Practical-8 Single-sign on(SSO)

Date:-02/04/2024 Submission Date:- 06/04/2024 Writeup:-

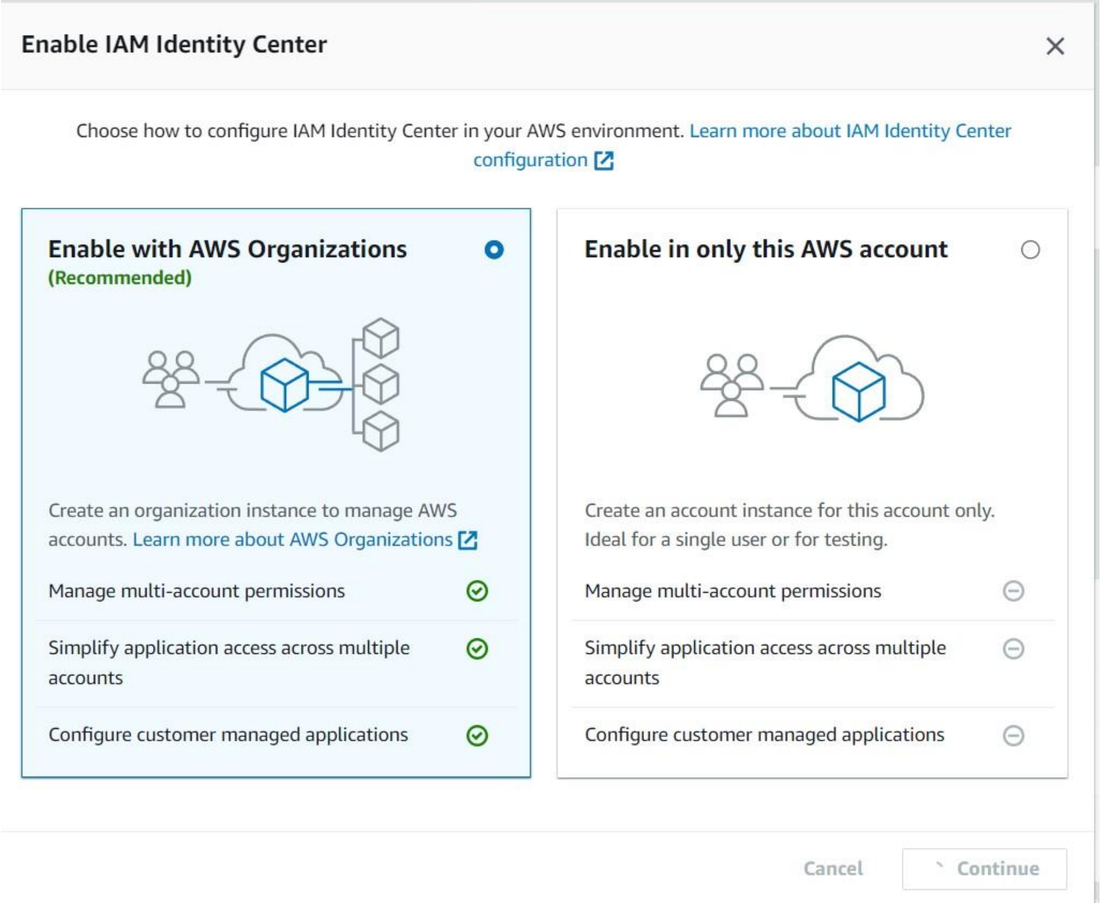
- **SSO**

Single Sign-On (SSO):

Definition:
Single Sign-On (SSO) is an authentication process that allows users to access multiple applications or systems with a single set of credentials (such as username and password).
Authentication Flow:
When a user attempts to access an application or system that supports SSO, they are redirected to a centralized authentication server.
The user enters their credentials (e.g., username and password) on the authentication server's login page.
The authentication server verifies the user's identity and generates a security token.
This token is then passed back to the application or system that the user initially tried to access.
Token-based Authentication:
Instead of re-entering credentials for each application, the security token serves as proof of authentication.
The token is used to grant access to the user without requiring them to provide their credentials again.
Key Components:
Identity Provider (IdP): The central authentication server that verifies user identities and issues security tokens. It is responsible for managing user authentication and access control.
Service Provider (SP): The application or system that the user wants to access. It relies on the IdP for user authentication.

-

Step 1 Go to IAM Management Console and you can enable any one from the below



Enable IAM Identity Center

Choose how to configure IAM Identity Center in your AWS environment. Learn more about IAM Identity Center configuration

Enable with AWS Organizations ●
(Recommended)

Create an organization instance to manage AWS accounts. Learn more about AWS Organizations

Manage multi-account permissions ✓

Simplify application access across multiple accounts ✓

Configure customer managed applications ✓

Enable in only this AWS account ○

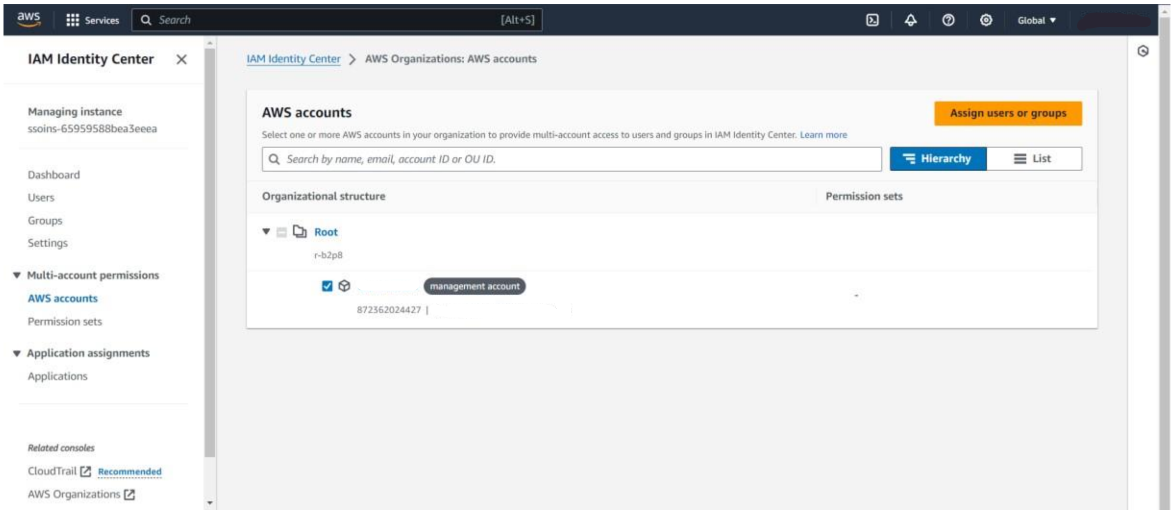
Create an account instance for this account only. Ideal for a single user or for testing.

