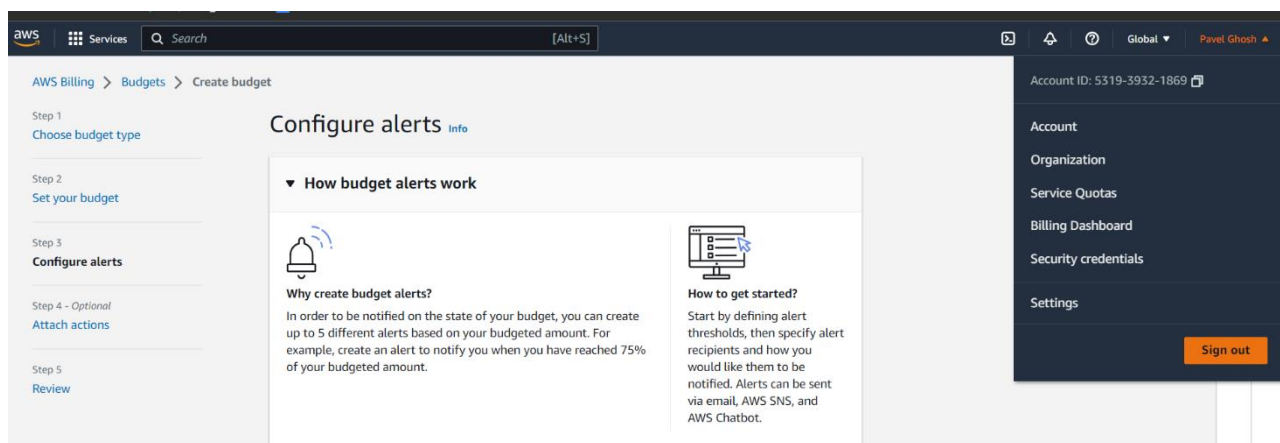


# Assignment 2

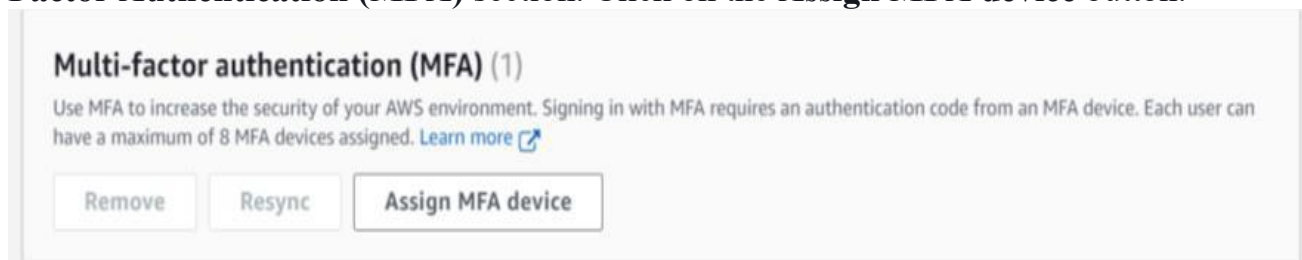
**Problem Statement:** Create Multi Factor Authentication(MFA) for account authentication.

