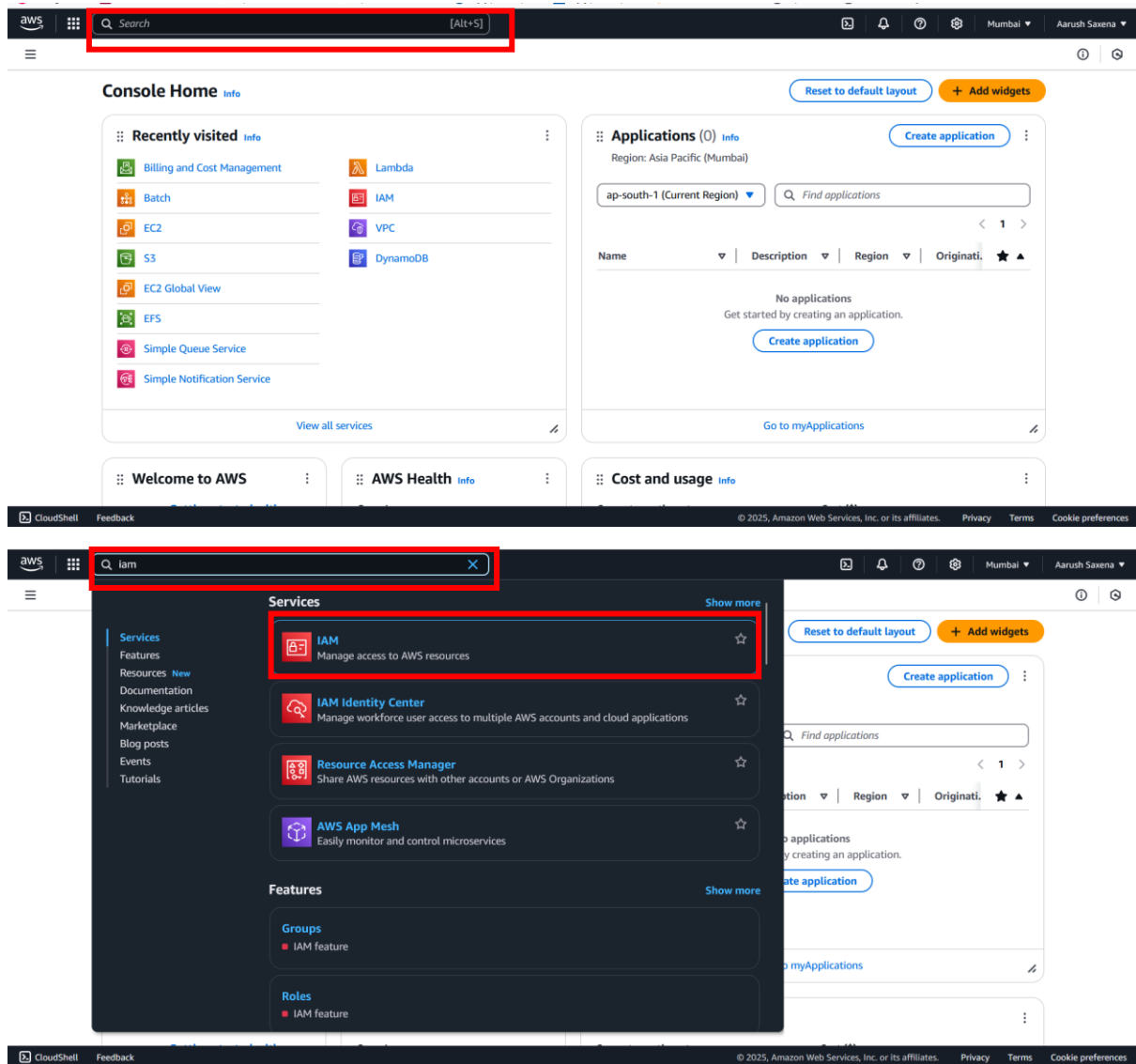