Manage multi-account permissions ⊖

Simplify application access across multiple accounts ⊖

Configure customer managed applications ⊖

Step 2- Under the IAM Identity Center Go to Multi Account Permissions and select AWS Accounts.
 Under AWS Account select any one of the Management Account



[redacted]

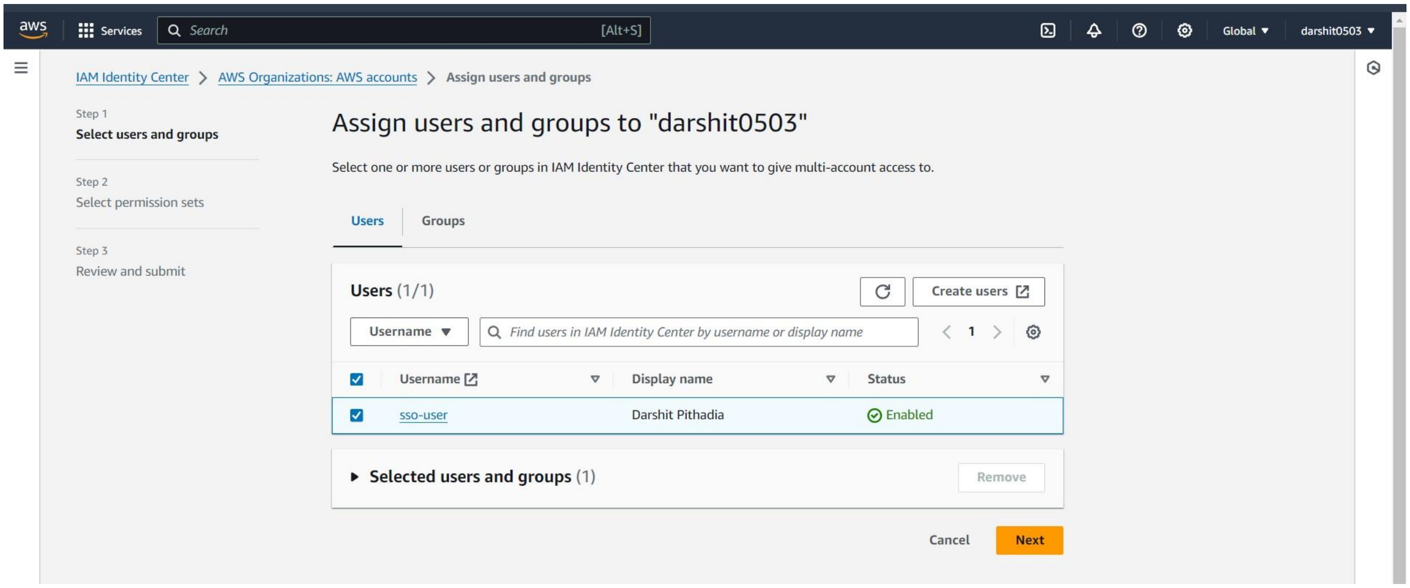
Managing instance
ssoins-65959588bea3eeea

AWS accounts

Select one or more AWS accounts in your organization to provide multi-account access to users and groups in IAM Identity Center. Learn more

Organizational structure	Permission sets
▾ □ Root r-b2p8	
☑ management account 872362024427 |	-

Step 3- Under the AWS Account select the Users and Groups you want to assign SSO



IAM Identity Center > AWS Organizations: AWS accounts > Assign users and groups

Step 1
Select users and groups

Step 2
Select permission sets

Step 3
Review and submit

Assign users and groups to "darshit0503"

Select one or more users or groups in IAM Identity Center that you want to give multi-account access to.

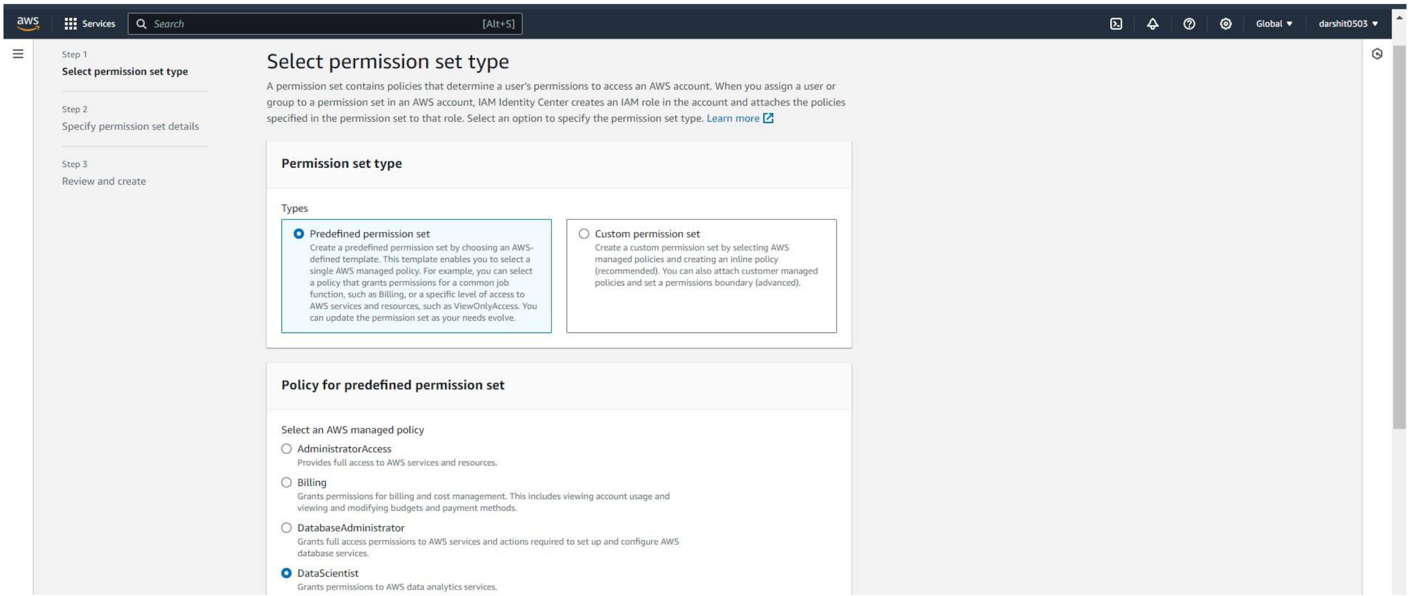
Users (1/1)

