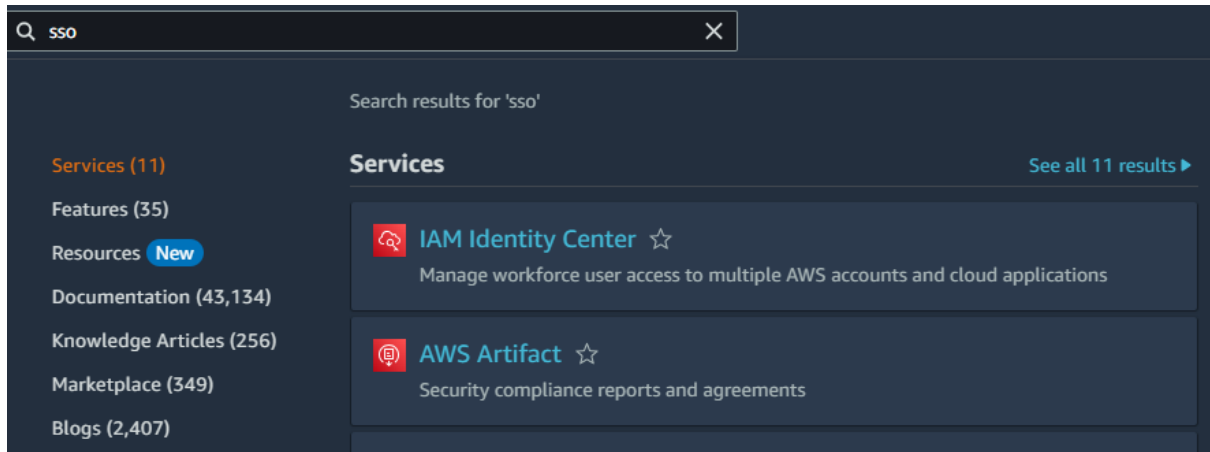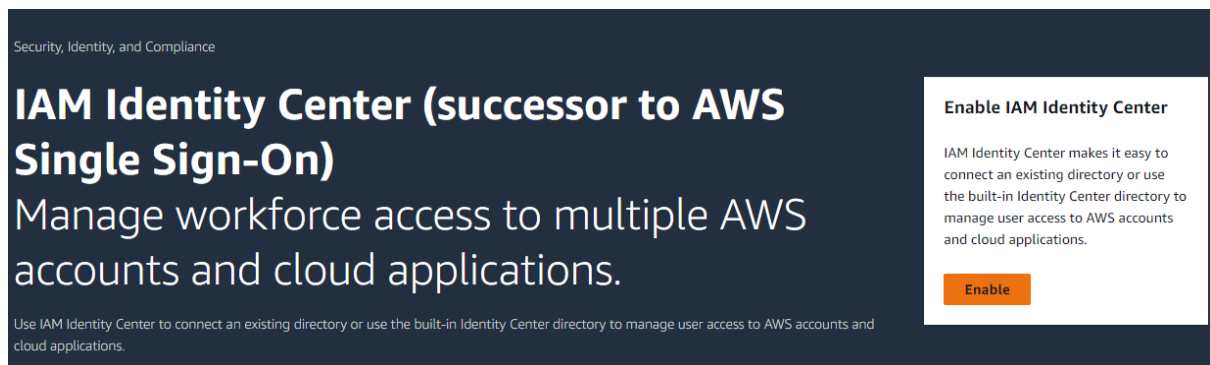# SINGLE SIGN ON

SHARMEEN SHAIKH   ROLL.NO: A016

GO TO CONSOLE

Enable it

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

Feature	
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.

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

Cancel   Continue

In the dashboard settings, click on edit

Settings summary

[Go to settings]

> ℹ️ Specify a unique name for your instance.

Instance name - Edit

-

Identity source

Identity Center directory

Region

US East (N. Virginia) | us-east-1

Organization ID

o-xdk0se4ozv

AWS access portal URL - Edit

🗗 https://d-9067fff609.awsapps.com/start 🔗

Issuer URL

🗗 https://identitycenter.amazonaws.com/ssoins-72235375d72a07c
3

Give any name to customize

Customize AWS access portal URL ✕

Enter a custom subdomain for the AWS access portal sign-in page where your
authenticated users will access their assigned AWS accounts and cloud applications.

