Creating Admin Account and Setting Up MFA on AWS

Objective: To create an admin account on AWS and set up Multi-Factor Authentication (MFA) to enhance security

Tools required: AWS

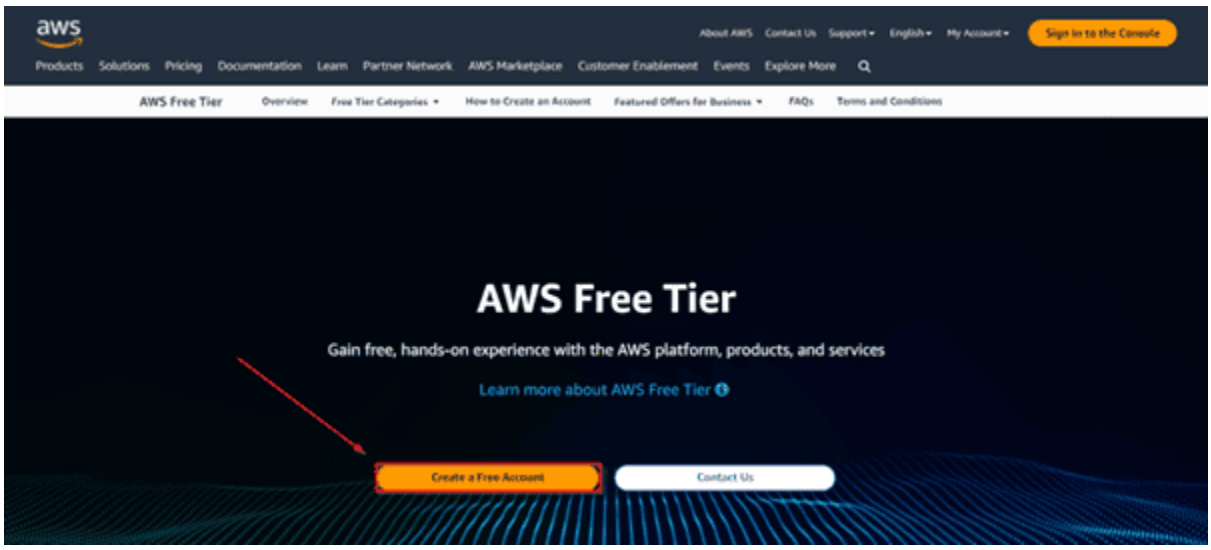
Prerequisites: None

Steps to be followed:

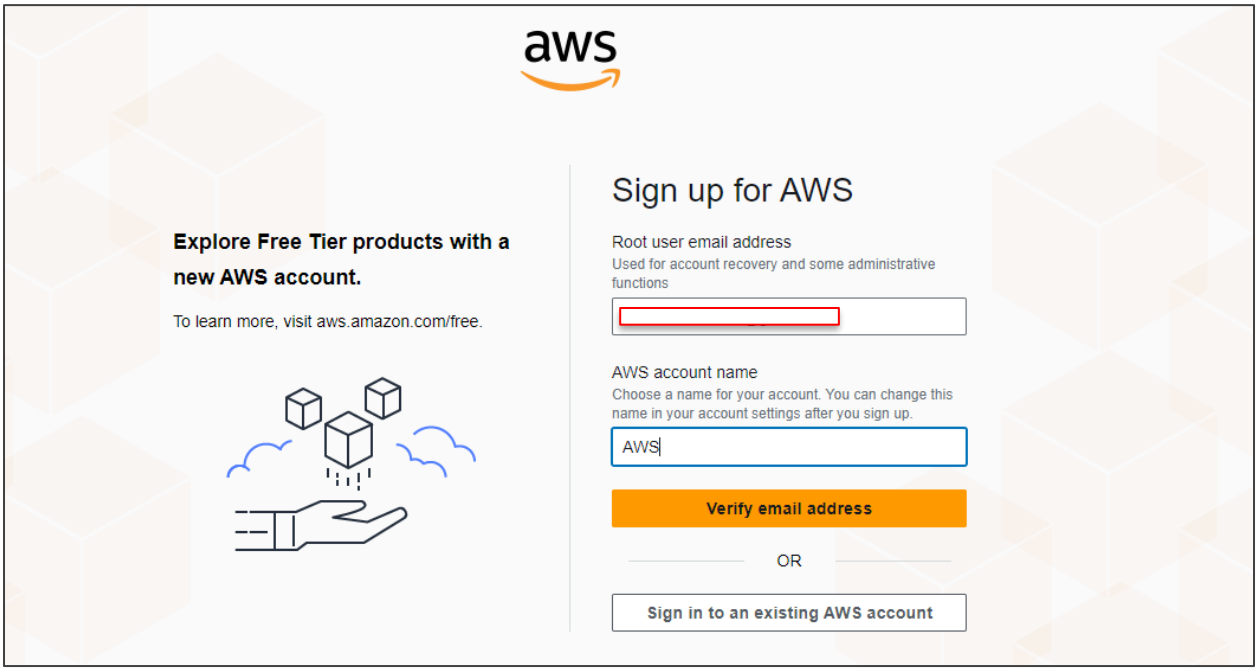
1. Register for an AWS Free Tier account
2. Log in to the AWS Management console
3. Create an IAM user
4. Enable MFA for the IAM User and configure the virtual MFA device
5. Access AWS Console using MFA
6. Verify your account plan

Step 1: Register for the AWS FREE-TIER account

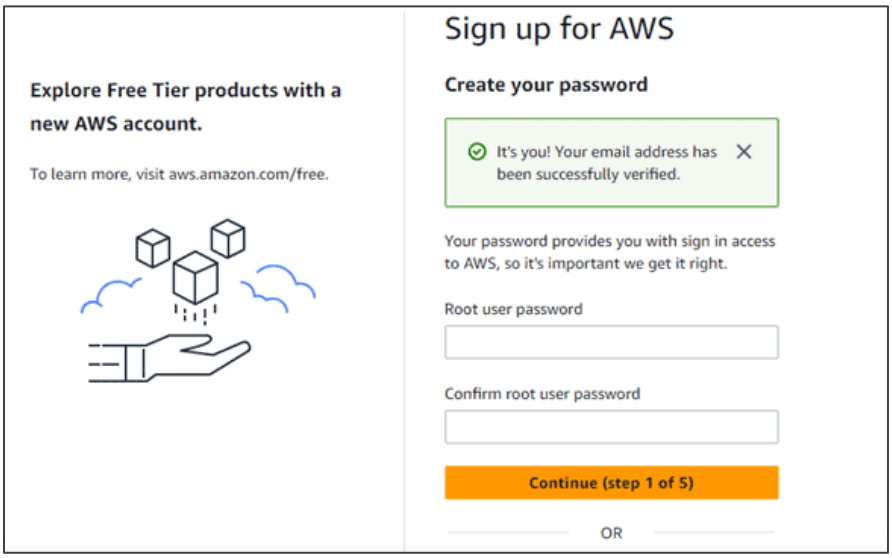
1.1 Open your web browser and navigate to the AWS Free Tier Page. Click On **Create a Free Account**



1.2 Verify your email address



1.3 Provide the details that you want to use to log in to your **AWS** account and click on **Continue**

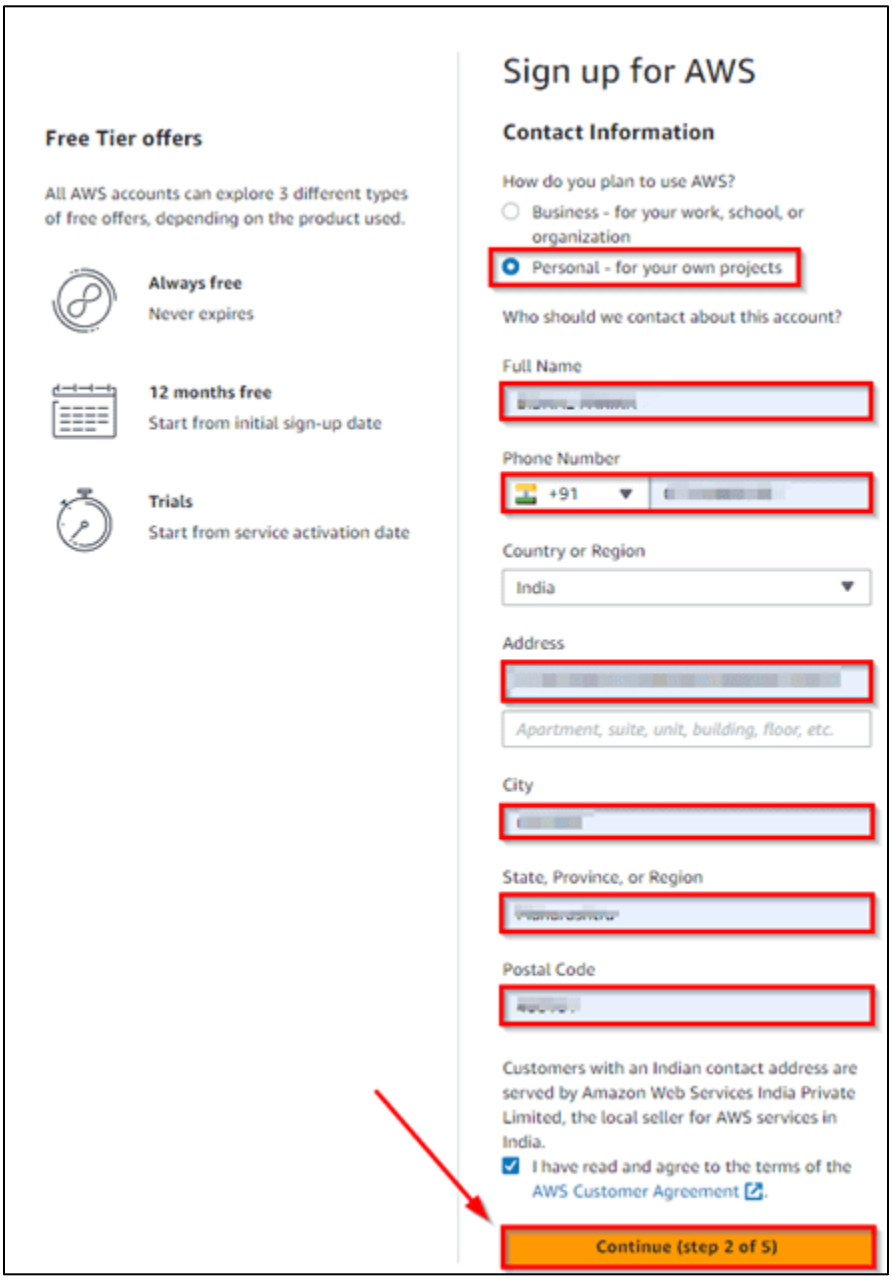


Note:

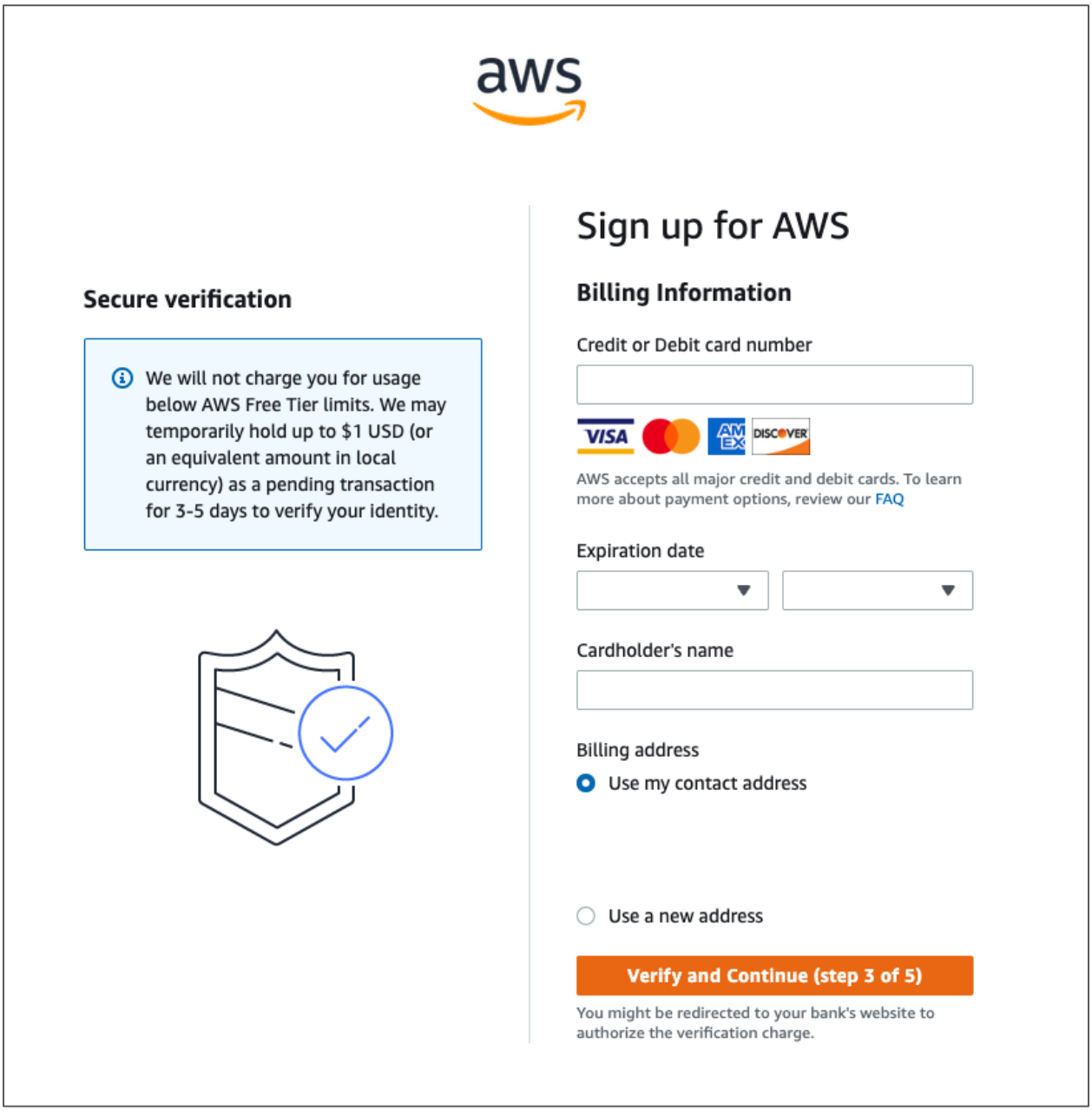
- Email address: Enter the email ID that hasn't registered yet with Amazon AWS
- Password: Type your Password
- Confirm password: Confirm the Password
- Captcha: enter the given security check

1.4 Select your AWS type (Professional/ Personal) and fill in the correct information to validate your account

If creating a personal account, click **Personal Account**. Otherwise, use **Company Account**. Accept the Terms and Conditions, click on Continue.

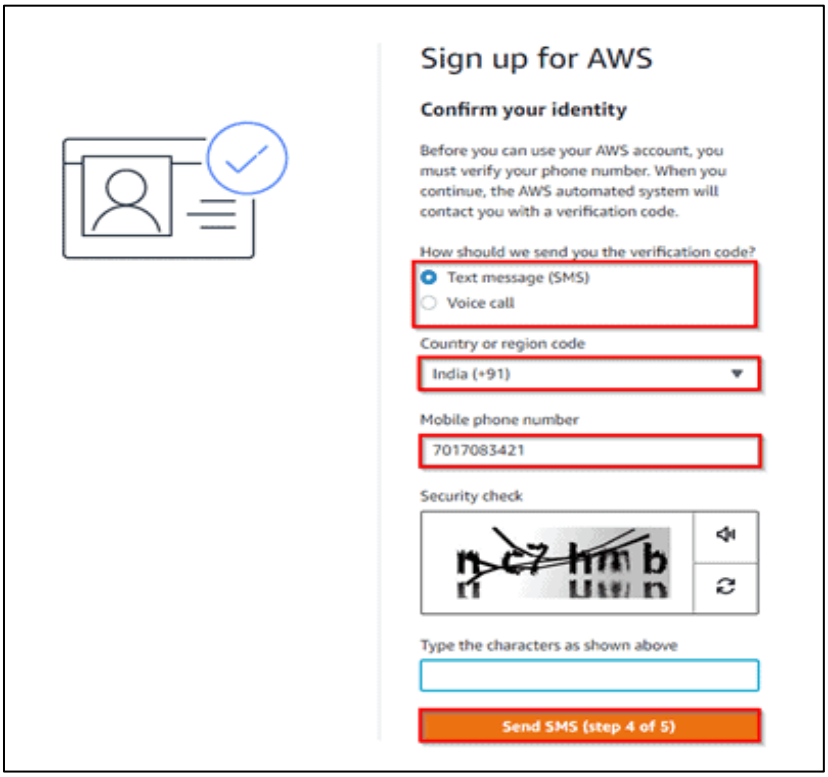


1.5 Please enter your credit card or debit card information and billing address and **click** on **Verify and Continue**

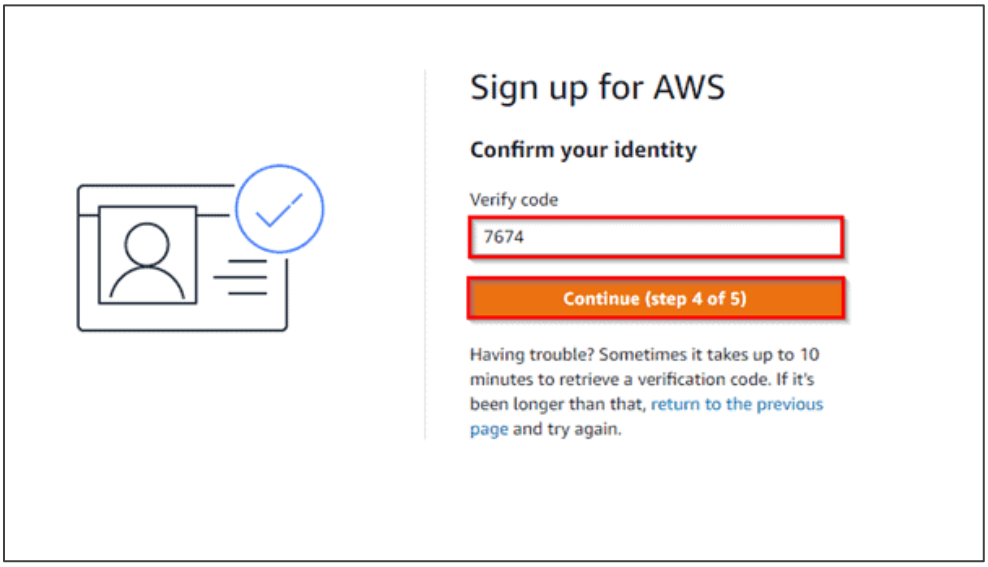


After this step, you will be taken to the payment gateway to validate your payment information. For your credit card verification, Amazon will charge the minimum price based on your Country.

