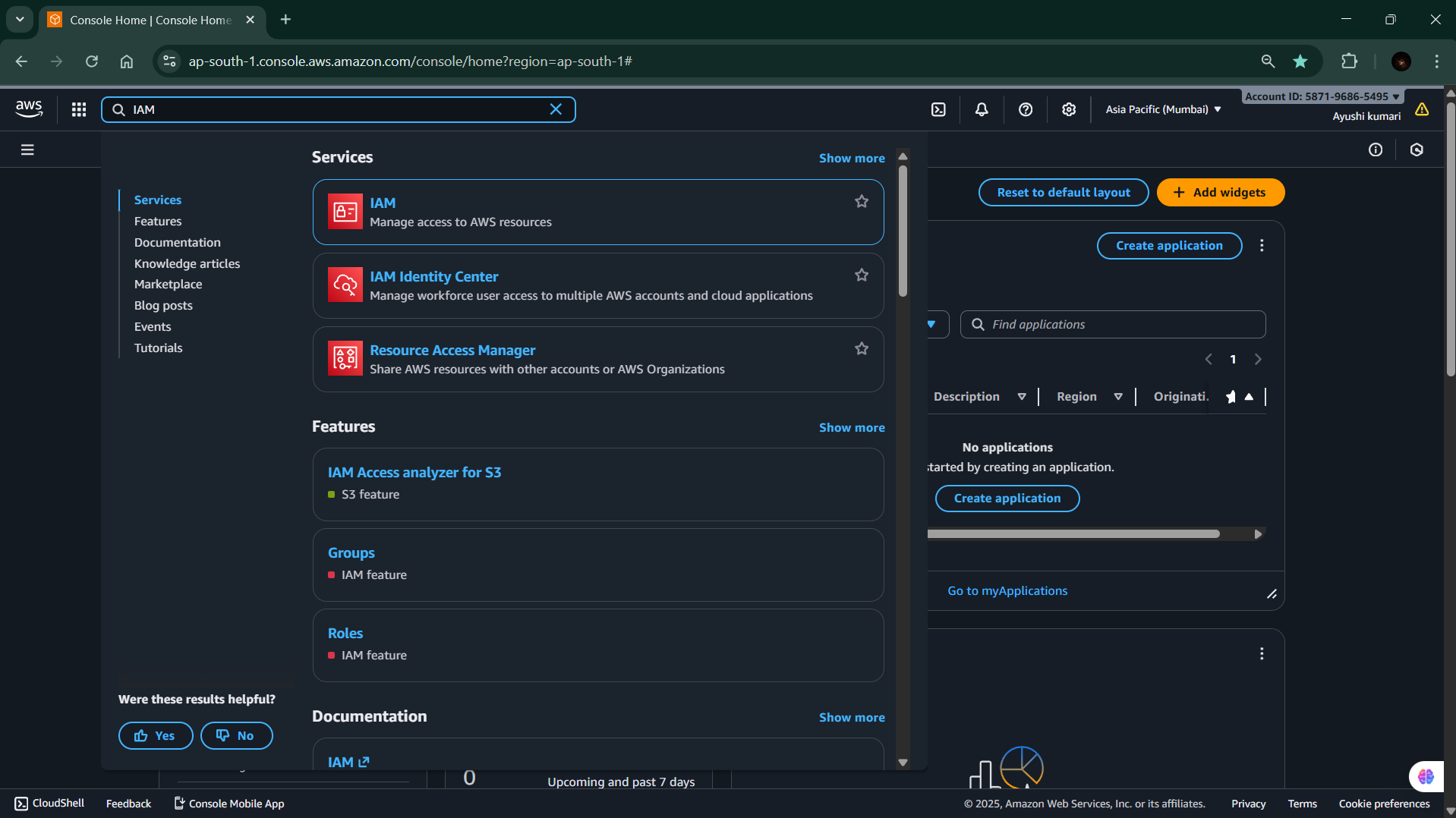
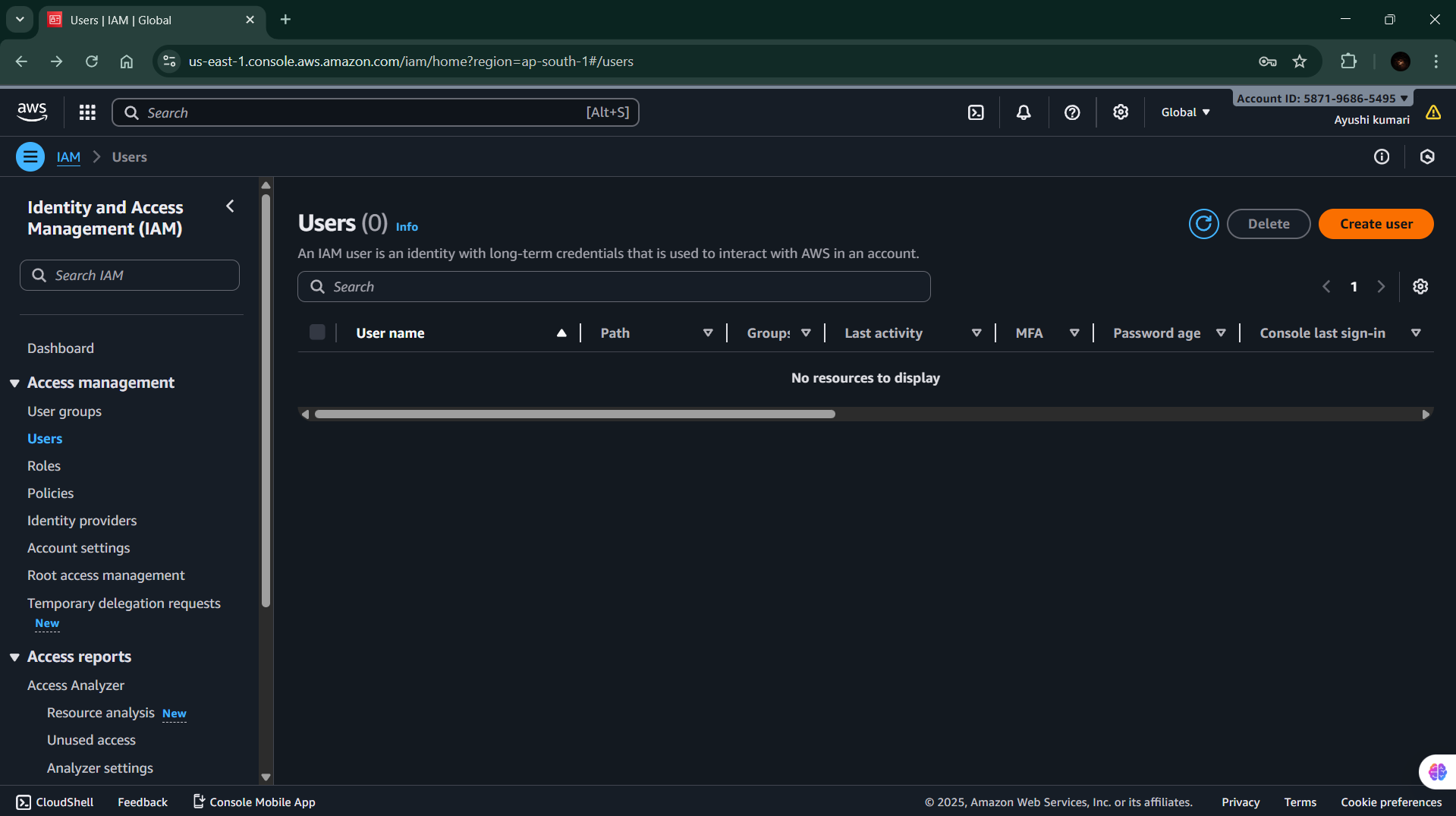
**PRACTICAL-5**

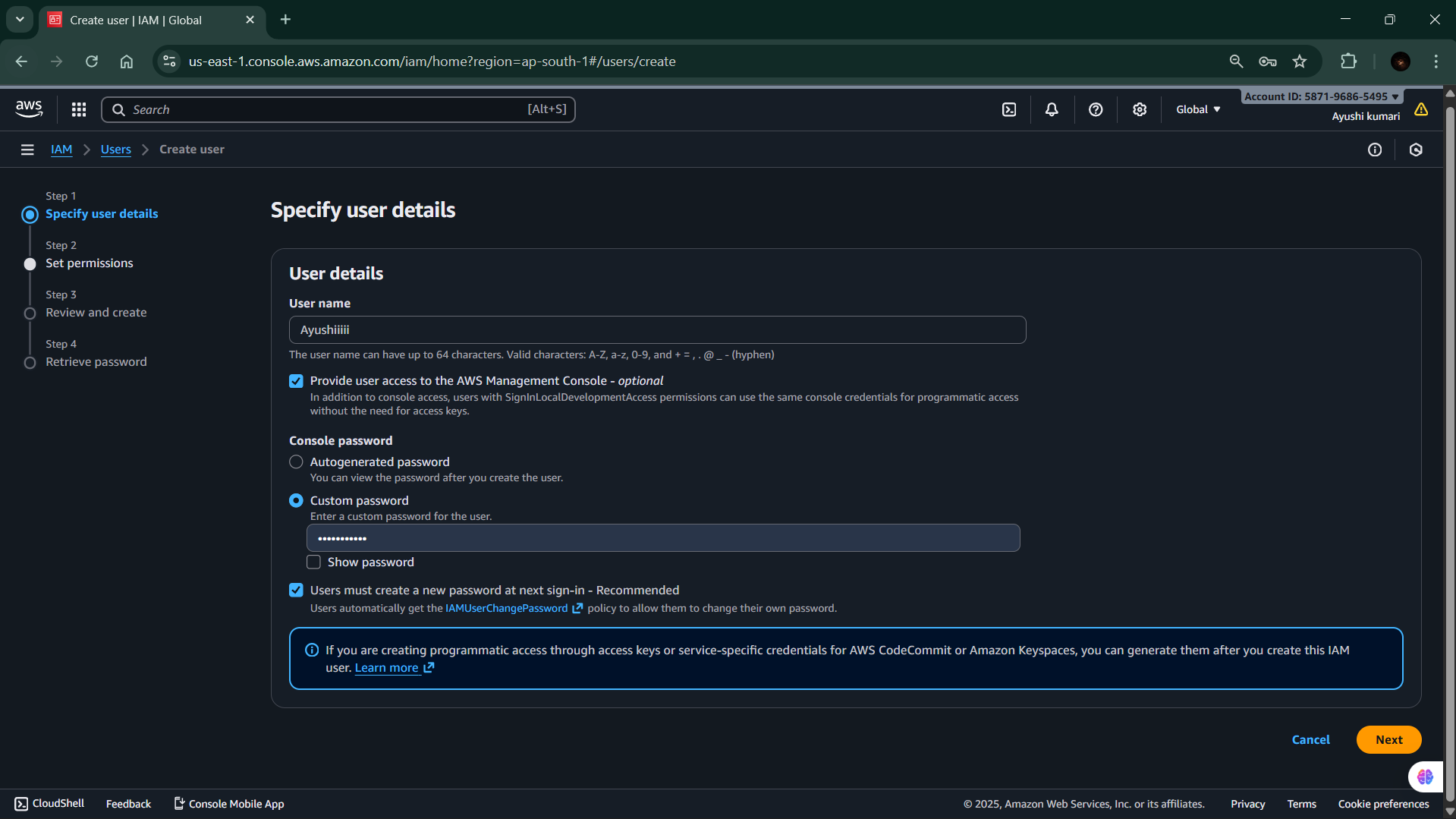
**Objective:- Creating an IAM (Identity and Access Management) user in AWS is to provide secure and controlled access to AWS resources for individuals or applications without using** **the root account**.

