

SVKM'S NMIM'S Nilkamal School of Mathematics, Applied Statistics & Analytics

Master of Science (Data Science)

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.


Implement of Single-Sign-On (SSO) in AWS.

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

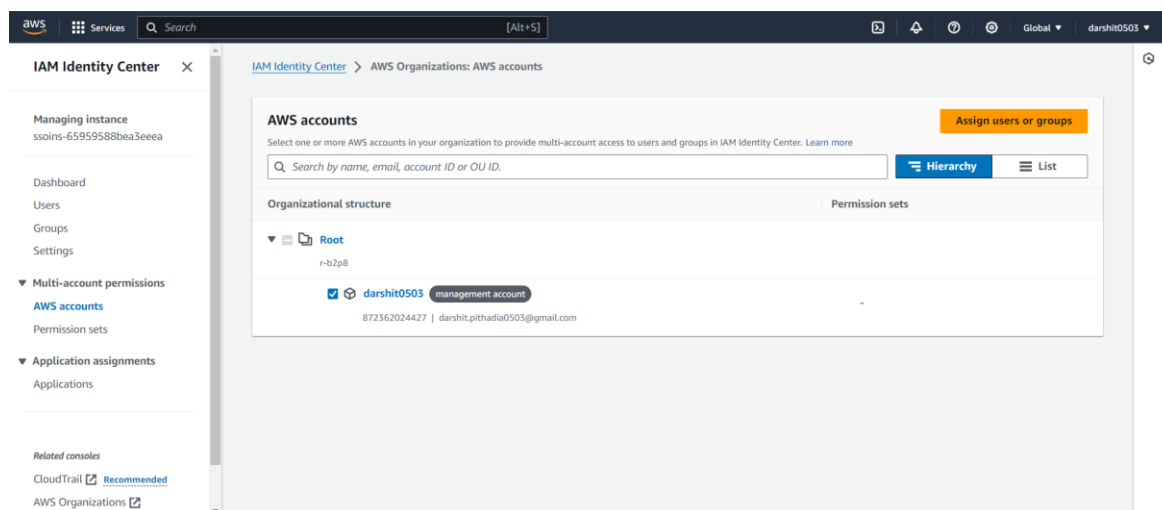


Create an account instance for this account only. Ideal for a single user or for testing.

- Manage multi-account permissions ☐
- Simplify application access across multiple accounts ☐
- Configure customer managed applications ☐

Cancel Continue

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



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

The screenshot shows the AWS IAM Identity Center console. The breadcrumb navigation is: IAM Identity Center > AWS Organizations: AWS accounts > Assign users and groups. The left sidebar shows the progress: Step 1: Select users and groups (active), Step 2: Select permission sets, and Step 3: Review and submit. The main heading is 'Assign users and groups to "darshit0503"'. Below this, it says 'Select one or more users or groups in IAM Identity Center that you want to give multi-account access to.' There are two tabs: 'Users' (selected) and 'Groups'. Under the 'Users' tab, there is a section 'Users (1/1)' with a search bar and a 'Create users' button. Below the search bar is a table with columns: Username, Display name, and Status. The table contains one entry: 'SSO-user' with display name 'Darshit Pithadia' and status 'Enabled'. Below the table is a section 'Selected users and groups (1)' with a 'Remove' button. At the bottom right are 'Cancel' and 'Next' buttons.

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 | Groups

Users (1/1) Create users

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

<input checked="" type="checkbox"/>	Username	Display name	Status
<input checked="" type="checkbox"/>	SSO-user	Darshit Pithadia	Enabled

Selected users and groups (1) Remove

Cancel Next

Step 4- Select Permission type we want to assign

The screenshot shows the AWS IAM Identity Center console. The breadcrumb navigation is: IAM Identity Center > AWS Organizations: AWS accounts > Assign users and groups. The left sidebar shows the progress: Step 1: Select permission set type (active), Step 2: Specify permission set details, and Step 3: Review and create. The main heading is 'Select permission set type'. Below this, it says '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'. There are two radio buttons: 'Predefined permission set' (selected) and 'Custom permission set'. Below the radio buttons is a section 'Policy for predefined permission set' with a heading 'Select an AWS managed policy'. There are four radio buttons: 'AdministratorAccess', 'Billing', 'DatabaseAdministrator', and 'DataScientist' (selected). Each radio button has a description of the policy.