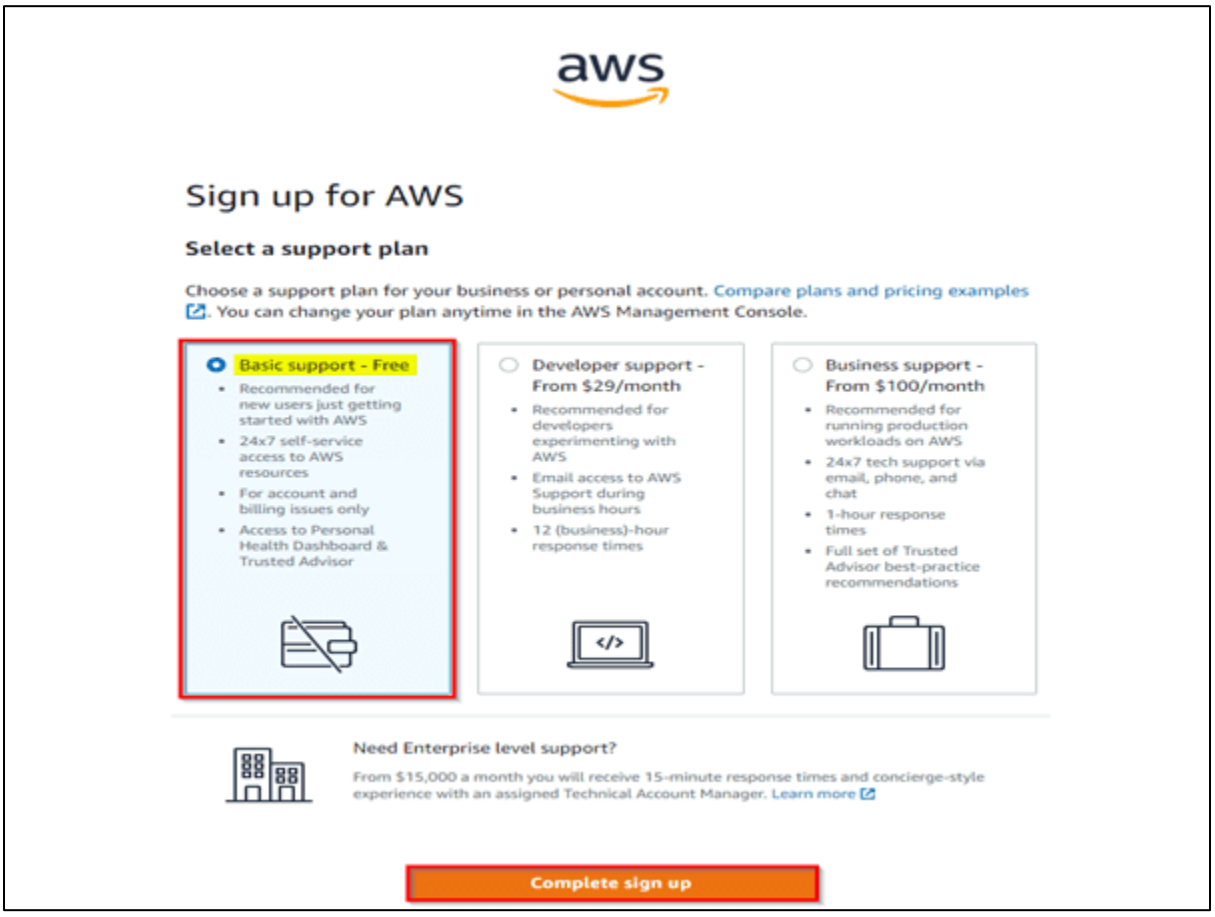
1.6 You will be taken to an identity verification page with your phone number. You must select either **Text message** or **Voice call**. Provide a valid phone number, solve the captcha, and then click on Send SMS or Call Me Now (depending upon your selection).



1.7 After clicking on Send SMS or Call me Now, you will immediately receive a call or SMS from Amazon; for verification code, enter your code, then click on **Continue**

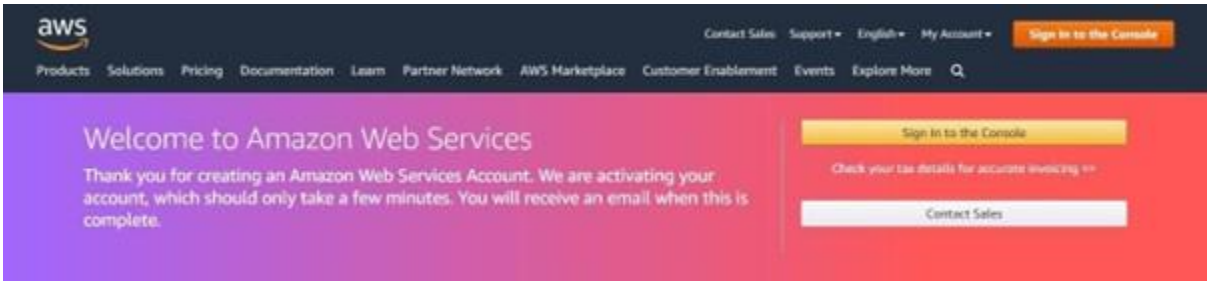


1.8 AWS support offers a selection of plans to meet your business needs. Select your suitable plan, then click **on Complete sign up**



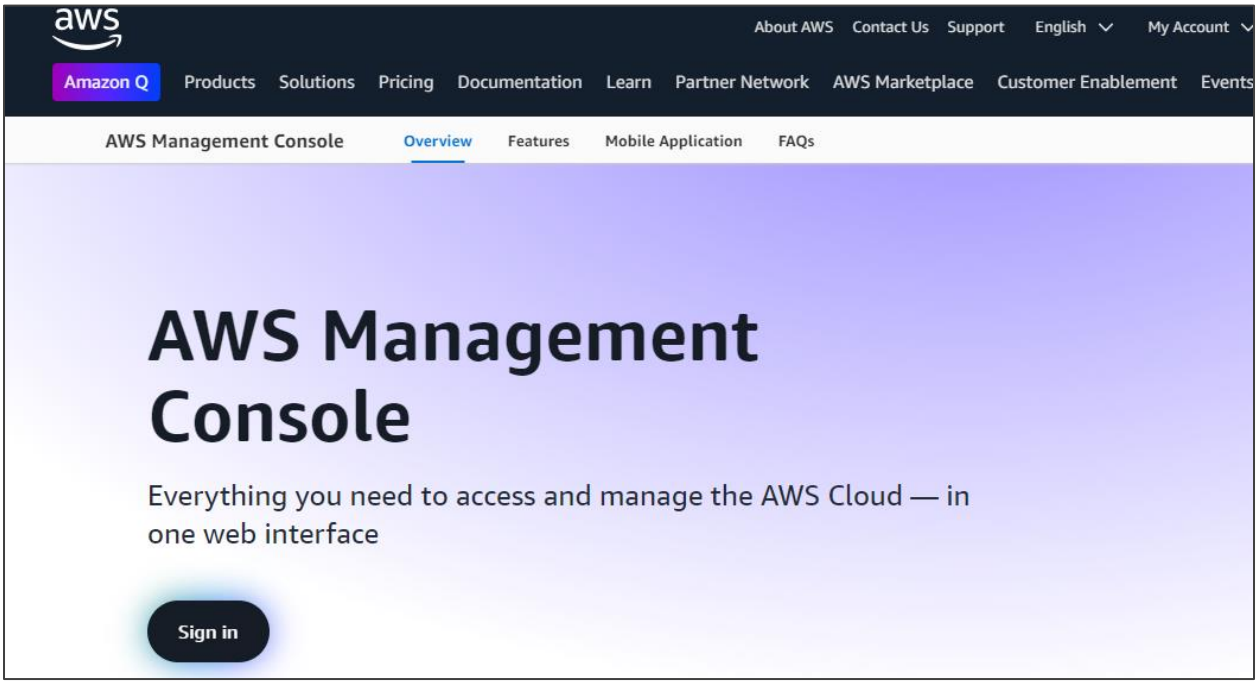
Registration Confirmation page

Once you complete the steps and processes, you'll see the confirmation page below. Your account will now be processed for activation. It may take 30 minutes to 1 hour for you to receive an email confirmation that your Amazon Cloud Services account has been activated.

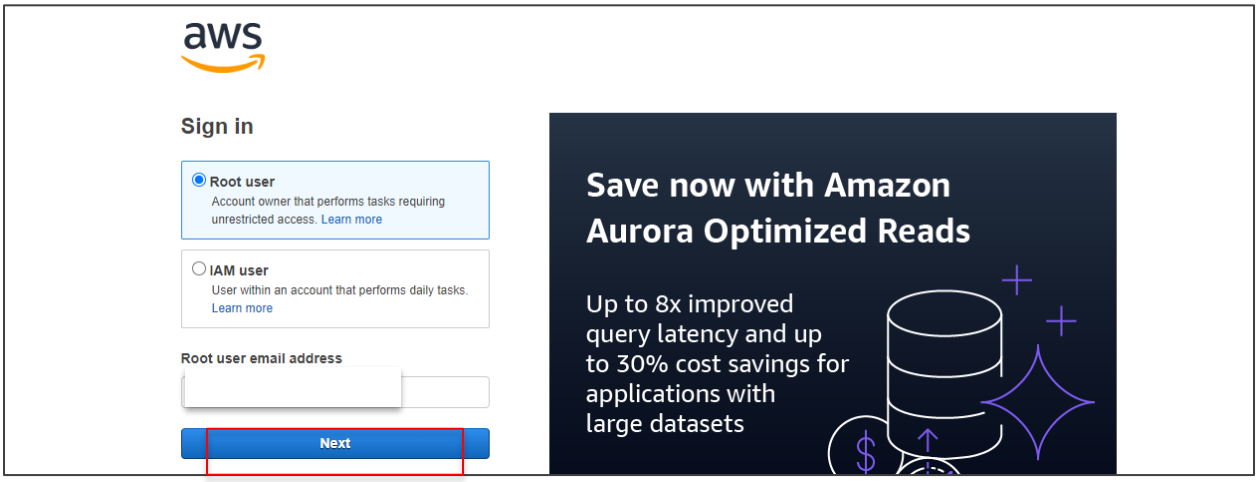


Step 2: Log in to the AWS Management Console

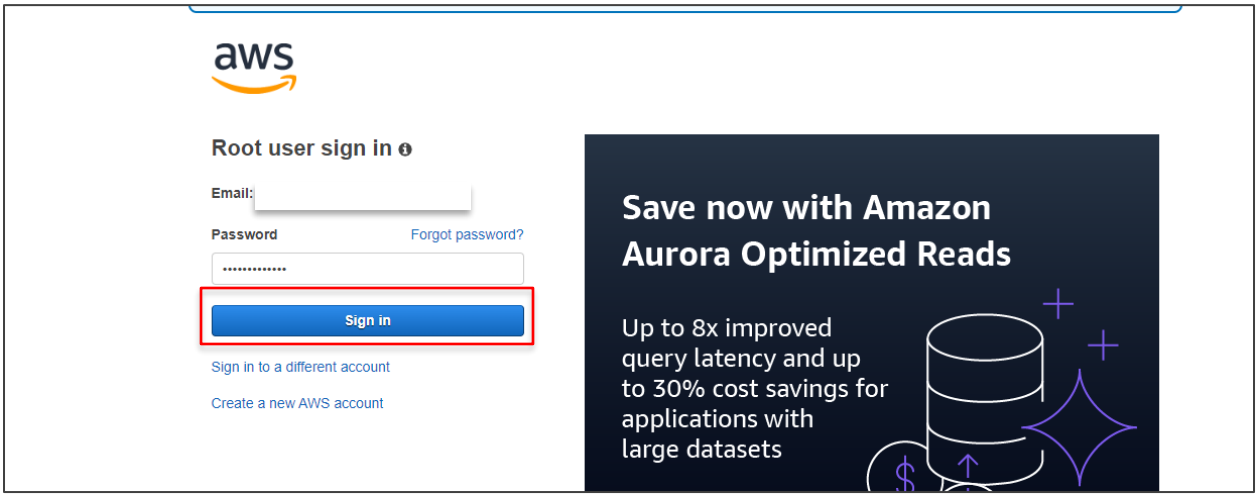
2.1 Open your web browser and go to the below link to **Sign in**:
[AWS Management Console]