AWS access portal URL
Once saved, you will not be able to change this later.

https:// [cloudtech] .awsapps.com/start

Type your subdomain to confirm:

[cloudtech]

Cancel   **Save**

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

---

IAM Identity Center > **AWS Organizations: AWS accounts**

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

🔍 Search by name, email, account ID or OU ID.

Organizational structure

▼ ☐ 🗂 **Root**

   r-7mbz

   ☐ 🔷 **Sharmeen Shaikh** ⬡management account⬢

   796329916611 | shaikhsharmin857@gmail.com

AWS Organizations > AWS accounts > Add an AWS account

Add an AWS account

You can add an AWS account to your organization either by creating an account or by inviting one or more existing AWS accounts to join your organization.

🔘 Create an AWS account
   Create an AWS account that is added to your organization.

⭘ Invite an existing AWS account
   Send an email request to the owner of the account. If they accept, the account joins the organization.

Create an AWS account

AWS account name

Cloud-Tech2

Email address of the account's owner

cloud-tech2@gmail.com

IAM role name
The management account can use this IAM role to access resources in the member account.

OrganizationAccountAccessRole

It is visible after creating

Now add an user

Organizational structure	Account created/joined date
▼ ☐ 🗗 **Root**	
r-7mbz	
☐ 🔷 **Cloud-Tech2**	Created 2024/04/04
533267442111 | cloud-tech2@gmail.com	
☐ 🔷 **Sharmeen Shaikh** management account	Joined 2024/04/04
796329916611 | shaikhsharmin857@gmail.com	

Then go to identity center-> GROUPS

IAM Identity Center > Groups > Create group

Create group

Group details

Group name

cloud-techdev

Maximum of 128 characters

Description - *optional*
Group description detailing the permissions assigned to this group.

cloud-techdev

Maximum of 256 characters

Create group

Go to users->add user

Specify user details

Primary information

Username
This username will be required for this user to sign in to the AWS access portal. The username can't be changed l...

Cloud-Tech2

Maximum length of 128 characters. Can only contain alphanumeric characters or any of the following: +=,.@-_

Password
Choose how you want this user to receive their password. Learn more [↗]

○ Send an email to this user with password setup instructions.
● Generate a one-time password that you can share with this user.

Email address

cloud-tech2@gmail.com

Confirm email address

cloud-tech2@gmail.com

First name

cloudtech2

Last name

cloudtech2

Display name
This is typically the full name of the workforce user (first and last name), is searchable, and appears in the users l...

cloudtech2 cloudtech2

Add user to groups - *optional*

You can assign this user to one or more groups.

Groups (1)

🔍 Find groups by group name

	Group name [↗]	▽	Description
☐	cloud-techdev		cloud-techdev

Click on the checkbox and next

Review and add user

Step 1: Specify user details

Primary information

Attribute key	Value
Username	Cloud-Tech2
Email	cloud-tech2@gmail.com
First name	cloudtech2
Last name	demo
Display name	cloudtech2 demo

▶ **Contact methods - *optional***

▶ **Job-related information - *optional***

Now add user

One-time password   ✕

⊘ User password was reset for user "Cloud-Tech2".

You can copy and share the instructions for signing in to the AWS access portal with this user, or email them the instructions. This is th̶_____ this password.

⊘ Sign in instructions copied

🗐 **Copy**

AWS access portal URL
🗐 https://cloudtech1.awsapps.com/start

Username
🗐 Cloud-Tech2

One-time password
🗐 **************
⬤ Show password

Close

Copy and paste in notepad

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

Keep administrative access and click next

Click next

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.

```
AdministratorAccess
```

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: & $ @ # \ / % ? = ~ - _ ' " | ! : , . ; * + [ ] ( ) { }

Click next

Review and create

Step 1: Select permission set type   [Edit]

Permission set type

Type	AWS managed policy
Predefined permission set	AdministratorAccess

Step 2: Define permission set details   [Edit]

Permission set details

Permission set name	Session duration
AdministratorAccess	1 hour
Description	Relay state
AdministratorAccess	-

Tags (not set)

Key ▲	Value ▽
No resources	
You have not added any tags	

Cancel   [Previous]   [Create]

Click create

IAM Identity Center now supports customer managed policies and permissions boundaries in your permission sets
This feature enables you to create customer managed policies in IAM and attach them to this permission set when you need to define custom permissions. You can also set a permissions boundary to control the maximum permissions for the permission set. Learn more

Permission sets (1)

Permission sets define the level of access that users in IAM Identity Center have to their assigned AWS accounts. The names of permission sets appear as available roles in the AWS access portal. Users who are assigned to multiple AWS permission sets can sign in to the AWS access portal, choose an account, and then choose a role that AWS created from an assigned permission set. Learn more

Delete | Create permission set

Find permission sets by full ARN or permission set ID (i.e., ps-abcdefg123456789).