**Procedure:**

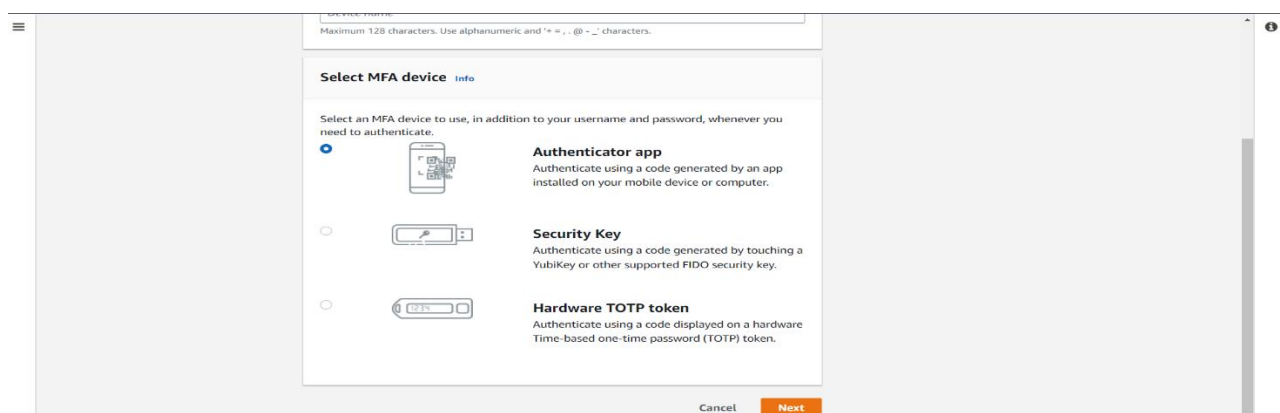
1. Sign-in to your AWS console. Then select the **down arrow** beside your **account name** in the top right side of the page.
2. Now select **Security Credentials** option in the drop-down menu.



3. Now after arriving in My Security Credentials page, now scroll down to **Multi-Factor Authentication (MFA)** section. Click on the **Assign MFA device** button.

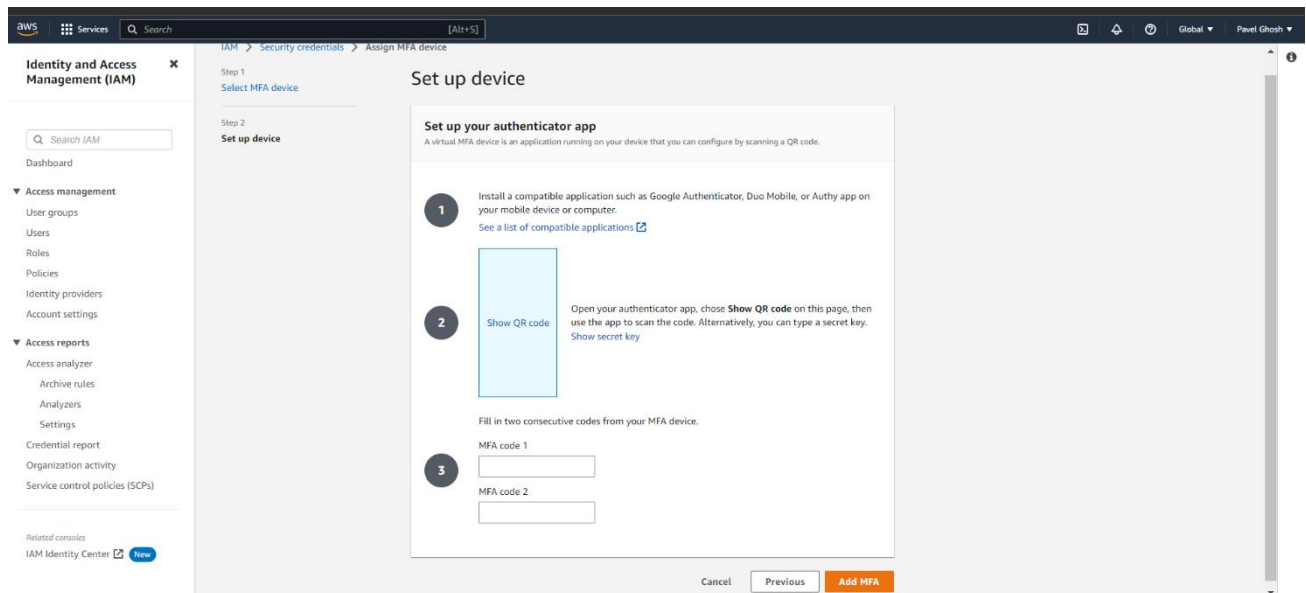


4. Next Assign a **unique device name** (very important and needs to be unique).  
This name is actually the name of the account that shows up in your authenticator app with the security codes and hence is essential for identification later. Select **Authenticator app** in **Select MFA device** section.