2.2 Enter the **username** you chose while creating the account and click **Next**

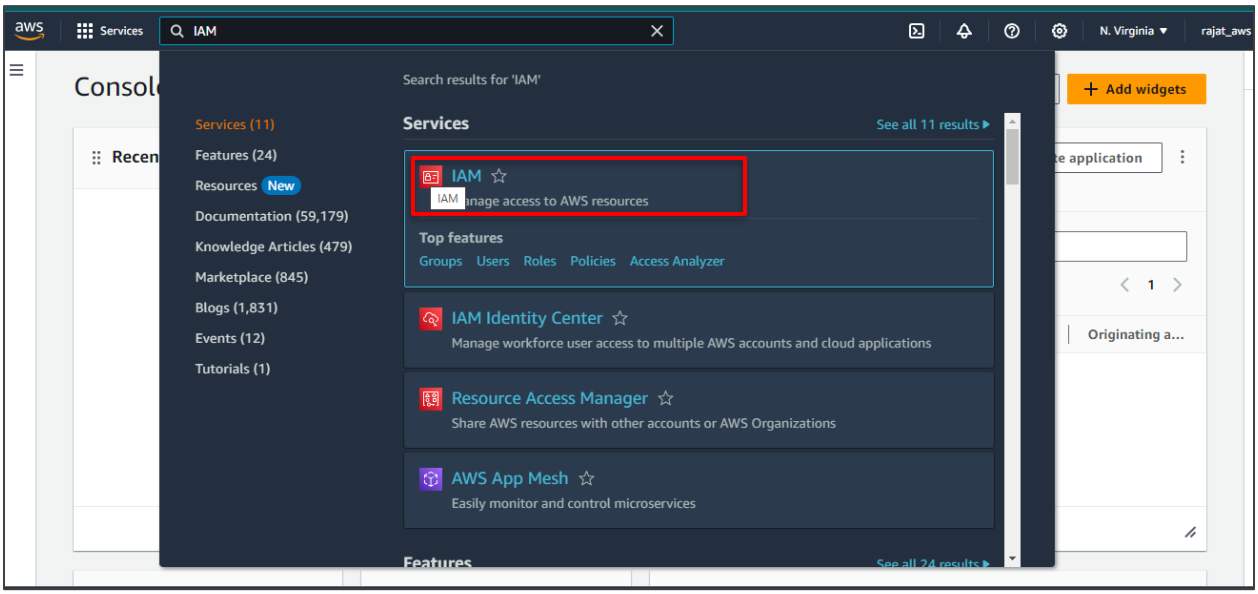


2.3 Enter the **password** and then click **on Sign in**

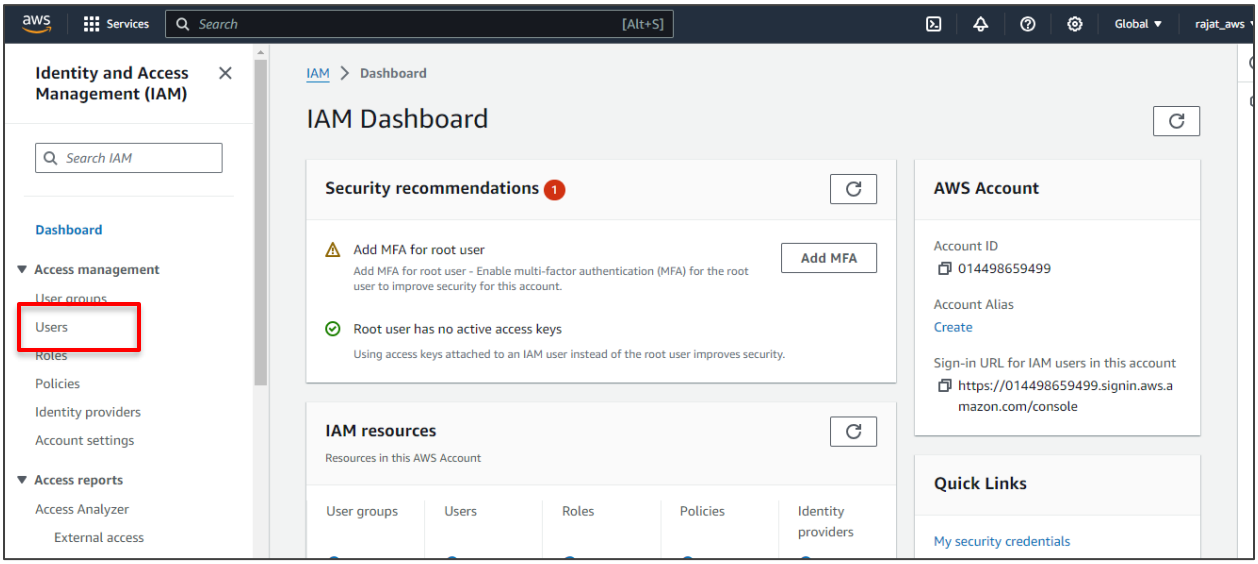


Step 3: Create an IAM user

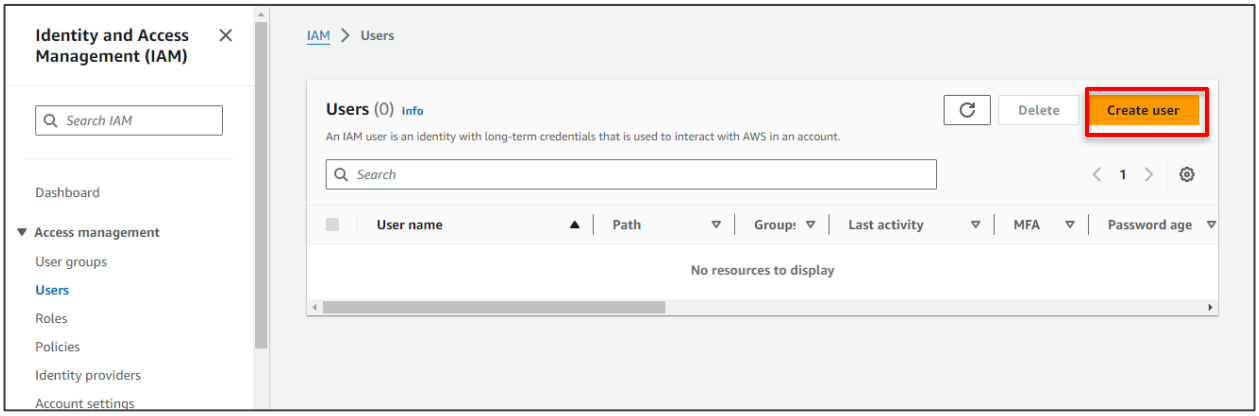
3.1 In the search bar, search for **IAM** and click on **IAM**



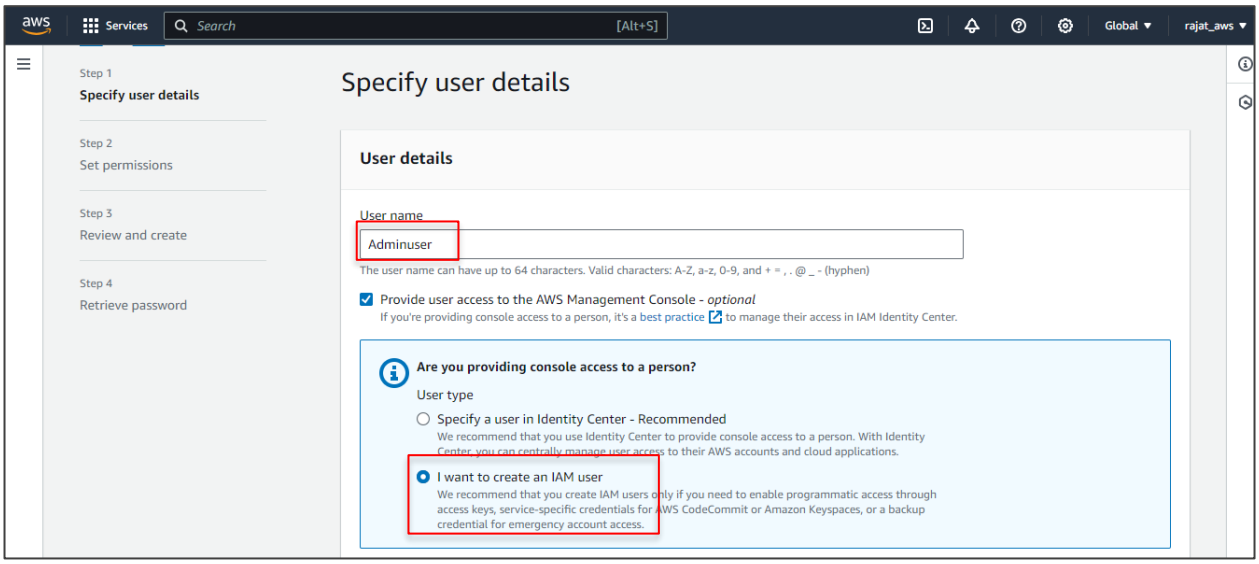
3.2 In the IAM dashboard, click on **Users**



