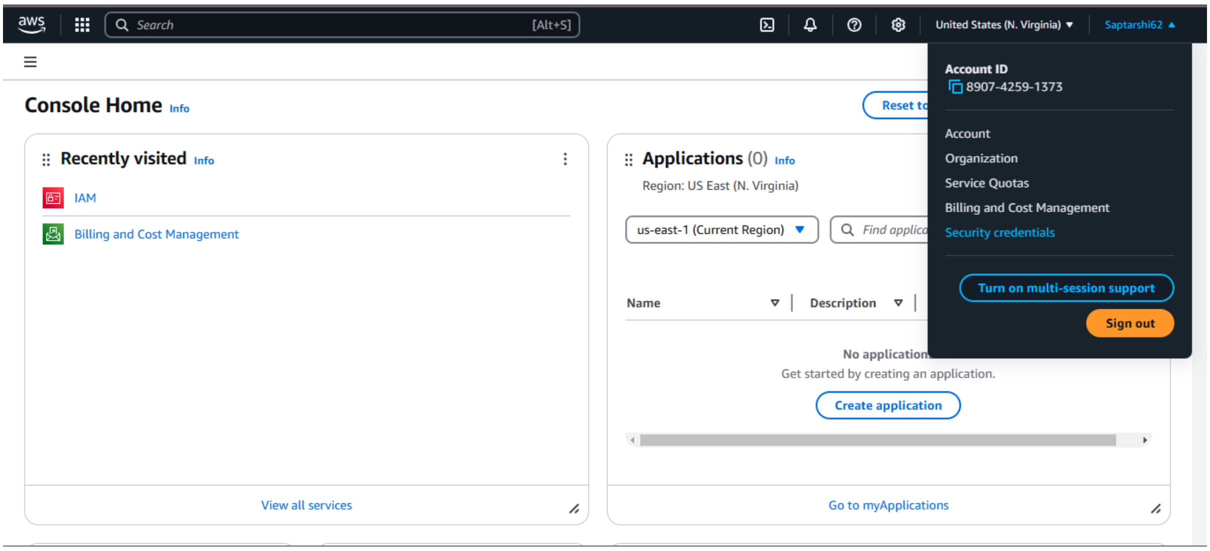
# Assignment No.: 02

## Problem Statement: Create MFA for Authentication.

## Solution Process:

1. At first go to security credentials.



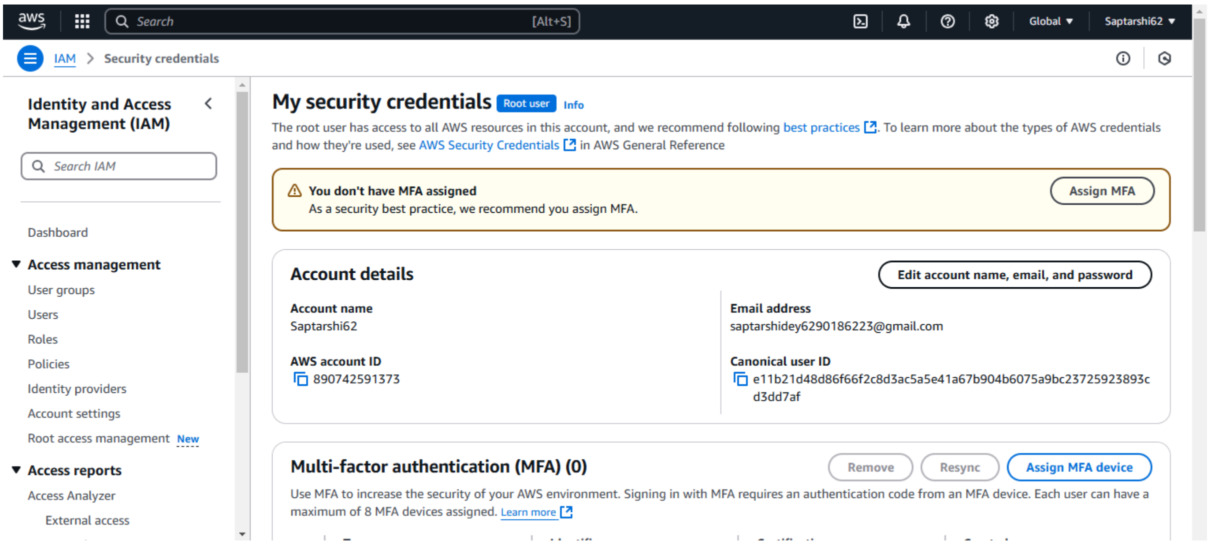
Account ID
8907-4259-1373

Region: US East (N. Virginia)

No application

Get started by creating an application.