Create users
Username ▼
Find users in IAM Identity Center by username or display name
1

☑	Username	Display name	Status
☑	sso-user	Darshit Pithadia	Enabled

▸ **Selected users and groups** (1)

Step 4- Select Permission type we want to assign



Step 1
Select permission set type

Step 2
Specify permission set details

Step 3
Review and create

Select permission set type

A permission set contains policies that determine a user's permissions to access an AWS account. When you assign a user or group to a permission set in an AWS account, IAM Identity Center creates an IAM role in the account and attaches the policies specified in the permission set to that role. Select an option to specify the permission set type. Learn more

Permission set type

Types

● Predefined permission set
Create a predefined permission set by choosing an AWS-defined template. This template enables you to select a single AWS managed policy. For example, you can select a policy that grants permissions for a common job function, such as Billing, or a specific level of access to AWS services and resources, such as ViewOnlyAccess. You can update the permission set as your needs evolve.

○ Custom permission set
Create a custom permission set by selecting AWS managed policies and creating an inline policy (recommended). You can also attach customer managed policies and set a permissions boundary (advanced).

Policy for predefined permission set

Select an AWS managed policy

○ AdministratorAccess
Provides full access to AWS services and resources.

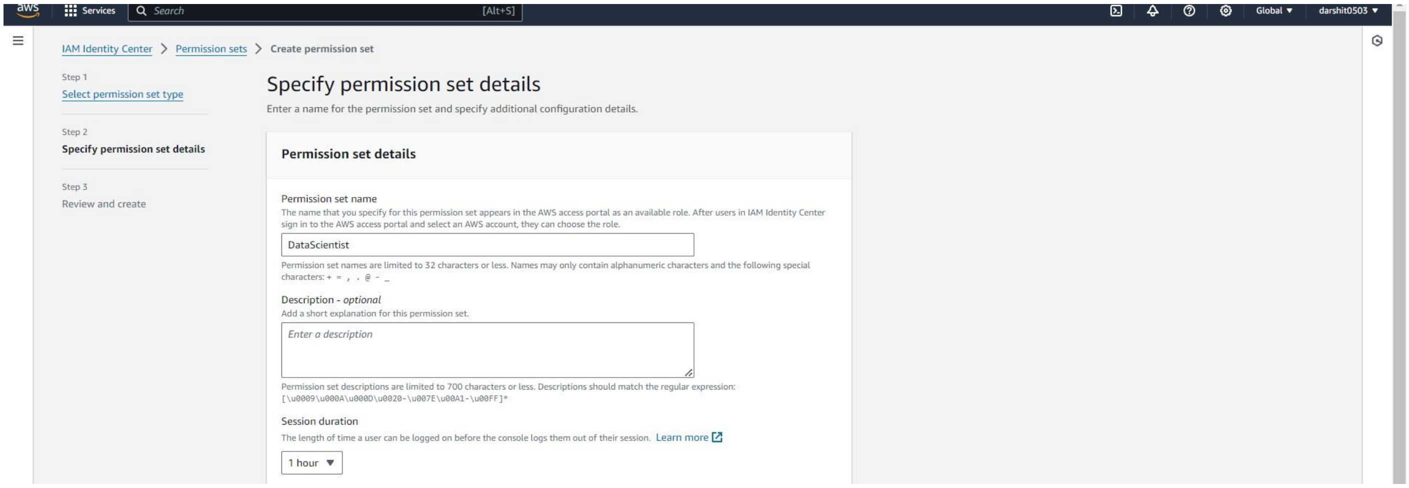
○ Billing
Grants permissions for billing and cost management. This includes viewing account usage and viewing and modifying budgets and payment methods.

○ DatabaseAdministrator
Grants full access permissions to AWS services and actions required to set up and configure AWS database services.

● DataScientist
Grants permissions to AWS data analytics services.

-

Step 5 Provide the Name for the same



IAM Identity Center > Permission sets > Create permission set

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.

DataScientist

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.