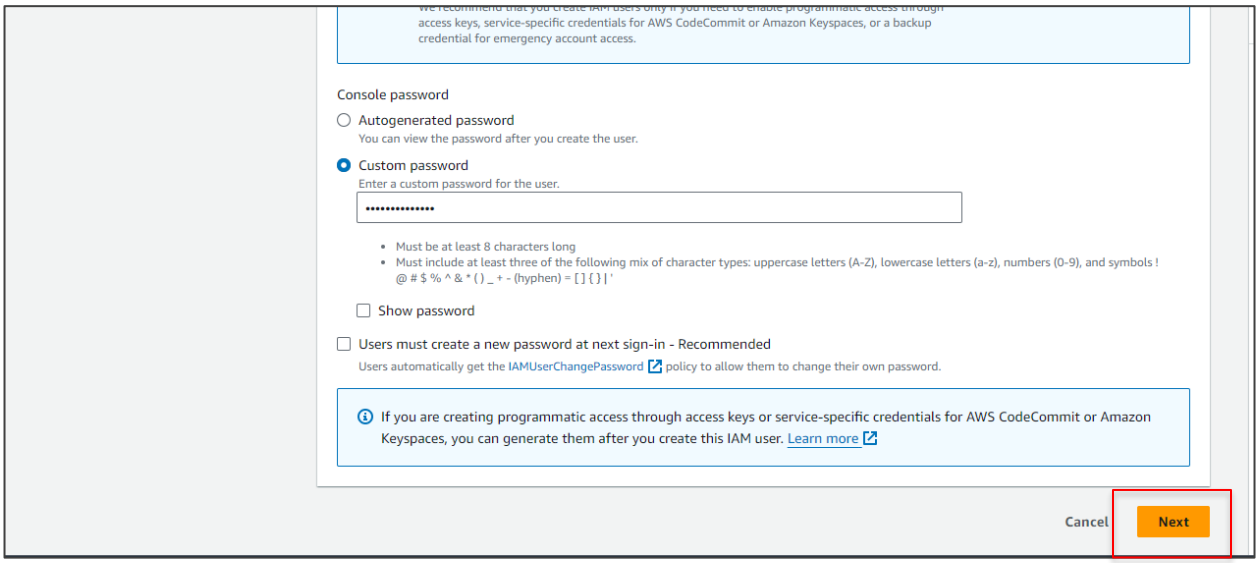
3.3 Click on **Create user**



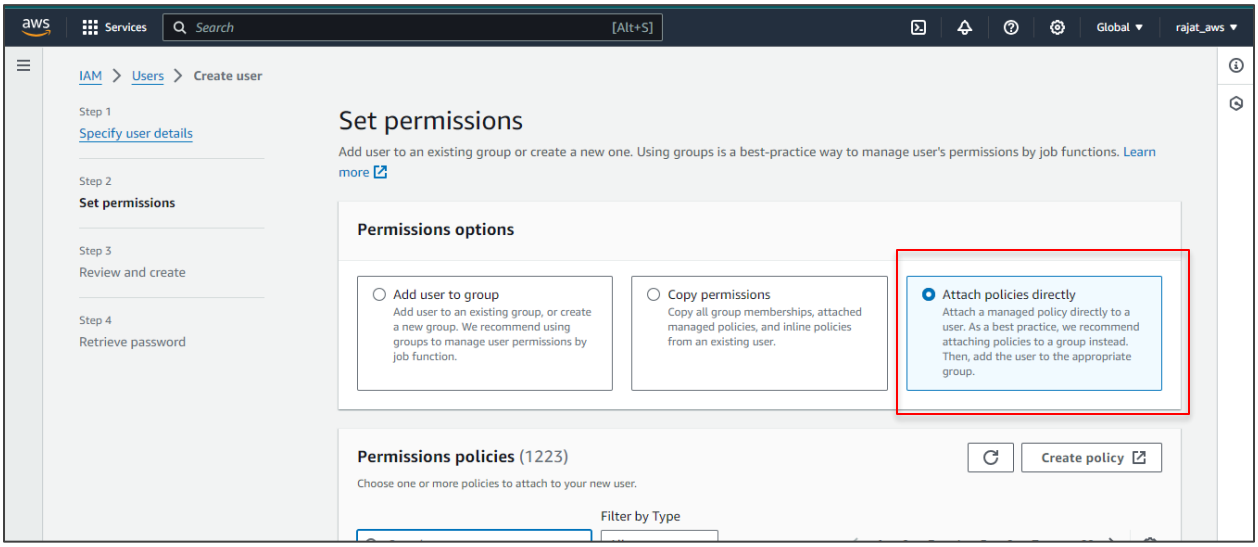
3.4 Enter the **User name**, select Provide user access to the AWS Management Console, then select **I want to create an IAM user**



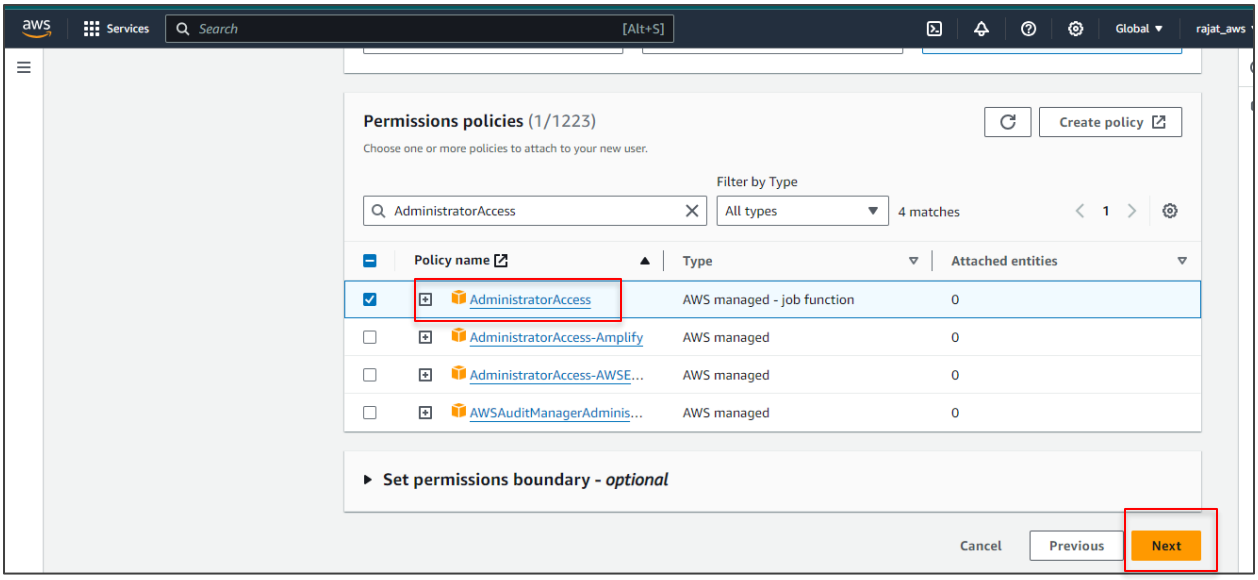
3.5 Create a strong **Custom password** and click on **Next**



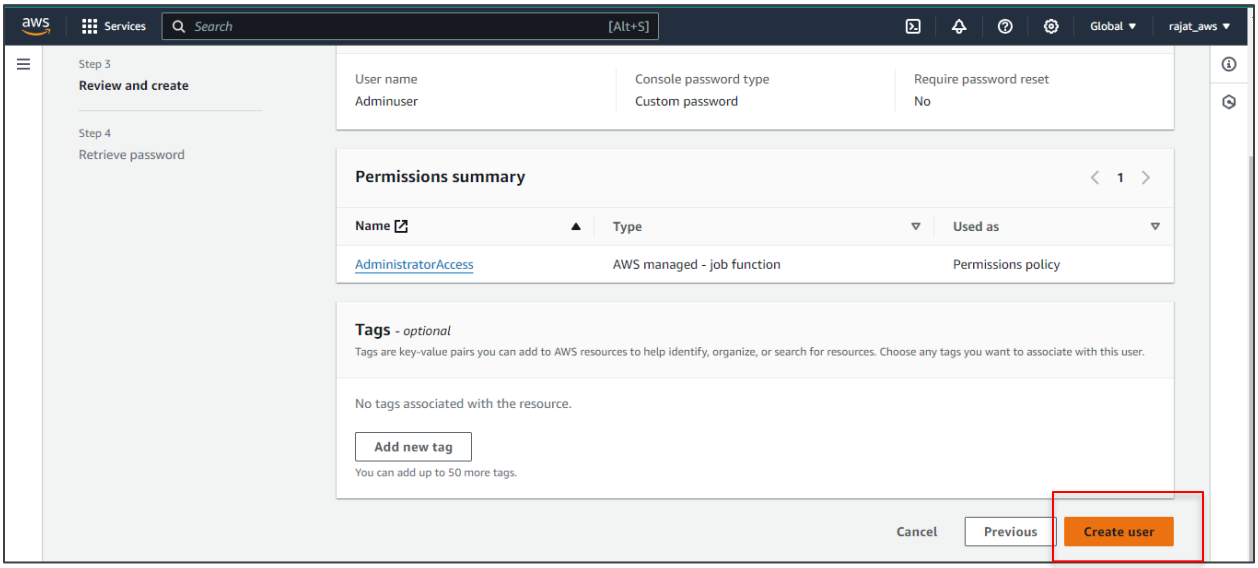
3.6 Under **Set permissions** select **Attach policies directly**