**Step 1:** Sign in to AWS Console Log in to your AWS Management Console using your root account or an IAM user who has Administrator privileges.

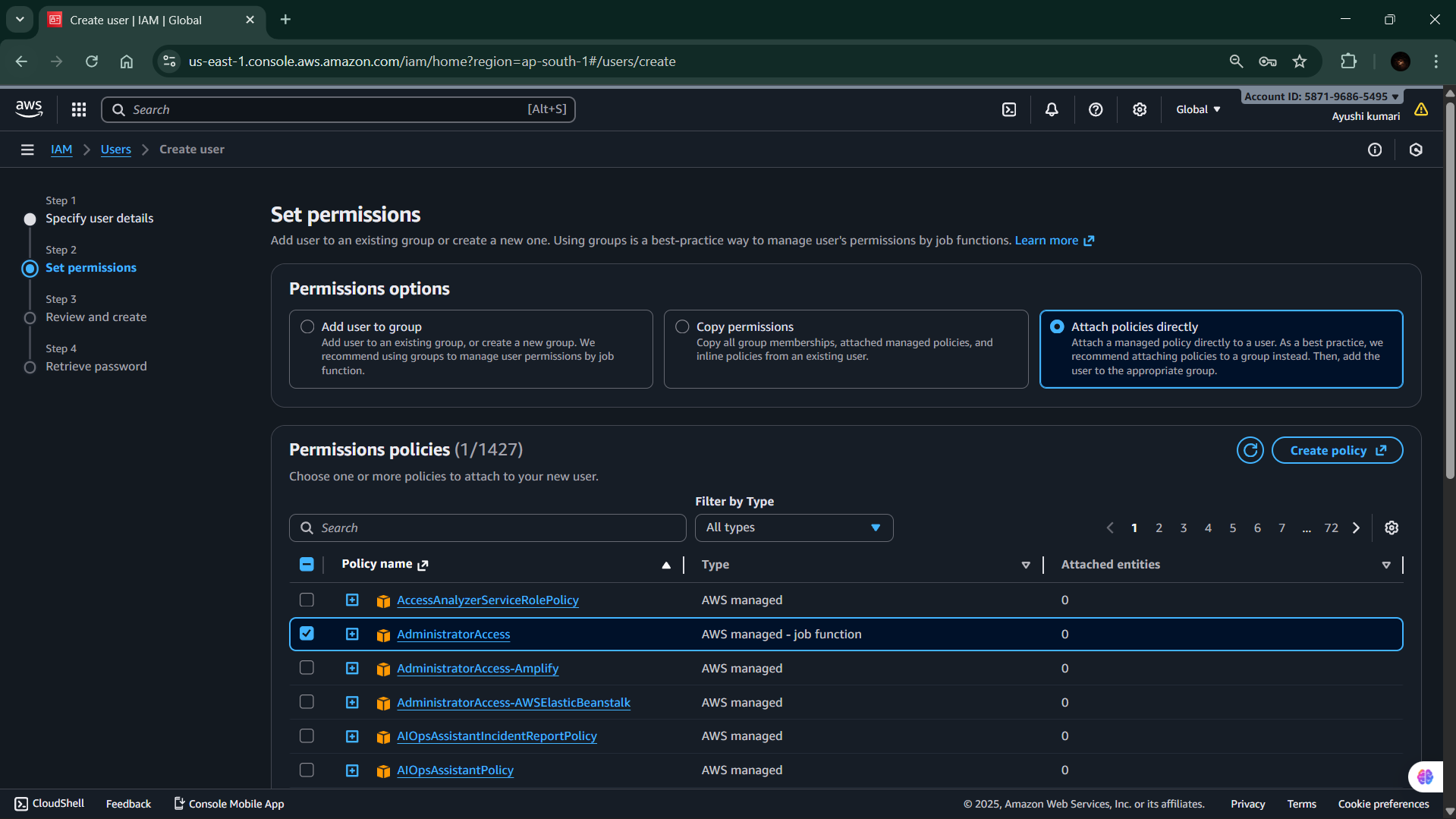
**Step 2:**  Open IAM Service In the search bar at the top, type IAM. Select IAM (Identity and Access Management).

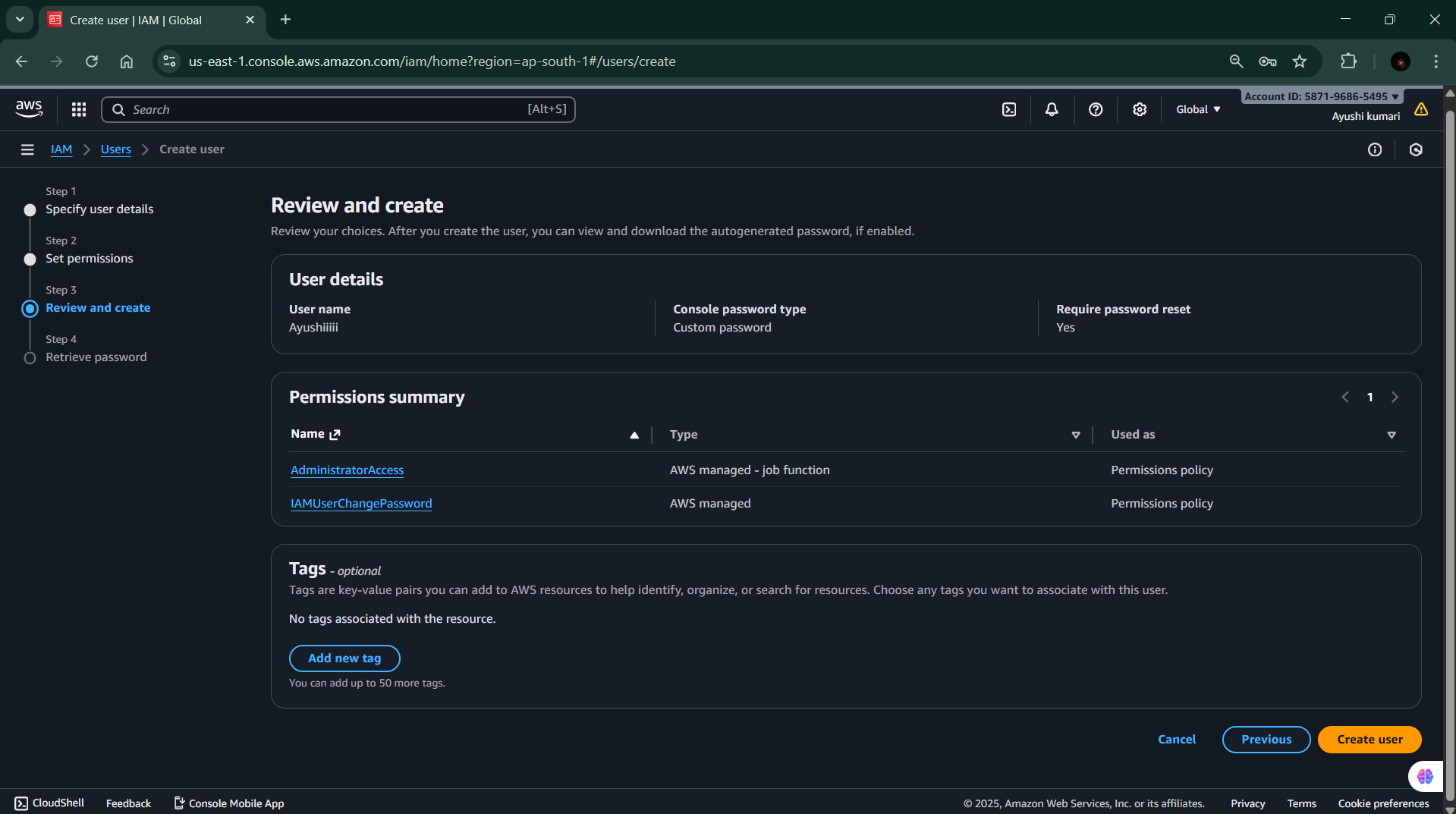


**Step 3:** Go to Users Section In the left sidebar, click on Users. You will see a list of all existing users. Click “Create user” to add a new one.

**Step 4:** Enter User Details Enter a User name . Choose the type of access: Password access → if the user needs to log in to the AWS Console. Click Next.

**Step 5:** Set Permissions Choose Attach policies directly → assign permissions manually (e.g., AmazonS3FullAccess, AdministratorAccess, etc.). Then click Next.



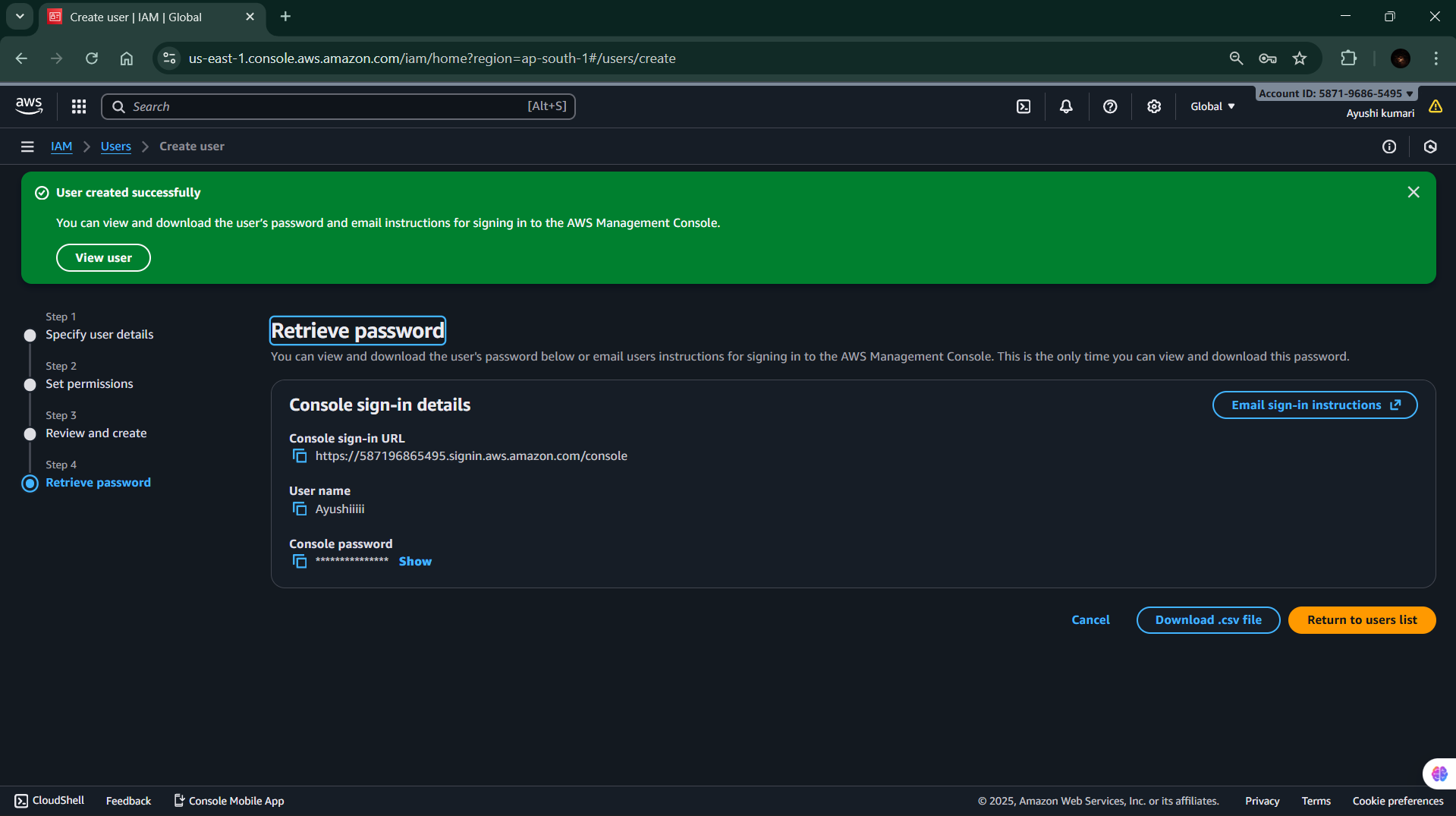
**Step 6:** Review and Create Review all details carefully. Click Create user.