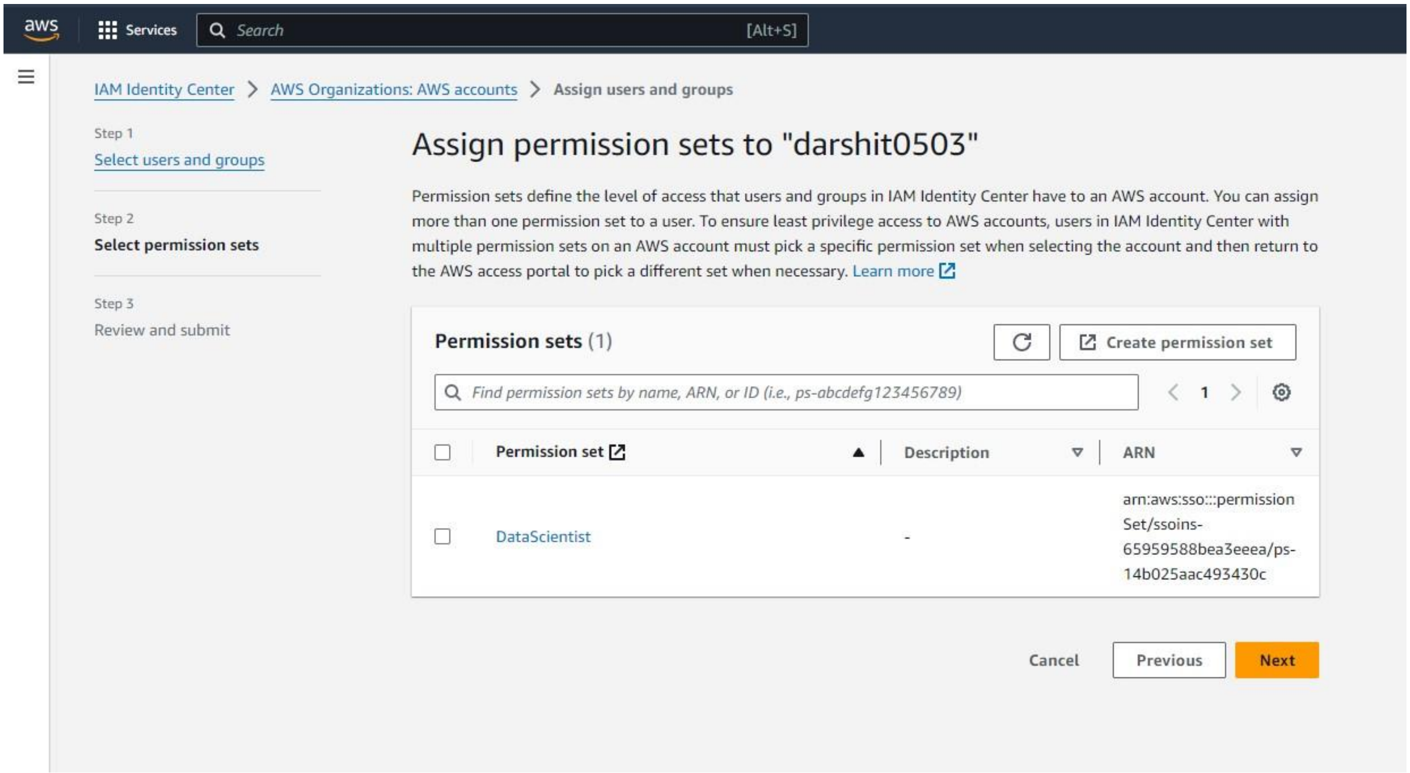
Enter a description

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 ▼

Step 6- Select the Permission Set we want to assign



IAM Identity Center > AWS Organizations: AWS accounts > Assign users and groups

Step 1
Select users and groups

Step 2
Select permission sets

Step 3
Review and submit

Assign permission sets to "darshit0503"

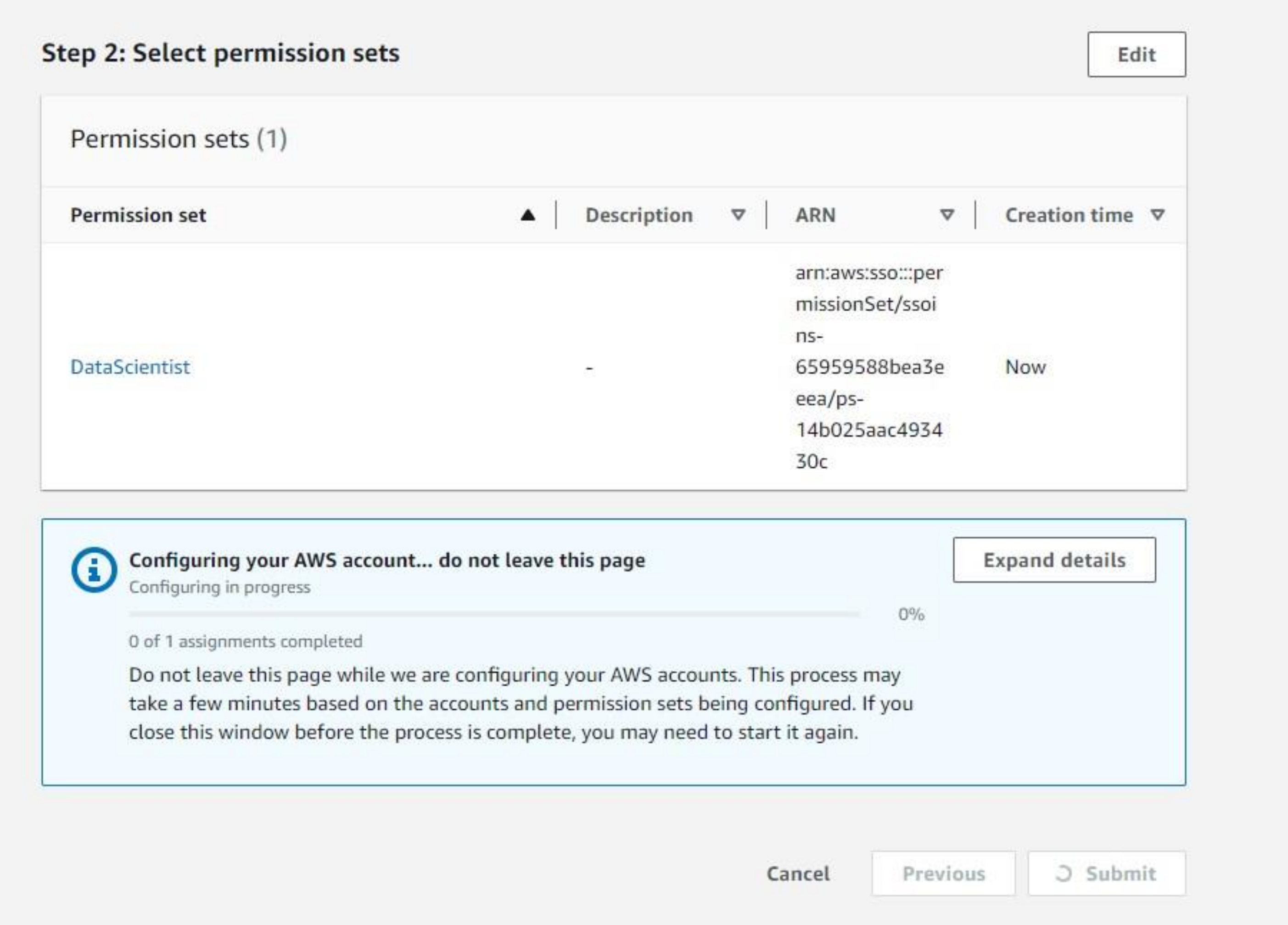
Permission sets define the level of access that users and groups in IAM Identity Center have to an AWS account. You can assign more than one permission set to a user. To ensure least privilege access to AWS accounts, users in IAM Identity Center with multiple permission sets on an AWS account must pick a specific permission set when selecting the account and then return to the AWS access portal to pick a different set when necessary. Learn more

Permission sets (1)

Create permission set
Find permission sets by name, ARN, or ID (i.e., ps-abcdefg123456789)
< 1 >