Permission set	Description	ARN	Provisioned status
AdministratorAccess	AdministratorAccess	arn:aws:sso:::permissionSet/ssoins-72235375d72a07c3/ps-4c319225262...	⊖ Not provisioned

AWS accounts

Select one or more AWS accounts in your organization to provide multi-account access to users and groups in

Search by name, email, account ID or OU ID.

Organizational structure

▼ ▣ 🗂 Root

r-7mbz

☑ 🔷 Cloud-Tech2

533267442111 | cloud-tech2@gmail.com

☐ 🔷 Sharmeen Shaikh   management account

796329916611 | shaikhsharmin857@gmail.com

Assign users

Assign users and groups to "Cloud-Tech2"

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

Users | **Groups**

Groups (1/1)

C   Create groups ↗

🔍 Find groups by group name   < **1** > ⚙

☑	Group name ↗ ▲	Description ▽
☑	cloud-techdev	cloud-techdev

▶ **Selected users and groups** (1)   Remove

Cancel   **Next**

Next

Assign permission sets to "Cloud-Tech2"

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)

C   ↗ Create permission set

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

☑	Permission set ↗ ▲	Description ▽	ARN ▽
☑	AdministratorAccess	AdministratorAccess	arn:aws:sso:::permission Set/ssoins-72235375d72a07c3/ps-4c319225262b4b7e

Cancel   Previous   **Next**

Review and submit assignments to "Cloud-Tech2"

Step 1: Select users and groups   Edit

Users and groups (1)

< 1 >

Username / group name ⬀ ▲	Type ▽
cloud-techdev	Group

Step 2: Select permission sets   Edit

Permission sets (1)

Permission set ▲	Description ▽	ARN ▽	Creation time ▽
AdministratorAccess	AdministratorAccess	arn:aws:sso:::permissionSet/ssoins-72235375d72a07c3/ps-4c319225262b4b7e	5 minutes ago

Cancel   Previous   **Submit**

Submit

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

IAM Identity Center > **AWS Organizations: AWS accounts**

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

🔍 Search by name, email, account ID or OU ID.

Organizational structure

▼ ☐ 🗁 **Root**
      r-7mbz

    ☐ 🔷 **Cloud-Tech2**
         533267442111 | cloud-tech2@gmail.com

    ☐ 🔷 **Sharmeen Shaikh** management account
         796329916611 | shaikhsharmin857@gmail.com

Now copy url from notepad and paste in incognito

*Untitled - Notepad

File   Edit   Format   View   Help

AWS access portal URL: https://cloudtech1.awsapps.com/start,
 Username: Cloud-Tech2,
One-time password: e7oRl<pHaE)0<O

aws

Sign in to cloudtech1

Username

[   ]

Next

By continuing, you agree to the **AWS Customer Agreement** or
other agreement for AWS services, and the **Privacy Notice**. This site
uses essential cookies. See our **Cookie Notice** for more information.

Copy username and password too

Set new password

Username: Cloud-Tech2

New password

•••••••••

Confirm password

•••••••••

☐ Show password   Matches

Set new password

After setting new password, an MFA code needs to be put twice for 2-factor authentication

Scan QR code and type the code

After successful sign in you'll get this page

AWS access portal

Accounts | Applications

AWS accounts (1)