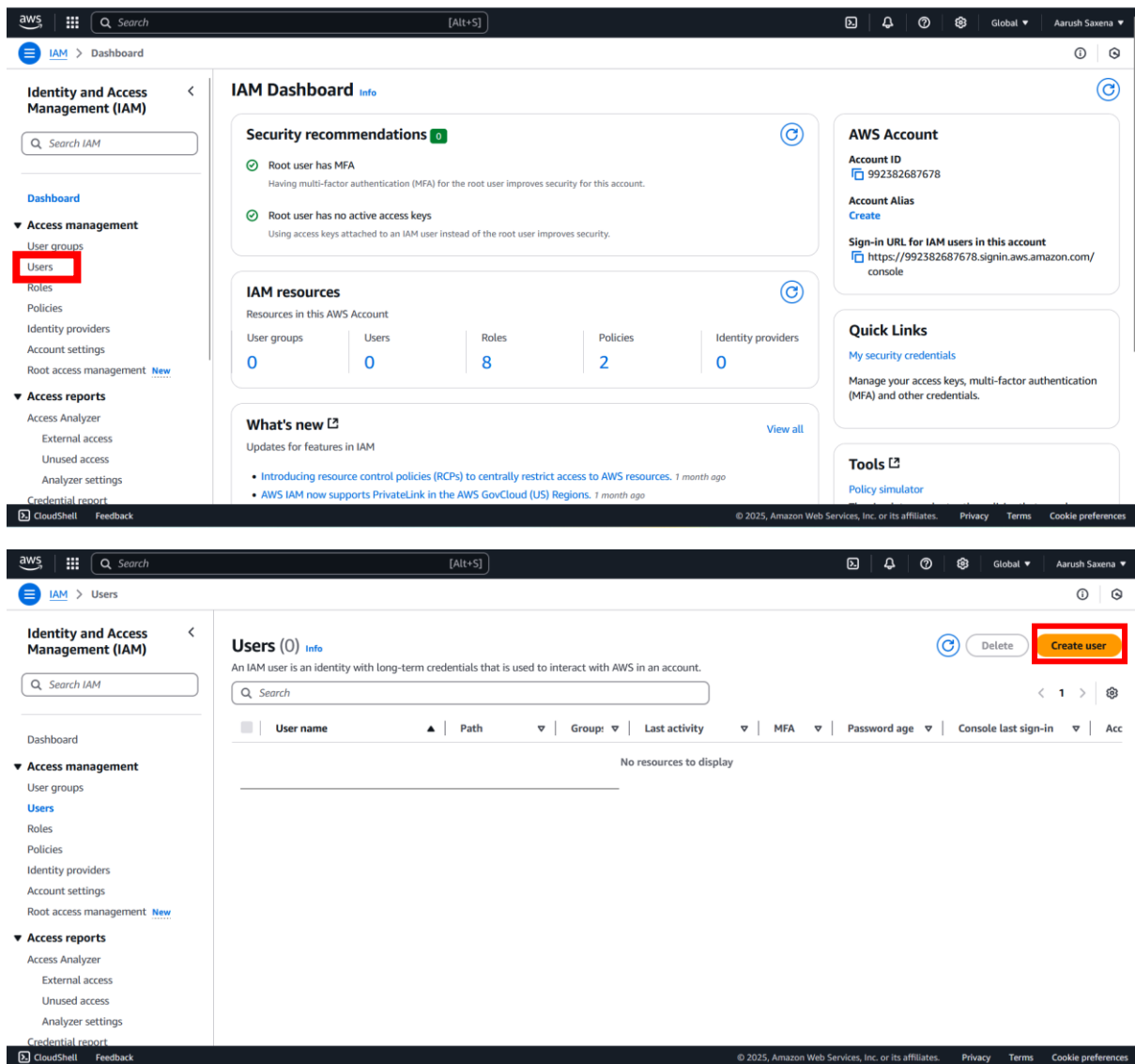