□	Permission set ▲	Description	ARN
□	DataScientist	-	arn:aws:sso:::permissionSet/ssoins-65959588bea3eeea/ps-14b025aac493430c

Step 7- It will start Cofirguring based on the Permissions



Step 2: Select permission sets

Permission sets (1)

Permission set	Description	ARN	Creation time
DataScientist	-	arn:aws:sso:::permissionSet/ssoins-65959588bea3eeea/ps-14b025aac493430c	Now

Configuring your AWS account... do not leave this page

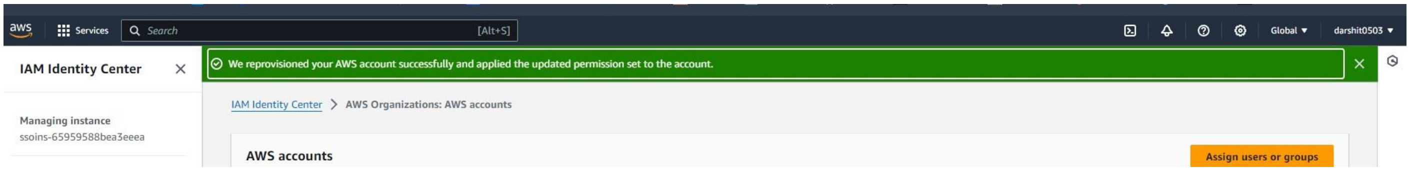
Configuring in progress

0%

0 of 1 assignments completed

Do not leave this page while we are configuring your AWS accounts. This process may take a few minutes based on the accounts and permission sets being configured. If you close this window before the process is complete, you may need to start it again.

Step 8 – SSO Assigned



IAM Identity Center

We reprovisioned your AWS account successfully and applied the updated permission set to the account.

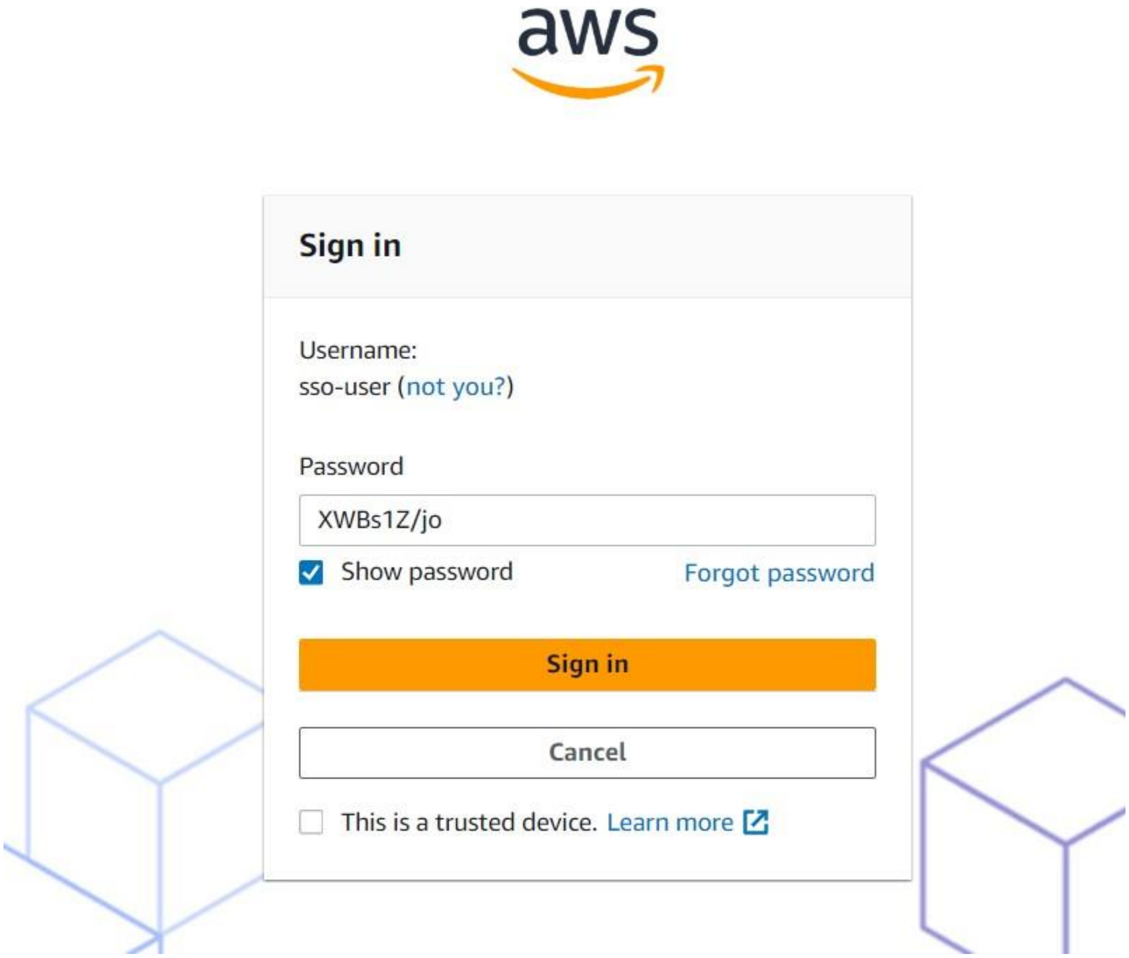
IAM Identity Center > AWS Organizations: AWS accounts

Managing instance
ssoins-65959588bea3eeea

AWS accounts

Step 9 SSO with One time Password provided

-



Sign in

Username:
sso-user (not you?)

