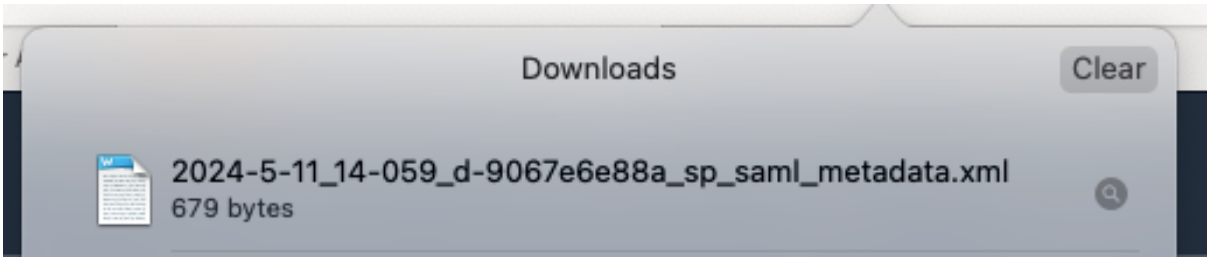


Choose Identity Source External identity provider.

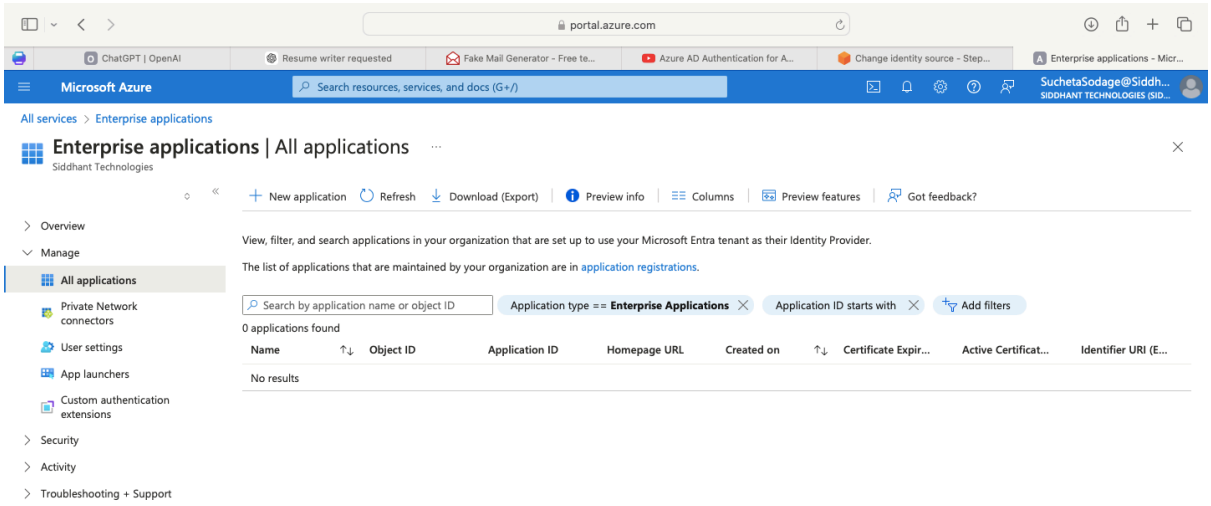


In Configure external identity provider Download metadata file.

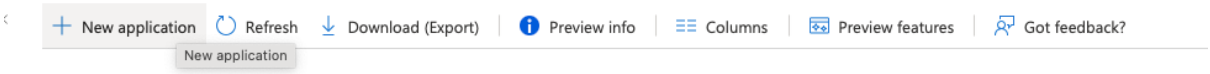




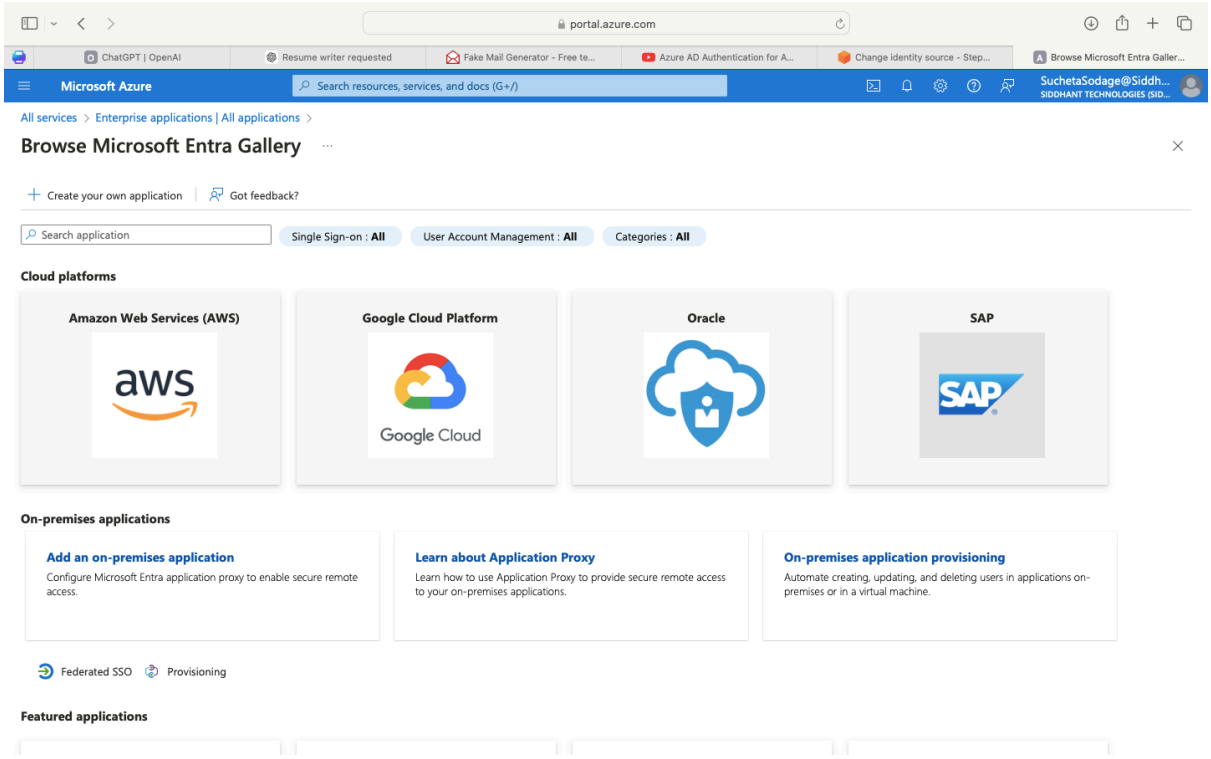
Then move Azure account and search for Enterprise applications.

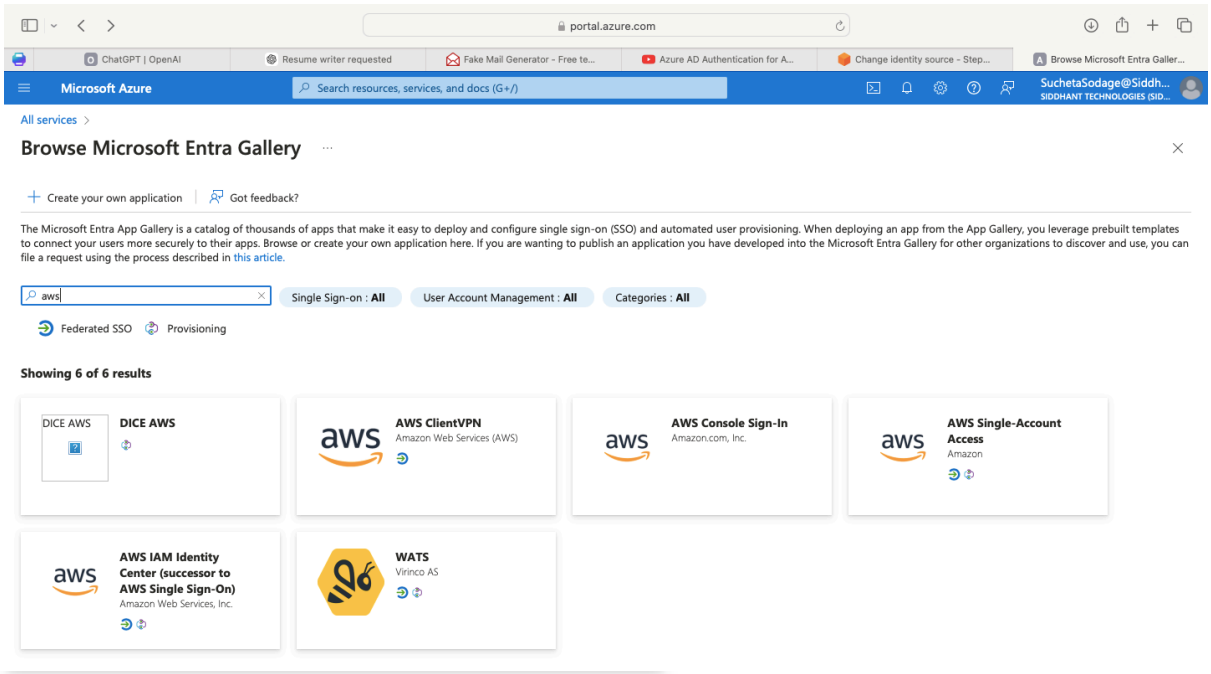


Then go to New Application. Here we are adding AWS Identity Centre to Azure AD.

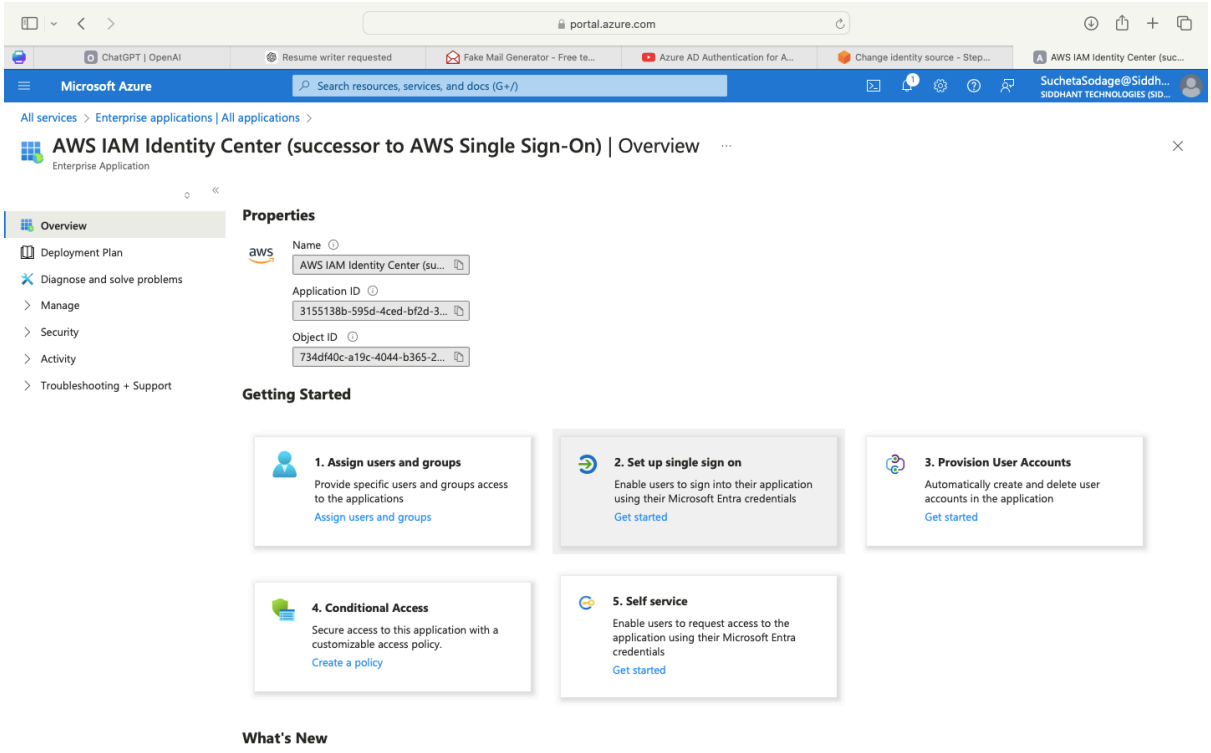


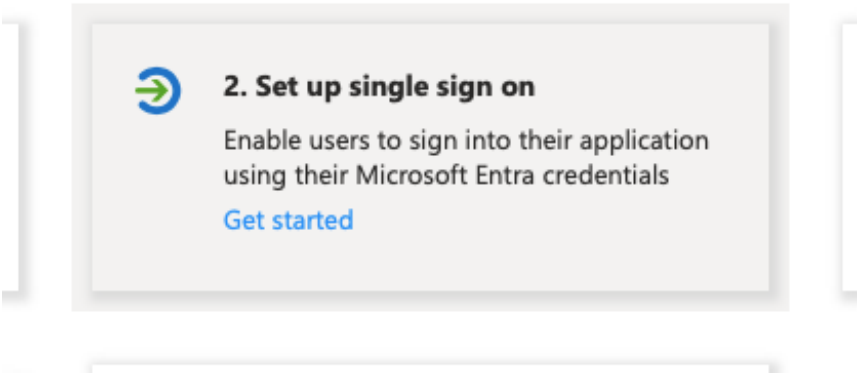
Here we will get multiple options we will search for AWS and select AWS AM Identity Center (successor to AWS Single Sign-On).


portal.azure.com
Microsoft Azure
Search resources, services, and docs (G+/)
All services > Enterprise applications | All applications >
Browse Microsoft Entra Gallery
Create your own application
Got feedback?
Search application
Single Sign-on : All
User Account Management : All
Categories : All
Cloud platforms
Amazon Web Services (AWS)
Google Cloud Platform
Google Cloud
Oracle
SAP
On-premises applications
Add an on-premises application
Configure Microsoft Entra application proxy to enable secure remote access.
Learn about Application Proxy
Learn how to use Application Proxy to provide secure remote access to your on-premises applications.
On-premises application provisioning
Automate creating, updating, and deleting users in applications on-premises or in a virtual machine.
Federated SSO
Provisioning
Featured applications


portal.azure.com
Microsoft Azure
Search resources, services, and docs (G+/)
All services >
Browse Microsoft Entra Gallery
Create your own application
Got feedback?
The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for other organizations to discover and use, you can file a request using the process described in this article.
aws
Single Sign-on : All
User Account Management : All
Categories : All
Federated SSO
Provisioning
Showing 6 of 6 results
DICE AWS
AWS ClientVPN
Amazon Web Services (AWS)
AWS Console Sign-In
Amazon.com, Inc.
AWS Single-Account Access
Amazon
AWS IAM Identity Center (successor to AWS Single Sign-On)
Amazon Web Services, Inc.
WATS
Virinco AS