IDENTITY AND ACCESS MANAGEMENT

Step1: Log-in to your aws account and search for IAM from the searchbar and click on it.



Step2: Dashboard will appear as shown in image given below now click on users to create users.



After clicking on it give name to your user and click on provide user access to the aws management console and write custom passwords there and if you want that your can change password after access it click on user must create new password

Step 1: Specify user details

Step 2: Set permissions

Step 3: Review and create

Step 4: Retrieve password

Specify user details

User details

User name
userforidm

☒ Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

Are you providing console access to a person?

☐ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and third applications.

☒ I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

☐ Autogenerated password
New users get the password after you create the user.

☒ Custom password
Enter a custom password for the user:
Sample@12345-
☒ Show password

☒ Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

☐ If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user.

Cancel Next

We are giving of EC2 full access to our user , select it and click on next.

Step 2: Set permissions

Step 3: Review and create

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

☐ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

☒ Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1319)
Choose one or more policies to attach to your new user.

Filter by Type: All types 1 match

Policy name	Type	Attached entities
<input checked="" type="checkbox"/> AmazonEC2FullAccess	AWS managed	0

► Set permissions boundary - optional

Cancel Previous Next

After that click on create user.

Step 3: Review and create

User details

User name: userForIAM

Console password type: Custom password

Require password reset: Yes

Permissions summary

Name	Type	Used as
AmazonEC2FullAccess	AWS managed	Permissions policy
IAMUserChangePassword	AWS managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

Key: name Value: IAMROLEFORSAMPLE

[Add new tag](#)

[Cancel](#) [Previous](#) [Create user](#)

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console. [View user](#)

Step 4: Retrieve password

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

[Email sign-in instructions](#)

Console sign-in details

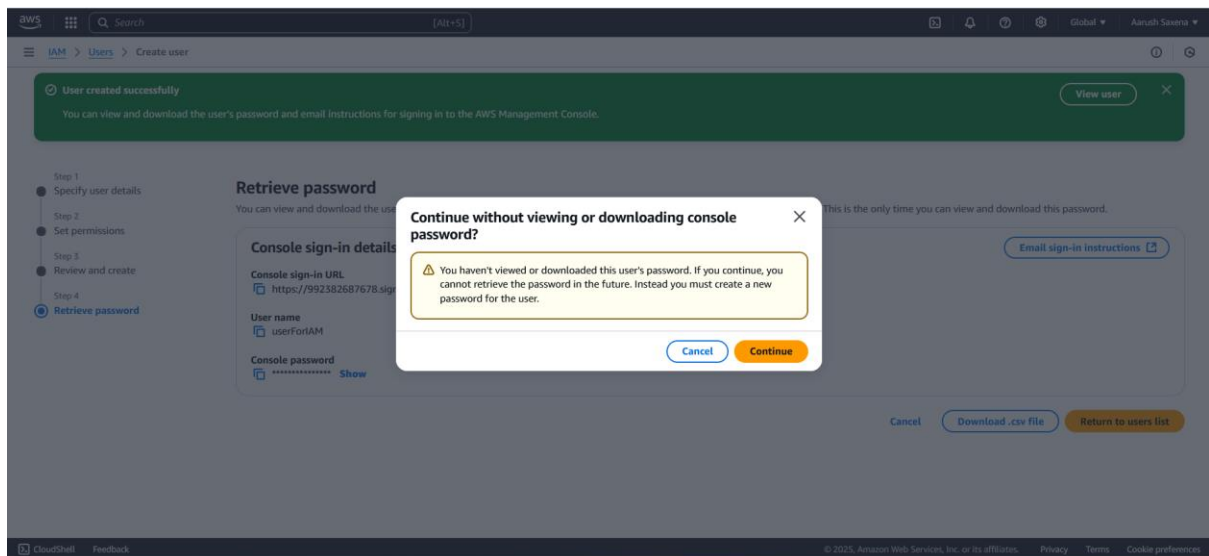
Console sign-in URL: <https://992382687678.signin.aws.amazon.com/console>

