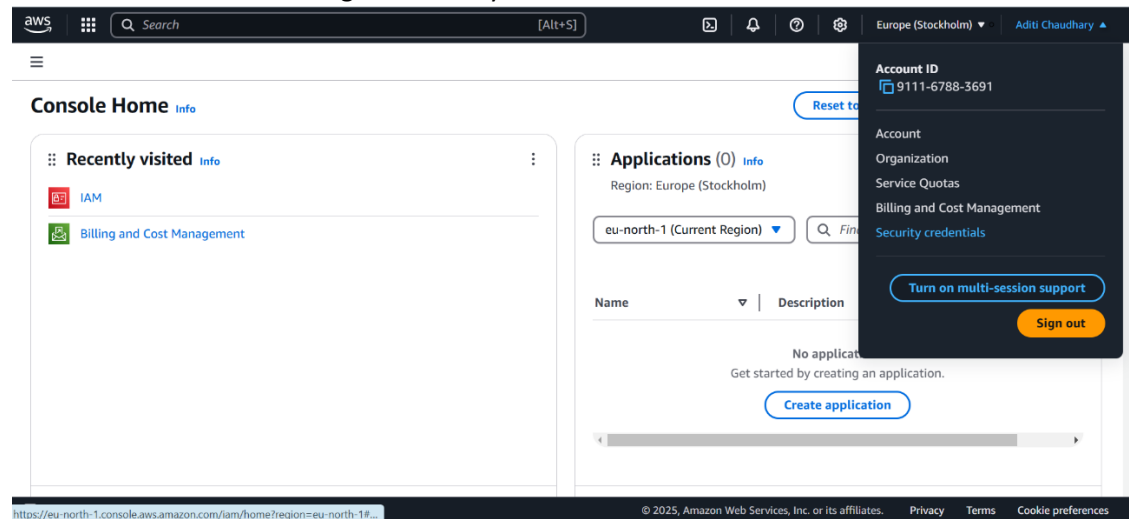


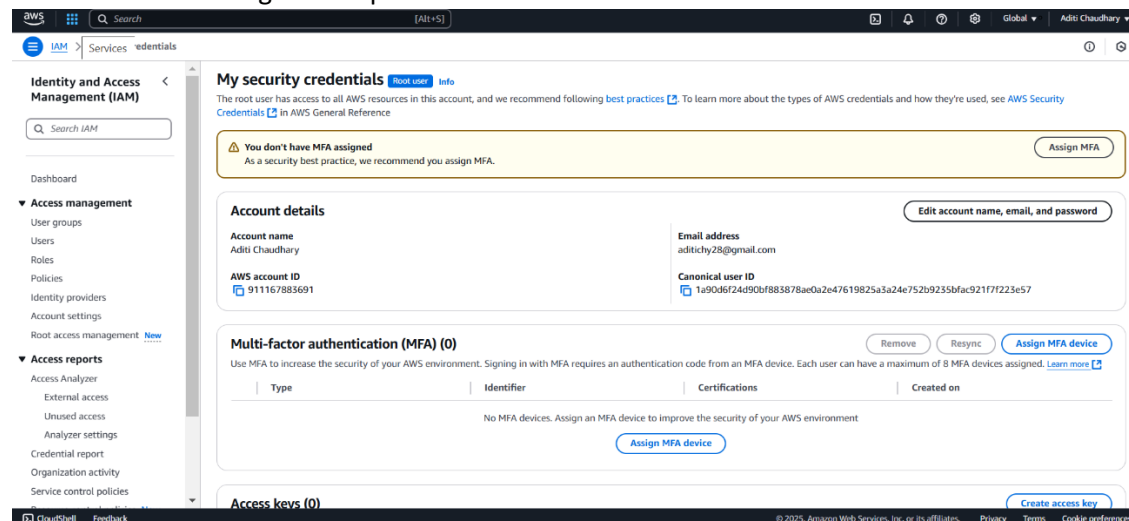
Assignment No.: 02

Problem Statement: Create MFA for Authentication.