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

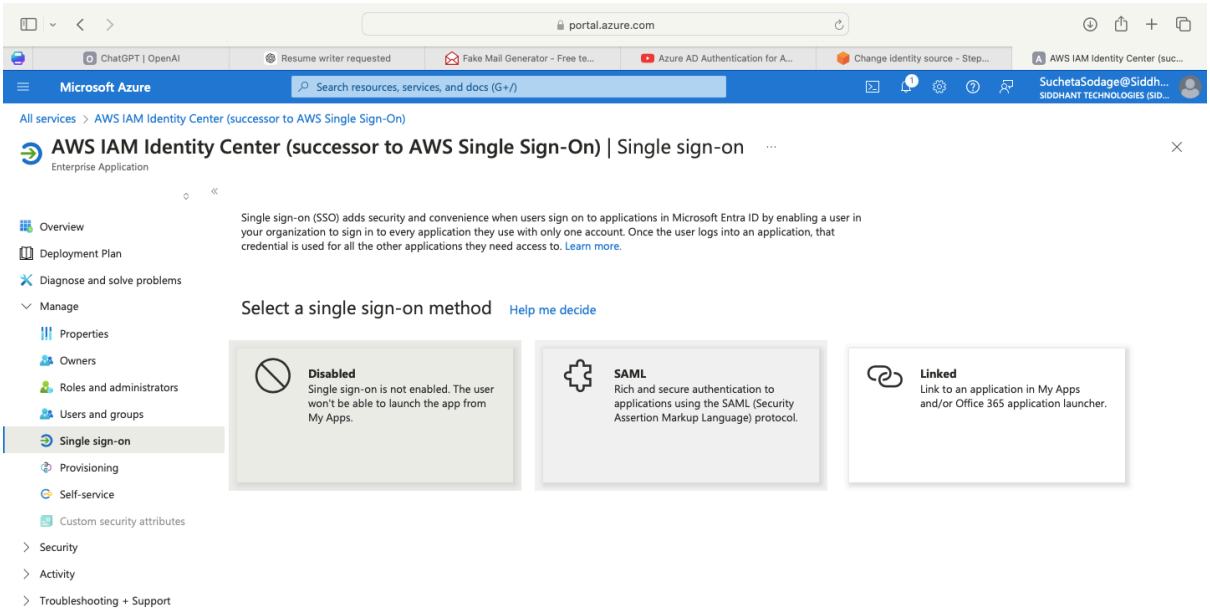

portal.azure.com
ChatGPT | OpenAI
Resume writer requested
Fake Mail Generator - Free te...
Azure AD Authentication for A...
Change identity source - Step...
AWS IAM Identity Center (suc...
Microsoft Azure
Search resources, services, and docs (G+/)
SuchetaSodage@Siddh...
SIDDHANT TECHNOLOGIES (SID...
All services > Enterprise applications | All applications >
AWS IAM Identity Center (successor to AWS Single Sign-On) | Overview
Enterprise Application
Overview
Deployment Plan
Diagnose and solve problems
Manage
Security
Activity
Troubleshooting + Support
Properties
Name
AWS IAM Identity Center (su...
Application ID
3155138b-595d-4ced-bf2d-3...
Object ID
734df40c-a19c-4044-b365-2...
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 Microsoft Entra 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 Microsoft Entra credentials
Get started
What's New

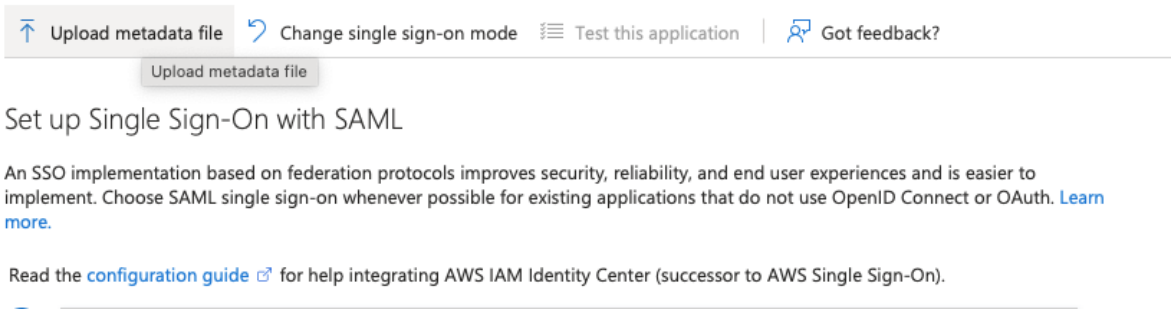

2. Set up single sign on
Enable users to sign into their application using their Microsoft Entra credentials
Get started

In Set up single sign on we are using SAML Rich and secure authentication to applications using the SAML (Securit) Assertion Markup Language) protocol.

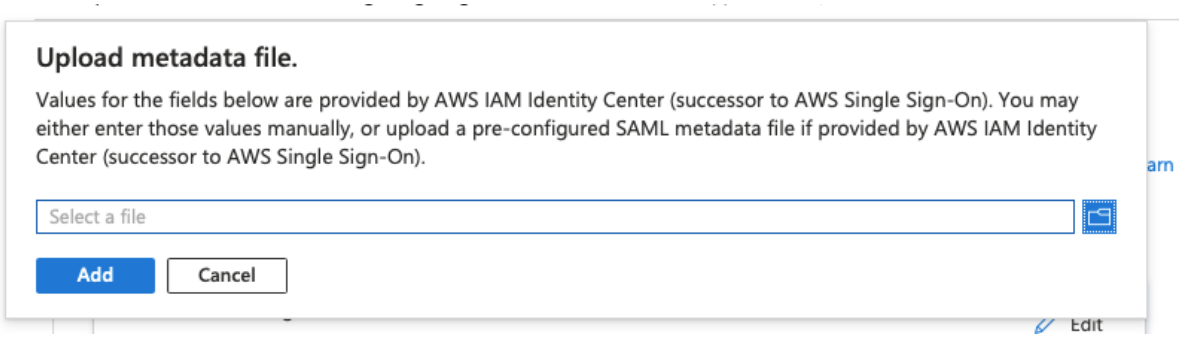
SAML, is a standardised way to tell external applications and services that a user is who they say they are.

Now we are going Set up Single Sign-On with SAML. For this we need to upload the downloaded metadata file from AWS identity source.

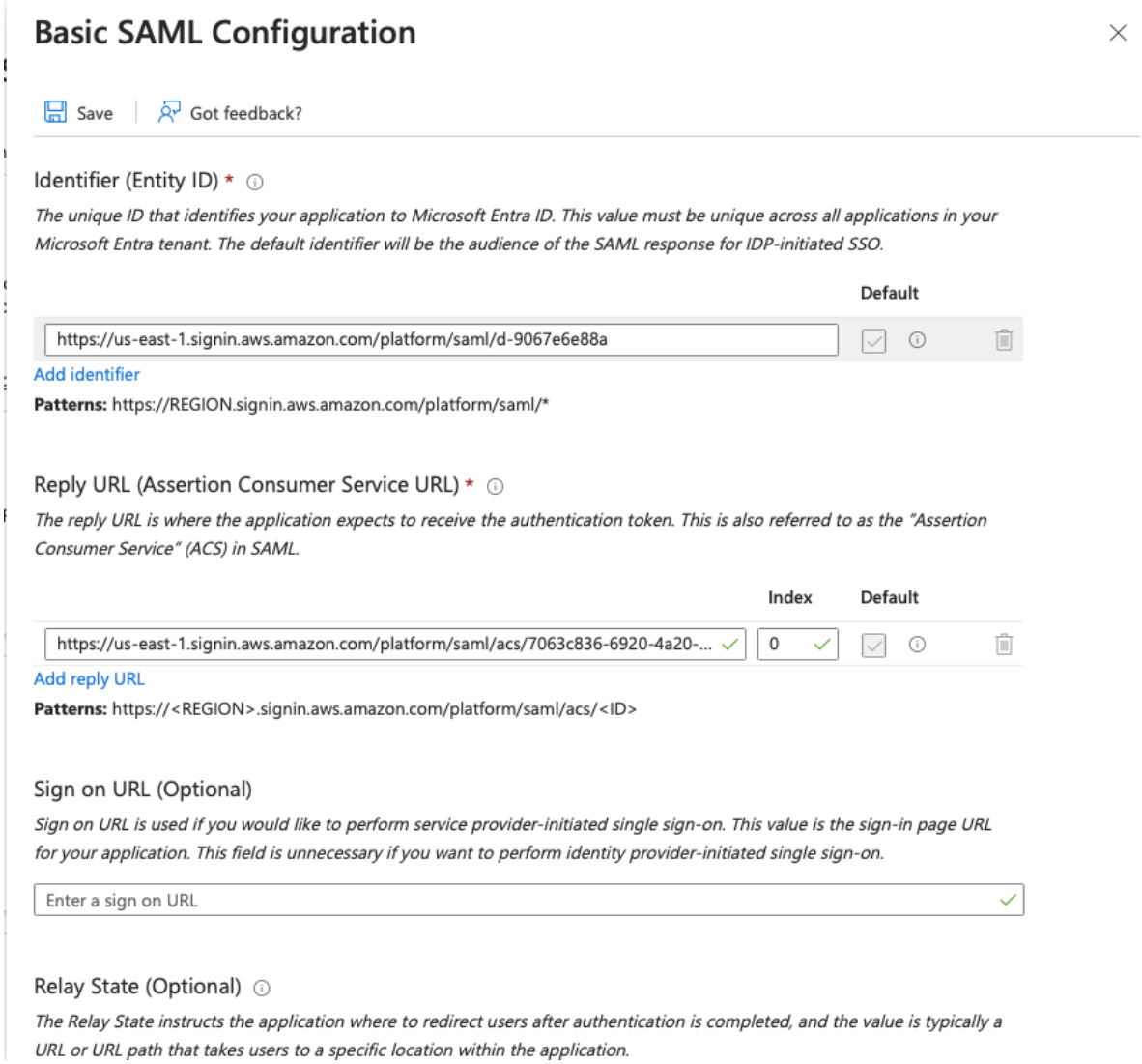


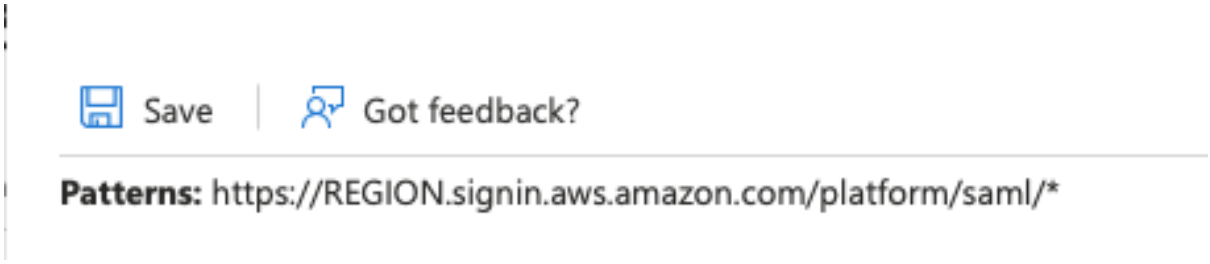


Here we are uploading metadata file which we have downloaded from AWS AM Identity Center.

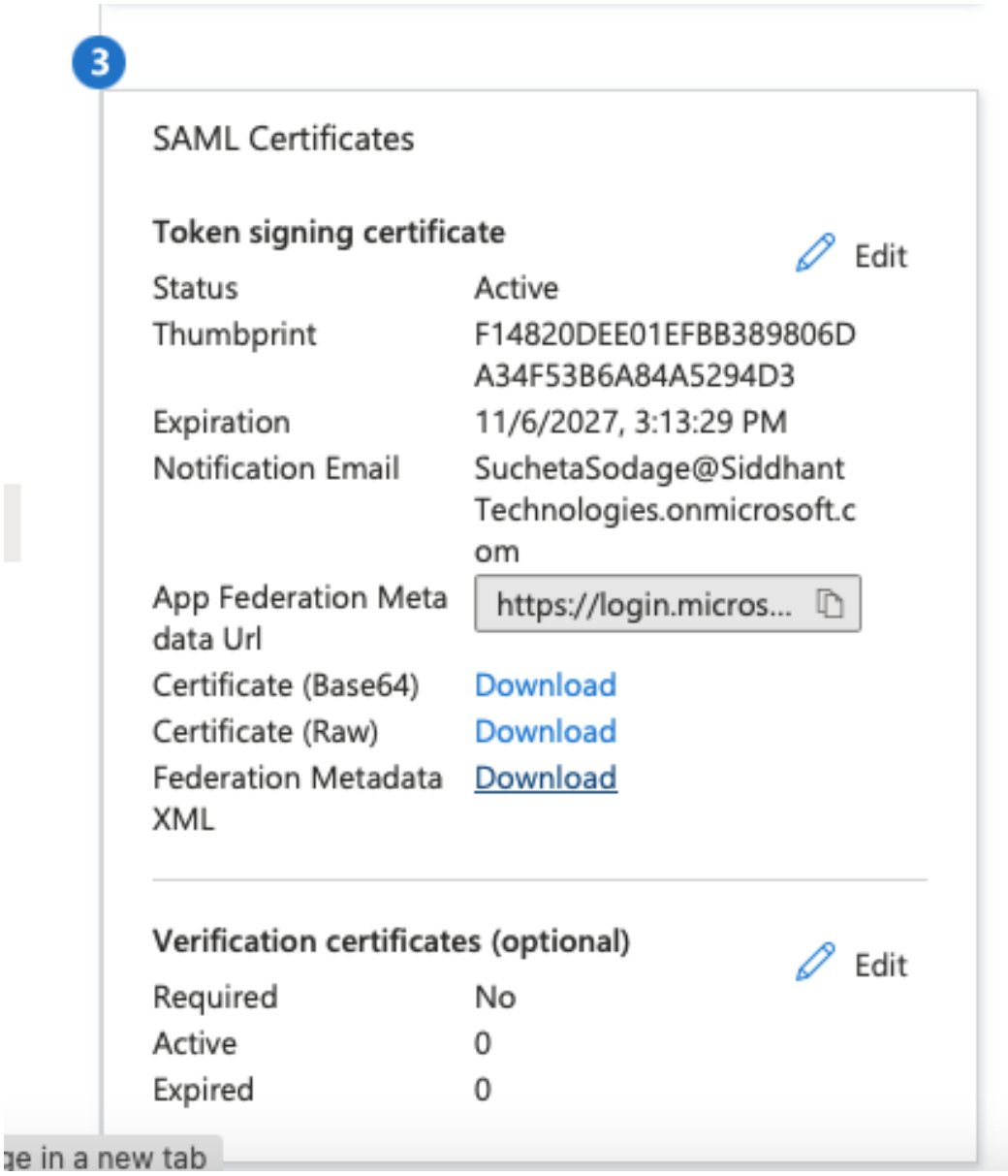


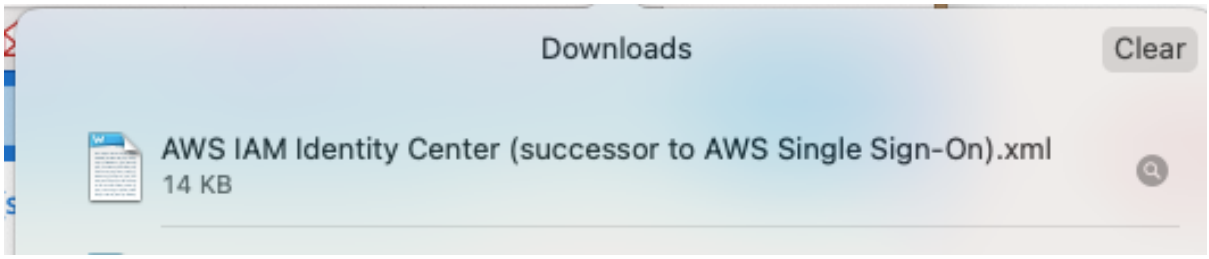
Check details and Save.