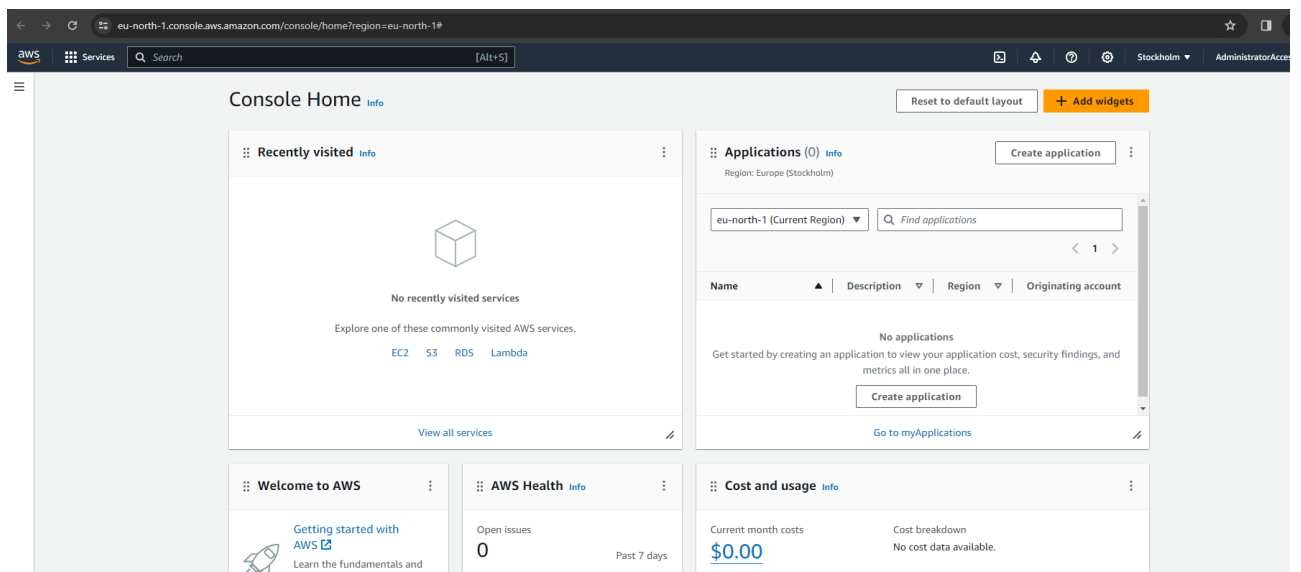Q *Filter accounts by name, ID, or email address*

▼ 🟧 **Cloud-Tech2**
        533267442111 | cloud-tech2@gmail.com

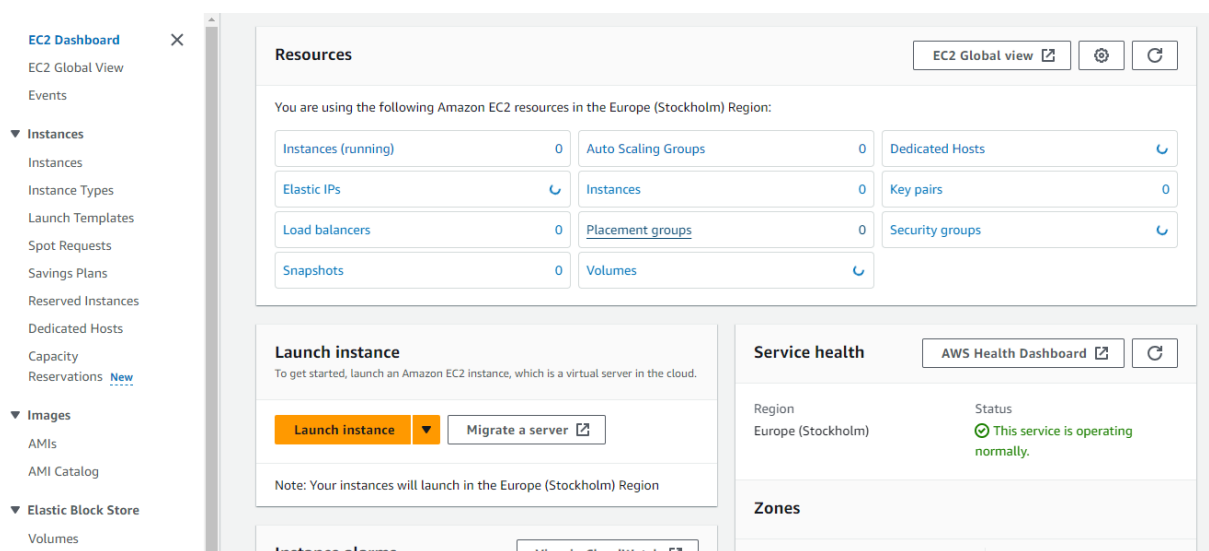   AdministratorAccess | Access keys 🔑

Click on administrator access

A new page is open with the access

Go to ec2

Service is showing since it was assigned to the user from group