User name: userForIAM

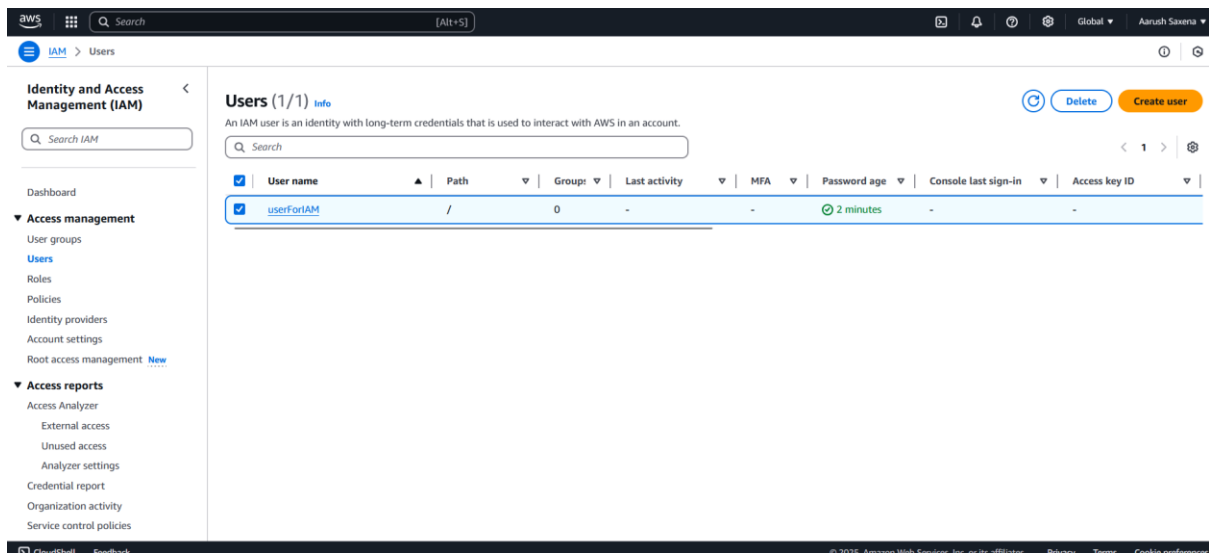
Console password: [Show](#)

[Cancel](#) [Download .csv file](#) [Return to users list](#)

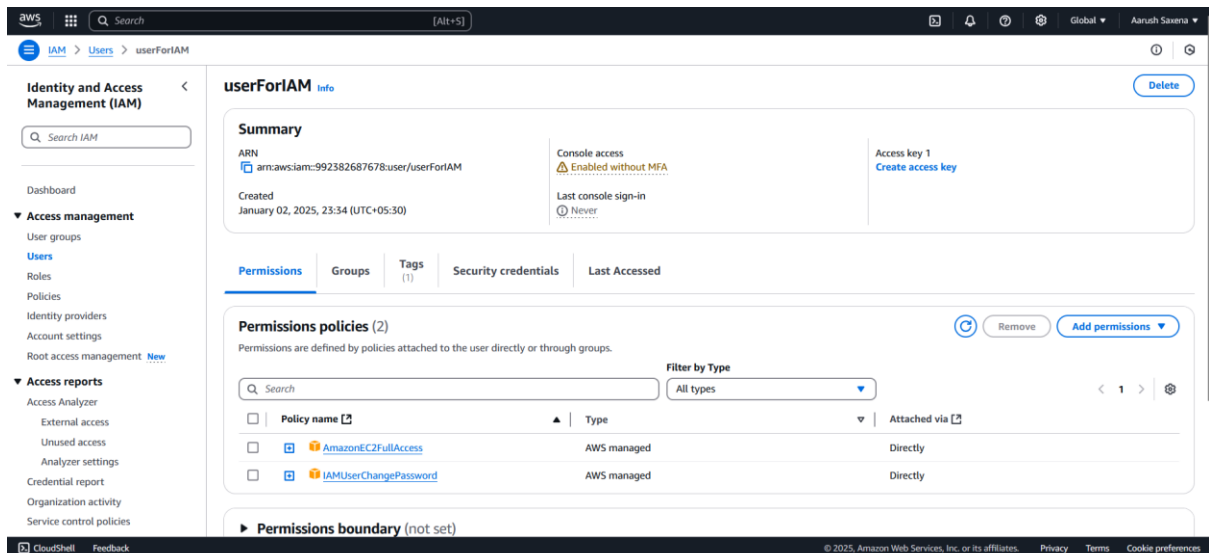
So we are not downloading .csv file which contains password and username but for your easiness download it. It will help at the time of login.