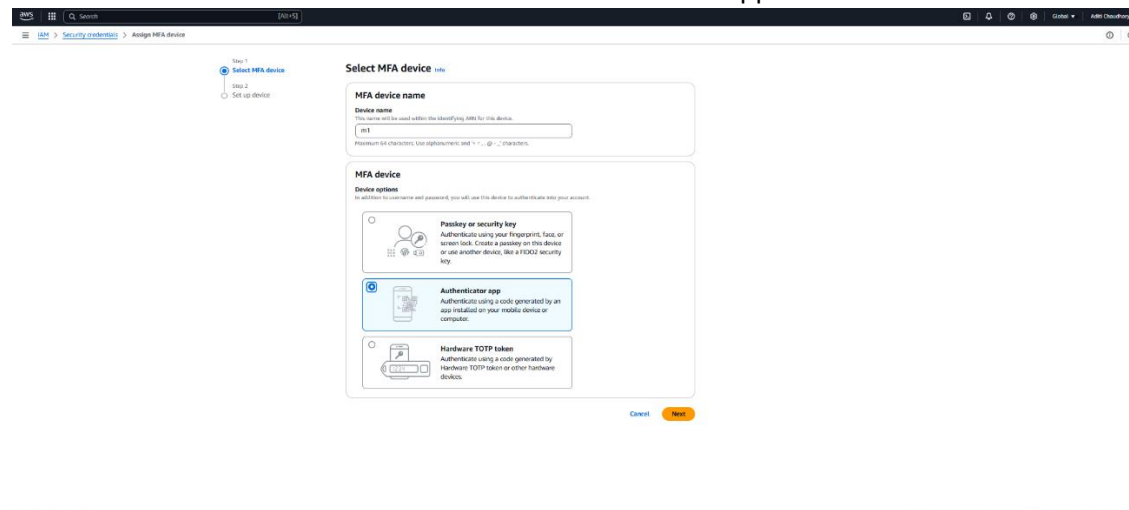
Solution Process: 1. At first go to security credentials.



2. Then click the Assign MFA option.



3. Give the MFA device name and choose the Authenticator app.




4. Download the Authenticator app on our mobile.
5. Then scan the QR and Enter the MFA1 code from the Authenticator app.
6. Wait 30 seconds and Enter the MFA2 code from the Authenticator app.

The screenshot shows the 'Set up device' page in the AWS IAM console. It includes a progress bar with 'Step 1: Select MFA device' and 'Step 2: Set up device'. The main content area is titled 'Authenticator app' and provides instructions for setting up a virtual MFA device. It includes a QR code for scanning and two input fields for entering MFA codes. The first code entered is '262804' and the second is '338422'. At the bottom, there are 'Cancel', 'Previous', and 'Add MFA' buttons.

Step 1: Select MFA device
Step 2: Set up device

Set up device [info](#)

Authenticator app
A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1. 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](#)
2. 
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](#)
3. Type two consecutive MFA codes below
Enter a code from your virtual app below

Wait 30 seconds, and enter a second code entry.

[Cancel](#) [Previous](#) [Add MFA](#)

7. At last click on the Add MFA option
8. Finally the MFA device is assigned.

The screenshot shows the AWS IAM console after the MFA device has been assigned. A green notification banner at the top states 'MFA device assigned' and provides information about registering multiple MFA devices. Below this, the 'Account details' section shows the account name 'Aditi Chaudhary', email address 'adichy28@gmail.com', and AWS account ID '911167883691'. The 'Multi-factor authentication (MFA)' section shows a table with one entry: 'Virtual' type, identifier 'amaws:iam:911167883691:mfa/m1', and created on 'Sat Jan 25 2025'. The 'Access keys' section shows 'No access keys' and a 'Create access key' button.

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.

Account details

Account name: Aditi Chaudhary
Email address: adichy28@gmail.com
AWS account ID: 911167883691
Canonical user ID: 1a90c6f24d90bf883878ae0a2e47619825a3a24e752b9235bfa921f7f223e57

Multi-factor authentication (MFA) (1)

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](#)

Type	Identifier	Certifications	Created on
<input type="radio"/> Virtual	amaws:iam:911167883691:mfa/m1	Not Applicable	Sat Jan 25 2025

Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

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](#)