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](#)

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.

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.

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](#)

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
Assign permission sets to "darshit0503"

Step 3
[Review and submit](#)

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)

< 1 >

<input type="checkbox"/>	Permission set	Description	ARN
<input type="checkbox"/>	DataScientist	-	arn:aws:sso::permissionSet/ssoins-65959588bea3eeea/ps-14b025aac493430c

Step 7- It will start Cofigring based on the Permissions

Step 2: Select permission sets

[Edit](#)

Permission sets (1)

Permission set ▲	Description ▼	ARN ▼	Creation time ▼
DataScientist	-	arn:aws:sso:::permissionSet/ssoins-65959588bea3e-eea/ps-14b025aac493430c	Now



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

Configuring in progress

[Expand details](#)

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.

[Cancel](#)[Previous](#)[Submit](#)

Step 8 – SSO Assigned

Services [Alt+S]

IAM Identity Center

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

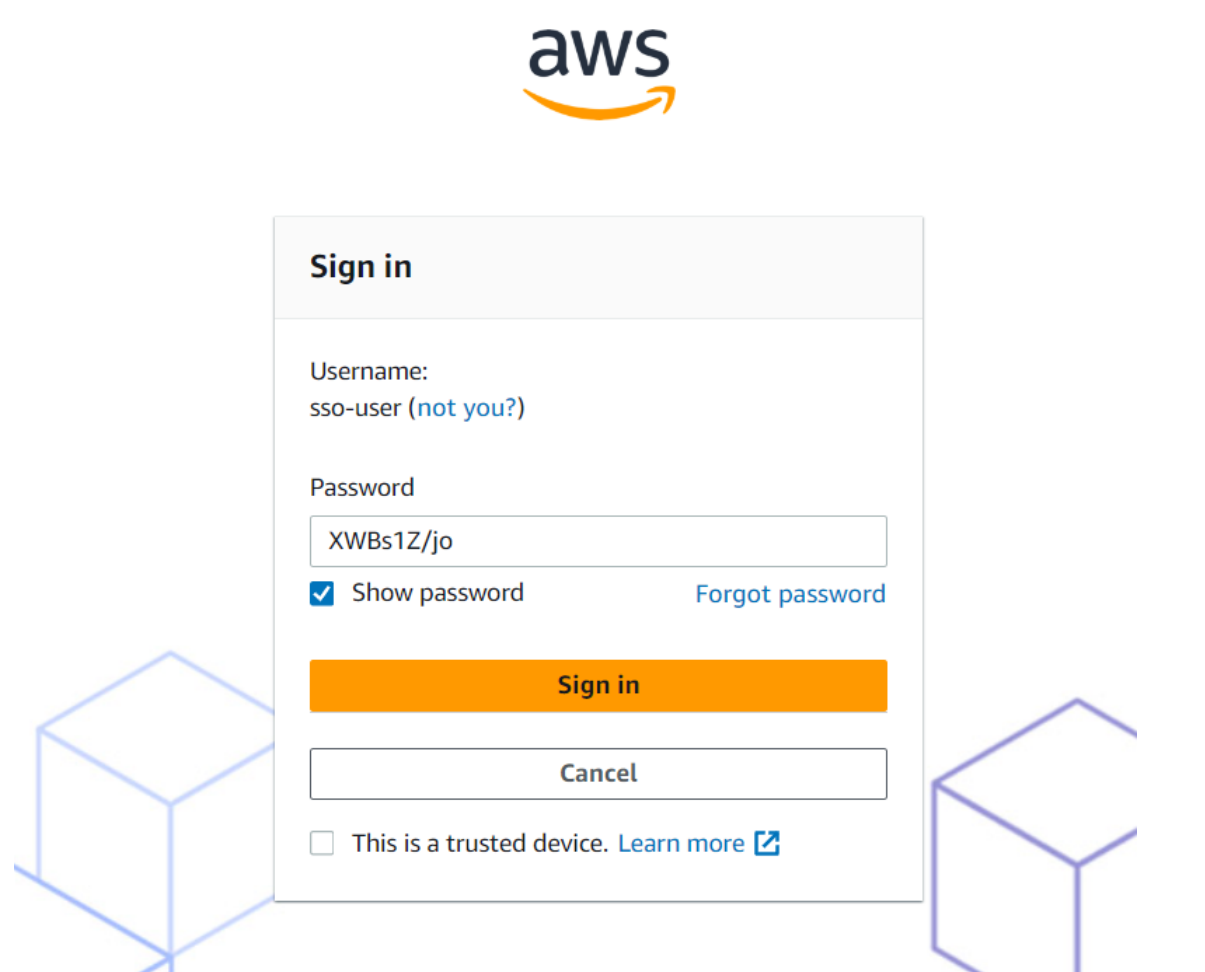
[IAM Identity Center](#) > AWS Organizations: AWS accounts