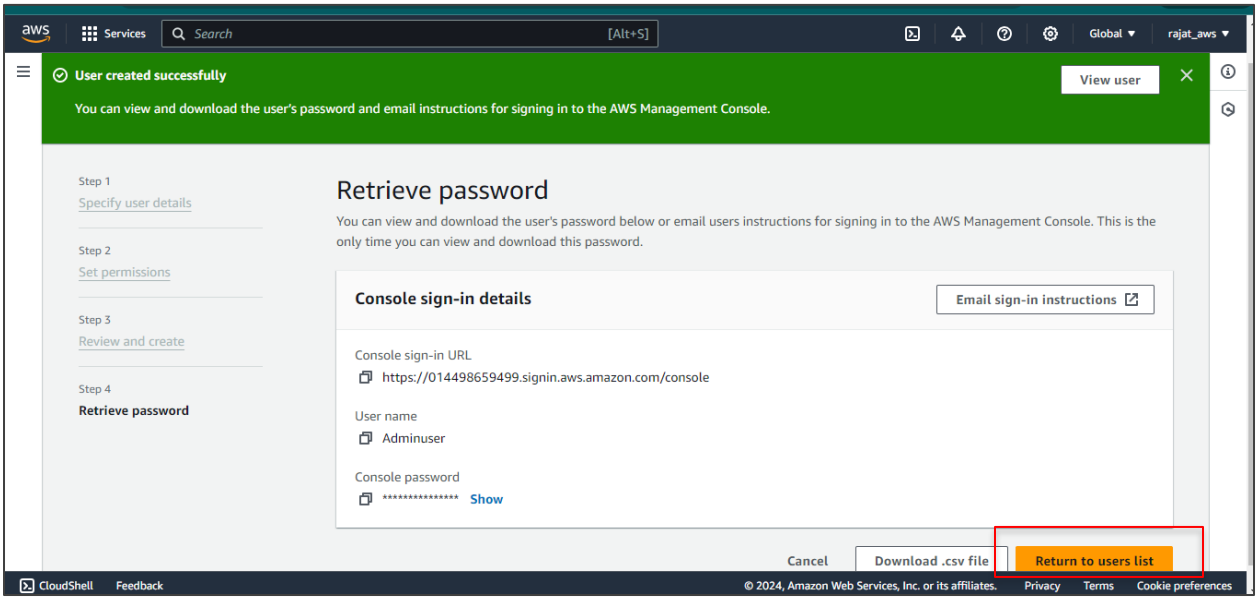
3.7 In the search bar, search for **AdministratorAccess** select it, and click on **Next**



3.8 Click on **Create user**



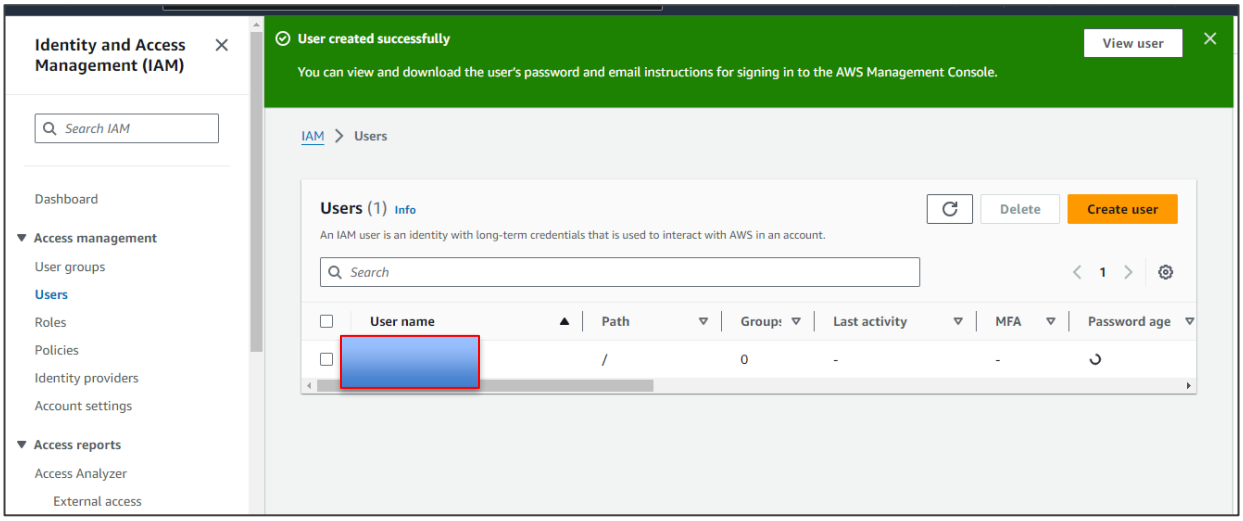
3.9 The user has been created successfully; now click on **Return to users list**



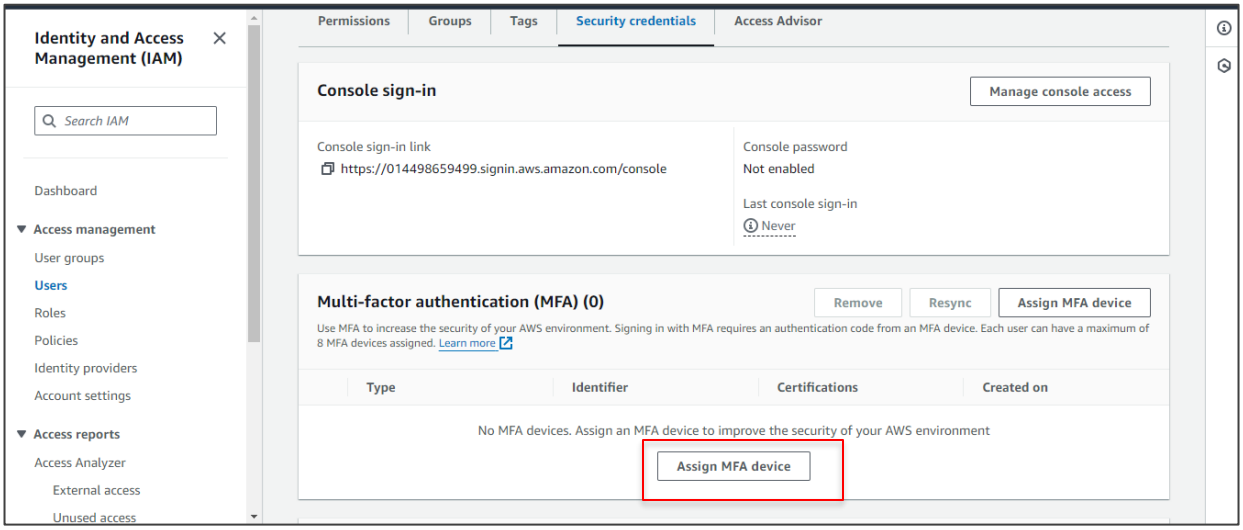
Note: Save the credentials for the future use

Step 4: Enable MFA for the IAM user and configure the virtual MFA device

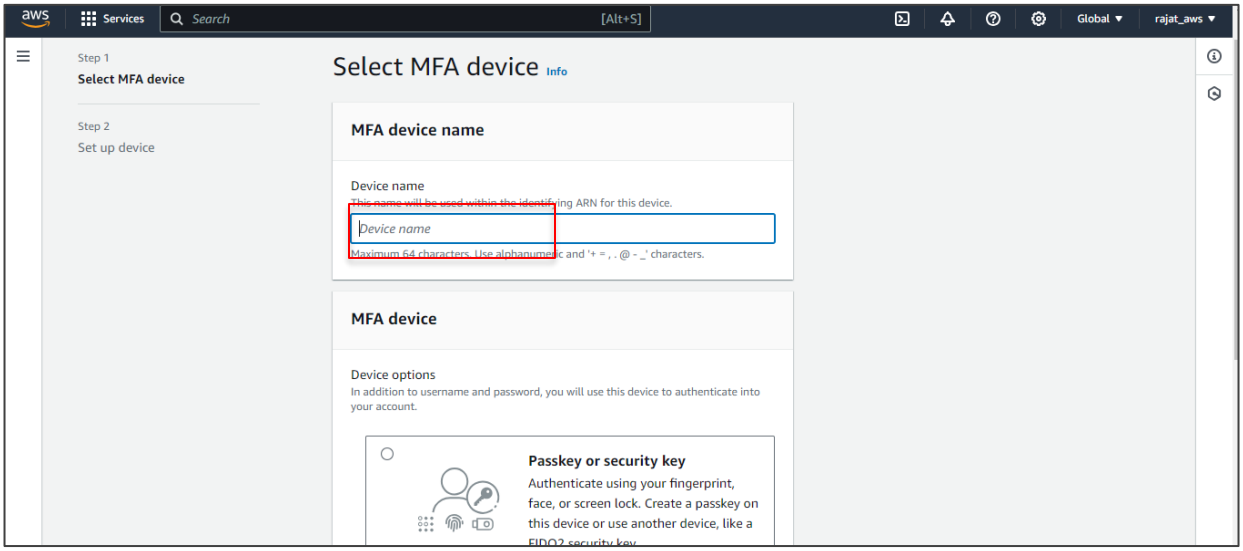
4.1 In the **IAM Dashboard**, click on the newly created user **Adminuser**