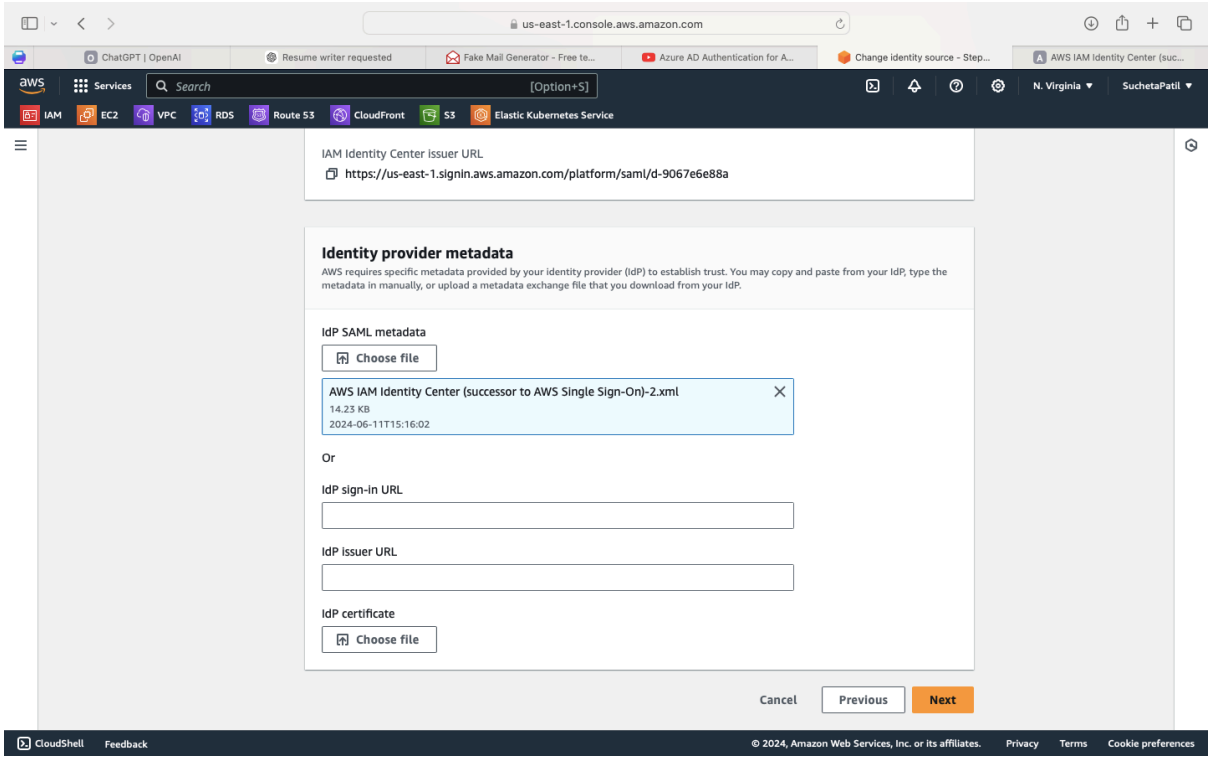


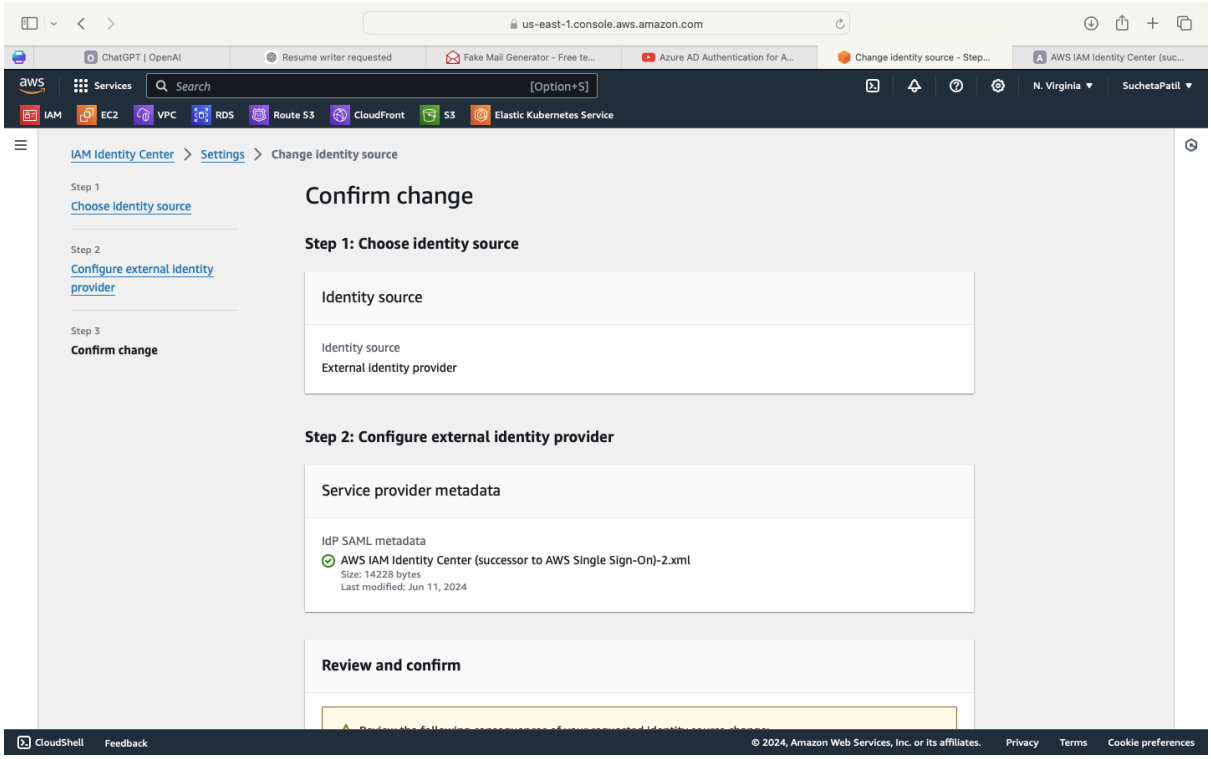
We need SAML Certificates to upload to AWS Identity Source. Here we are downloading Federation Metadata XML file.

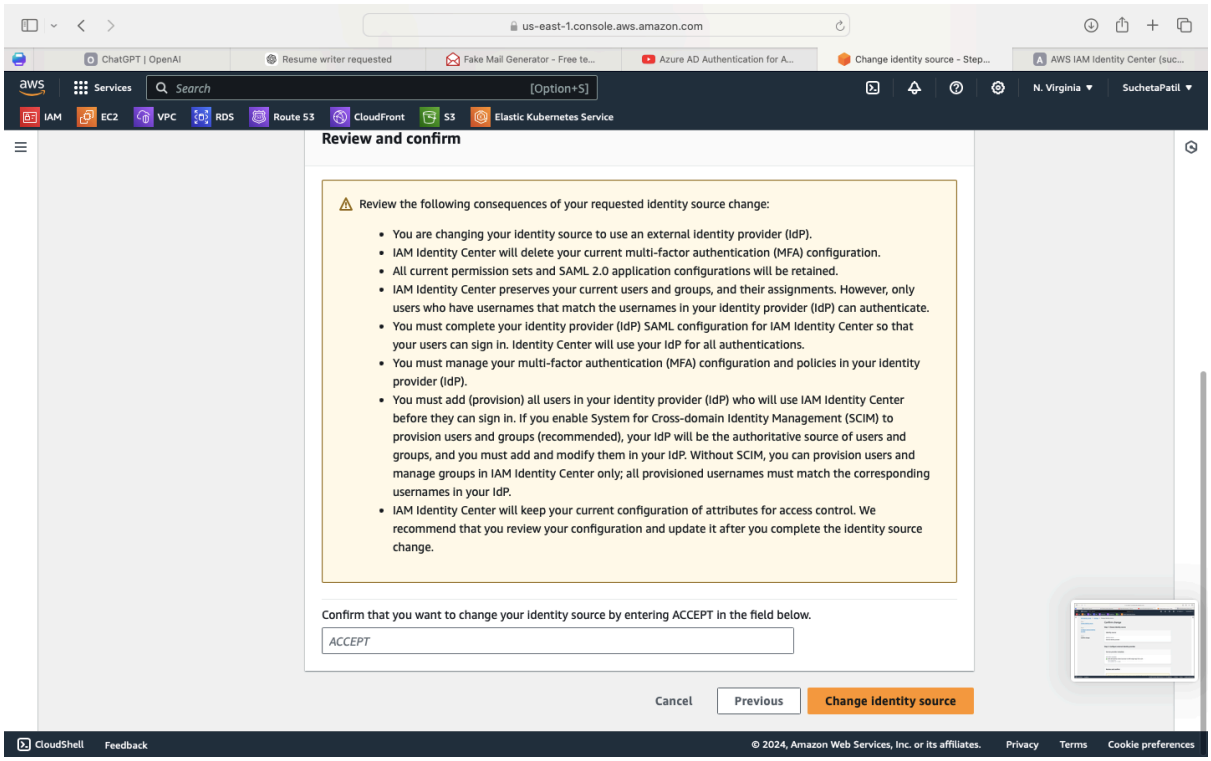




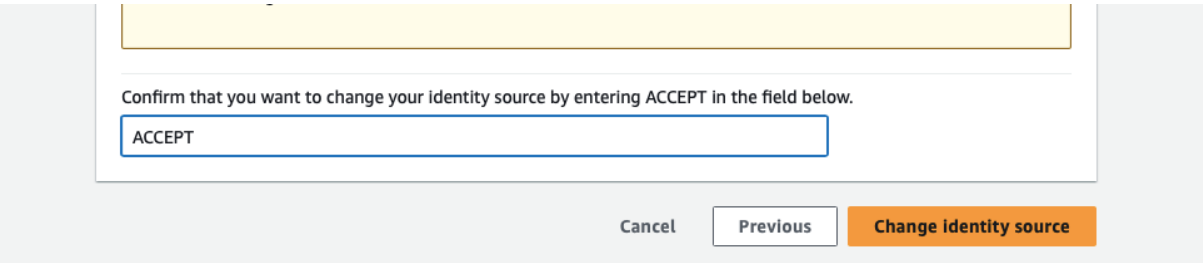
Now go back to Identity provider metadata in AWS identity provider centre. And upload AWS AM Identity Center (successor to AWS Single Sign-On).xml file.

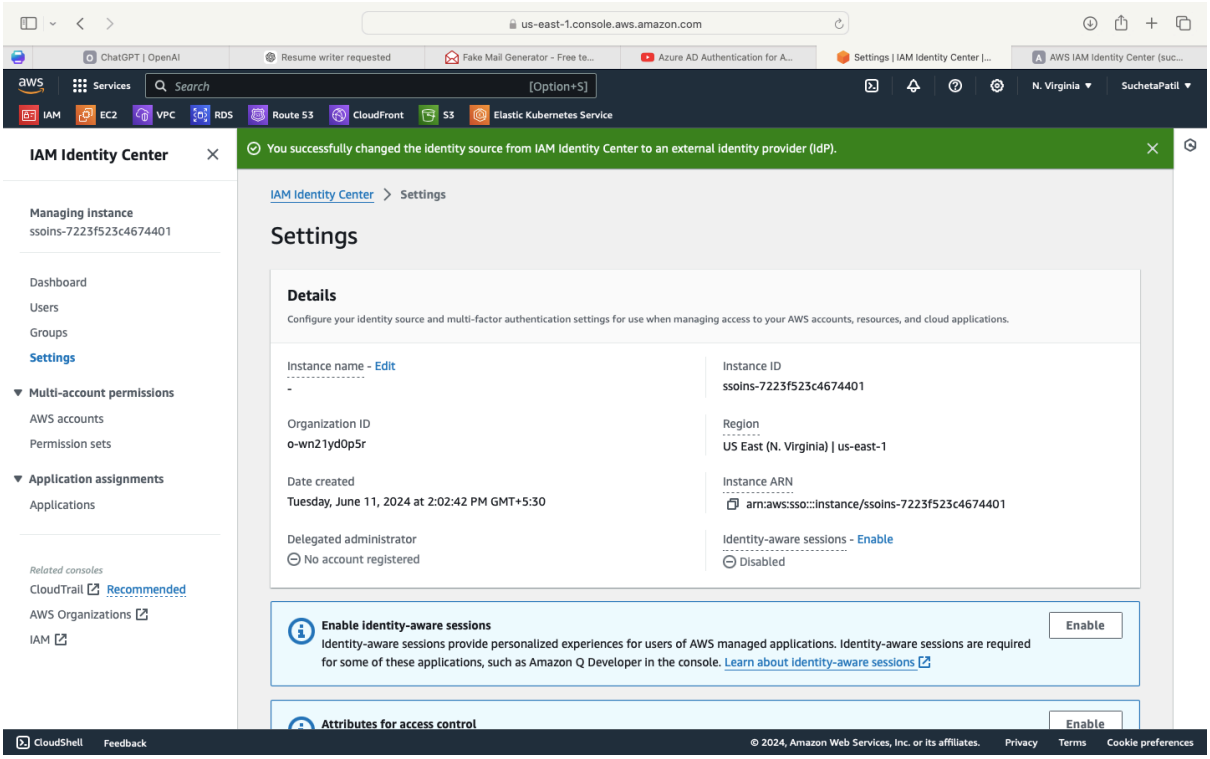



us-east-1.console.aws.amazon.com
IAM Identity Center > Settings > Change identity source
Step 1
Choose identity source
Step 2
Configure external identity provider
Step 3
Confirm change
Confirm change
Step 1: Choose identity source
Identity source
Identity source
External identity provider
Step 2: Configure external identity provider
Service provider metadata
IdP SAML metadata
AWS IAM Identity Center (successor to AWS Single Sign-On)-2.xml
Size: 14228 bytes
Last modified: Jun 11, 2024
Review and confirm
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

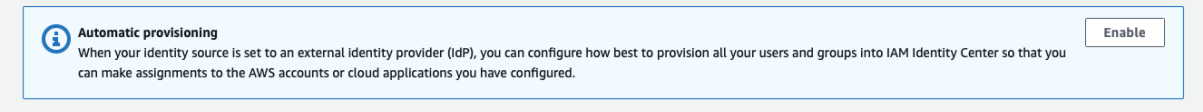

us-east-1.console.aws.amazon.com
Review and confirm
Review the following consequences of your requested identity source change:
You are changing your identity source to use an external identity provider (IdP).
IAM Identity Center will delete your current multi-factor authentication (MFA) configuration.
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
Cancel
Previous
Change identity source
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Type ACCEPT and click on Change identity source.

