

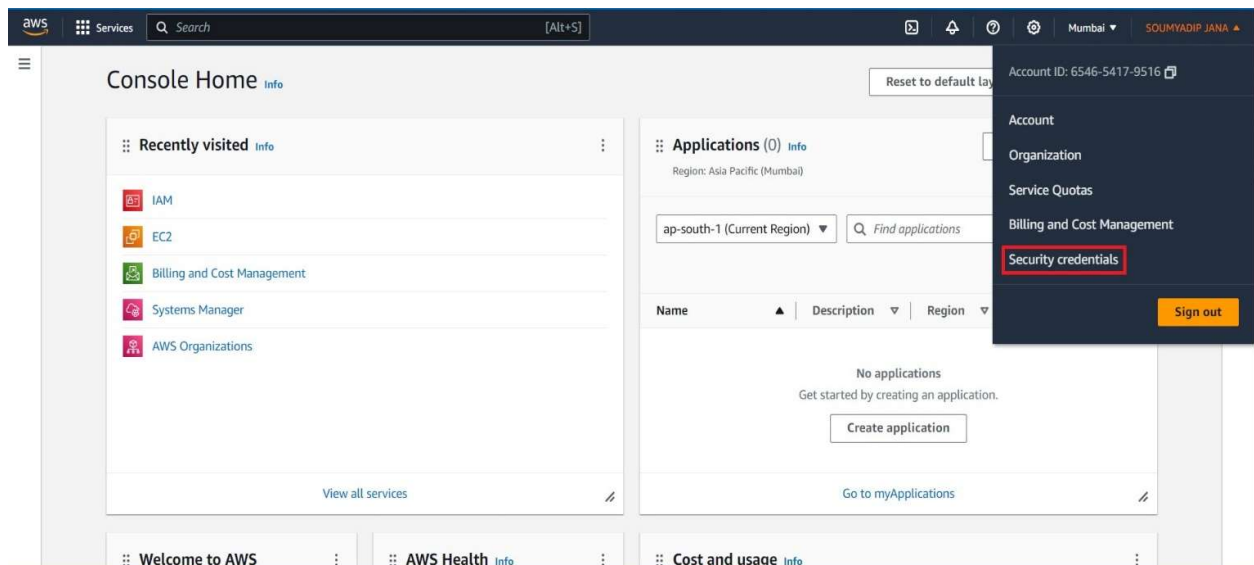
# Assignment 2

**Problem Statement:** Create MFA for your AWS Account

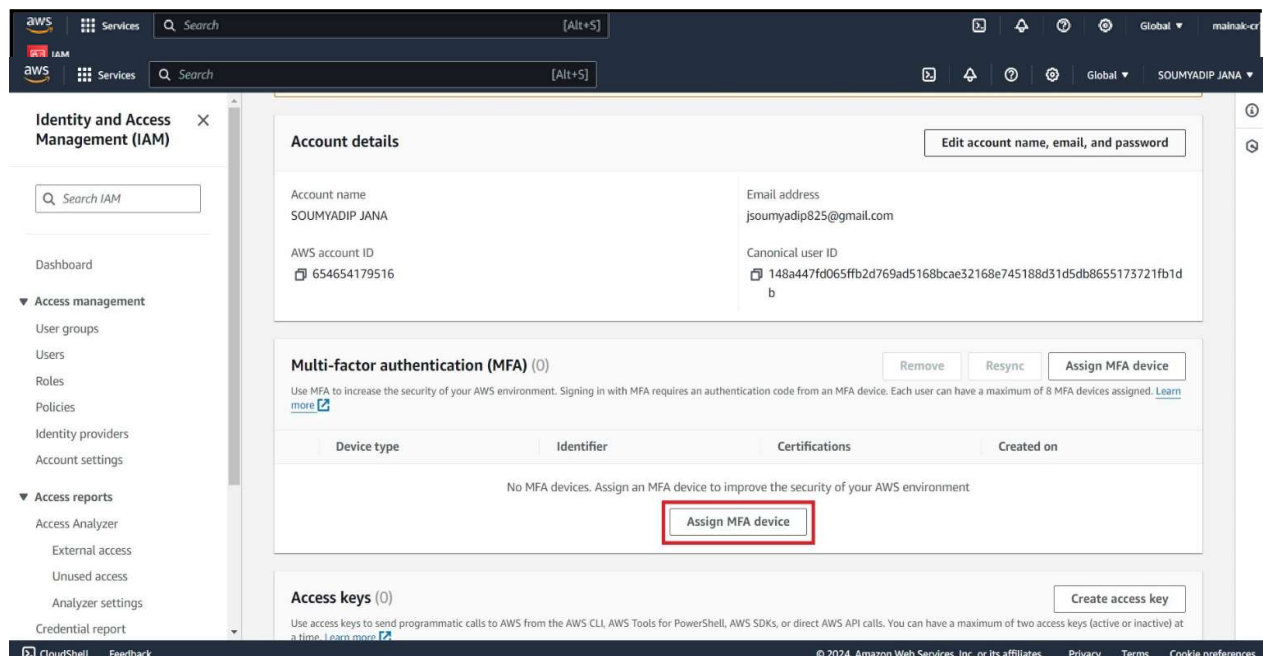
**Solution:**

**MFA:** Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong **identity and access management (IAM)** policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber attack.

**Step 1:** At first open your **AWS Console** and click on your account, then select **Security credentials**



**Step 2:** Scroll down and you can find the **MFA** section. Click on **Assign MFA device** to add an MFA device



### Step 3: Enter the MFA device name, type of MFA device and click on Next

The screenshot shows the AWS IAM console interface for setting up an MFA device. The breadcrumb trail is IAM > Security credentials > Assign MFA device. The left sidebar shows 'Step 1: Select MFA device' and 'Step 2: Set up device'. The main content area is titled 'Select MFA device' with an 'info' icon. It contains a form with two sections. The first section, 'MFA device name', has a text input field with the value 'Soymya\_aws' and a red border. Below it, the 'MFA device' section has three radio button options: 'Authenticator app' (selected), 'Security Key', and 'Hardware TOTP token'. At the bottom right, there are 'Cancel' and 'Next' buttons, with the 'Next' button highlighted by a red box.

**Step 4: Download an MFA device** for example **Google Authenticator** on your **Android device** and scan the **QR code** (for security purposes it is fake on the image). You can find the **MFA codes generated in the app**, enter **two consecutive MFA codes**, and click on **Add MFA** to complete your MFA setup. You should find a dialog box showing that you have successfully completed the MFA setup

The screenshot shows the AWS IAM console interface for setting up an authenticator app. The breadcrumb trail is IAM > Security credentials > Assign MFA device. The left sidebar shows 'Step 1: Select MFA device' and 'Step 2: Set up device'. The main content area is titled 'Set up device' with an 'info' icon. It contains a form with three numbered steps. Step 1 is 'Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer: See a list of compatible applications'. Step 2 is 'Open your authenticator