**Step 7:** Save Login Details

• Once the user is created, AWS will show:

**o User ARN (Amazon Resource Name)**

**o Console login link**

 **o Password or Access key/Secret key** (Download the .csv file — it won’t be shown again).

**PRACTICAL-6**

**Objective- To secure an AWS IAM user account by enabling Multi-Factor Authentication (MFA), adding an extra verification step to prevent unauthorized access.**

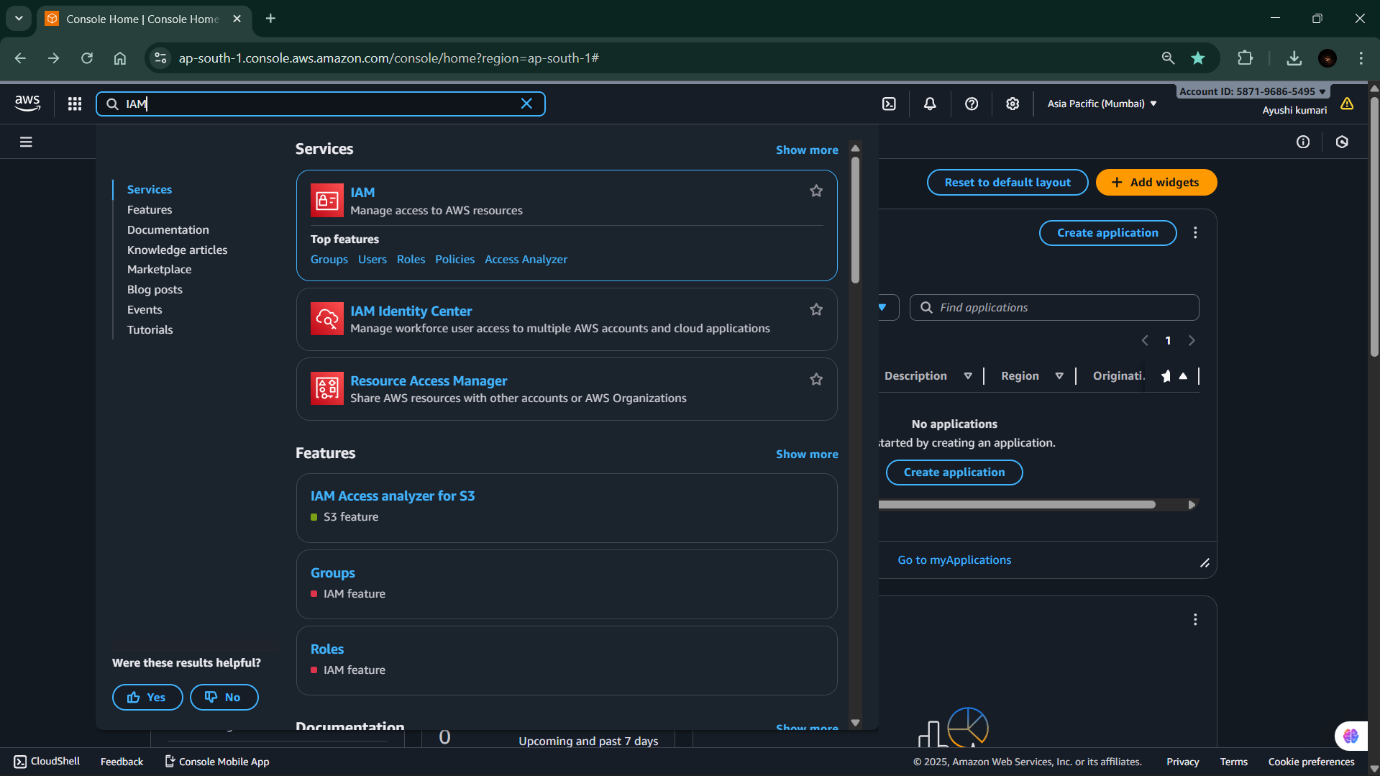
**Step 1:-** Sign in to AWS Management Console

• Log in using your root account or IAM admin user.

• Open the console.

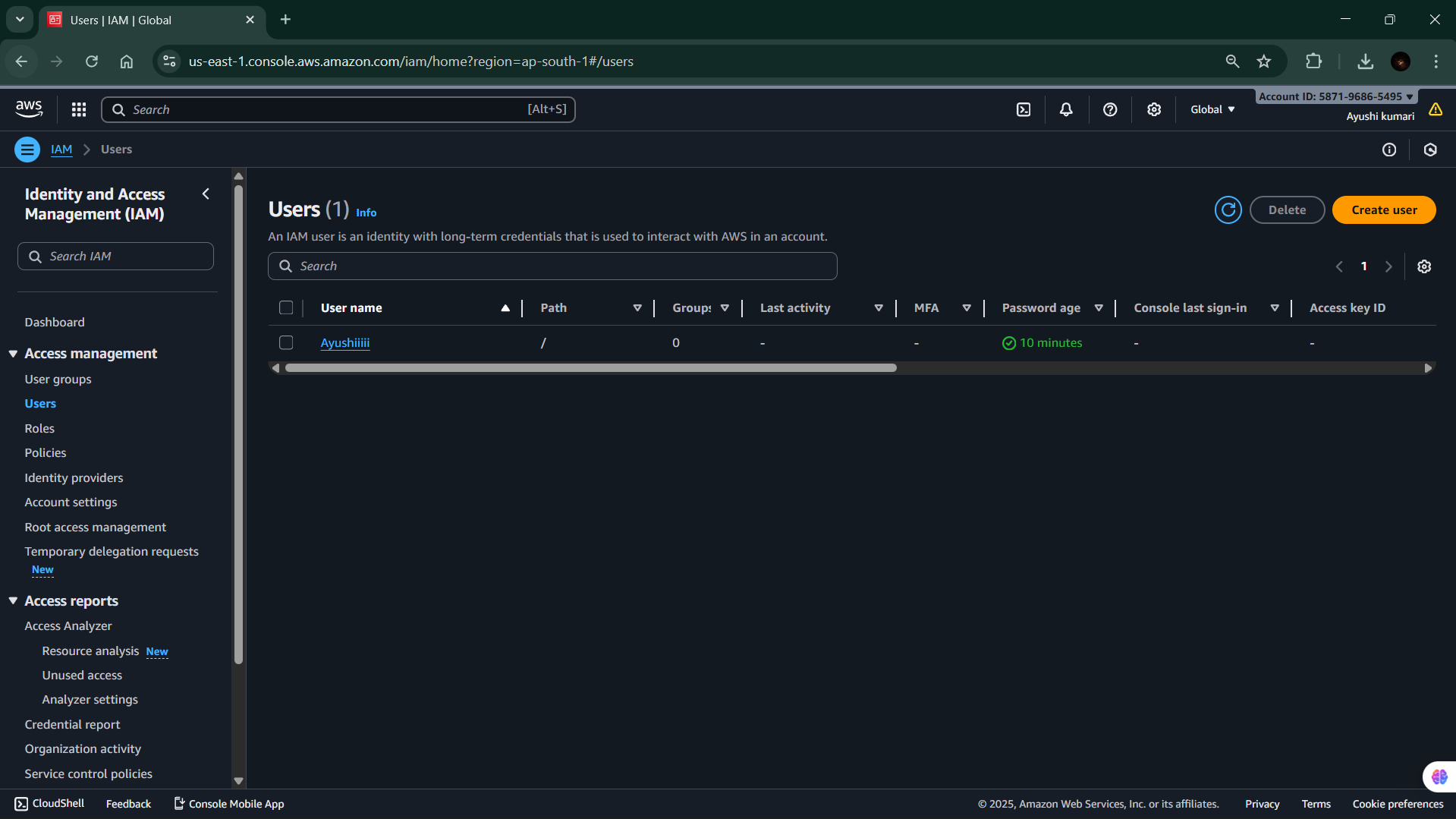
**Step 2:-** Go to IAM Service

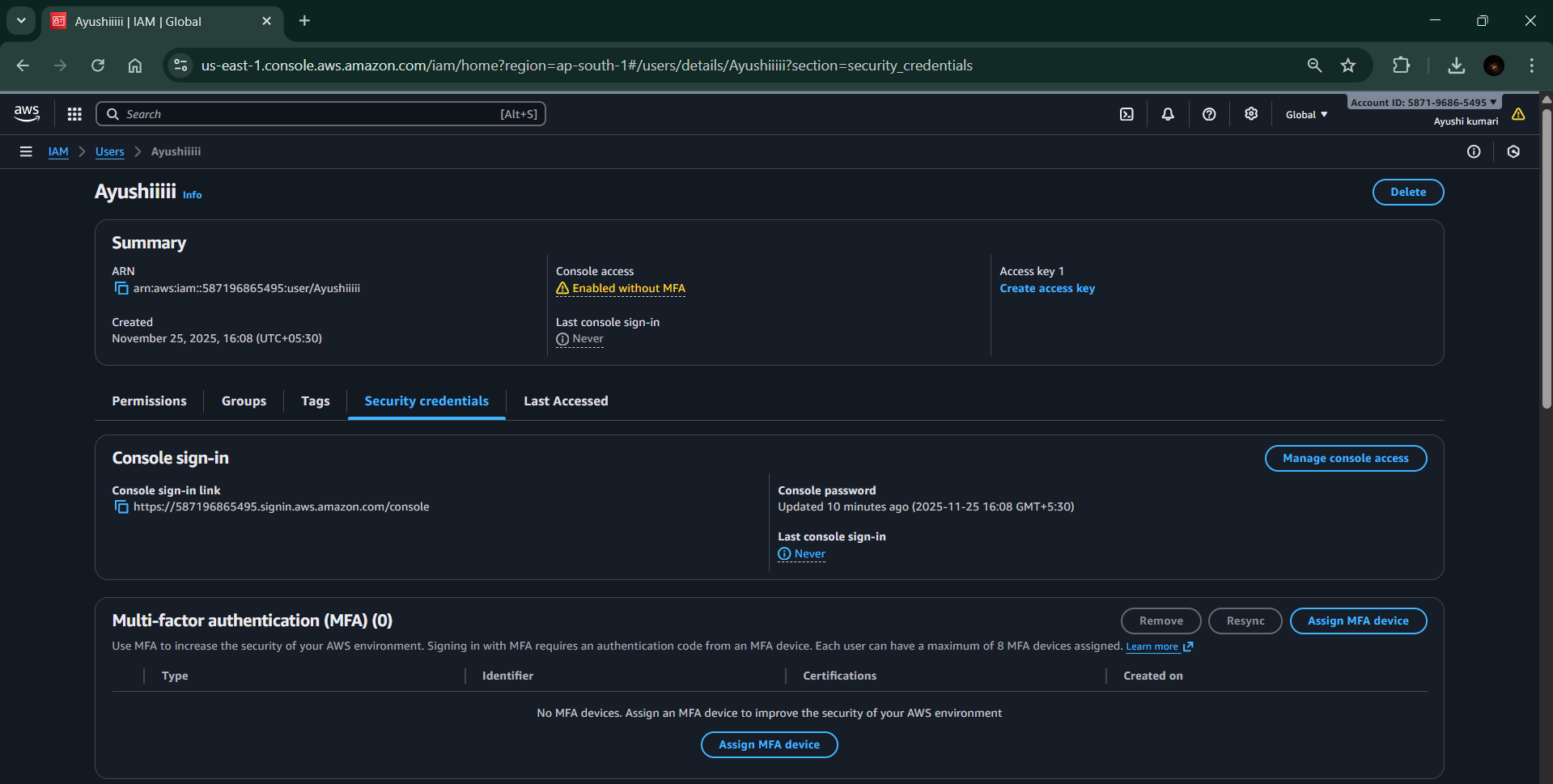
• In the search bar, type IAM.