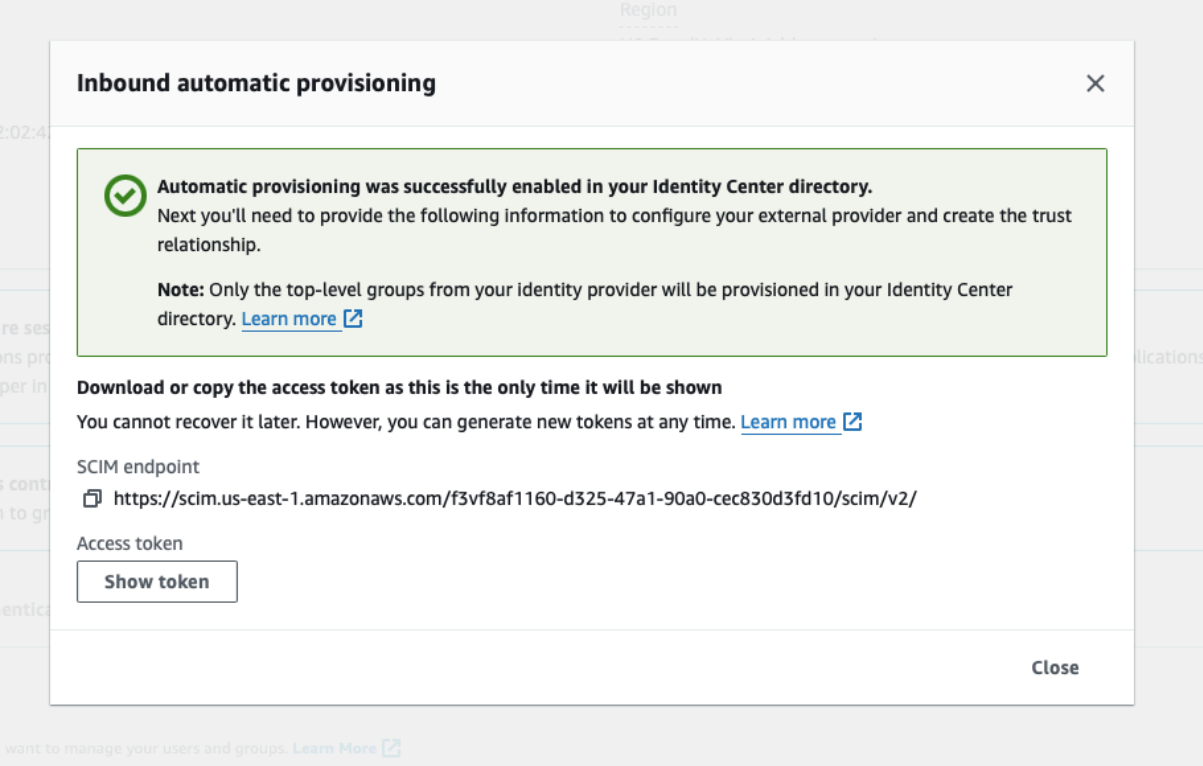


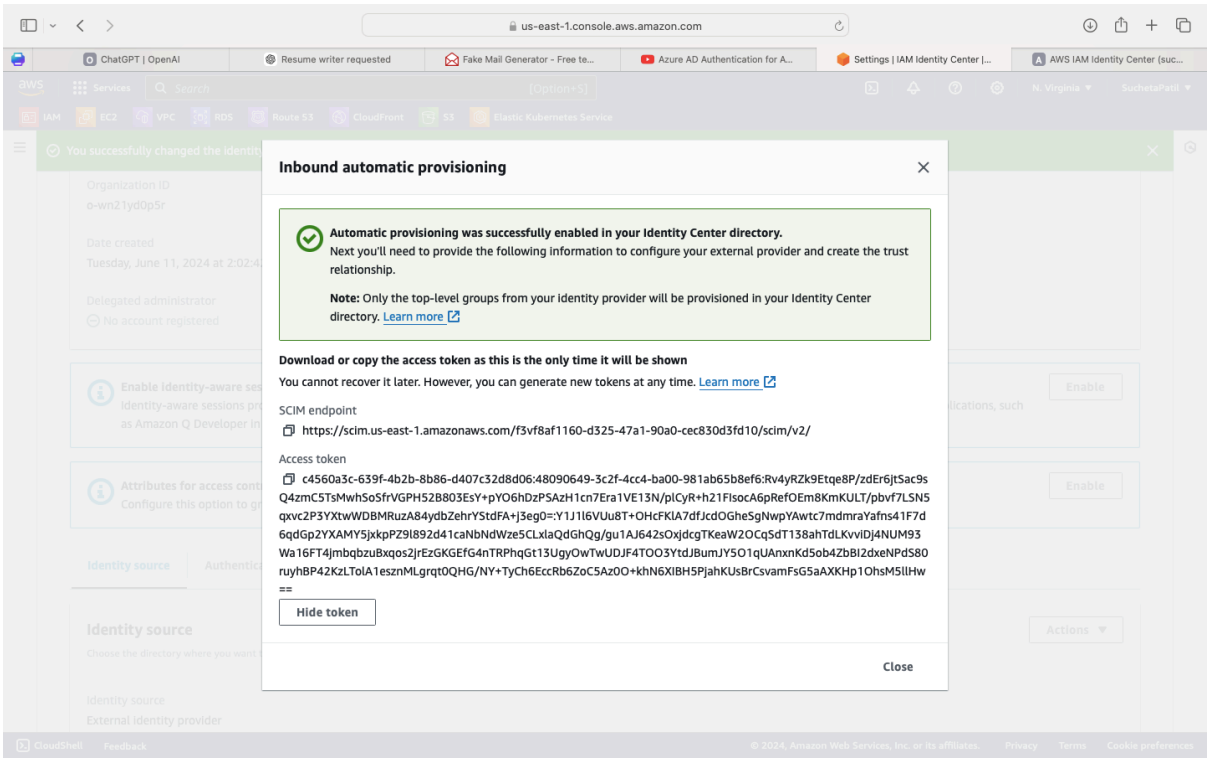


In the Setting page we need to enable Automatic provisioning.



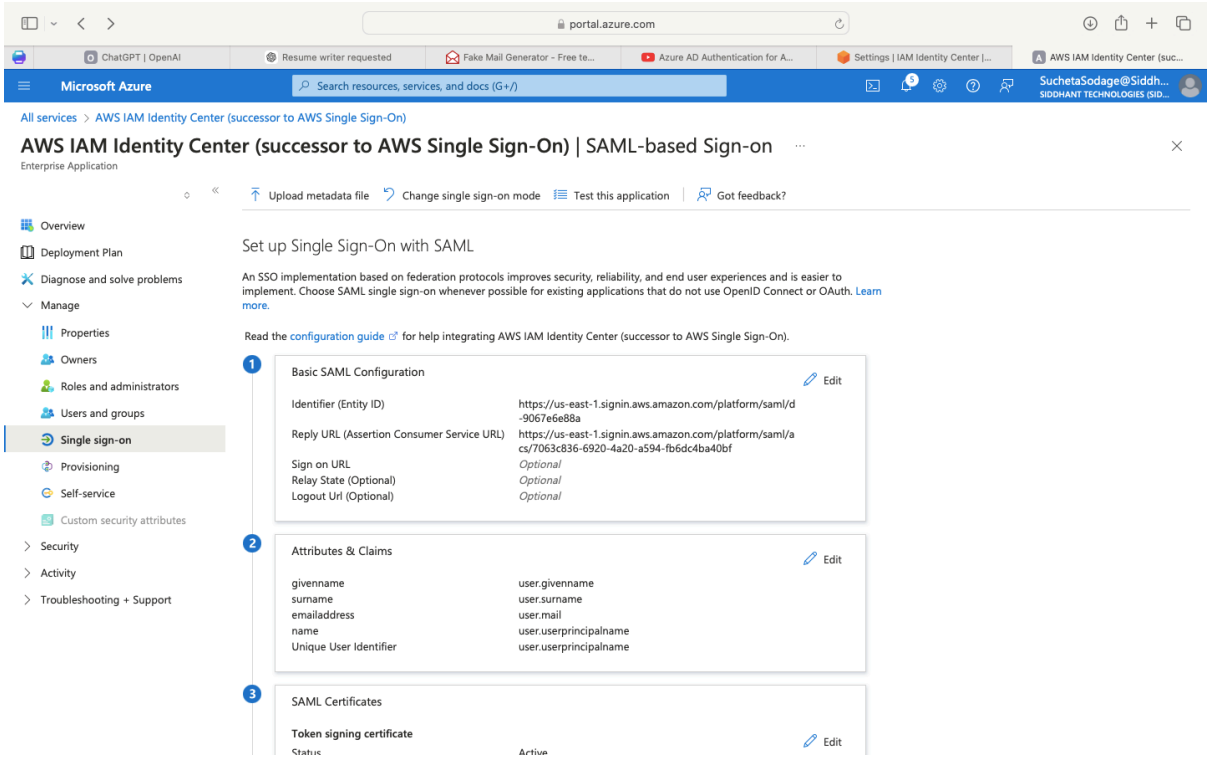
In this page click on Show Token. Which we need for further steps.



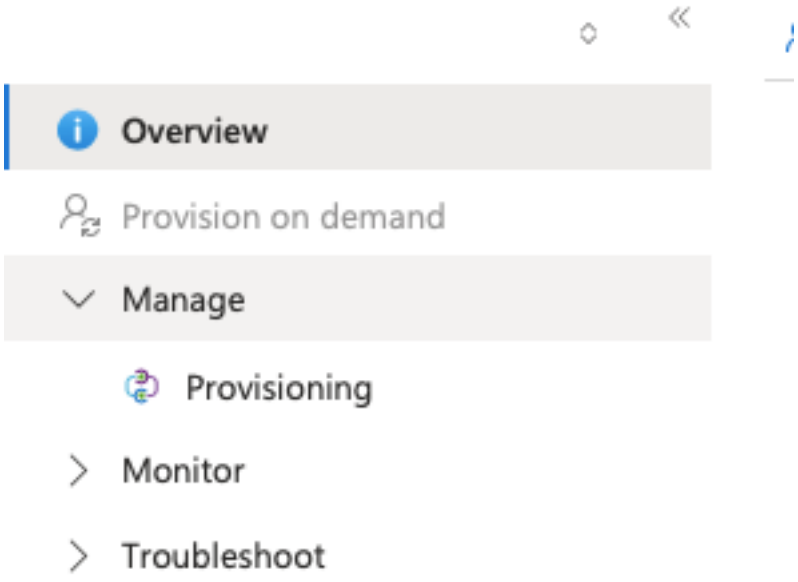


Copy Token Tenant URL and Secret Token and save it in Notes.

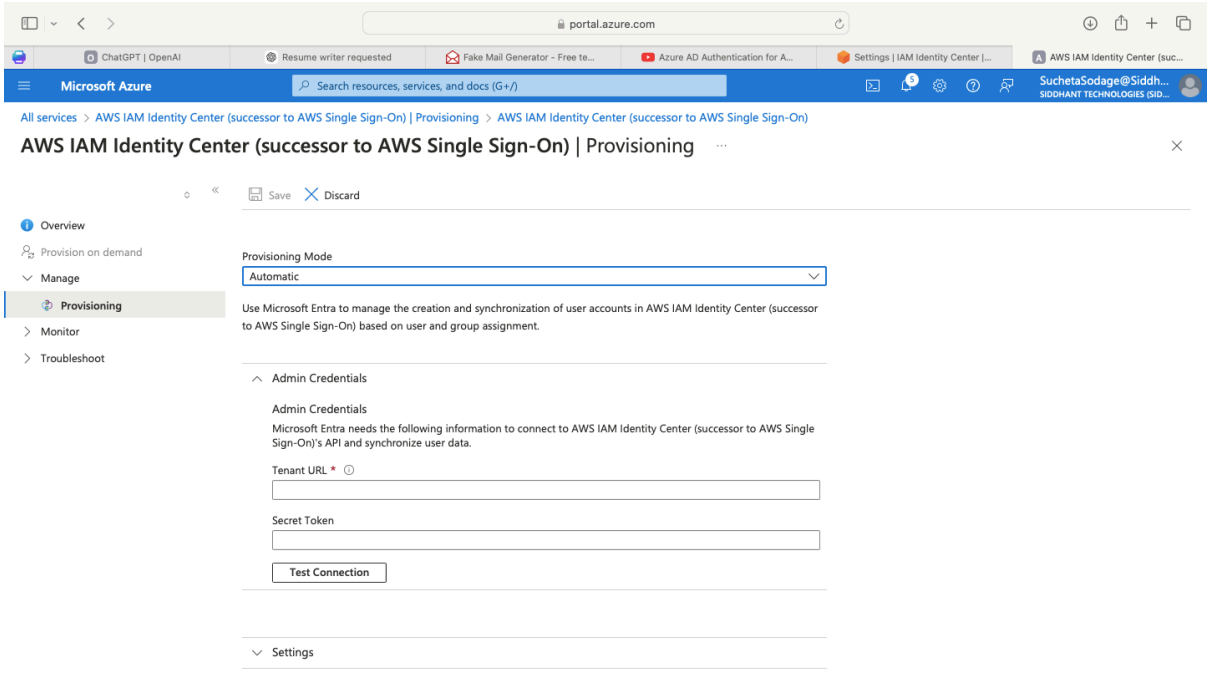
Now go back to Azure AWS AM Identity Center (successor to AWS Single Sign-On) page.



