

## Assignment No: 2

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.

The screenshot shows a web application interface for setting up Multi-Factor Authentication (MFA). The breadcrumb navigation at the top reads: IAM > Security credentials > Assign MFA device. On the left, a progress indicator shows two steps: 'Step 1: Select MFA device' (which is active) and 'Step 2: Set up device'. 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 containing 'TamoghnaB' and a note: 'This name will be used within the identifying AIN for this device. Maximum 64 characters. Use alphanumeric and '+', '-', '@', '.', '\_' characters.' The 'MFA device' section, titled 'Device options', lists three choices: 'Passkey or security key' (with a radio button), 'Authenticator app' (selected with a blue radio button), and 'Hardware TOTP token' (with a radio button). Each option includes a brief description of how it works. At the bottom right, there are 'Cancel' and 'Next' buttons.

4. Download the Authenticator app on our mobile.
5. Then scan the QR and Enter the MFA1 code from the authenticator app.
6. And wait for 30 sec then fill the MFA2 code from the authenticator app.
7. At last click on the Add MFA option.



## 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

885723

Wait 30 seconds, and enter a second code entry.

478164

[Cancel](#)

[Previous](#)

[Add MFA](#)

## 8. Finally the MFA device is Assigned.

### My security credentials [Reset 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

Account name  
Tamoghna Basu

AWS account ID  
 664418979640

Email address  
basu.tamoghna12@gmail.com

Canonical user ID  
 1726294fe3daf0d2a7d1313d7ce3cea305dbf7aac7f612063dedd8ee688cb0b0

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

#### 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](#)

[Remove](#)

[Resync](#)

[Assign MFA device](#)

Type	Identifier	Certifications	Created on
<input type="radio"/> Virtual	arn:aws:iam:664418979640:mfa/TamoghnaB	Not Applicable	Sun Jan 26 2025