 • Click IAM (Identity and Access Management).

**Step 3:-** Open “Users”

• In the left navigation panel, select Users.

 • Click the username for which you want to enable MFA.

**Step 4:-**Go to the “Security Credentials” Tab • After opening the user’s profile, click on Security credentials. • Scroll down to the section Multi-Factor Authentication (MFA).

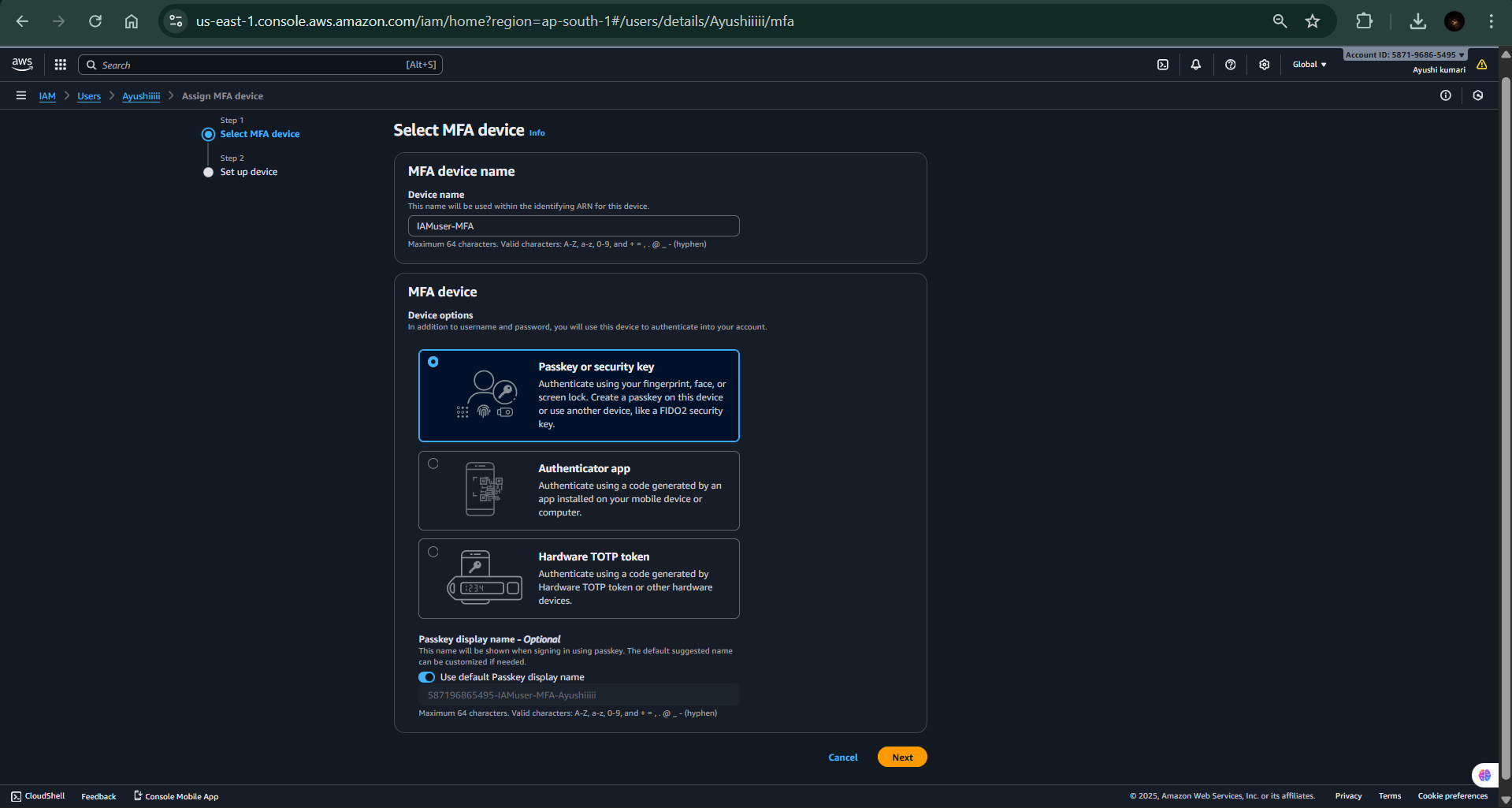
**Step 5:-** Click “Assign MFA Device”

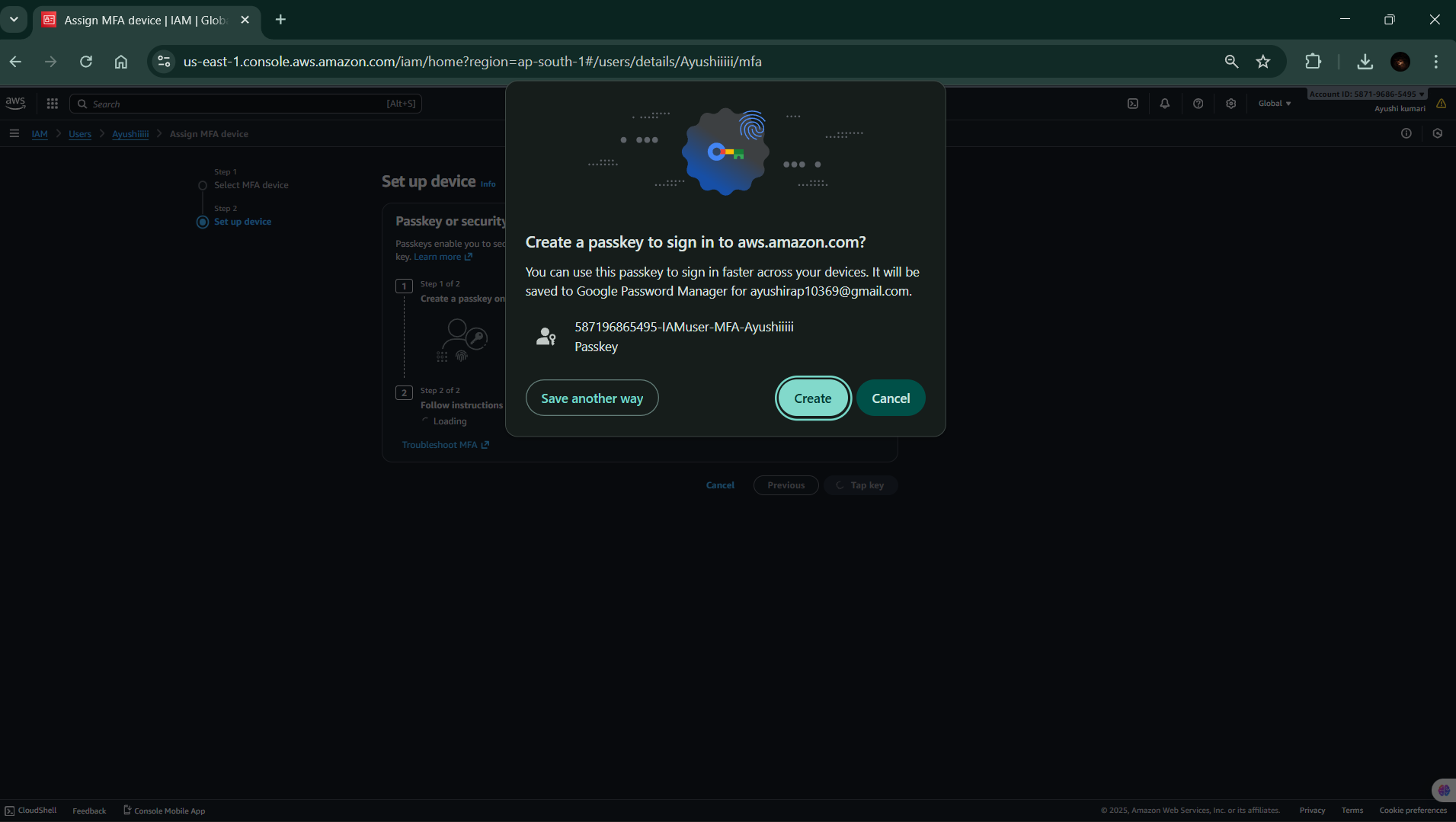
• A popup will open with 3 options:

1. Passkey or Security Key

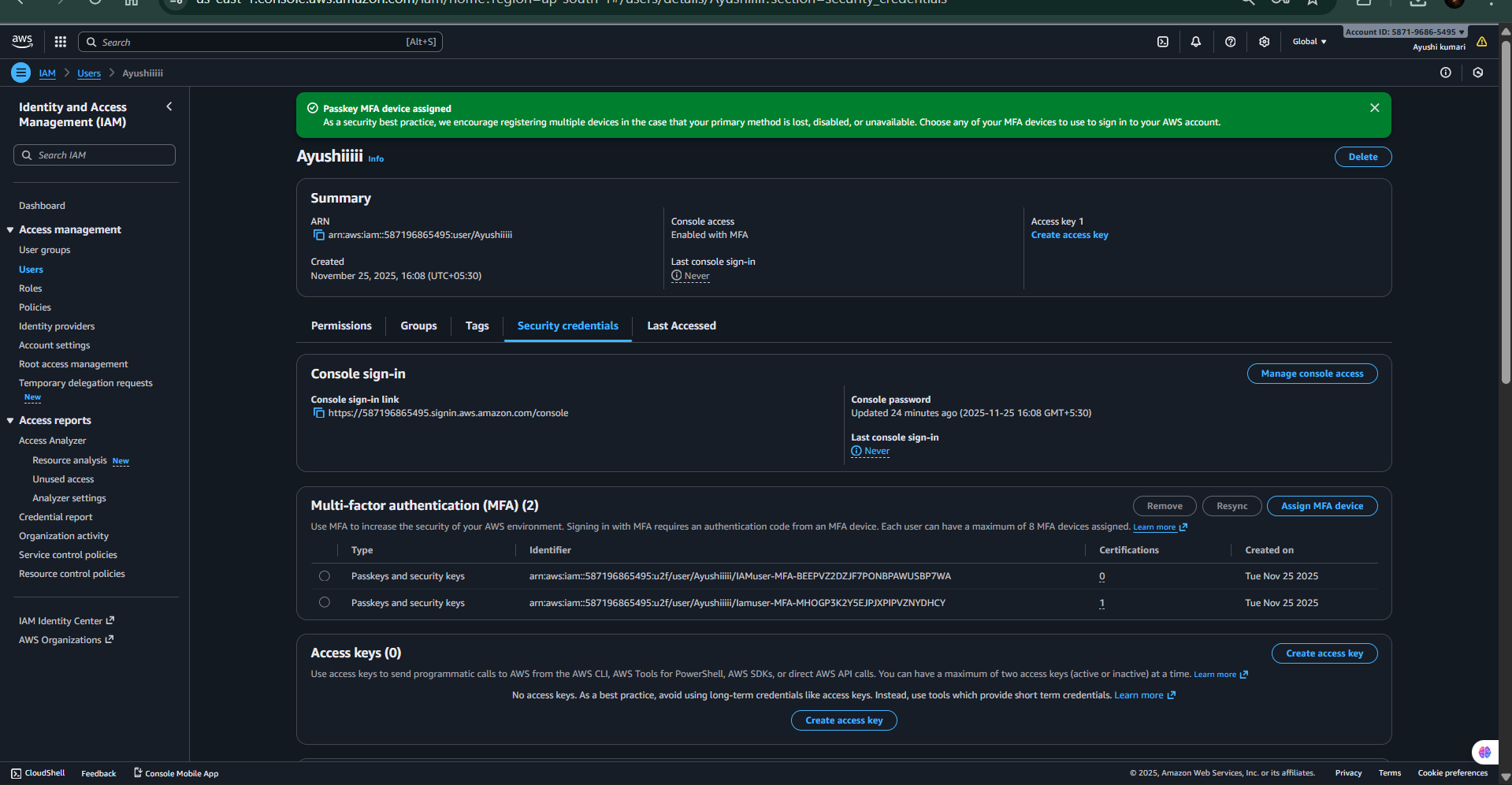
2. Authenticator App (Google Authenticator / Authy / Microsoft Authenticator)