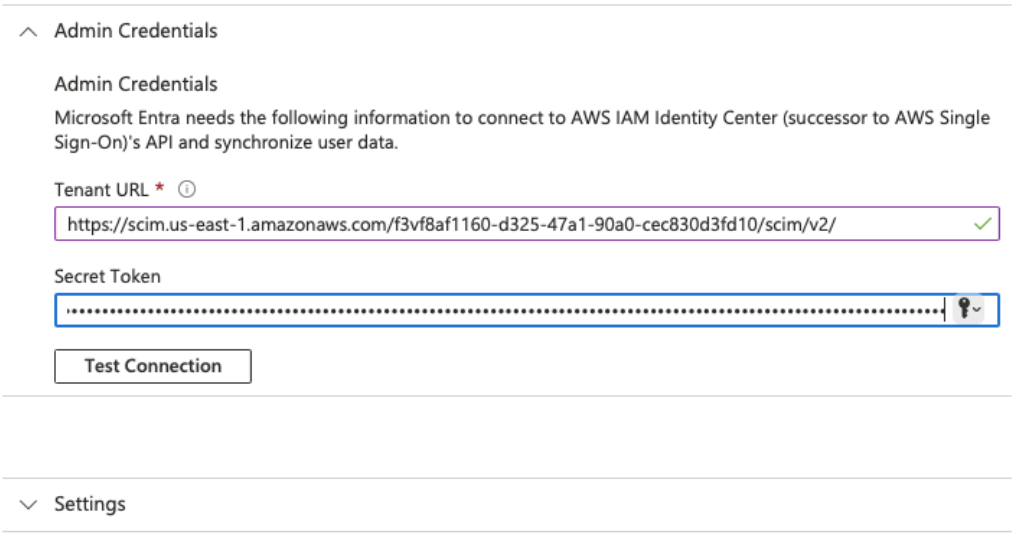
In left side manu select Manage, in that Provisioning option.



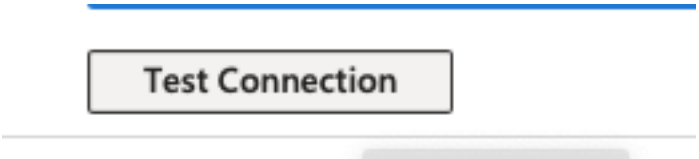
In Provisioning Mode select Automatic.

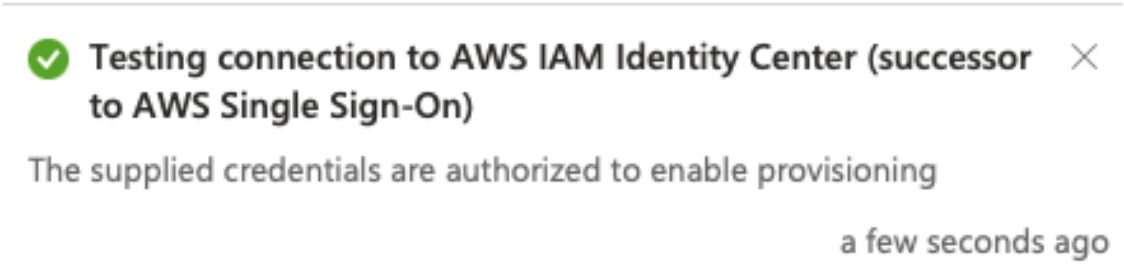


Paste copied Tenant URL and Secret Token.

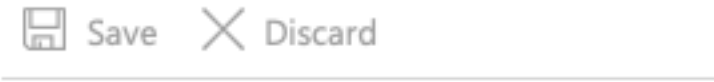


Test Connection.

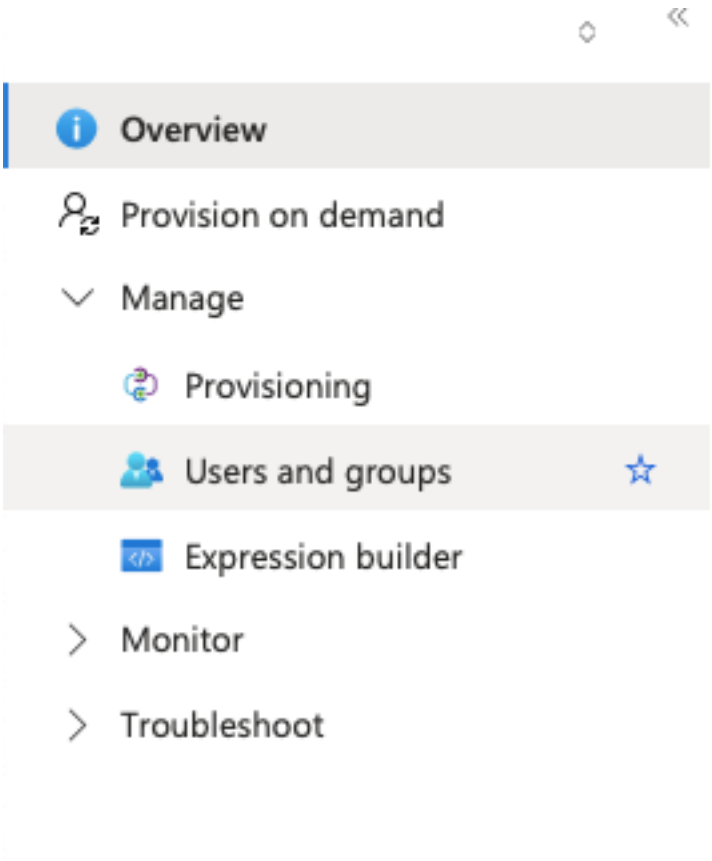




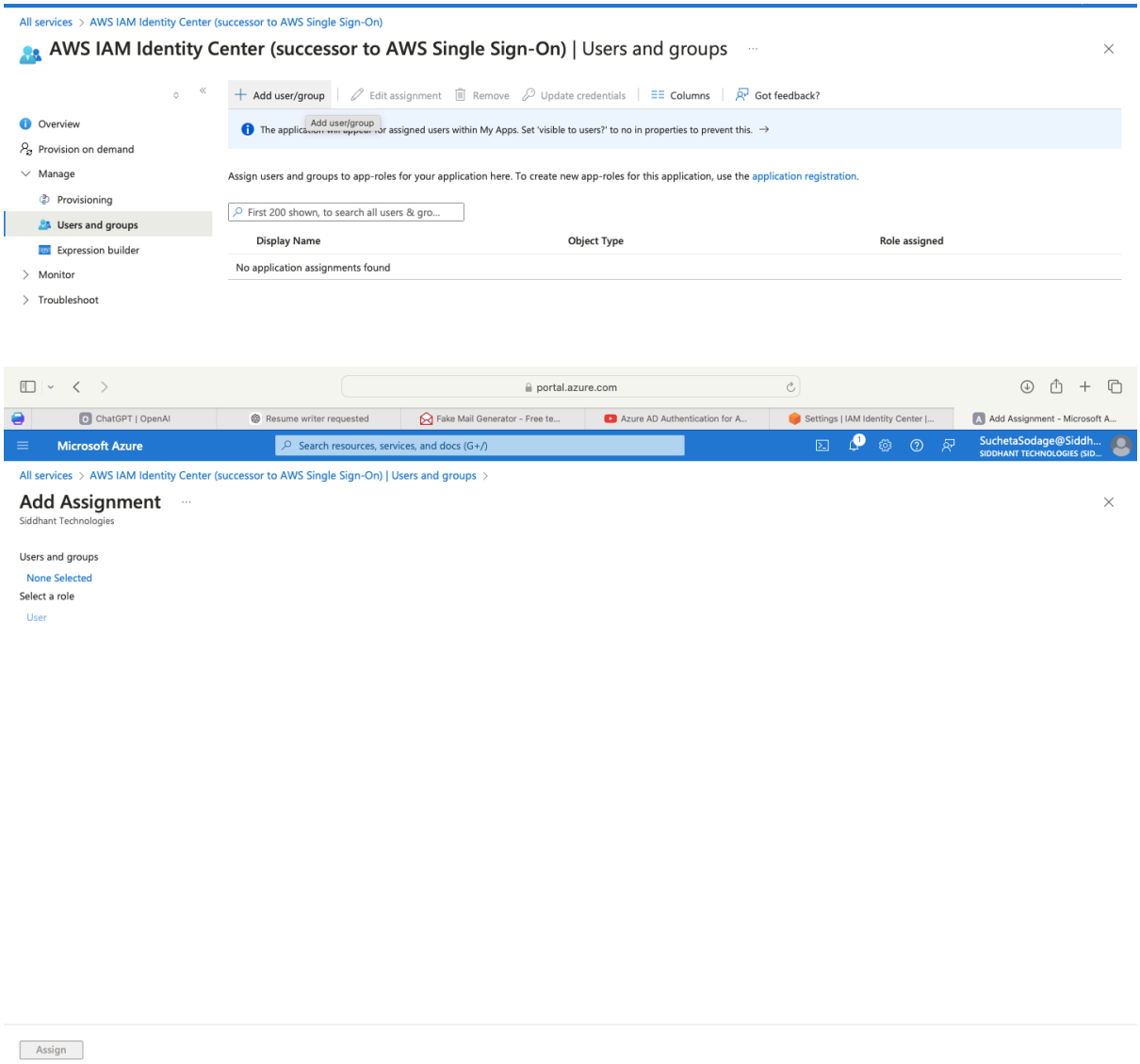
Save the changes.



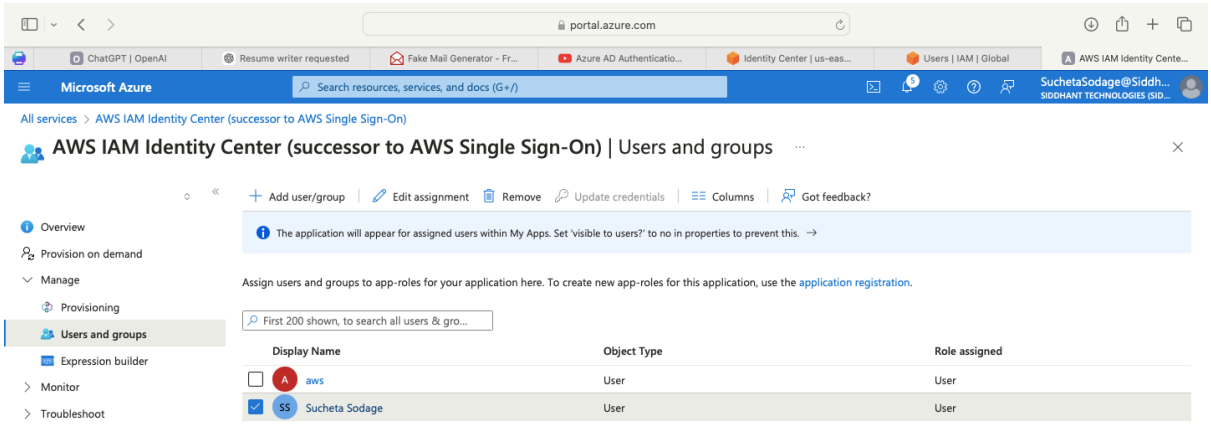
Now select Users and group option from left side options.

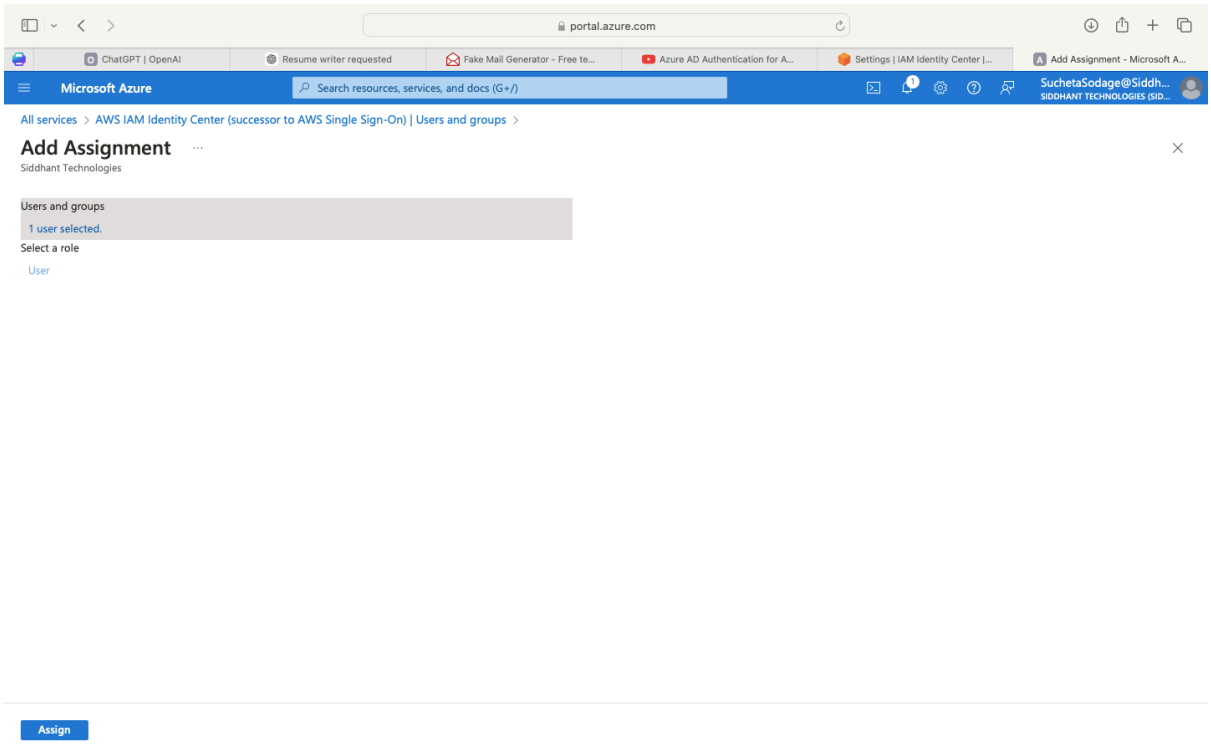


Add users and group.