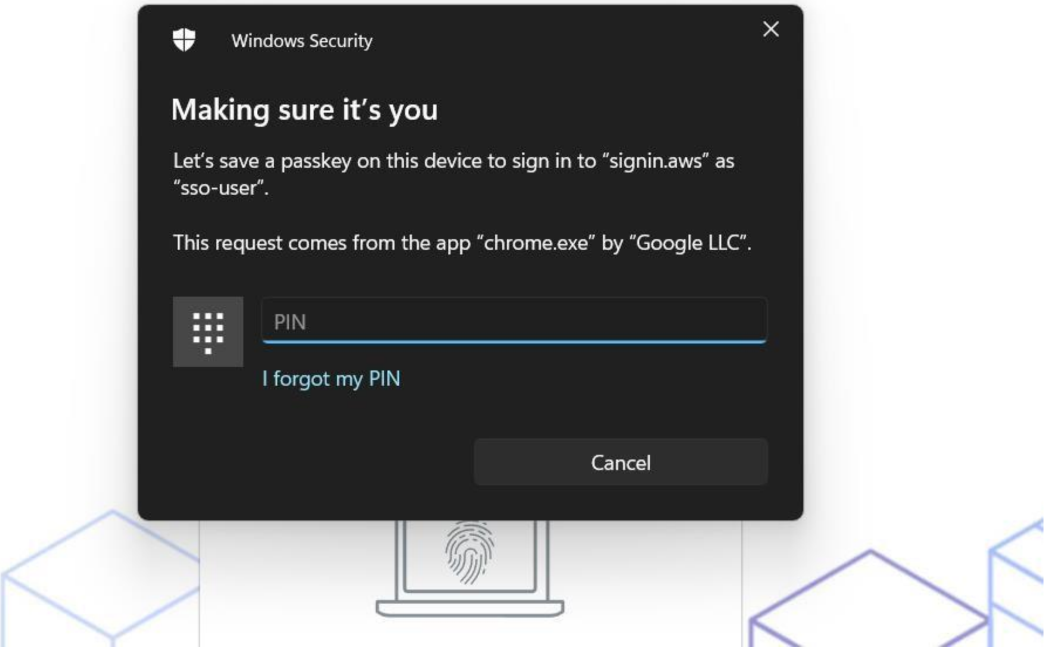
Password

XWBs1Z/jo

☑ Show password Forgot password

□ This is a trusted device. Learn more

Step 10- Assign MFA from the provided options provided



Windows Security

Making sure it’s you

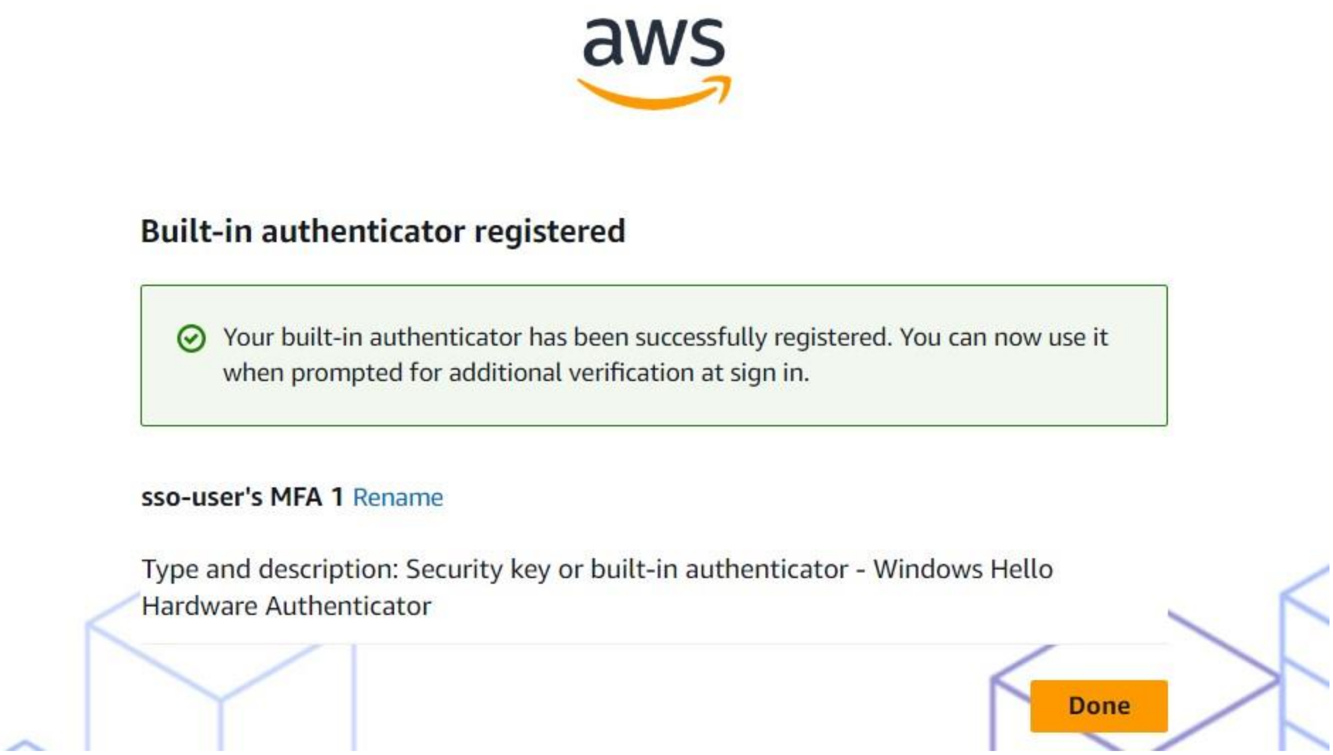
Let’s save a passkey on this device to sign in to “signin.aws” as “sso-user”.

This request comes from the app “chrome.exe” by “Google LLC”.