3. Hardware TOTP Device For most labs, choose Authenticator App.

**Step 6:-**Select “Passkey or security key” and Continue the rest process of authentication.

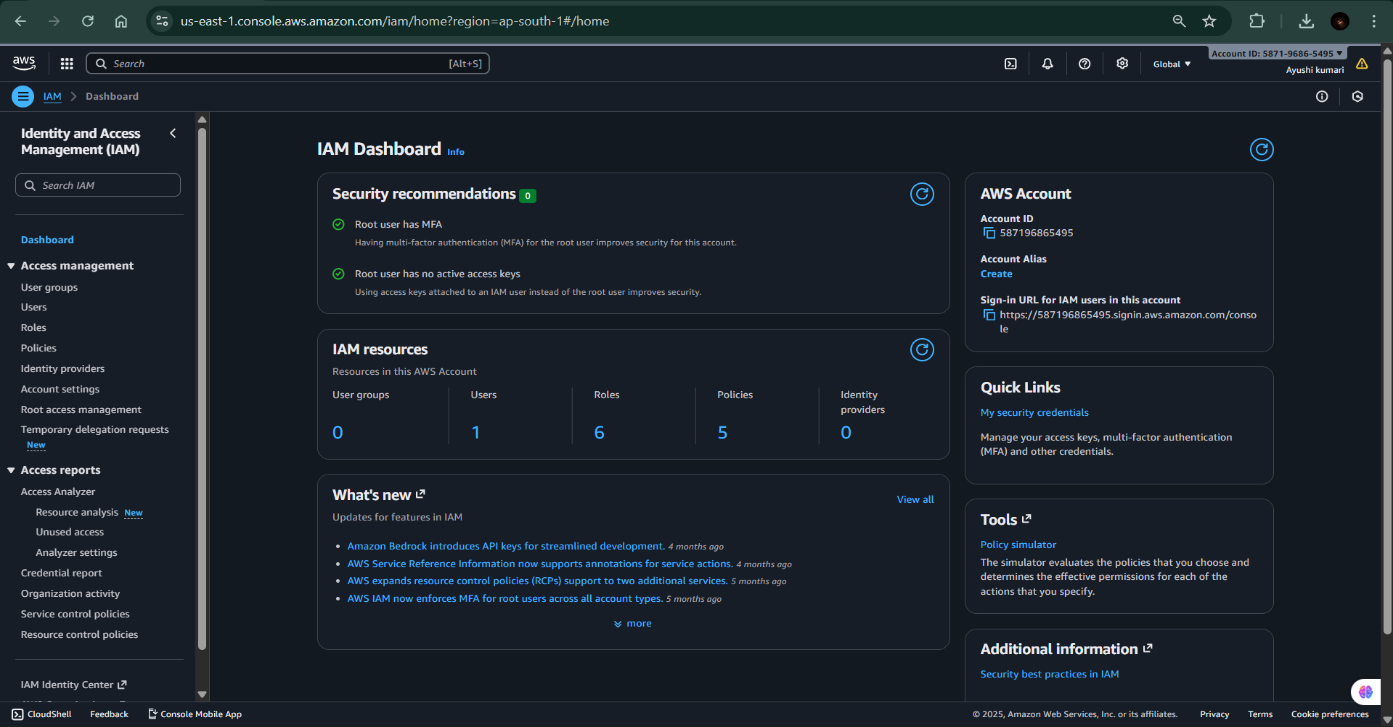


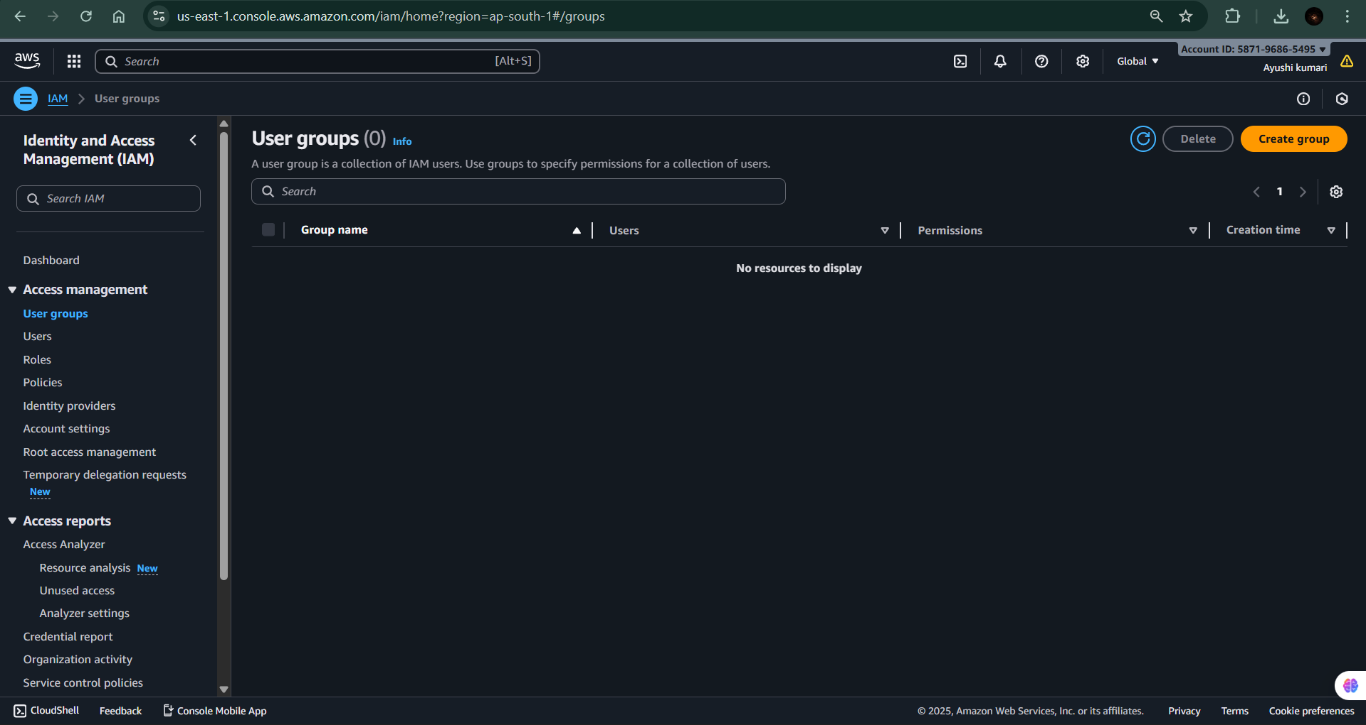
**Step 8:-** MFA Successfully Enabled “MFA device assigned successfully”



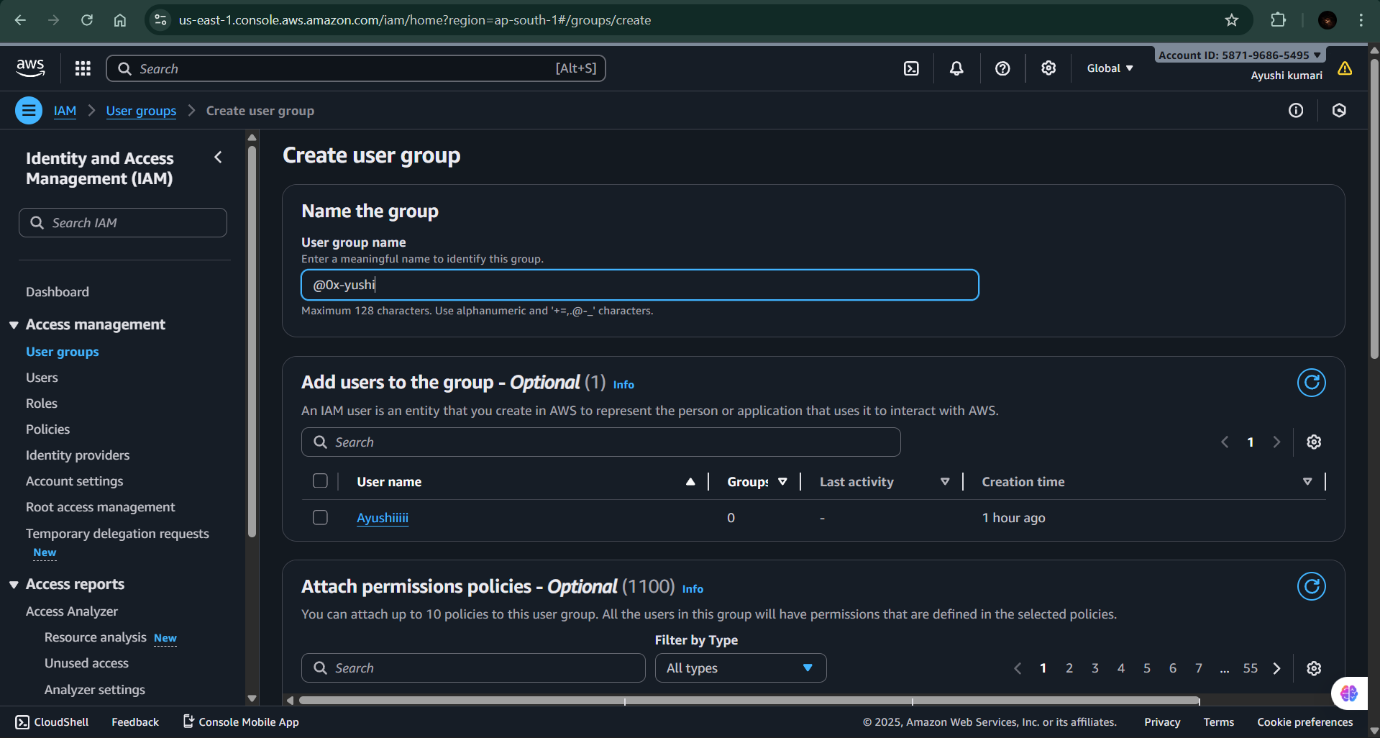
**PRACTICAL-7**

**Objective: To create a user group in AWS IAM in order to manage permissions collectively for multiple users having similar roles or responsibilities.**

**Step1:-** Open the IAM Service: In the search bar at the top of the console, type IAM, then select Identity and Access Management from the results.

**Step 2:-** Go to User Groups Section: In the left-hand sidebar, click on User groups.

**Step 3:-** Click on “Create group”: On the User Groups page, click the “Create group” button to start creating a new group.