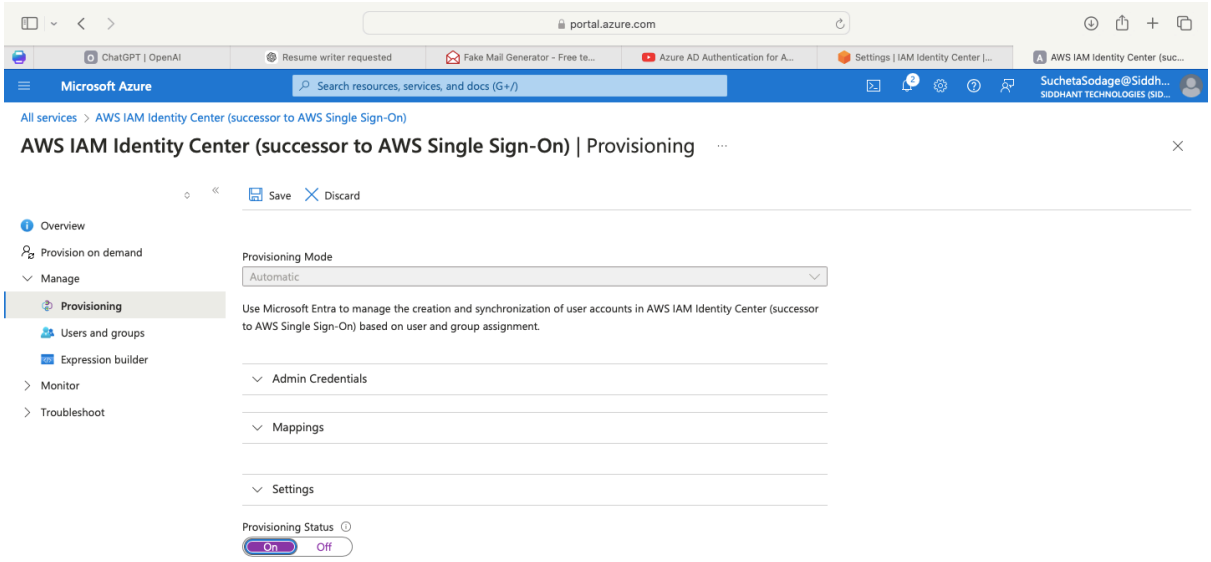


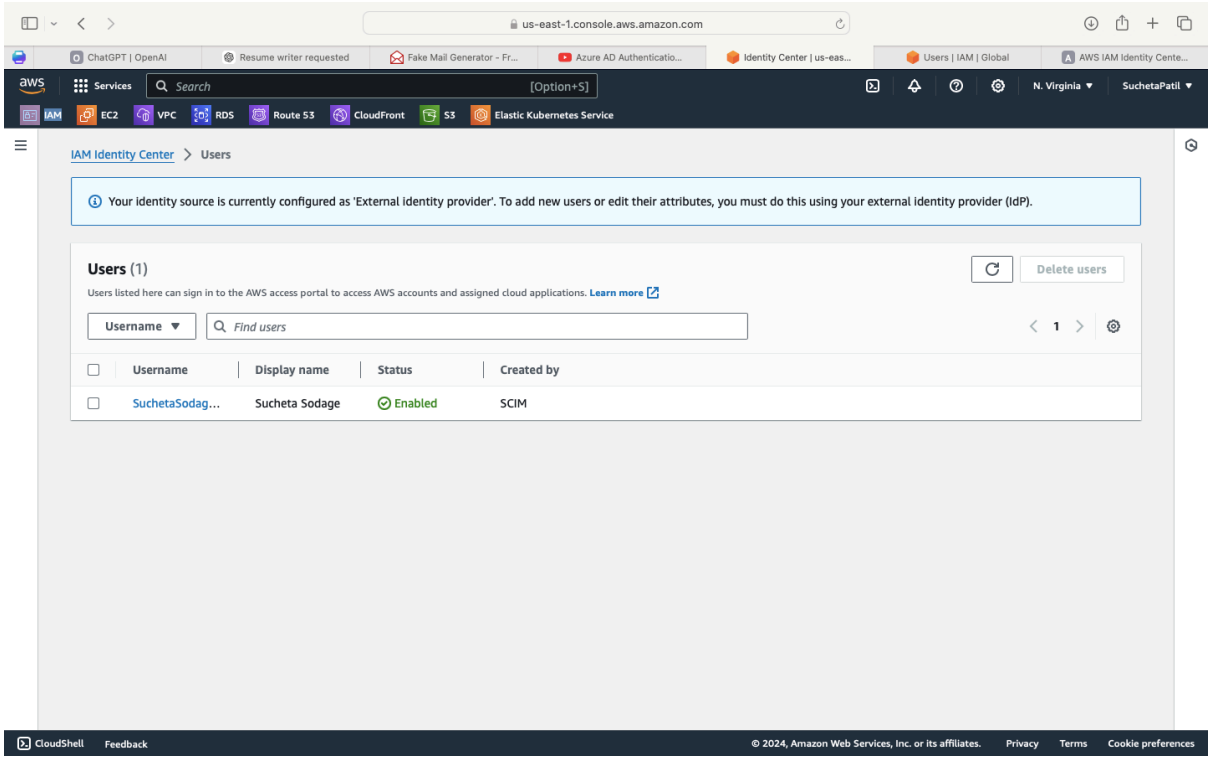
Click on Users and select User we want add to AWS account.





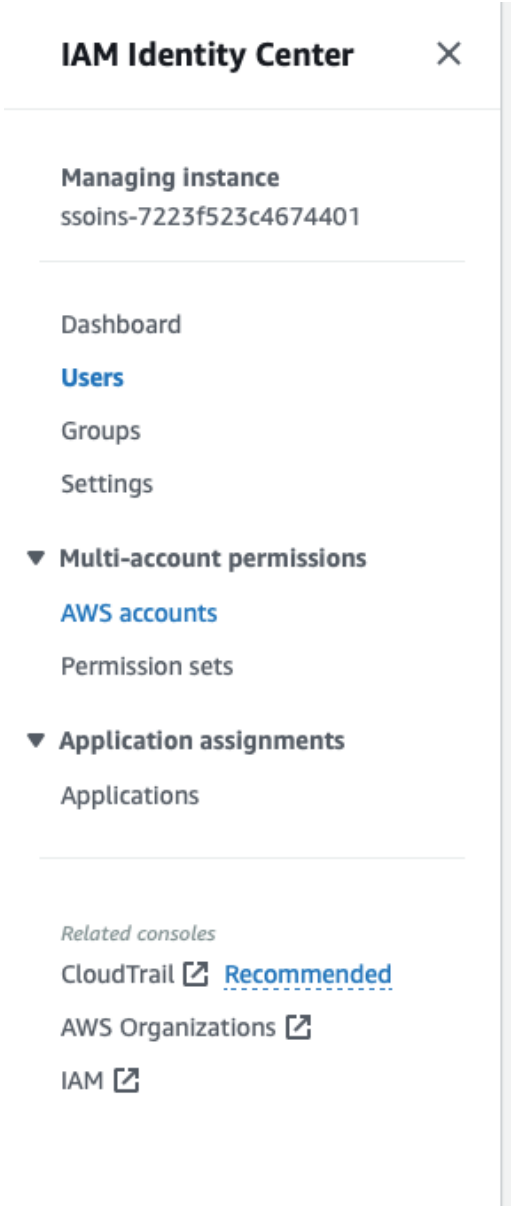
Again go back to Provisioning and change Provisioning Status to On.



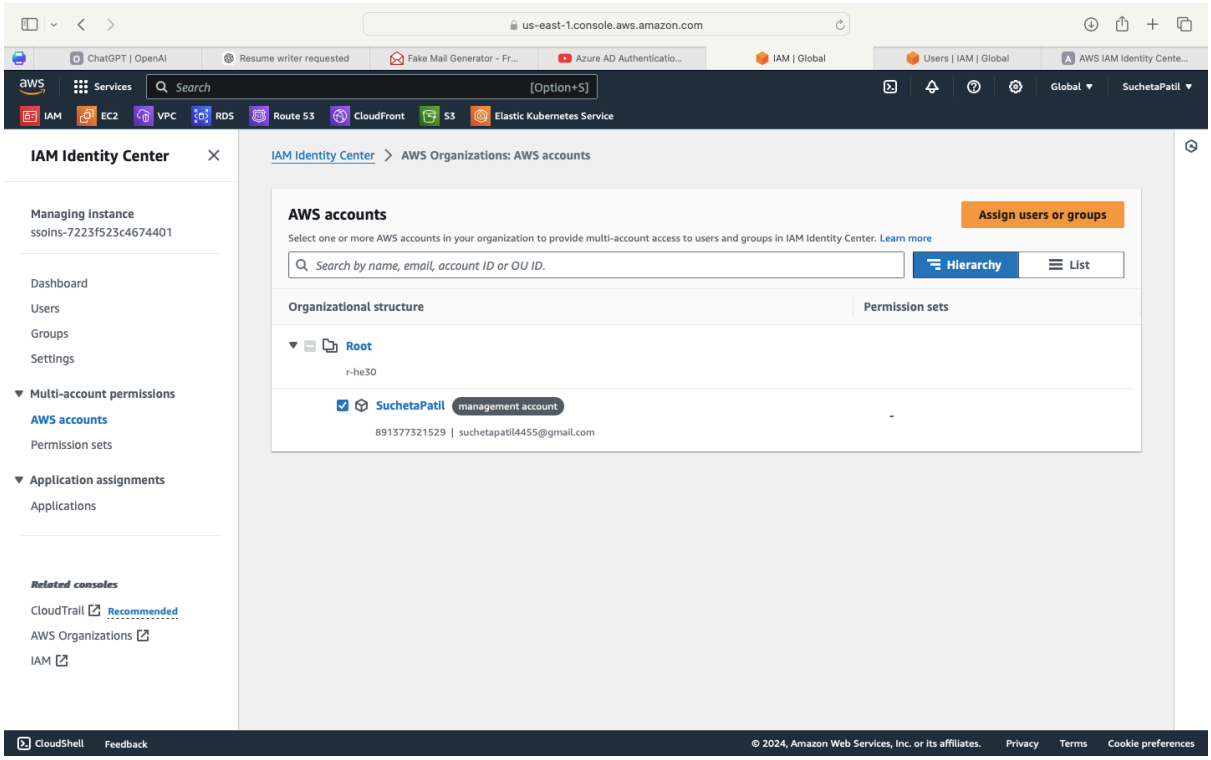


Now we can able to see our Azure Active Directory user in our AWS IAM Identity Center.

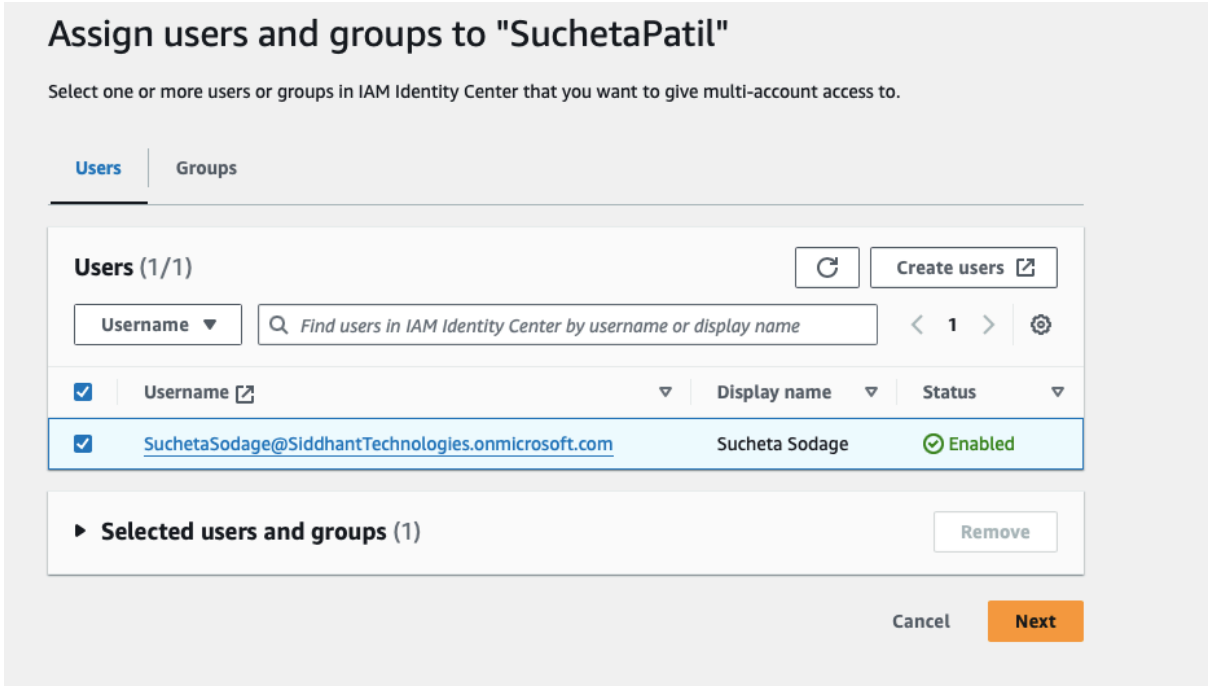
Now go to AWS Account option from left side options.



Select our user from there.