Managing instance
ssoins-65959588bea3e

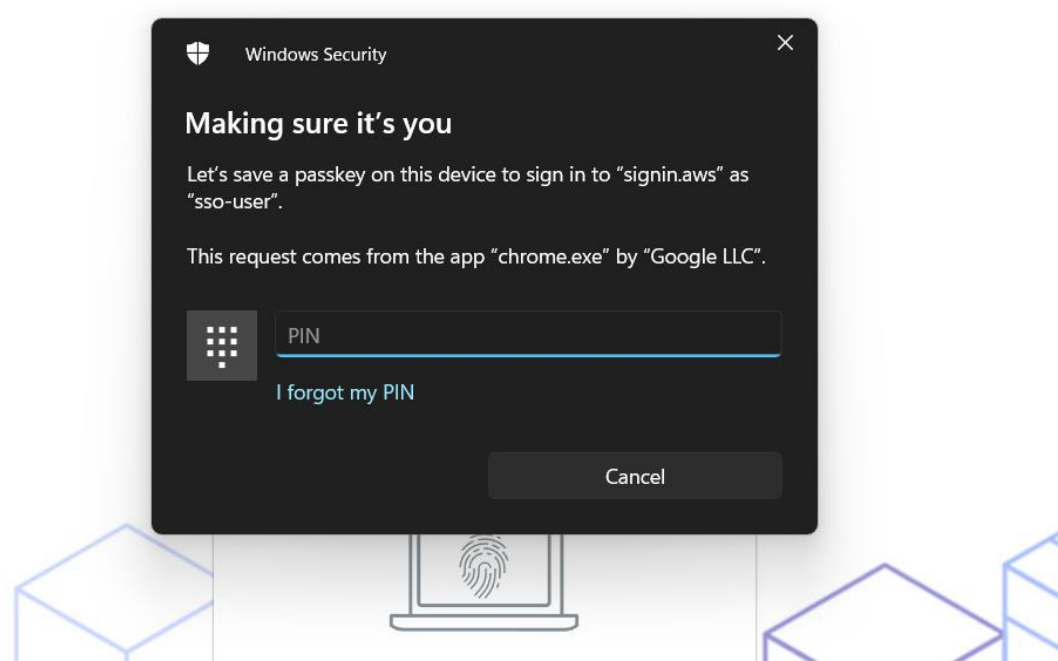
AWS accounts

Assign users or groups

Step 9 - SSO with One time Password provided



Step 10- Assign MFA from the provided options provided



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

Done

Step 12- Assign New Password for the following User



Set new password

Username: sso-user

New password

.....