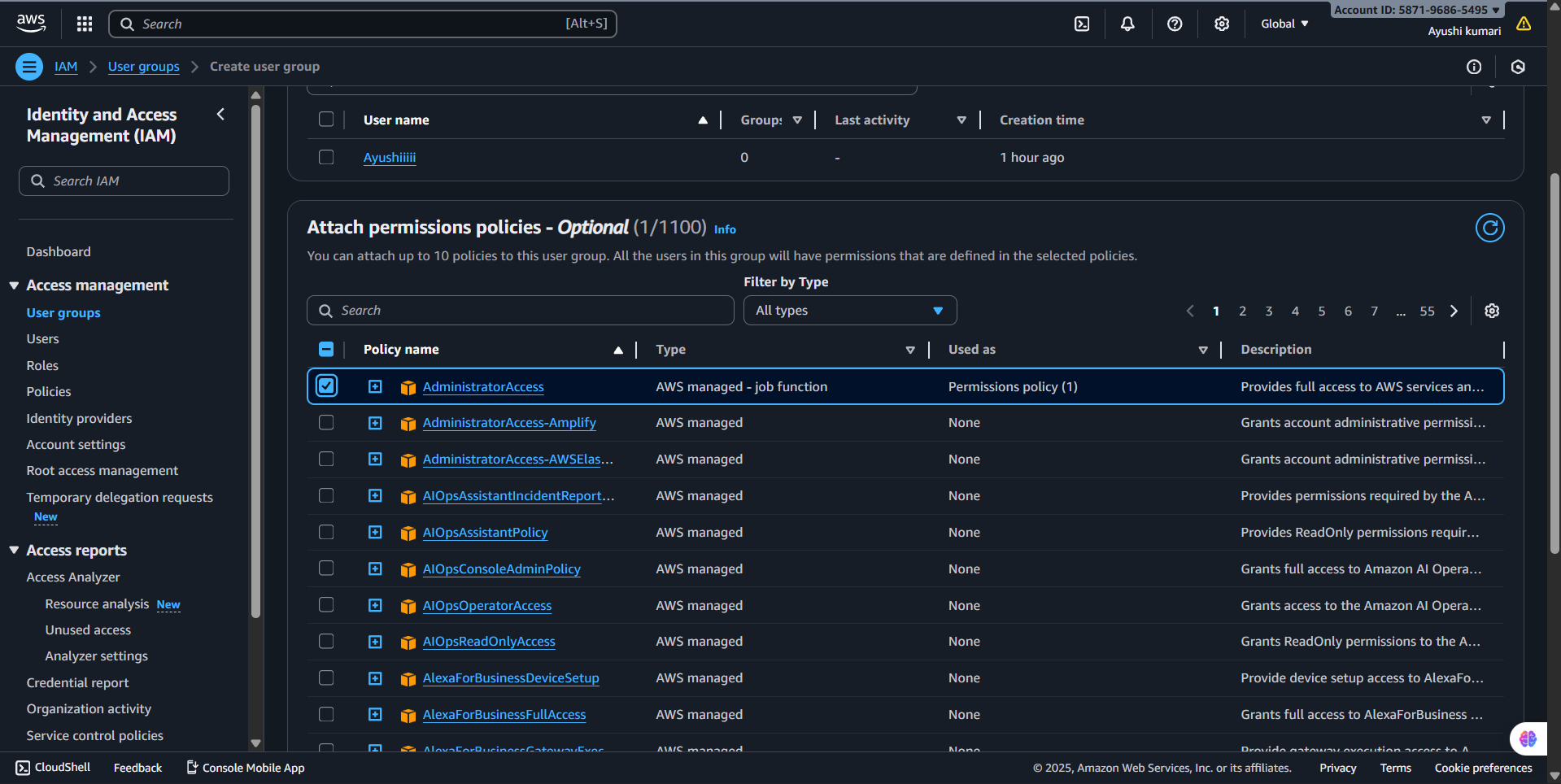
**Step 4:-** Enter Group Name: Type a unique name for your group (for example, Developers, Admins, or ReadOnlyUsers).

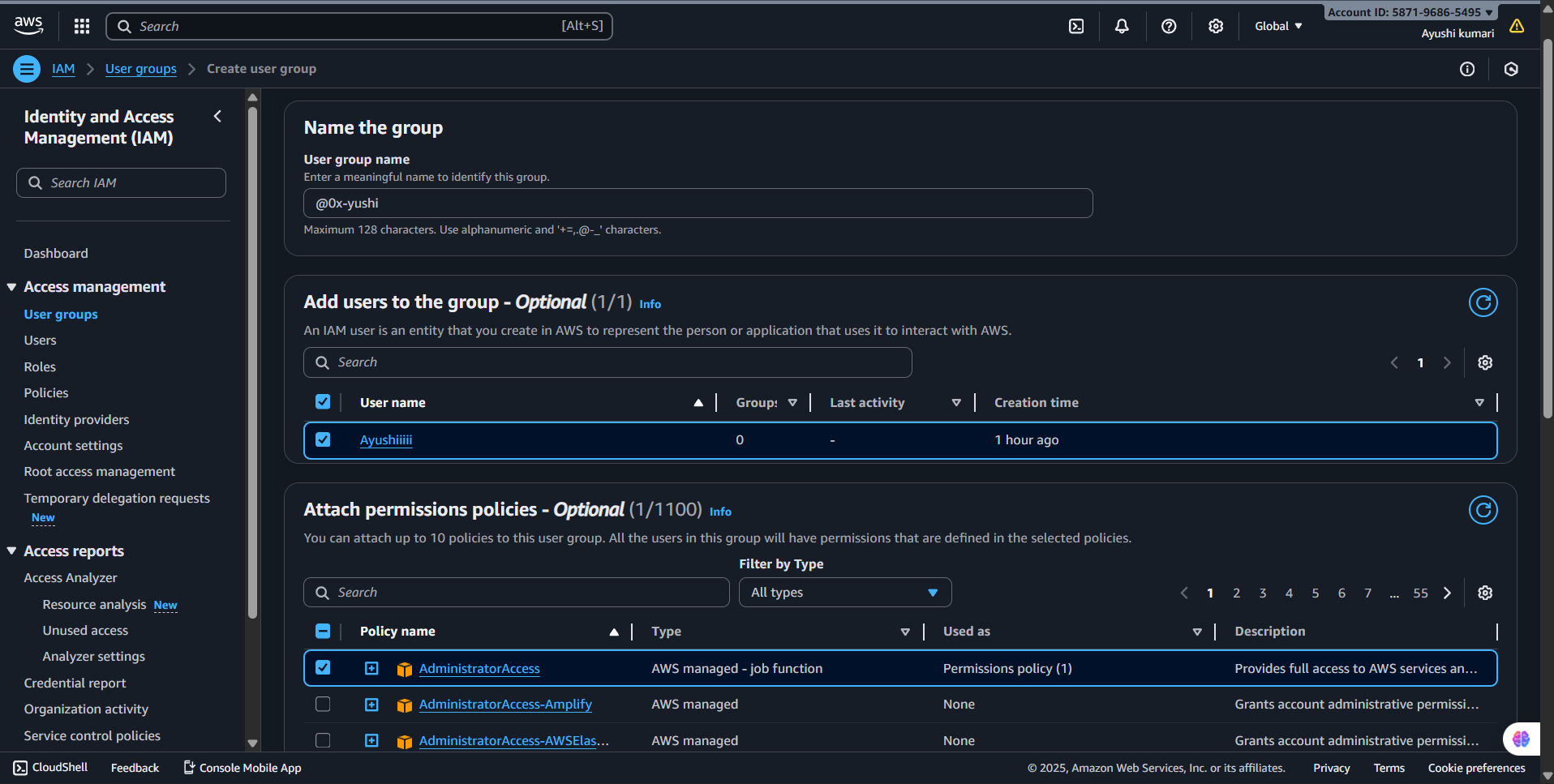
**Step 5:-** Attach Permissions Policies (Optional): You can choose policies to attach to this group, such as:

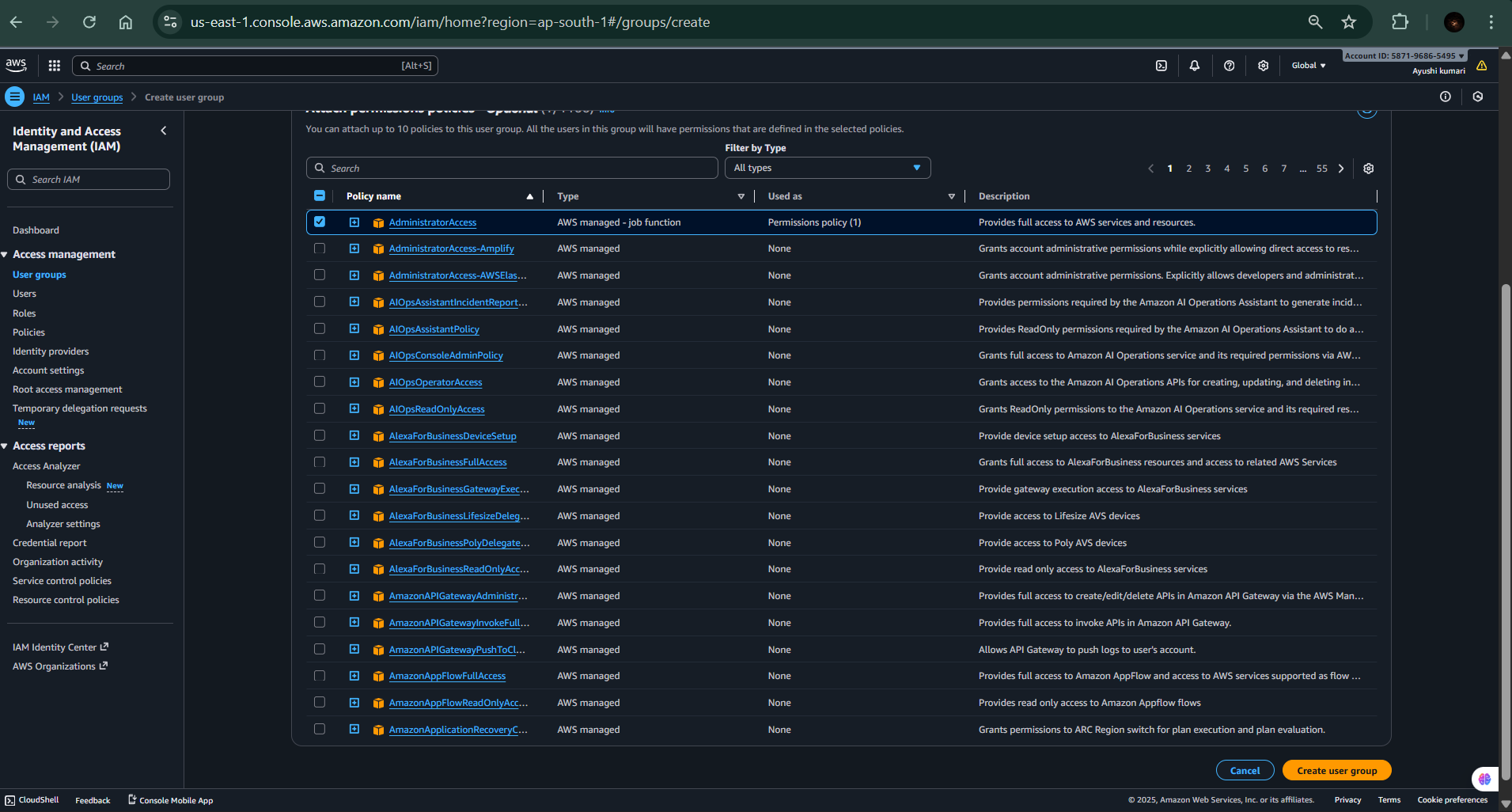
• AmazonS3FullAccess

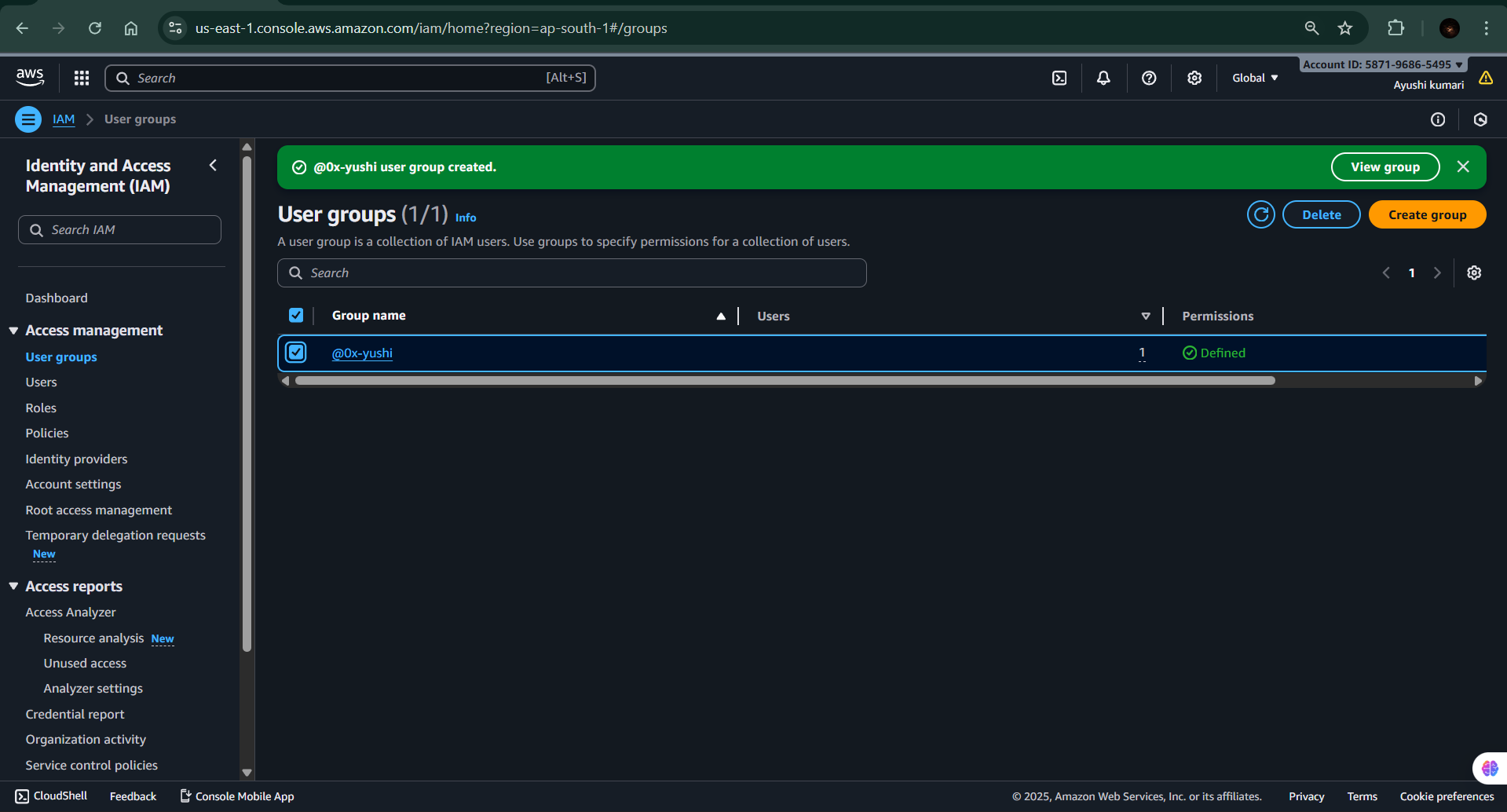
• AmazonEC2ReadOnlyAccess

• AdministratorAccess

* If you want to add permissions later, you can skip this step and click Next.

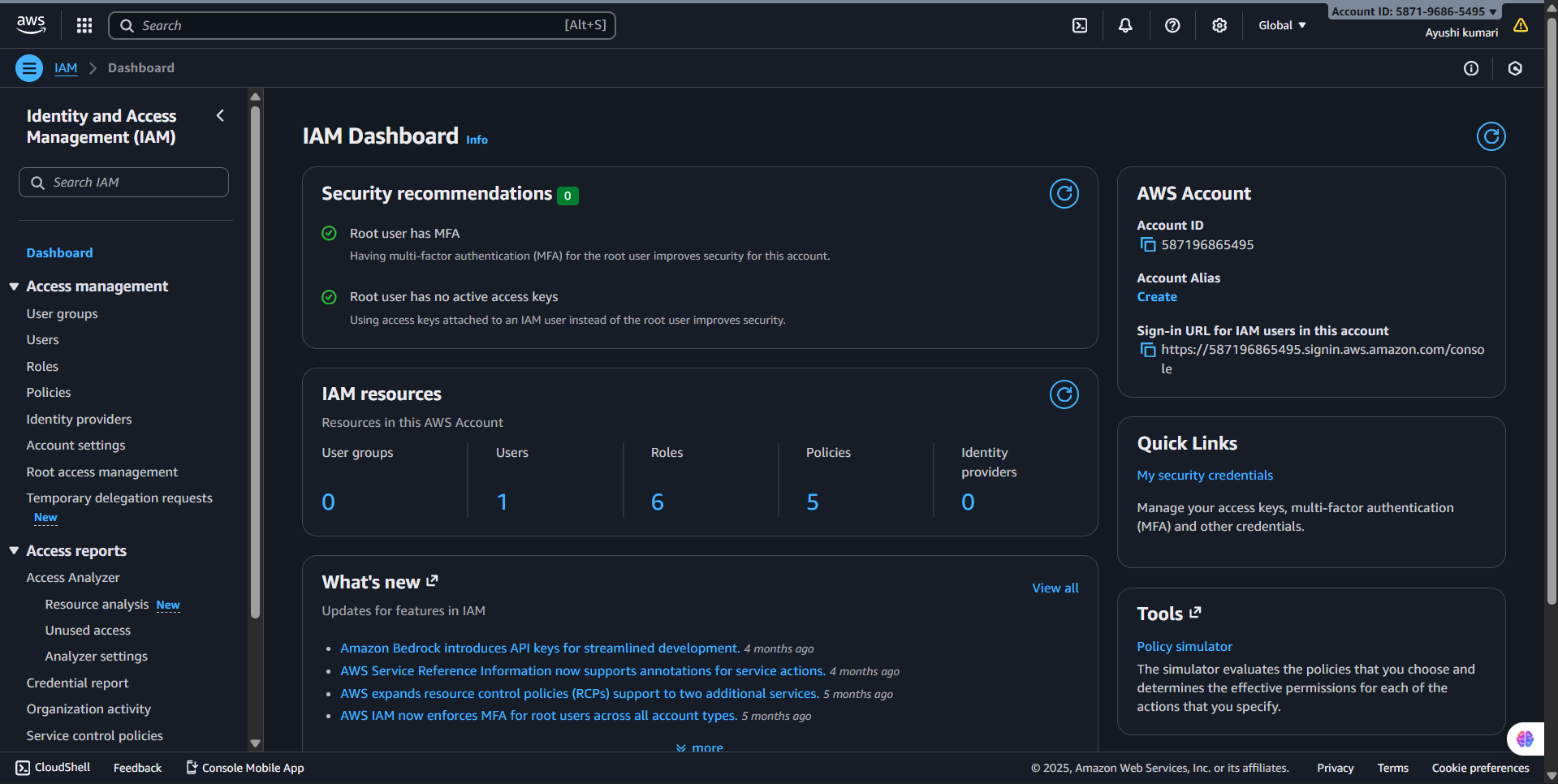
**Step 6:-** Add Users to the Group (Optional): You can select existing IAM users to include in this group now, or you can add users later after creating the group.

**Step 7:-** Review and Create Group: Review the group details and attached policies, then click Create group.



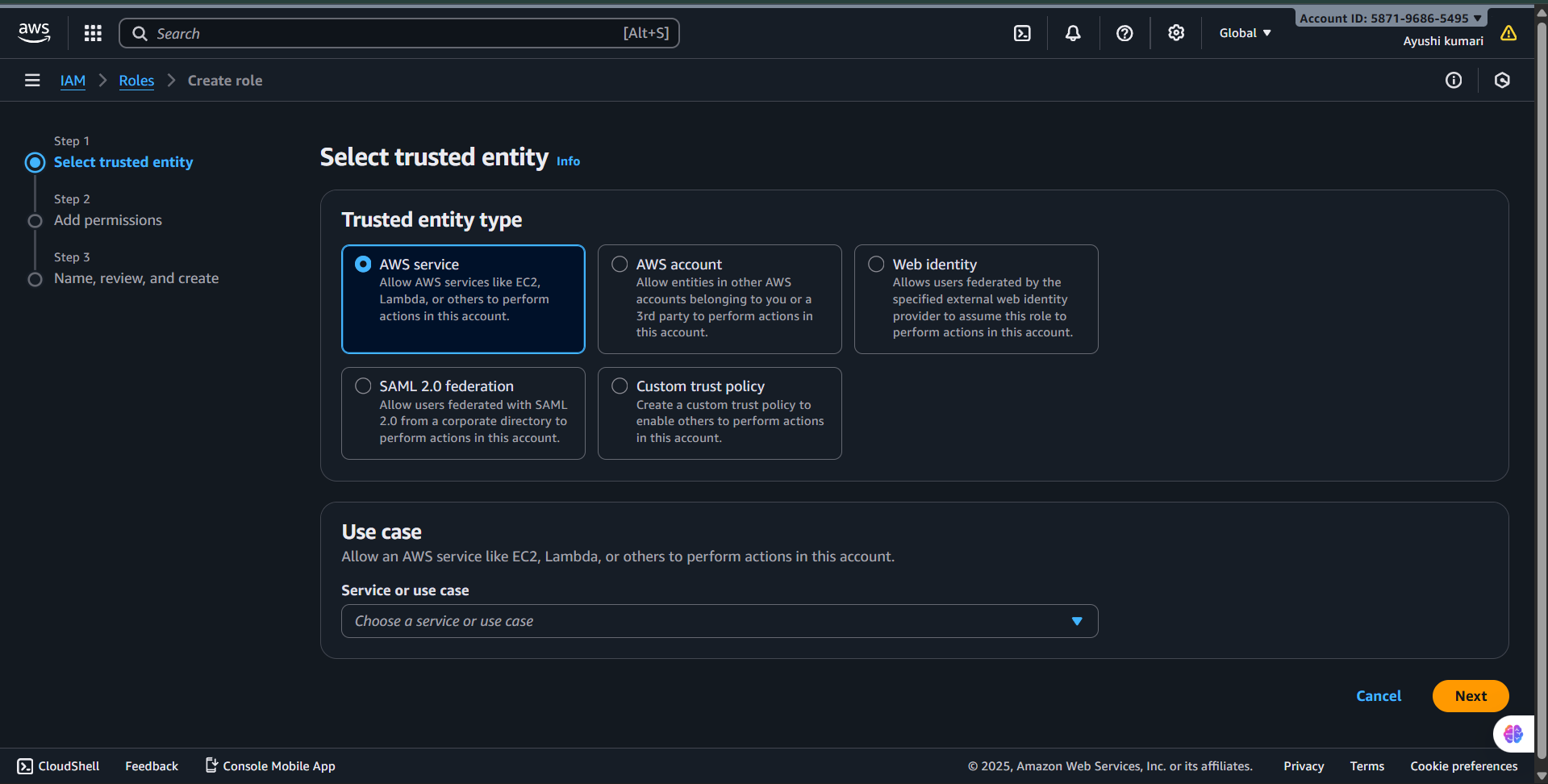
**PRACTICAL-8**

**Objective:-To create a security role in AWS IAM that allows AWS services or users to securely access specific AWS resources with defined permissions, ensuring controlled and temporary access without sharing long-term credentials.**

**Step 1:-** Open the IAM Service: In the search bar at the top of the console, type IAM, then select Identity and Access Management from the results.