PIN

I forgot my PIN

Step 11- MFA Registered Successfully



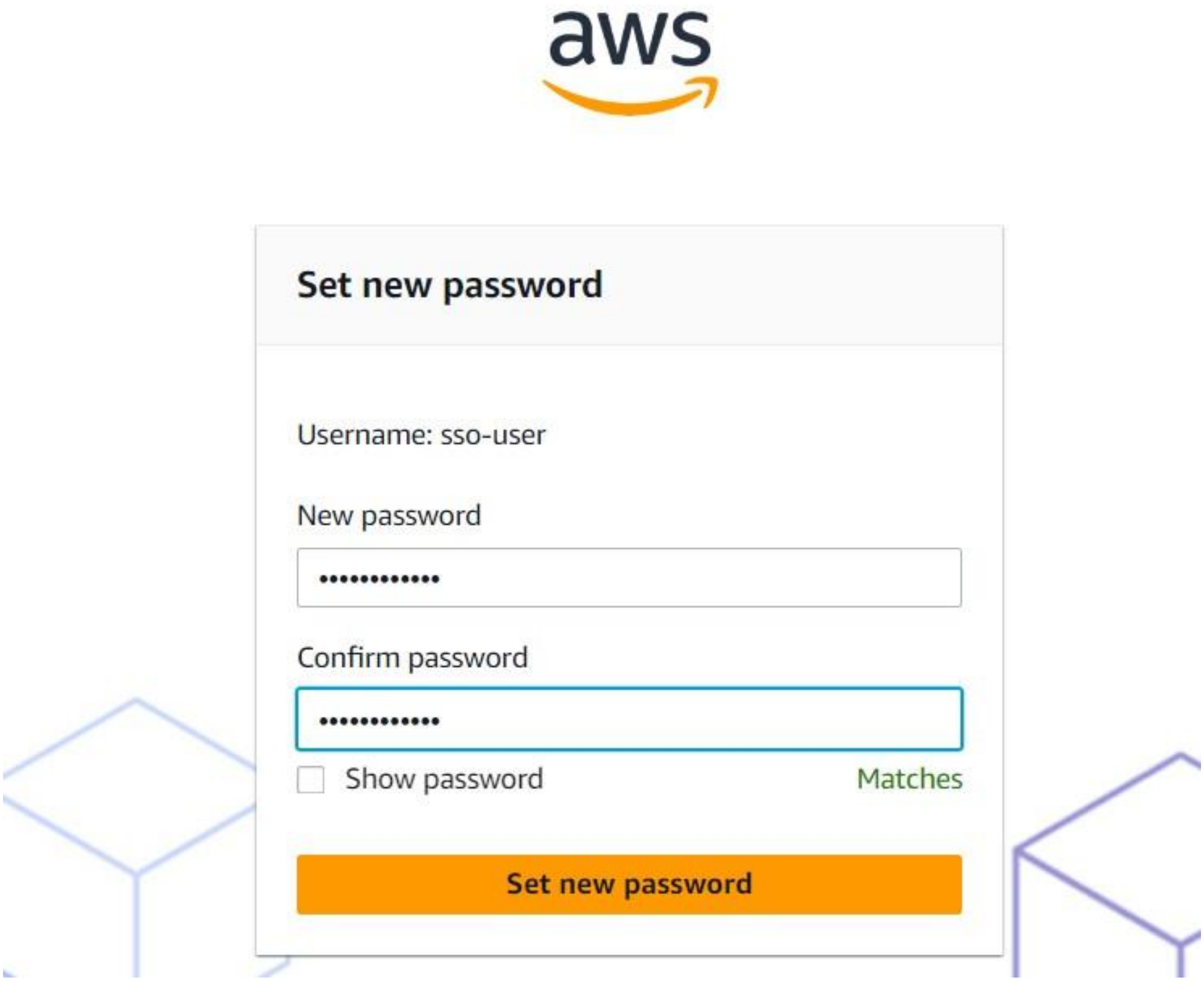
Built-in authenticator registered

Your built-in authenticator has been successfully registered. You can now use it when prompted for additional verification at sign in.

sso-user's MFA 1 Rename

Type and description: Security key or built-in authenticator - Windows Hello Hardware Authenticator

