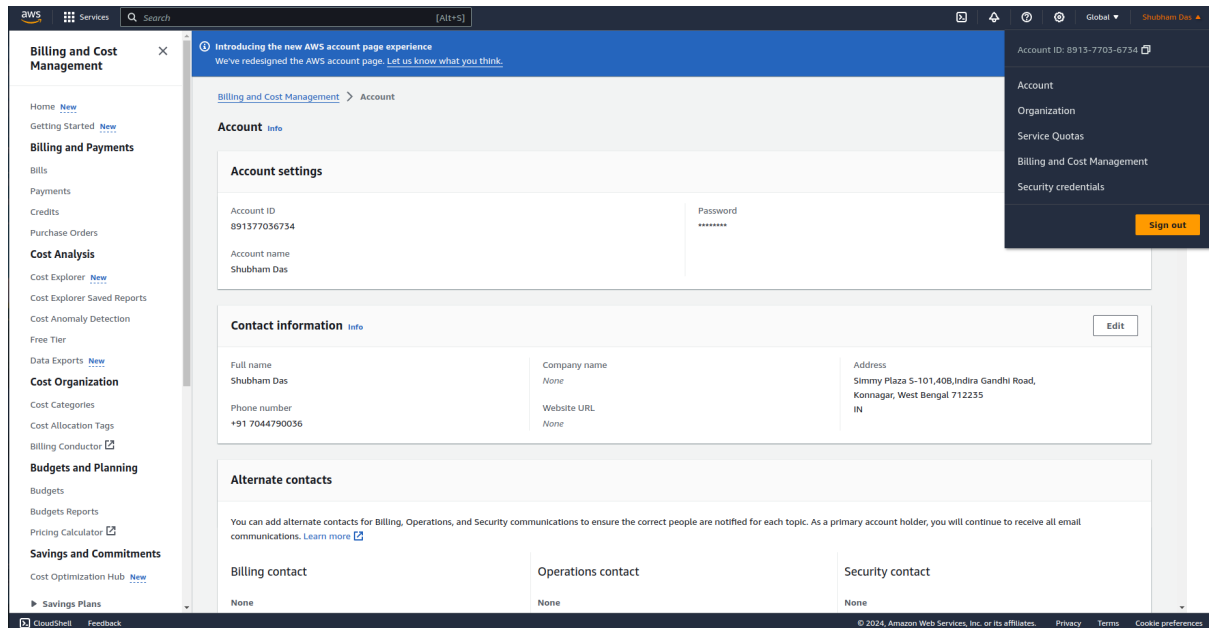


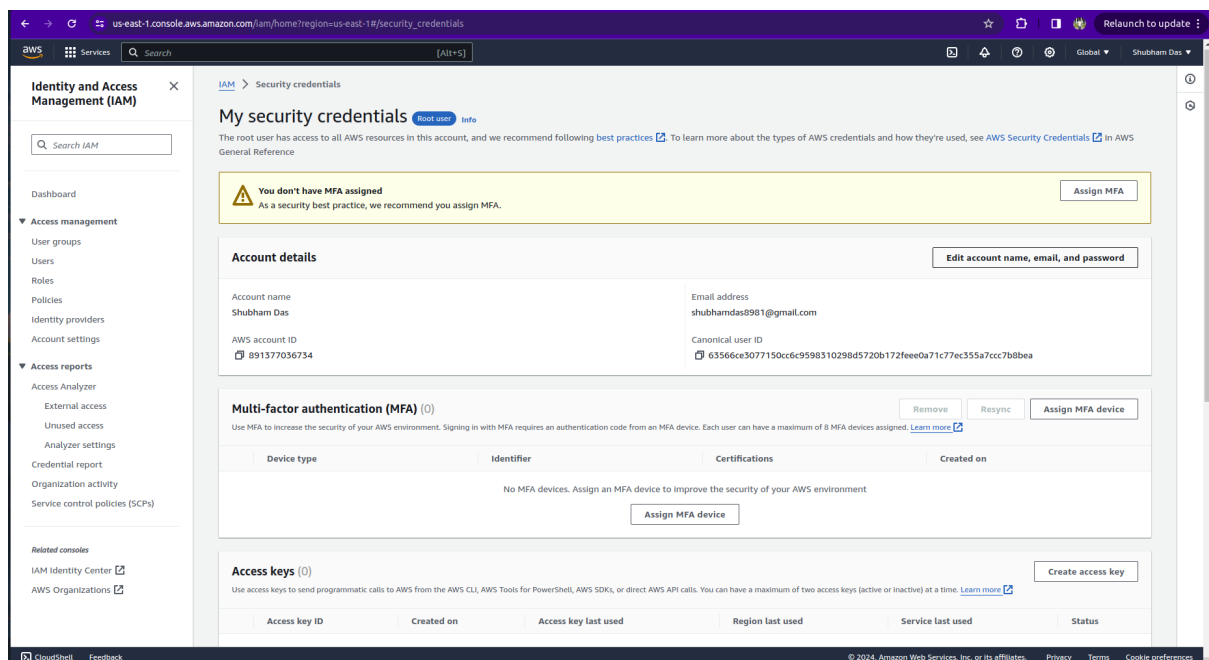
# Assignment 2

## Problem Statement: Create MFA for authentication

### Step 1.1: Go to your Profile > Security credentials



### Step 1.2: Click on Assign MFA Device



## Step 1.3: Add the MFA Device name

The screenshot shows the AWS IAM console interface. The breadcrumb navigation is IAM > Security credentials > Assign MFA device. The left sidebar shows 'Step 1: Select MFA device' as the active step, with 'Step 2: Set up device' below it. The main content area is titled 'Select MFA device' with an 'Info' link. It contains two sections: 'MFA device name' and 'MFA device'. The 'MFA device name' section has a text input field labeled 'Device name' with a placeholder 'Enter a meaningful name to identify this device.' and a note 'Maximum 128 characters. Use alphanumeric and '+', '.', '@', '-', '\_' characters.' The 'MFA device' section is titled 'Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.' and lists three options: 'Authenticator app' (selected with a radio button), 'Security Key', and 'Hardware TOTP token'. Each option has a small icon and a brief description.

## Step 1.4: Scan the QR code with your other device Authenticator app and input two MFA codes as required

The screenshot shows the AWS IAM console interface for the 'Set up device' step. The breadcrumb navigation is IAM > Security credentials > Assign MFA device. The left sidebar shows 'Step 1: Select MFA device' and 'Step 2: Set up device' as the active step. The main content area is titled 'Set up device' with an 'Info' link. It contains a section for 'Authenticator app' with the subtitle 'A virtual MFA device is an application running on your device that you can configure by scanning a QR code.' The setup process is shown in three numbered steps: 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' with a link. 2. 'Show QR code' with a large blue box containing a QR code and instructions to open the authenticator app and scan the code. 3. 'Fill in two consecutive codes from your MFA device.' with two input fields labeled 'MFA code 1' and 'MFA code 2'. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Add MFA'.

## Step 1.5: Your MFA has been set up.

aws

Services

Search

[Alt+S]

Global

Shubham Das

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access Analyzer
  - External access
  - Unused access
  - Analyzer settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Related consoles

- [IAM Identity Center](#)
- [AWS Organizations](#)

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

Root user

Info

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

Shubham Das

Email address

shubhamdas8981@gmail.com

AWS account ID

891377036734

Canonical user ID

63566ce3077150cc6c9598310298d5720b172fee0a71c77ec355a7ccc7b8bea

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::891377036734:mfa/device1 | Not Applicable | Now        |

Access keys (0)

Create access key

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](#)

CloudShell

Feedback

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