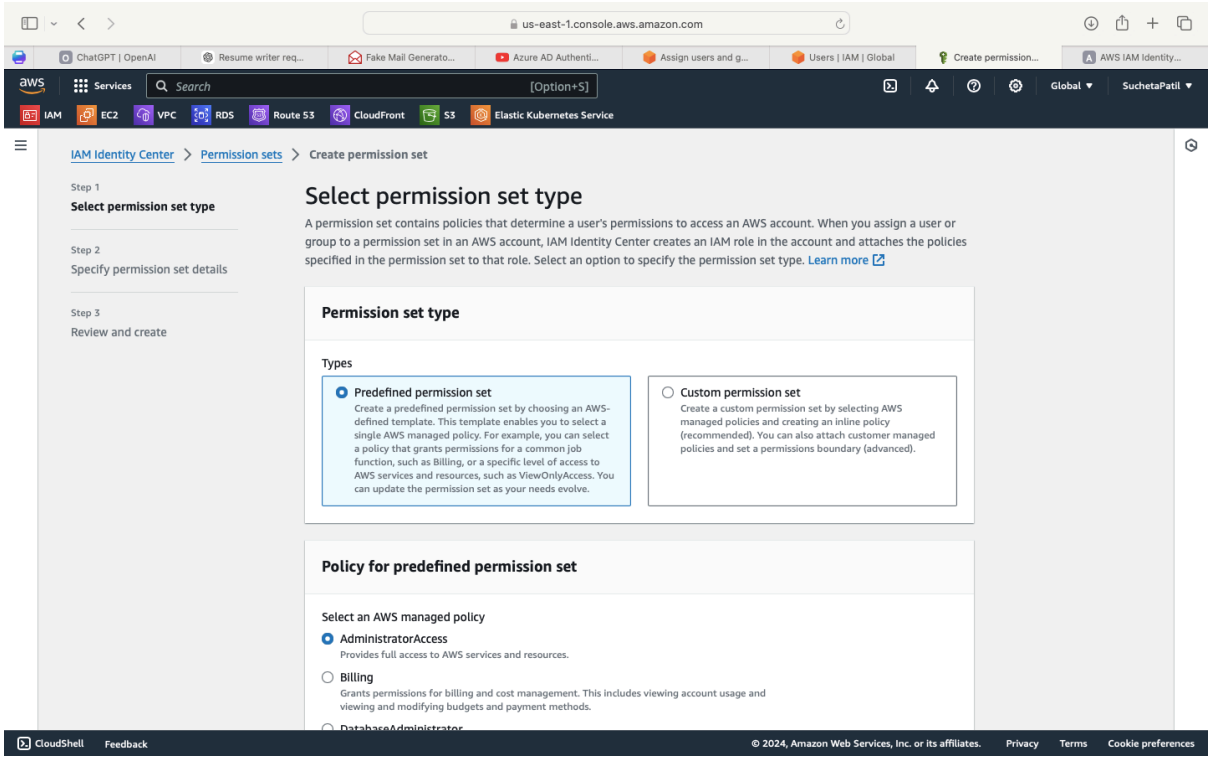
Now Assign users and groups you want to give multi-account access to.



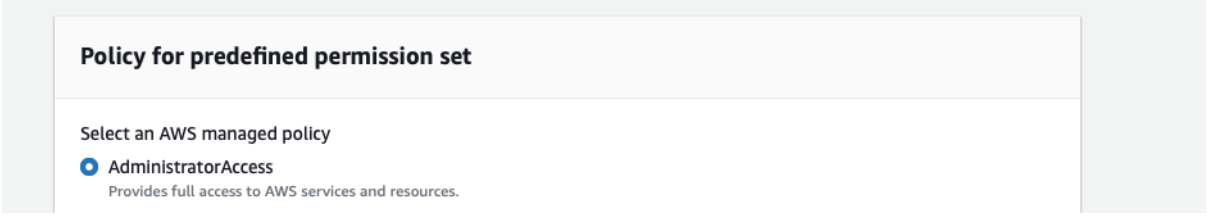
We have to assigne permission to the user for this select, Select permission set type

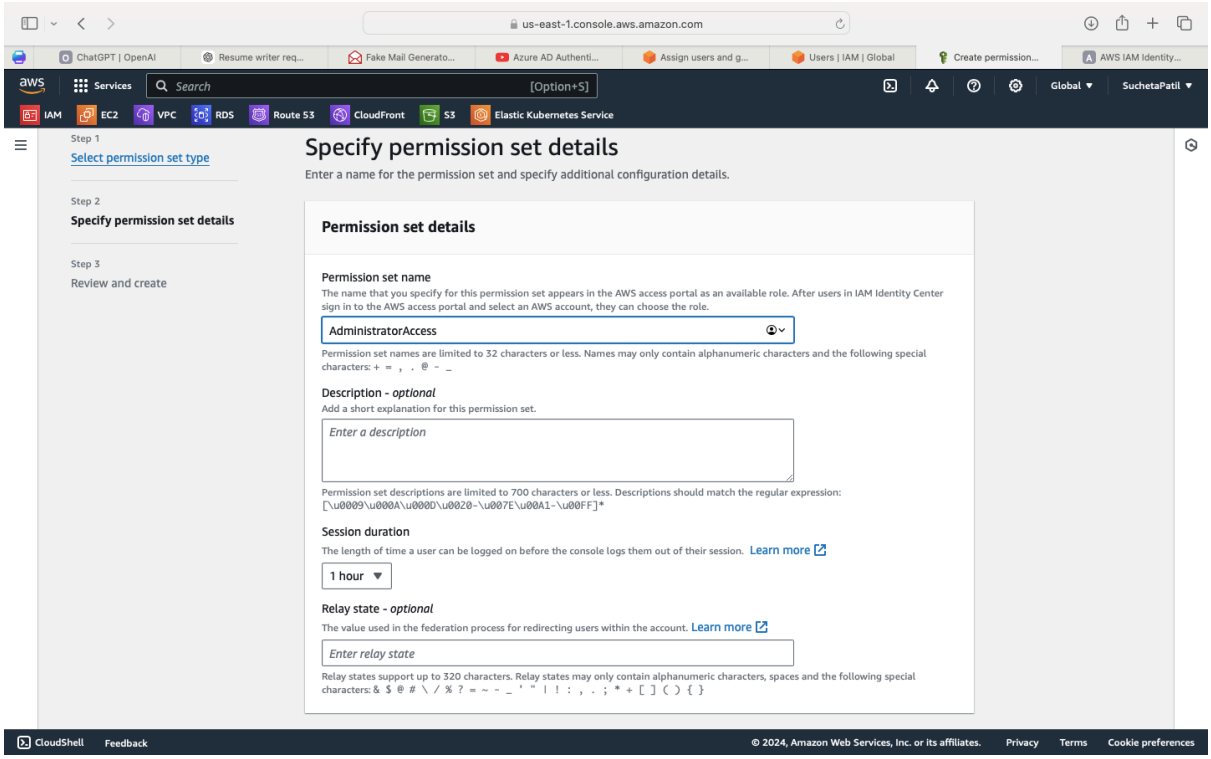
For assigning permission we have 2 options, Predefined permission set and Custom permission set.

Here we are Predefined permission set.

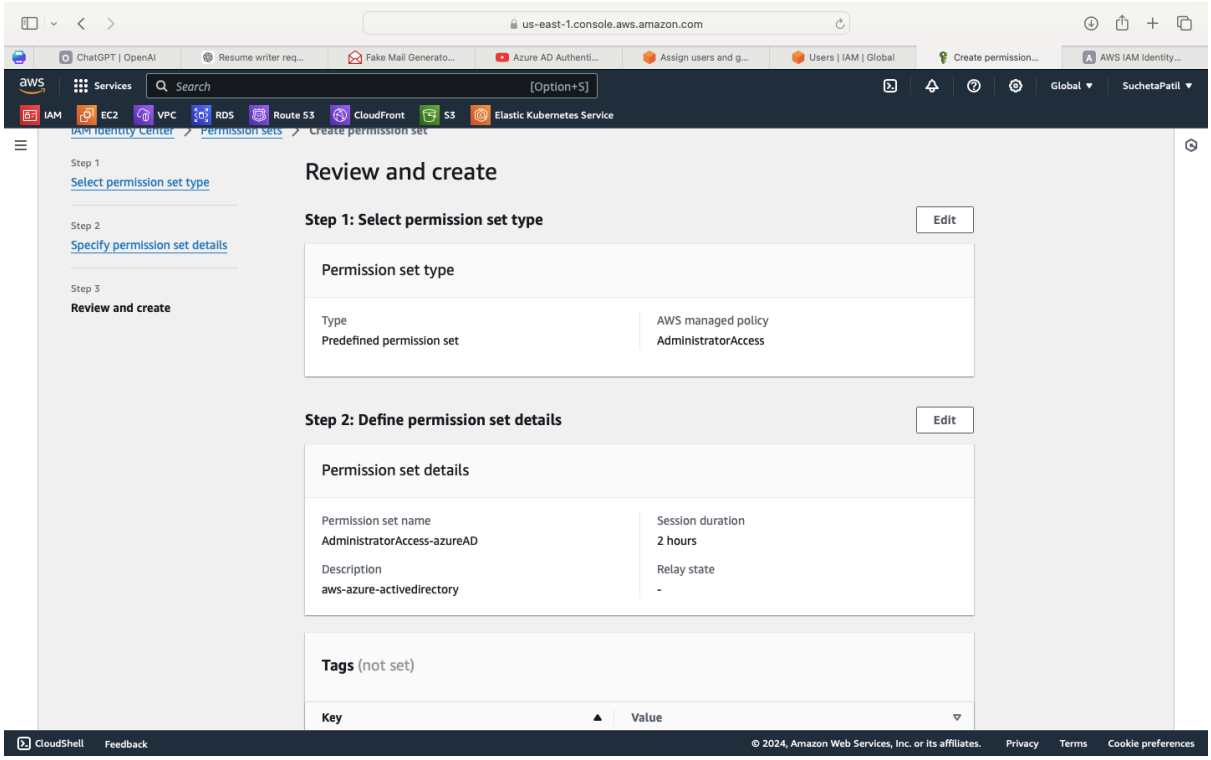


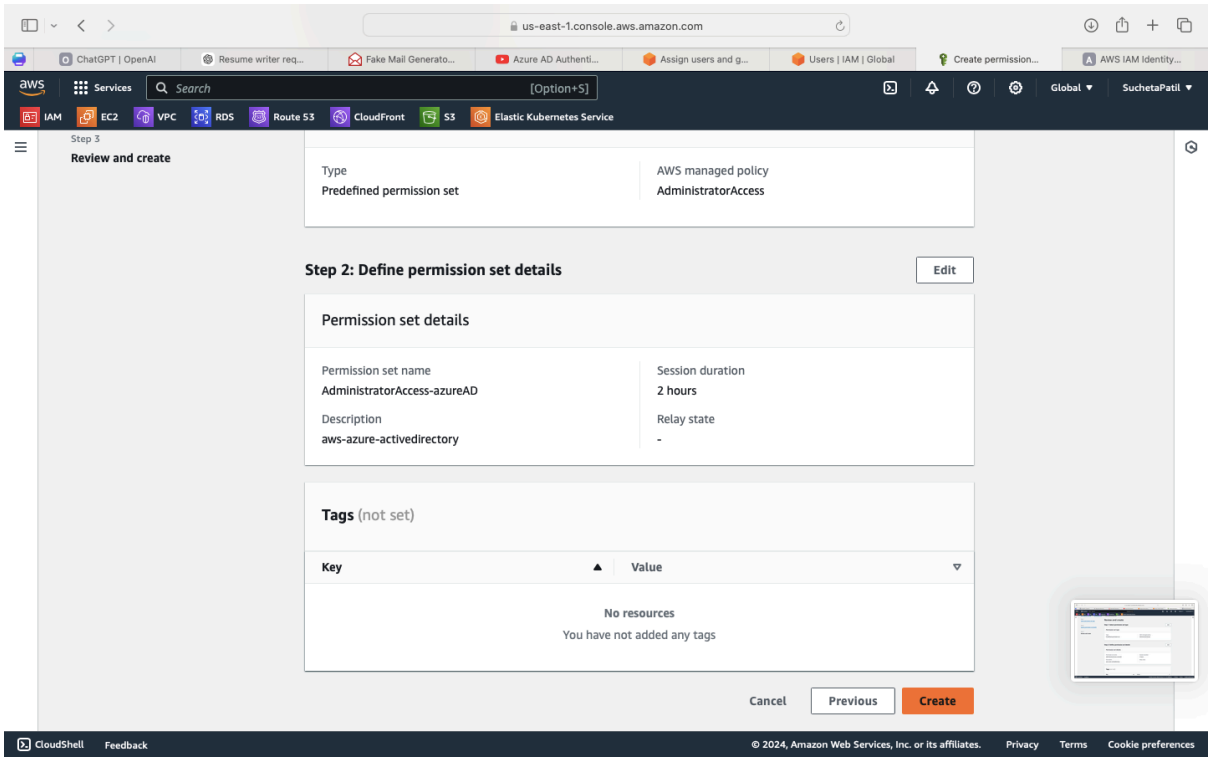
In this case we are providing Administrator Access.

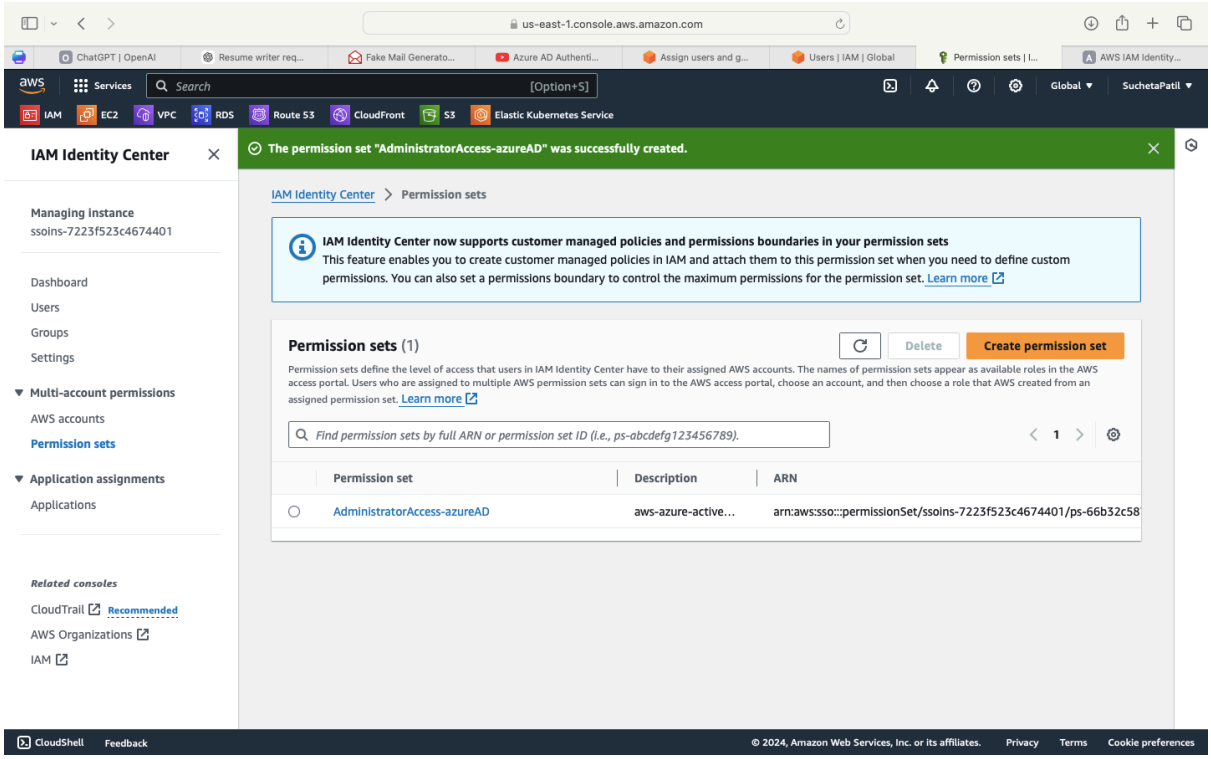



us-east-1.console.aws.amazon.com
ChatGPT | OpenAI
Resume writer req...
Fake Mail Generato...
Azure AD Authenti...
Assign users and g...
Users | IAM | Global
Create permission...
AWS IAM Identity...
Services
Search
[Option+S]
Global
SuchetaPatil
IAM
EC2
VPC
RDS
Route 53
CloudFront
S3
Elastic Kubernetes Service
Step 1
Select permission set type
Step 2
Specify permission set details
Step 3
Review and create
Specify permission set details
Enter a name for the permission set and specify additional configuration details.
Permission set details
Permission set name
The name that you specify for this permission set appears in the AWS access portal as an available role. After users in IAM Identity Center sign in to the AWS access portal and select an AWS account, they can choose the role.
AdministratorAccess
Permission set names are limited to 32 characters or less. Names may only contain alphanumeric characters and the following special characters: + = , . @ - _
Description - optional
Add a short explanation for this permission set.
Enter a description
Permission set descriptions are limited to 700 characters or less. Descriptions should match the regular expression: [\u0009\u000A\u000D\u0020-\u007E\u00A1-\u00FF]*
Session duration
The length of time a user can be logged on before the console logs them out of their session. Learn more
1 hour
Relay state - optional
The value used in the federation process for redirecting users within the account. Learn more
Enter relay state
Relay states support up to 320 characters. Relay states may only contain alphanumeric characters, spaces and the following special characters: & $ @ # \ / % ? = ~ - _ ' " ! : , . ; * + [ ] ( ) { }
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