Confirm password

.....

☐ Show password

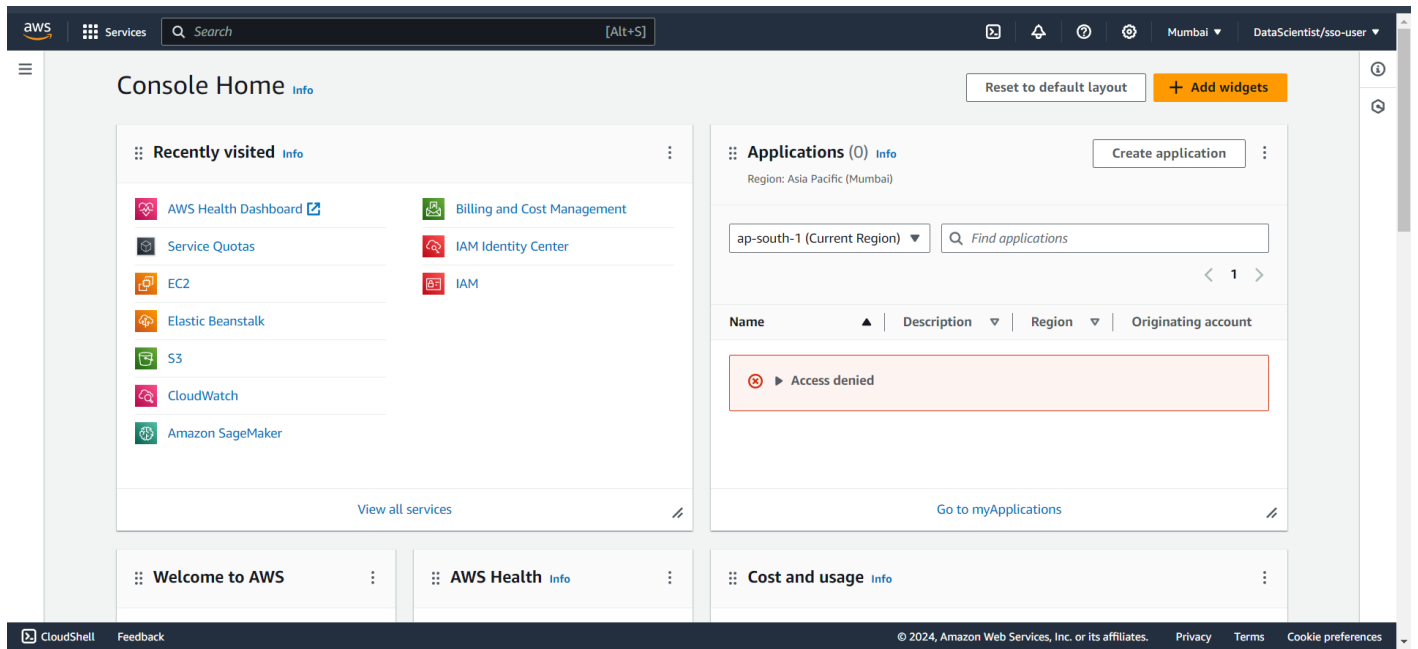
Matches

Set new password

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

The screenshot shows the AWS access portal interface. At the top, there's a navigation bar with the AWS logo, the user name 'Darshit', 'MFA devices', and 'Sign out'. Below this is a blue banner with a message about the 'Create shortcut' button. The main content area is titled 'AWS access portal' and has two tabs: 'Accounts' (selected) and 'Applications'. Under the 'Accounts' tab, there's a section 'AWS accounts (1)' with a search bar and a 'Create shortcut' button. The search results show a single user: 'darshit0503' with ID '872362024427' and email 'darshit.pithadia0503@gmail.com'. The user's role is 'DataScientist' and there's a link for 'Access keys'.

Step 14- Console Home Page for the User



Step 15- Removing the Access for the User