2. Then click the Assign MFA option.



**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

**You don't have MFA assigned**

As a security best practice, we recommend you assign MFA.

**Account details**

Account name
Saptarshi62

Email address
saptarshidey6290186223@gmail.com

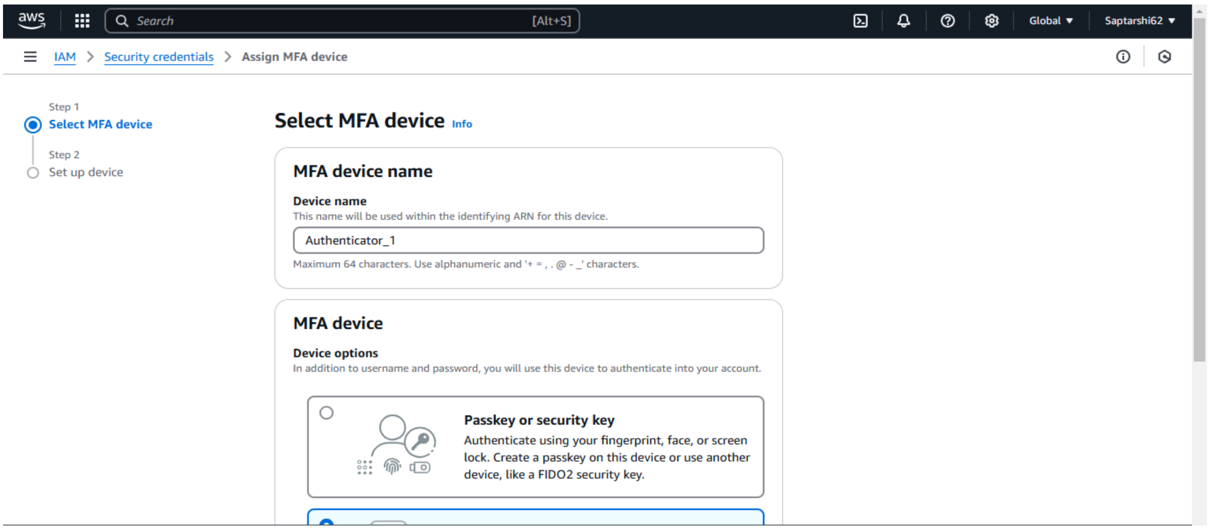
AWS account ID
890742591373

Canonical user ID
e11b21d48d86f66f2c8d3ac5a5e41a67b904b6075a9bc23725923893c d3dd7af