Step 12- Assign New Password for the following User



Set new password

Username: sso-user

New password

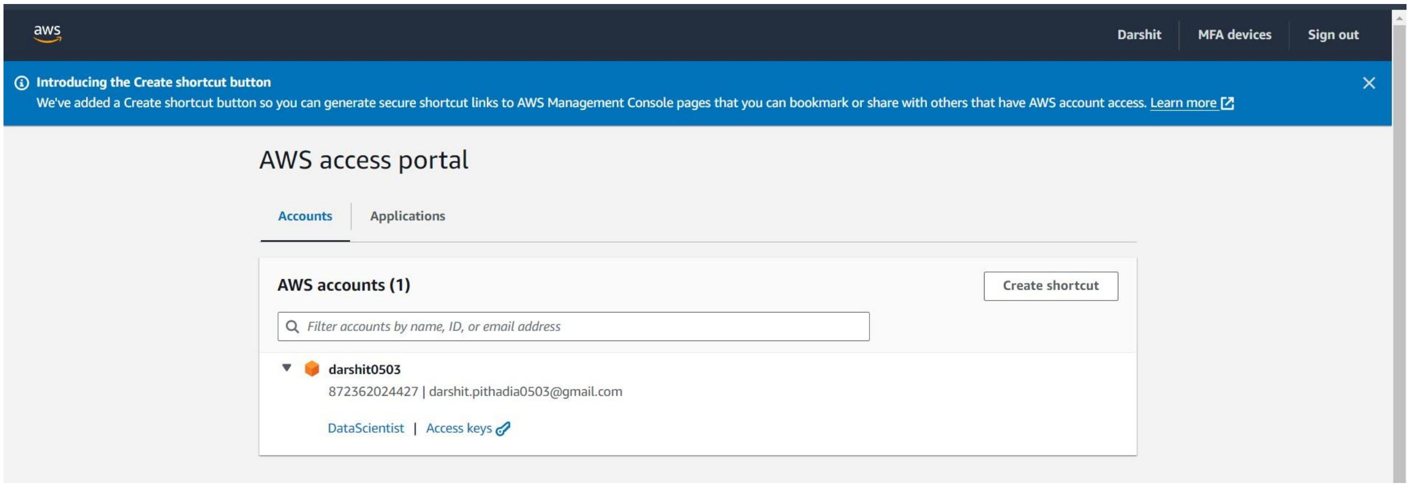
•••••••••••••

Confirm password

•••••••••••••

□ Show password Matches

Step 13- We can see the name of the Permission assigned to the following User



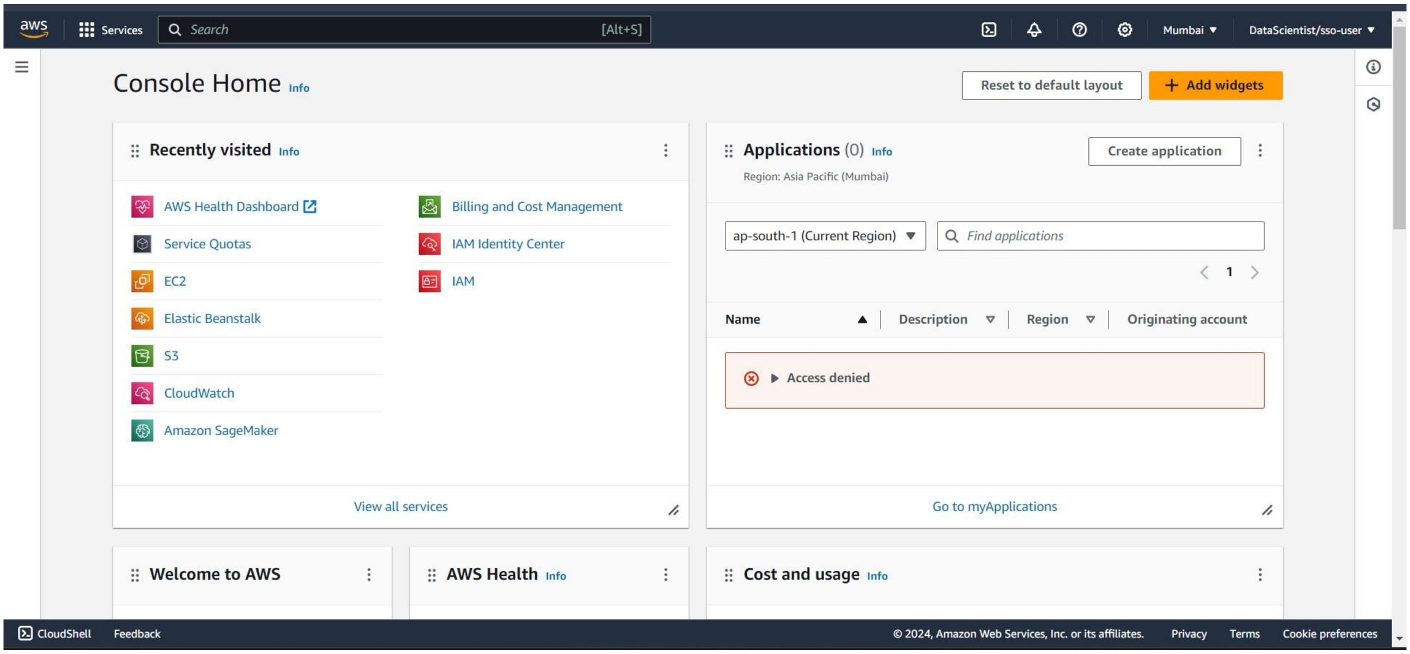
Introducing the Create shortcut button
We've added a Create shortcut button so you can generate secure shortcut links to AWS Management Console pages that you can bookmark or share with others that have AWS account access. Learn more

AWS access portal

AWS accounts (1)

darshit0503
872362024427 | darshit.pithadia0503@gmail.com
DataScientist | Access keys

Step 14- Console Home Page for the User



Console Home Info

Recently visited Info

- AWS Health Dashboard
- Service Quotas
- EC2
- Elastic Beanstalk
- S3
- CloudWatch
- Amazon SageMaker
- Billing and Cost Management
- IAM Identity Center
- IAM

Applications (0) Info

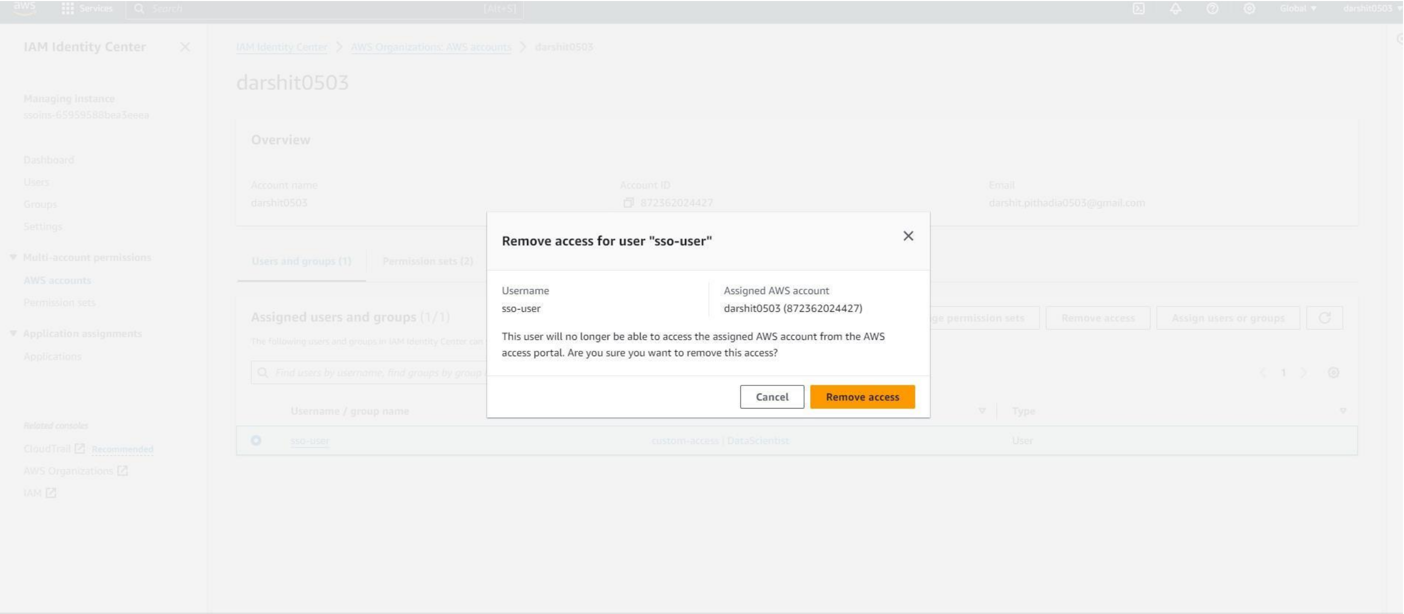
Region: Asia Pacific (Mumbai)

ap-south-1 (Current Region) ▾ | Find applications

Name ▲	Description ▽	Region ▽	Originating account

▶ Access denied

Step 15- Removing the Access for the User



Managing instance
ssoins-65959588bea3eeea

darshit0503

Overview

Account name: darshit0503
Account ID: 872362024427
Email: darshit.pithadia0503@gmail.com

Assigned users and groups (1/1)

The following users and groups in IAM Identity Center can ...

Username / group name		Type
sso-user	custom-access | DataScientist	User

Remove access for user "sso-user"

Username: sso-user

Assigned AWS account: darshit0503 (872362024427)

This user will no longer be able to access the assigned AWS account from the AWS access portal. Are you sure you want to remove this access?