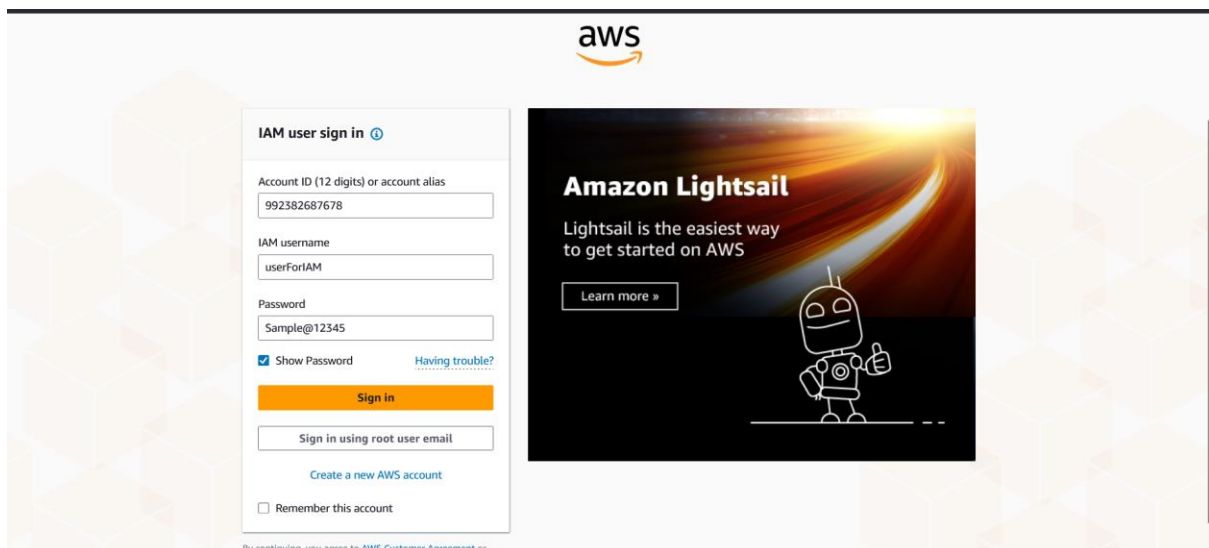
Now you can see our iam user has been create select it and click on it




After clicking on it user interface will appear as shown in image given below. Copy ARN from there and paste it to web browser.



At this time type account id and iam username and password and sign in to it.



As we provide permission that user can change password it will show to change password as shown in image given below.

 You must change your password to continue

AWS account 992382687678

IAM user name userForIAM

Old password

New password

Retype new password


[Confirm password change](#)

[Sign in using your user email](#)

English

[Terms of Use](#) [Privacy Policy](#) © 1996-2025, Amazon Web Services, Inc. or its affiliates.


Now you can see your iam user account has been created.

 Search [Alt+S] Europe (Stockholm) userForIAM @ 9923-8268-7678

Console Home [Info](#)

[Reset to default layout](#) [+ Add widgets](#)

Recently visited [Info](#)



No recently visited services

Explore one of these commonly visited AWS services.

[EC2](#) [S3](#) [RDS](#) [Lambda](#)

[View all services](#)

Applications (0) [Info](#)

Region: Europe (Stockholm)

eu-north-1 (Current Region) [Find applications](#)

< 1 >

Name	Description	Region	Originati	Star
<div>Access denied to servicecatalog:ListApplications</div>				

[Go to myApplications](#)

Welcome to AWS

AWS Health [Info](#)

Cost and usage [Info](#)

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)