**Step 2:-** Go to Roles Section: In the left-hand navigation pane, click on Roles.

**Step 3:-** Click on “Create role”: On the Roles page, click the “Create role” button to start the process.



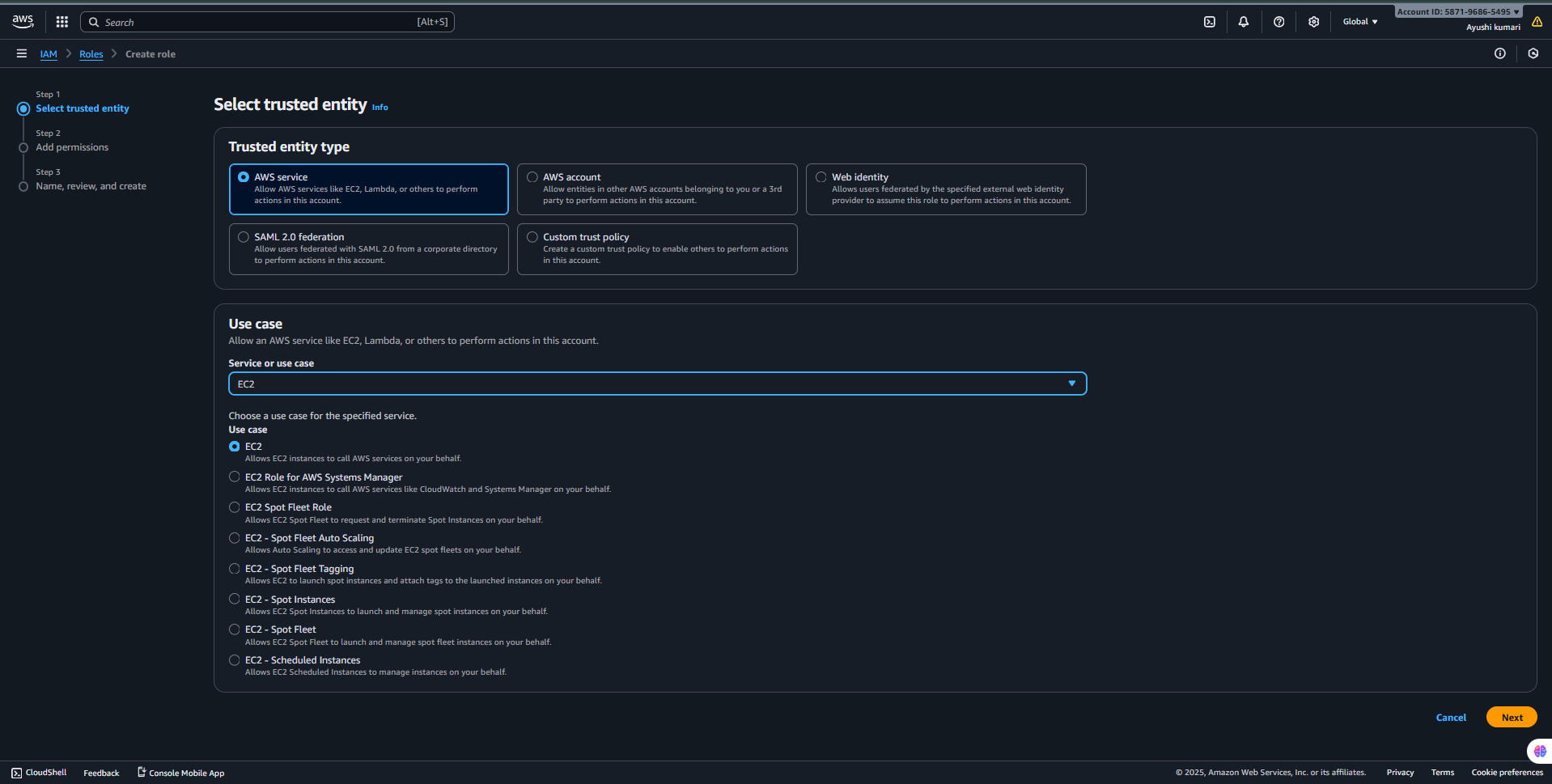
**Step 4:-** Select Trusted Entity Type:

Choose who will use the role, such as:

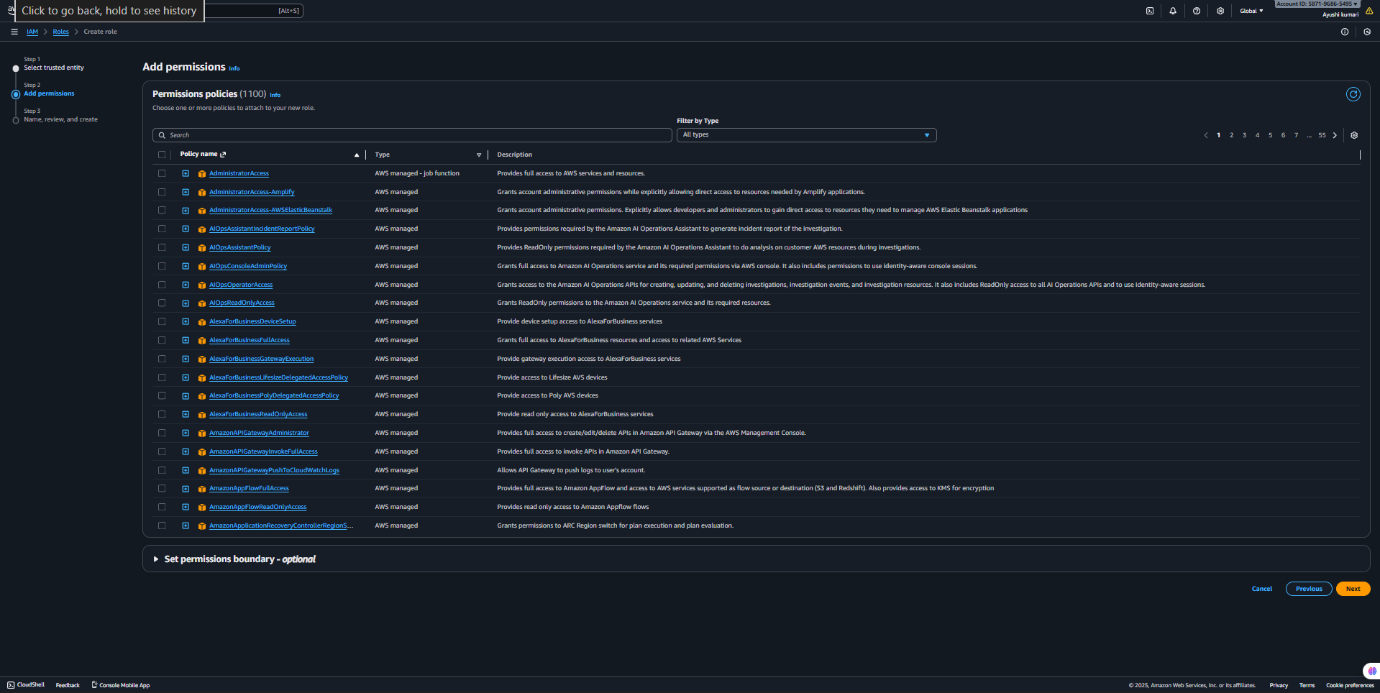
• AWS Service (e.g., EC2, Lambda)

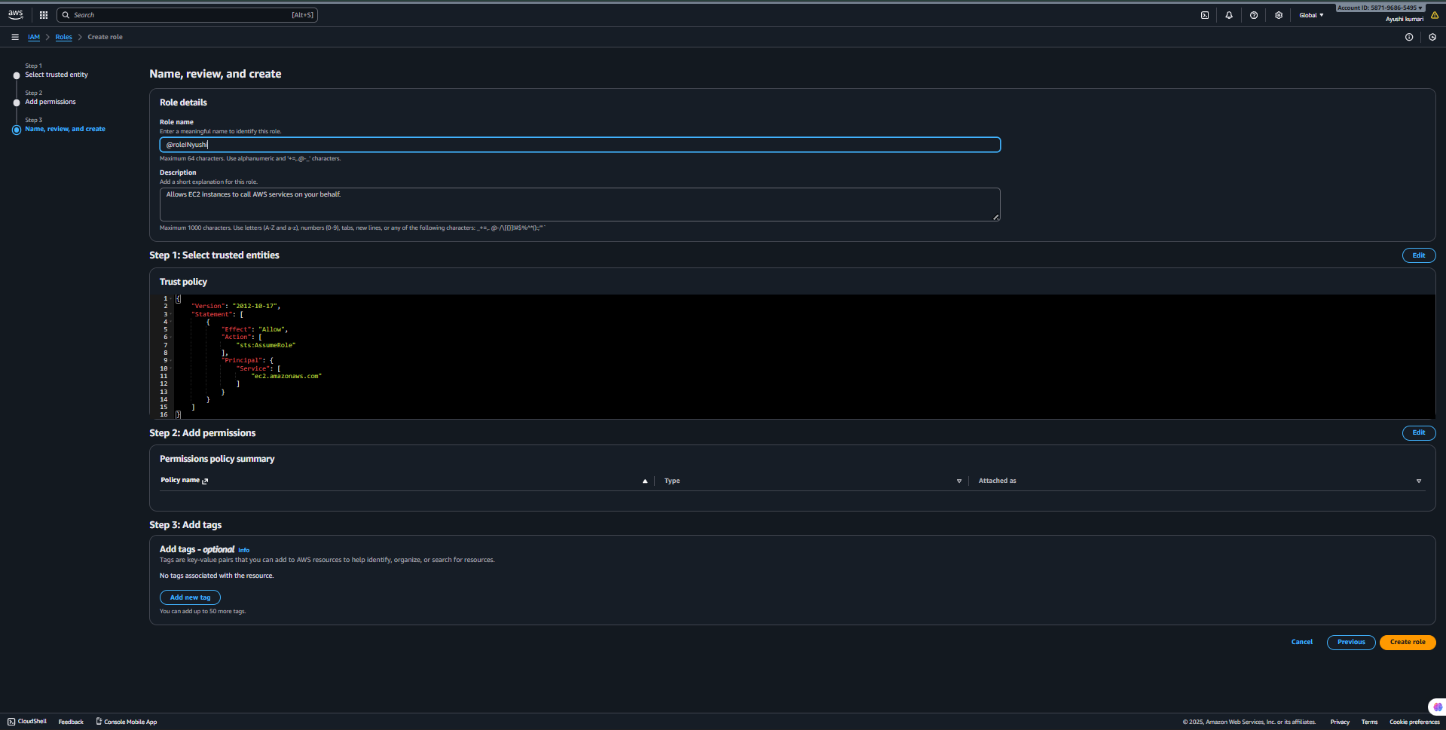
• Another AWS Account

• Web Identity or SAML 2.0 Federation

 Click Next after selecting the appropriate option.

**Step 5:-**Attach Permissions Policies:

*  Select the permissions policies that define what actions the role can perform (for example, AmazonS3FullAccess or AmazonEC2FullAccess).

**Step 6:-** Name and Review the Role: Enter a role name (for example, EC2SecurityRole or LambdaAccessRole) and review all selected settings.