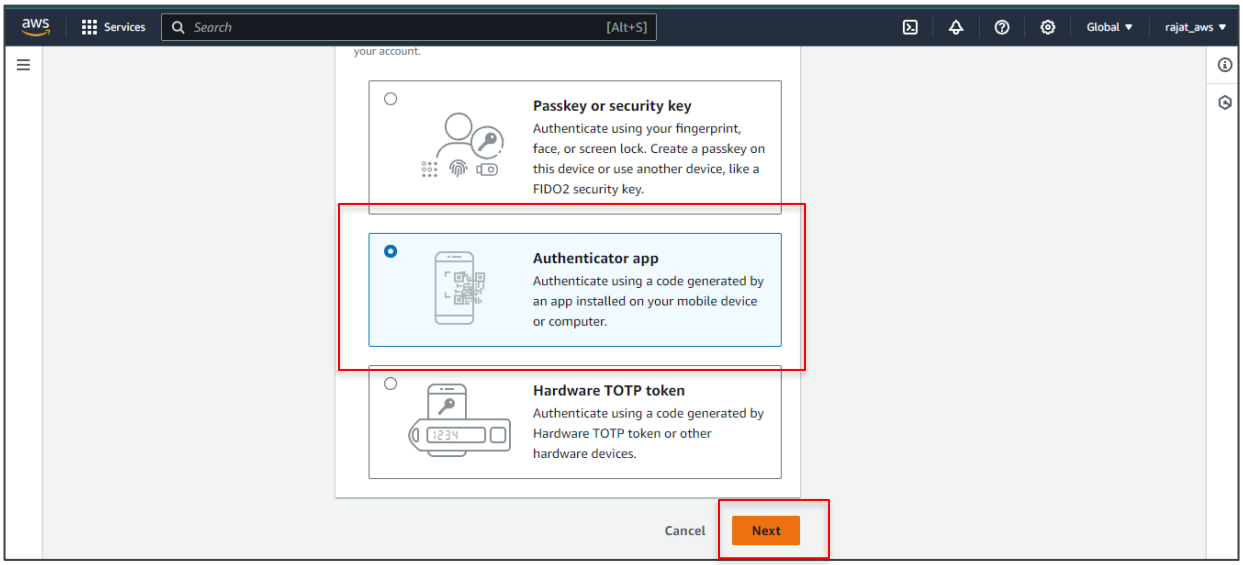


4.2 Under Security credentials scroll down to **Multi-factor authentication (MFA)** and click on **Assign MFA device**



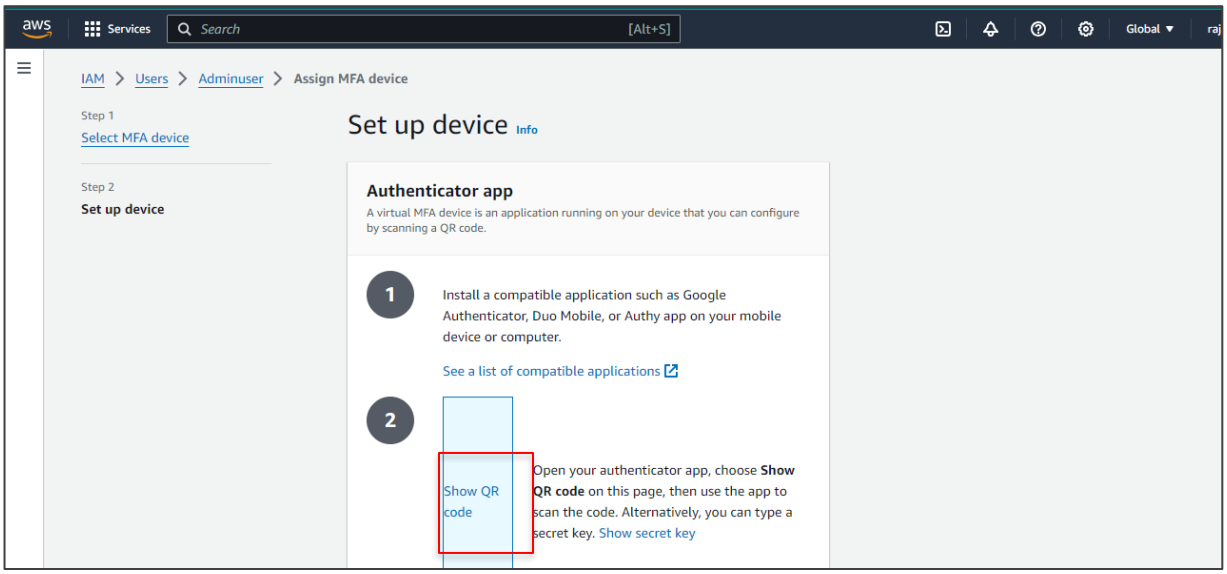
4.3 Enter the **Device name** and select **Authenticator app** as **MFA device**, then click on **Next**

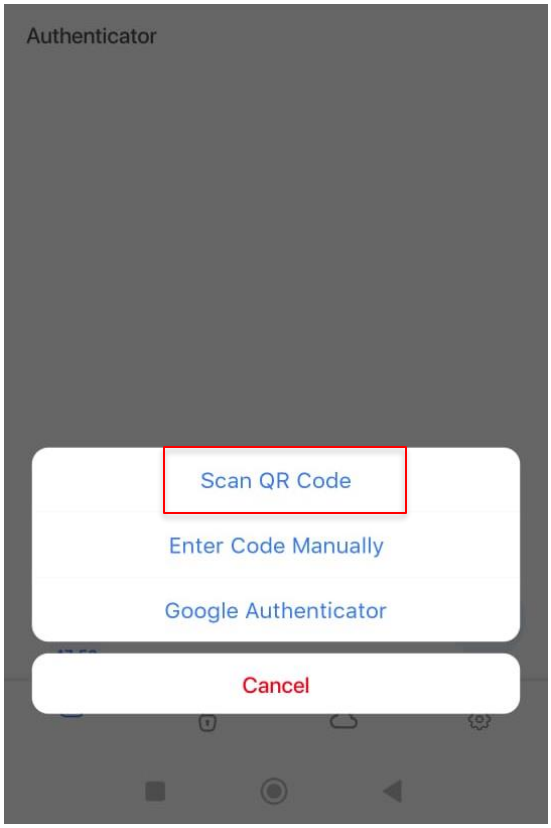


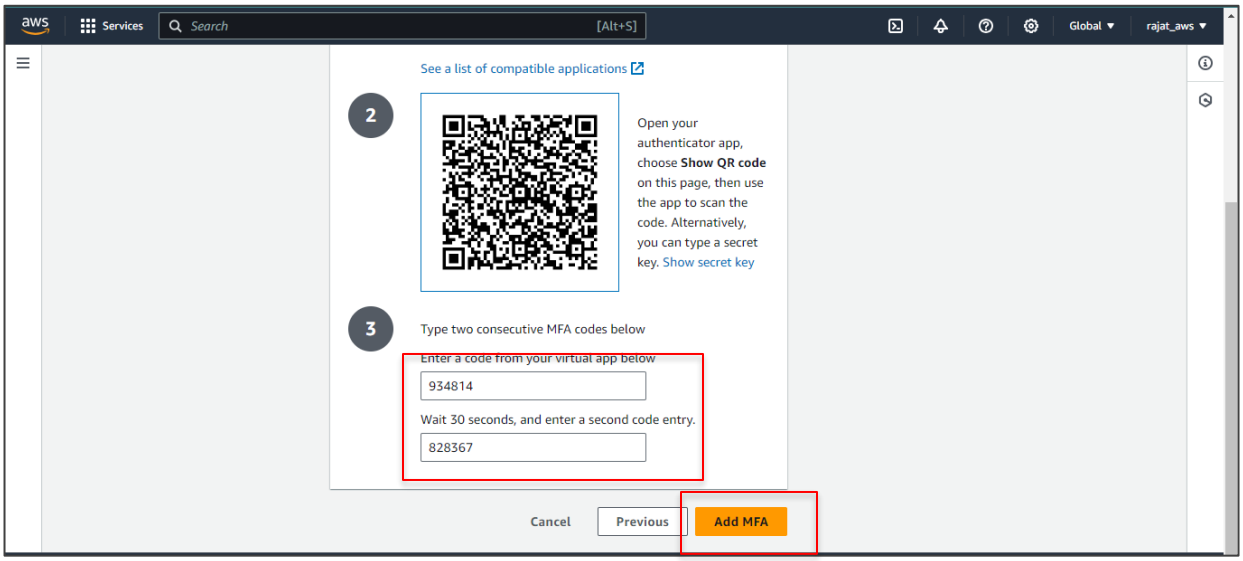


Note: Install Google Authenticator on your phone.
Android: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en_IN
IOS: https://apps.apple.com/us/app/google-authenticator/id388497605

4.4 Click on **Show QR Code** and **open the Google Authenticator app on your phone. Click on Scan QR Code,** scan the code on the phone, and enter the code from your phone into MFA code 1 and MFA code 2. Then click on the **Add MFA** button.