5. Click on **Next**.

6. After that you have to make sure you download an authenticator app from app store in your android/iOS device. Google/Microsoft authenticator is preferred. After installation, click on the **Show QR code box** here in the website. Scan the QR code with your authenticator app. Your device name given will show up in your authenticator main page.

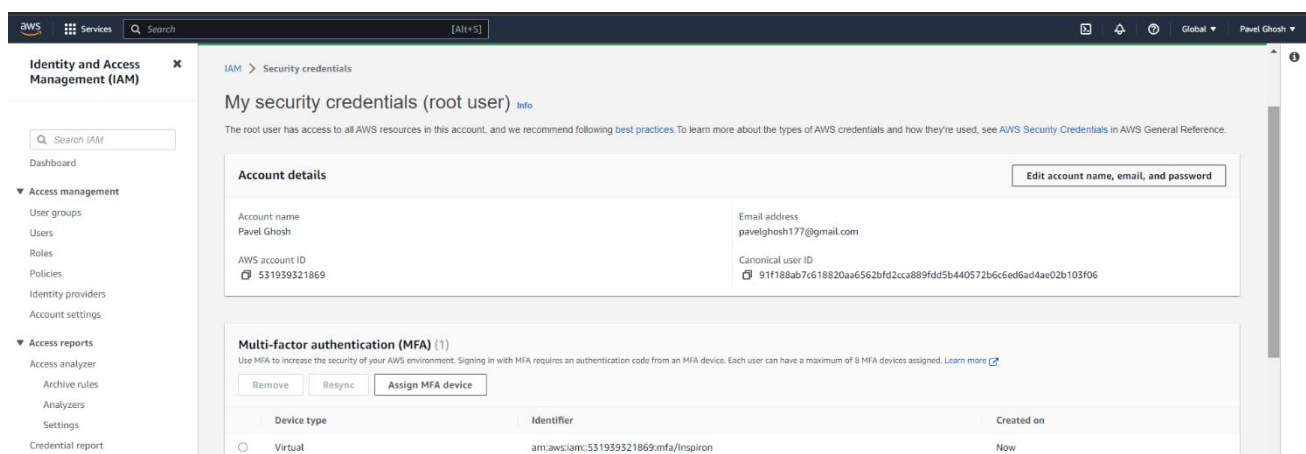


The screenshot shows the AWS IAM console's 'Set up device' page. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Access reports, and Related consoles. The main content area is titled 'Set up device' and includes a 'Step 2: Set up device' section. It provides instructions for installing an authenticator app, showing a QR code, and entering two consecutive MFA codes. At the bottom, there are 'Cancel', 'Previous', and 'Add MFA' buttons.

7. We will see a certain unique combination appearing against our given device name for our AWS account and stays only for 30-60 seconds. Enter 2 consecutive codes appearing in the given box in the website to authenticate your MFA.

8. After successfully verifying your MFA, click on the Add MFA button.

9. You will be redirected to the security credentials page and see your newly added MFA method with your given device name for your account.



The screenshot shows the AWS IAM console's 'My security credentials' page for the root user. The page displays account details such as the account name 'Pavel Ghosh', email address 'pavelghosh177@gmail.com', and AWS account ID '531939321869'. It also shows the canonical user ID. Under the 'Multi-factor authentication (MFA)' section, there is a table listing the assigned MFA device. The table has columns for 'Device type', 'Identifier', and 'Created on'. The device is listed as 'Virtual' with the identifier 'am:aws:iam:531939321869:mfa/inspiron' and was created 'Now'.

Device type	Identifier	Created on
<input type="radio"/> Virtual	am:aws:iam:531939321869:mfa/inspiron	Now

10. Hence, we have successfully added an MFA device.

11. Now sign-out and try to re-login to the console.

12. Now after providing user email and password, from now on you have to enter the MFA code which is given by the authenticator app in your phone. Be mindful that the code changes every 30-60 seconds and we have to enter the current or existing one which has not expired (or in this case stopped showing).



#### Multi-factor authentication

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

Email address: pavelghosh177@gmail.com

MFA code

Submit

[Troubleshoot MFA](#)

[Cancel](#)



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

English ▼