**Multi-factor authentication (MFA) (0)**

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

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



Step 1
Select MFA device

Step 2
Set up device

### Select MFA device Info

**MFA device name**

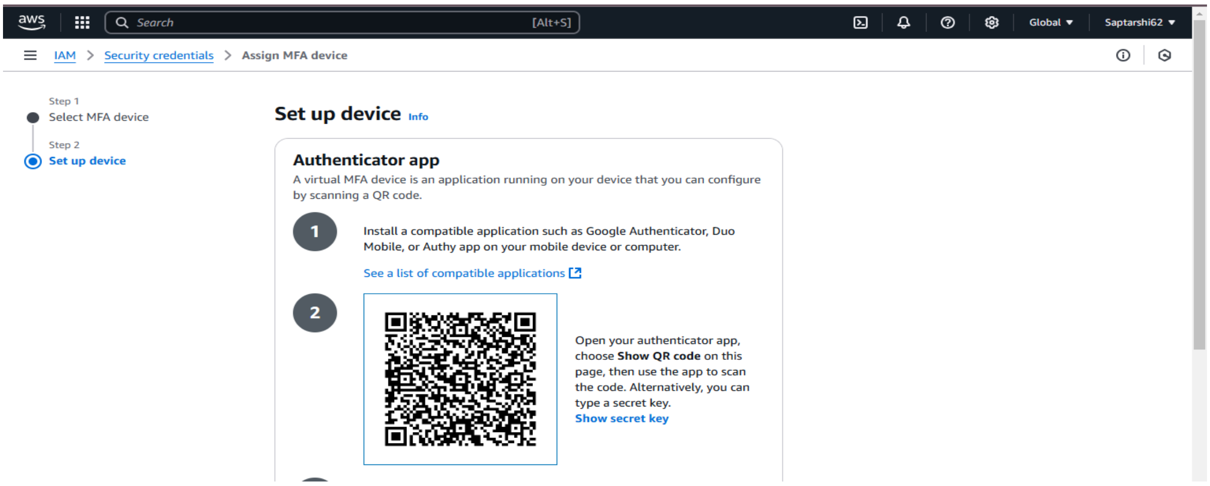
**Device name**
This name will be used within the identifying ARN for this device.
Authenticator_1
Maximum 64 characters. Use alphanumeric and '+ = , . @ - _' characters.

**MFA device**

**Device options**
In addition to username and password, you will use this device to authenticate into your account.

○ **Passkey or security key**
Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.

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.



Step 1
Select MFA device

Step 2
Set up device

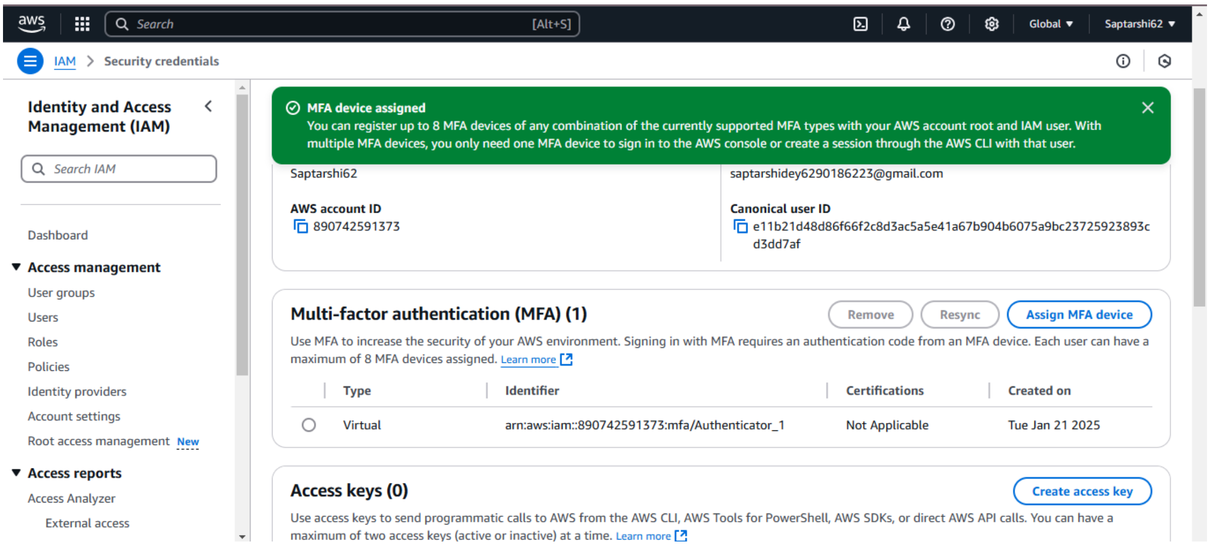
### Set up device Info

**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**

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



**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.

Saptarshi62 saptarshidey6290186223@gmail.com

**AWS account ID**
890742591373

**Canonical user ID**
e11b21d48d86f66f2c8d3ac5a5e41a67b904b6075a9bc23725923893cd3dd7af

**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

| | Type | Identifier | Certifications | Created on |
|---|---|---|---|---|
| ○ | Virtual | arn:aws:iam::890742591373:mfa/Authenticator_1 | Not Applicable | Tue Jan 21 2025 |

**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