app, choose Show QR code on this page, then use the app to scan the code. Alternatively, you can type a secret key. Show secret key'. Step 3 is 'Fill in two consecutive codes from your MFA device:'. Below step 3, there are two input fields for 'MFA code 1' and 'MFA code 2'. At the bottom right, there are 'Cancel', 'Previous', and 'Add MFA' buttons, with the 'Add MFA' button highlighted by a red box.

## Step 5: Finally MFA is assign for your AWS account.

The screenshot displays the AWS IAM console interface. A green banner at the top states "MFA device assigned" with a note: "You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user." Below this, the "My security credentials" page is shown for the user "SOURMYADIP JANA". The "Account details" section includes fields for Account name, Email address, AWS account ID, and Canonical user ID. The "Multi-factor authentication (MFA)" section is highlighted with a red box and shows a table with one entry: a Virtual device with identifier "arn:aws:iam::654654179516:mfa/Sourmya\_aws". The "Access keys" section is empty, with a "Create access key" button and a note about avoiding long-term credentials.

**MFA device assigned**  
You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.

**My security credentials**  
The root user has access to all AWS resources in this account, and we recommend following best practices. To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

**Account details** [Edit account name, email, and password](#)

Account name	SOURMYADIP JANA	Email address	sourmyadip025@gmail.com
AWS account ID	654654179516	Canonical user ID	148a447f0065fb2d769ads168bcae32168e745188d51d5db8855173721fb1db

**Multi-factor authentication (MFA)** (1) [Remove](#) [Resync](#) [Assign MFA device](#)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Device type	Identifier	Certifications	Created on
<input type="radio"/> Virtual	arn:aws:iam::654654179516:mfa/Sourmya_aws	Not Applicable	Now

**Access keys** (0) [Create access key](#)

Access key ID	Created on	Access key last used	Region last used	Service last used	Status
No access keys					

As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. [Learn more](#)

[Create access key](#)

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)