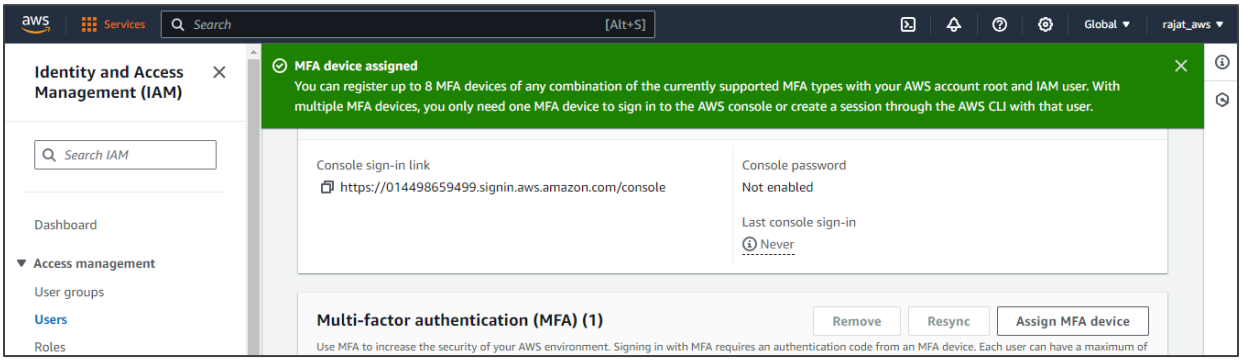




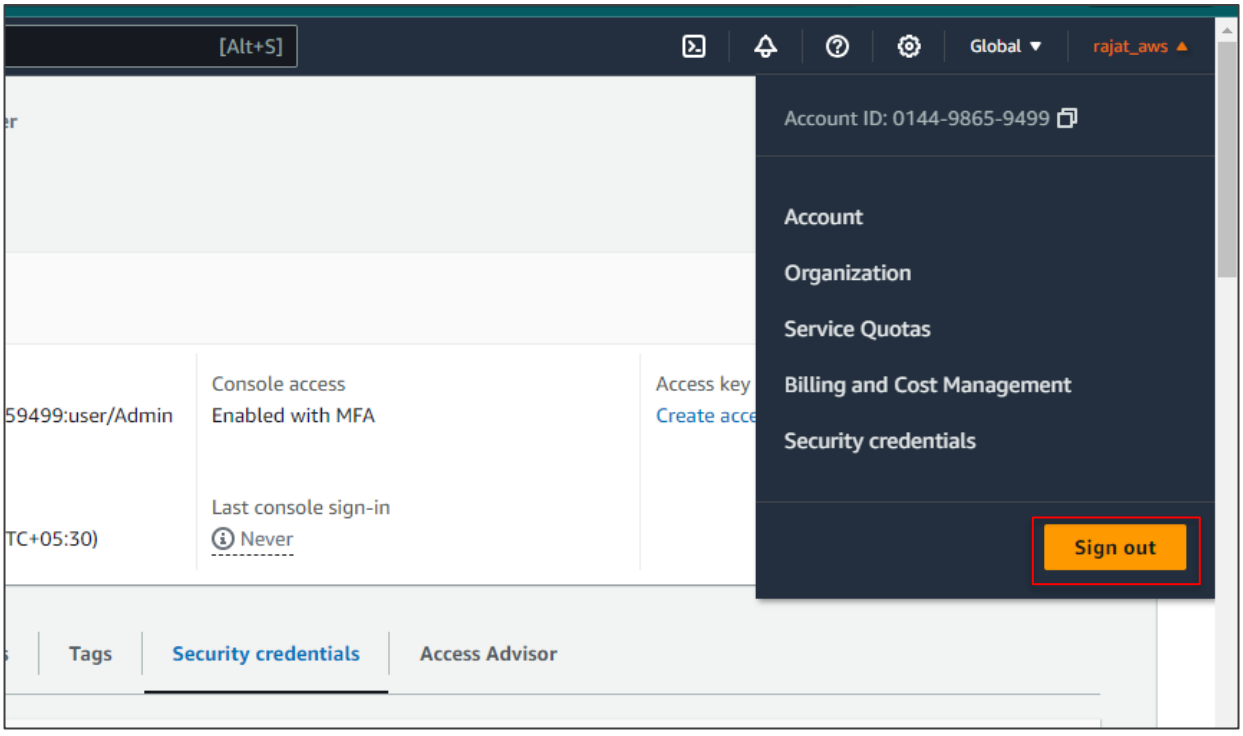


Note: Take a screenshot of the code so that if you lose your phone in the future, you can use it to re-enable MFA.

Now, you can see that the MFA device has been added successfully.



3.3 After adding the MFA, **Sign out** from the account

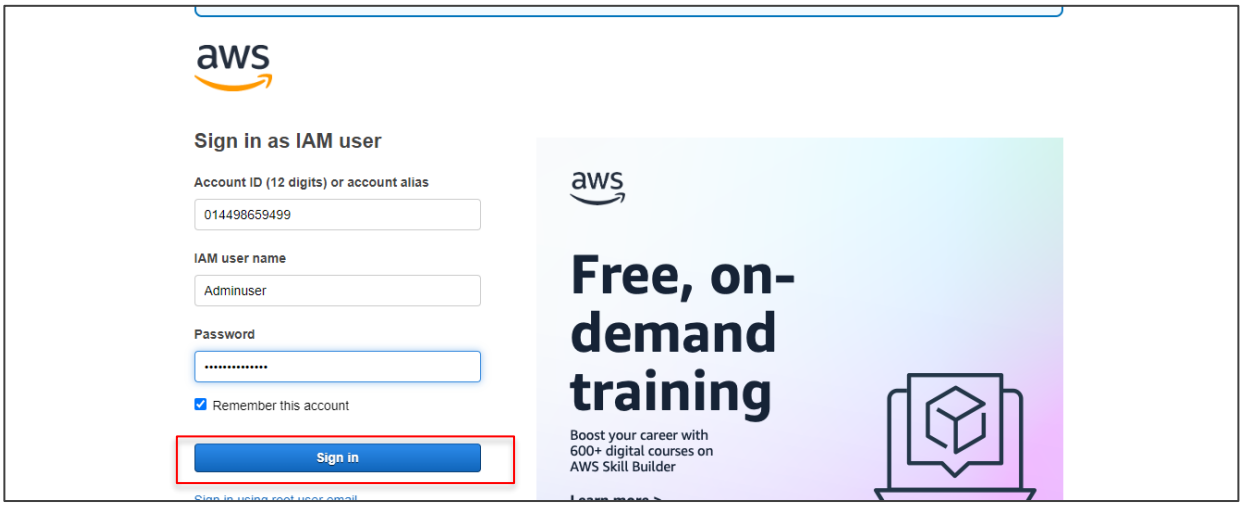


Step 5: Access AWS Console using MFA

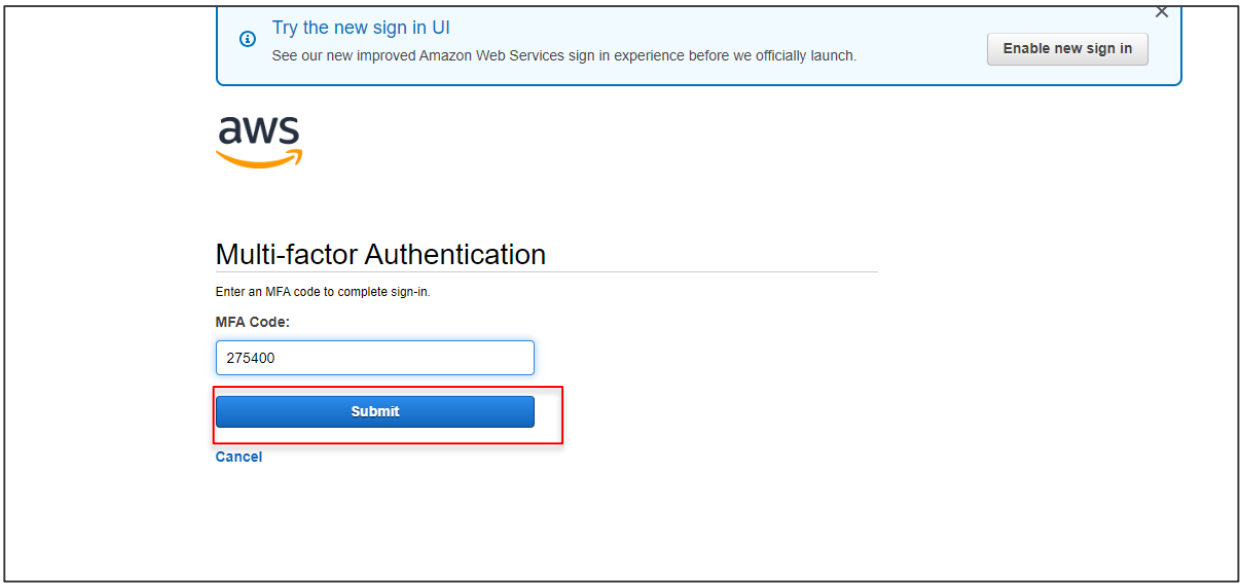
5.1 Open your AWS console login page, click **on IAM user** and enter the **Account ID**, then click on **Next**

Note: You can get the Account ID from the console sign-in link which is in the credentials you have saved before.

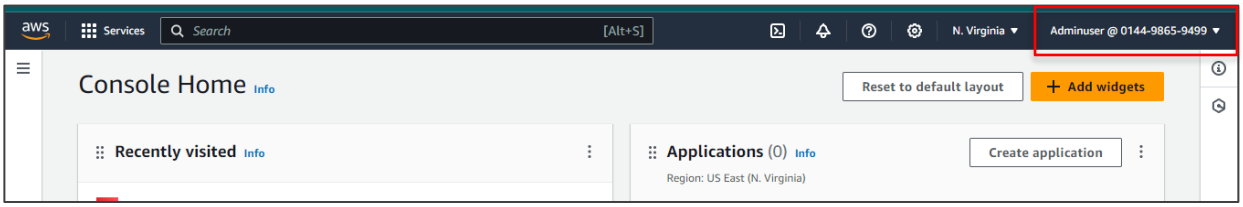
5.2 Again, enter your **Account ID, IAM user name,** and **Password,** then click on Sign in



5.3 Enter the **MFA Code**, then click on **Submit**



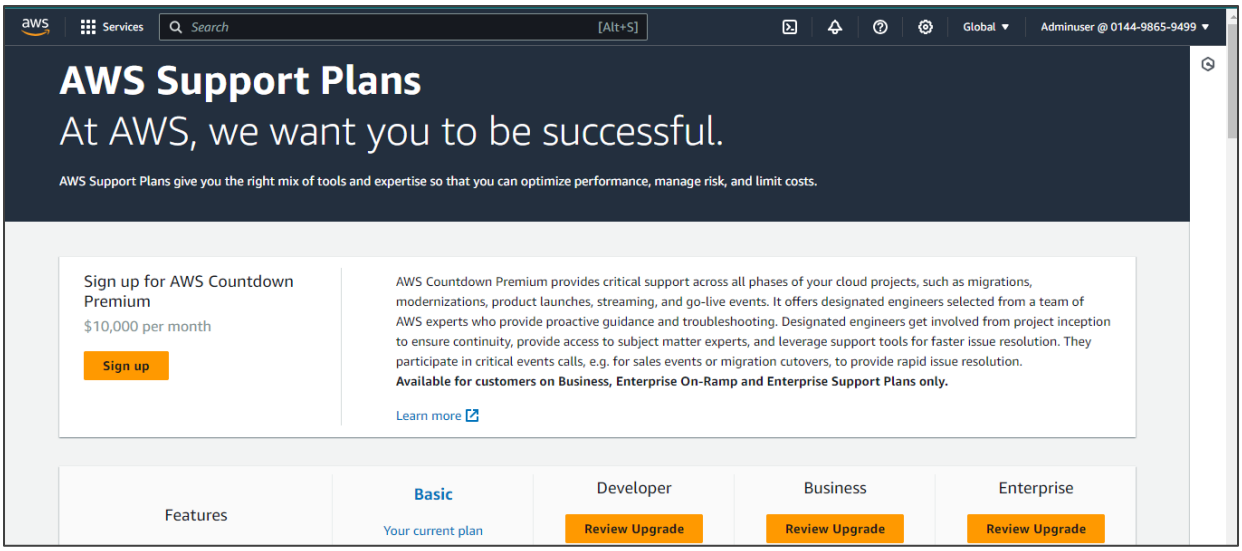
Note: To get your MFA code, open your authenticator app (Google Authenticator) and find the 6-digit code for your AWS account. Enter this code when prompted during AWS login.



You can see you have been logged in as an IAM user.

Step 6: Verify your account plan

6.1 To verify your account plan, navigate to the below link:
https://us-east-1.console.aws.amazon.com/support/plans/home?region=us-east-1#/



Note: AWS Support offers four support plans: Basic, Developer, Business, and Enterprise. By default, we have a basic plan; if you want to change your plan, you can change it accordingly.

By following the above steps, you can successfully create a free tier account on AWS with MFA enabled for an extra layer of security.