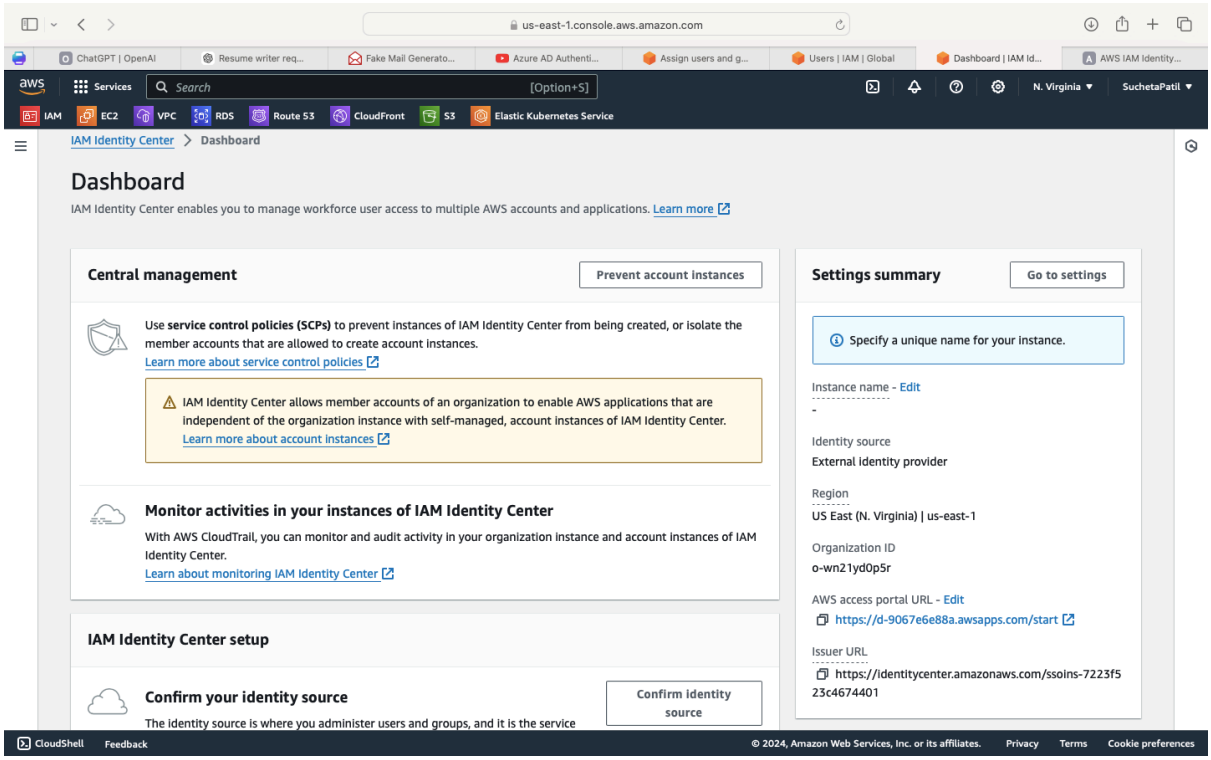
Review and create.



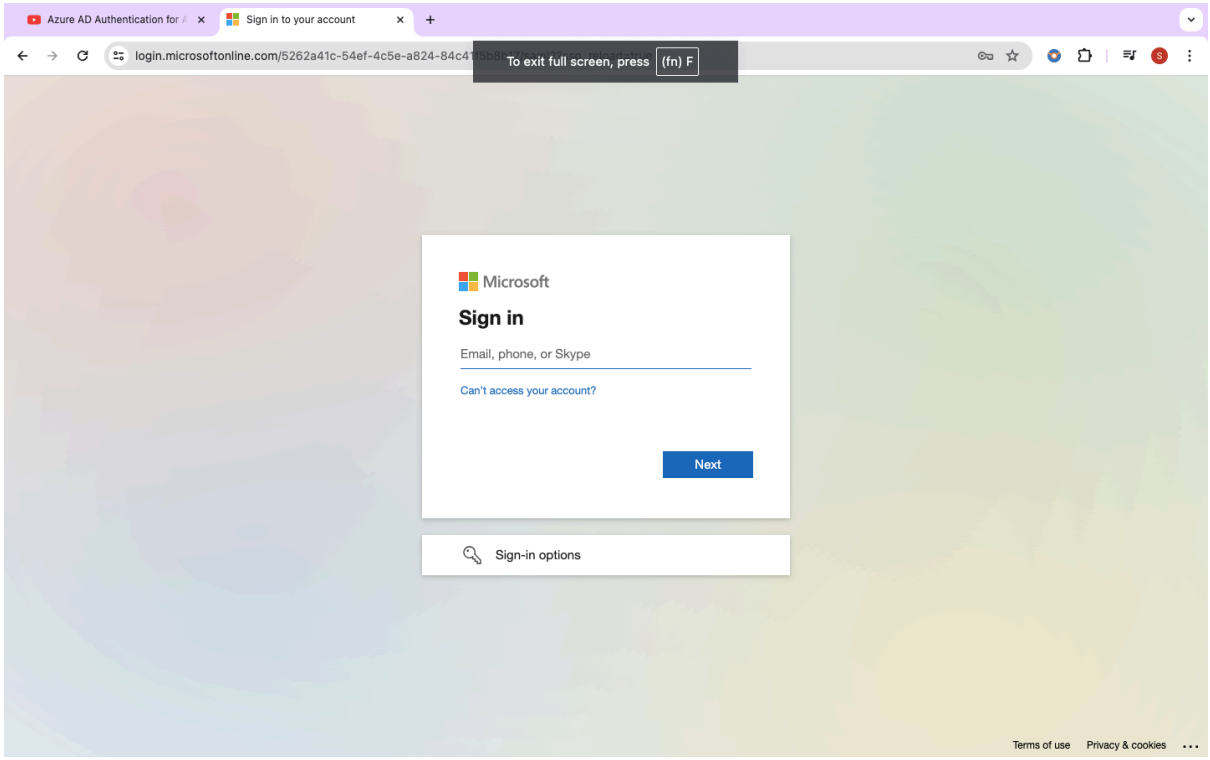


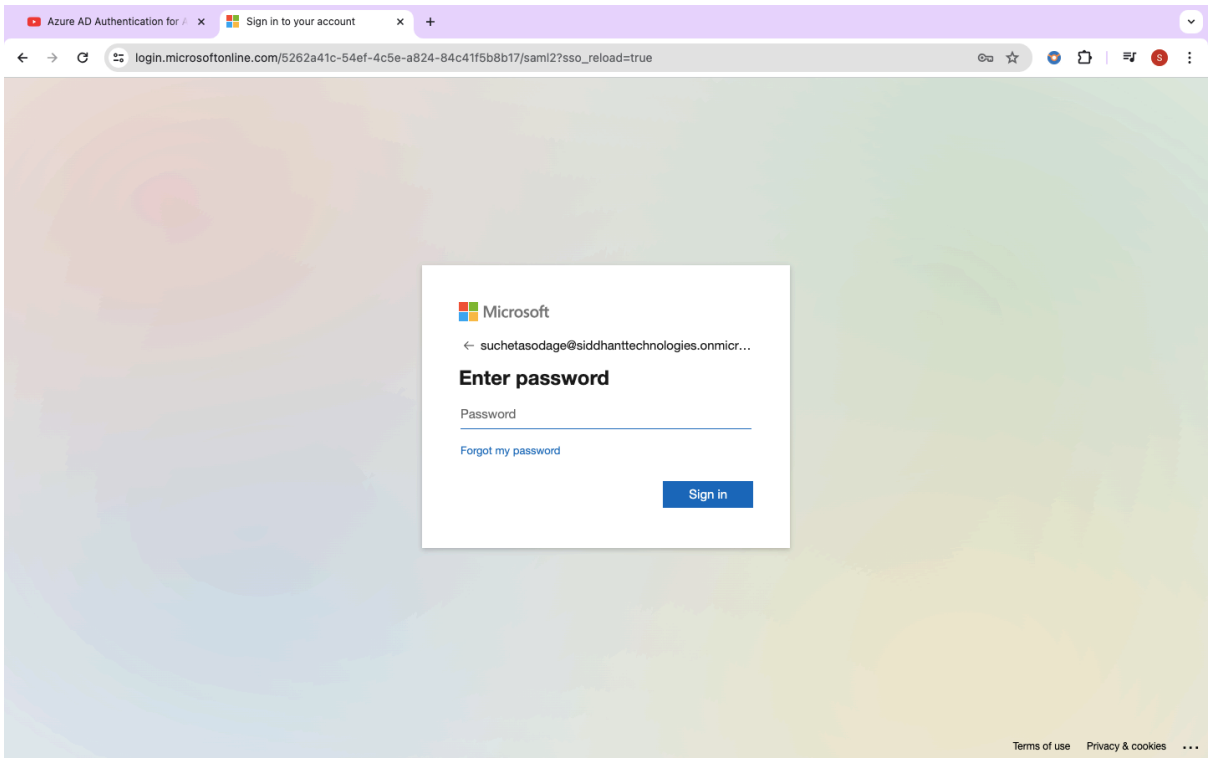


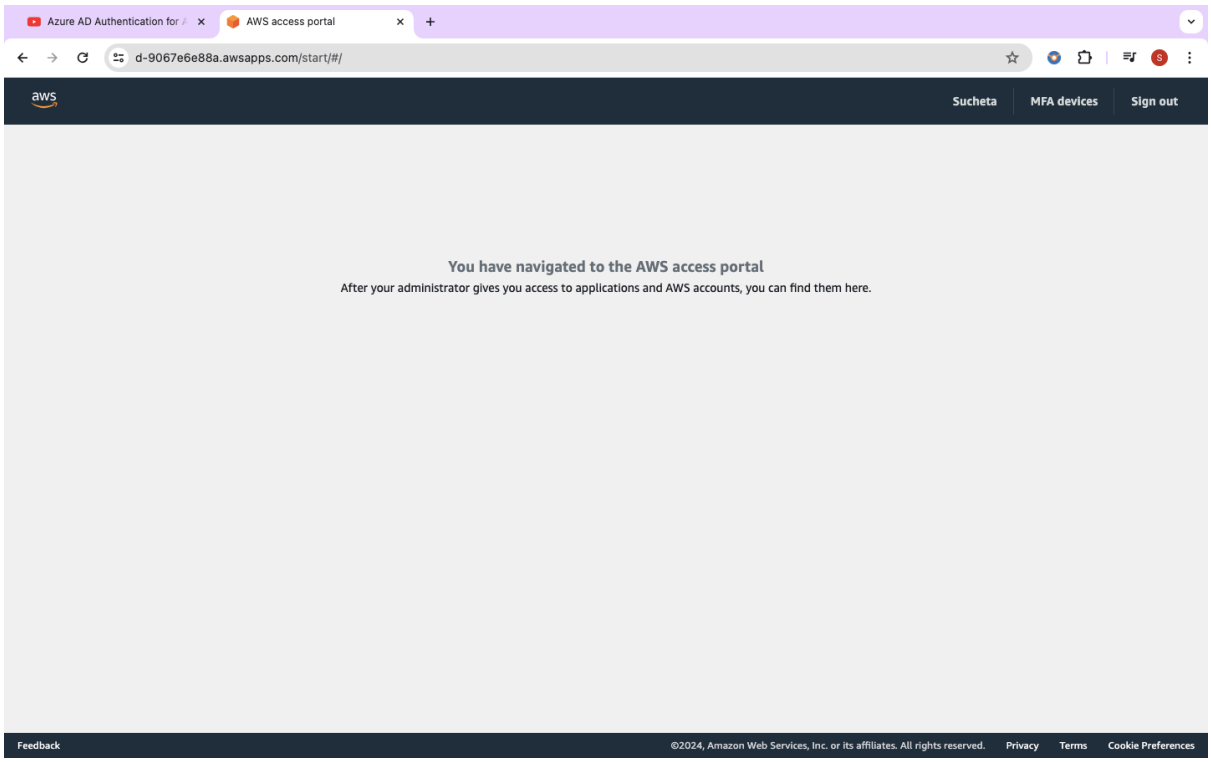
Move to IAM Identity Center Dashboard.



In right side Settings summary, copy AWS access portal URL. Hit the URL.






Azure AD Authentication for
AWS access portal
d-9067e6e88a.awsapps.com/start/#/
aws
Sucheta
MFA devices
Sign out
You have navigated to the AWS access portal
After your administrator gives you access to applications and AWS accounts, you can find them here.
Feedback
©2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy
Terms
Cookie Preferences