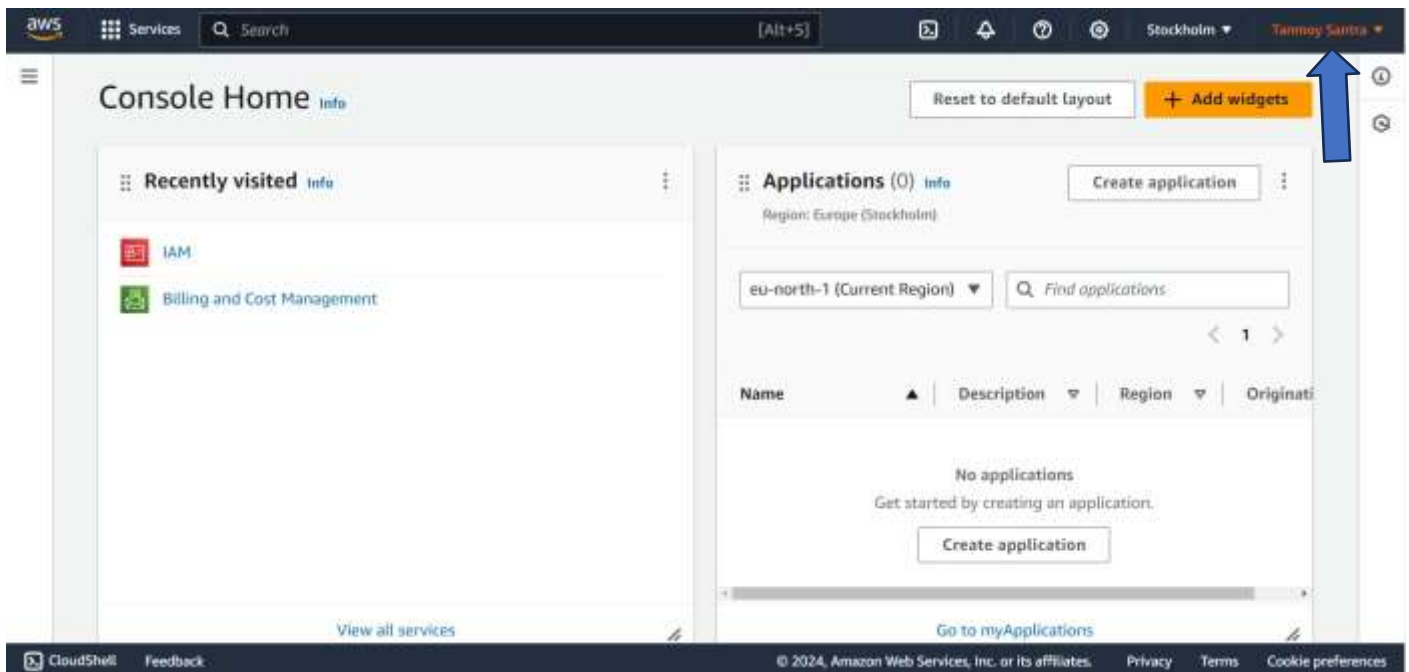


Assignment: 2

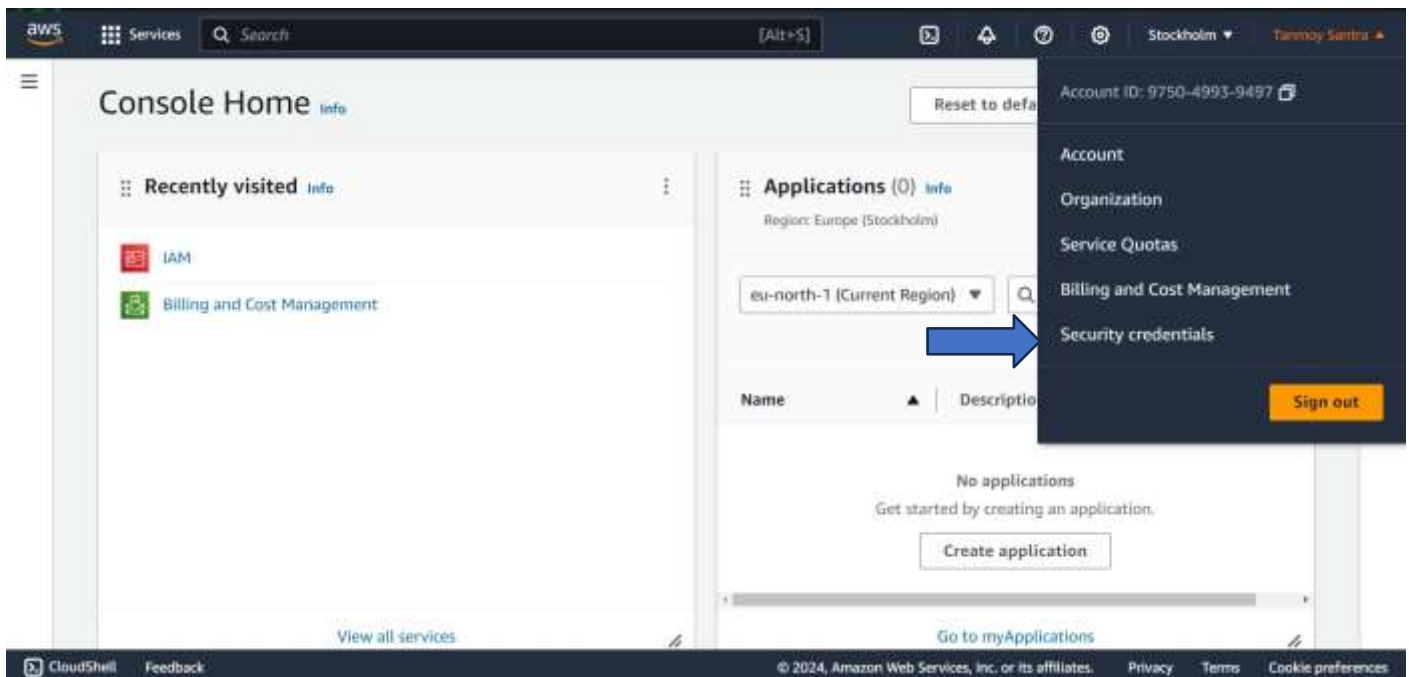
Problem Statement: Create MFA for authentication.

Steps to create MFA:-

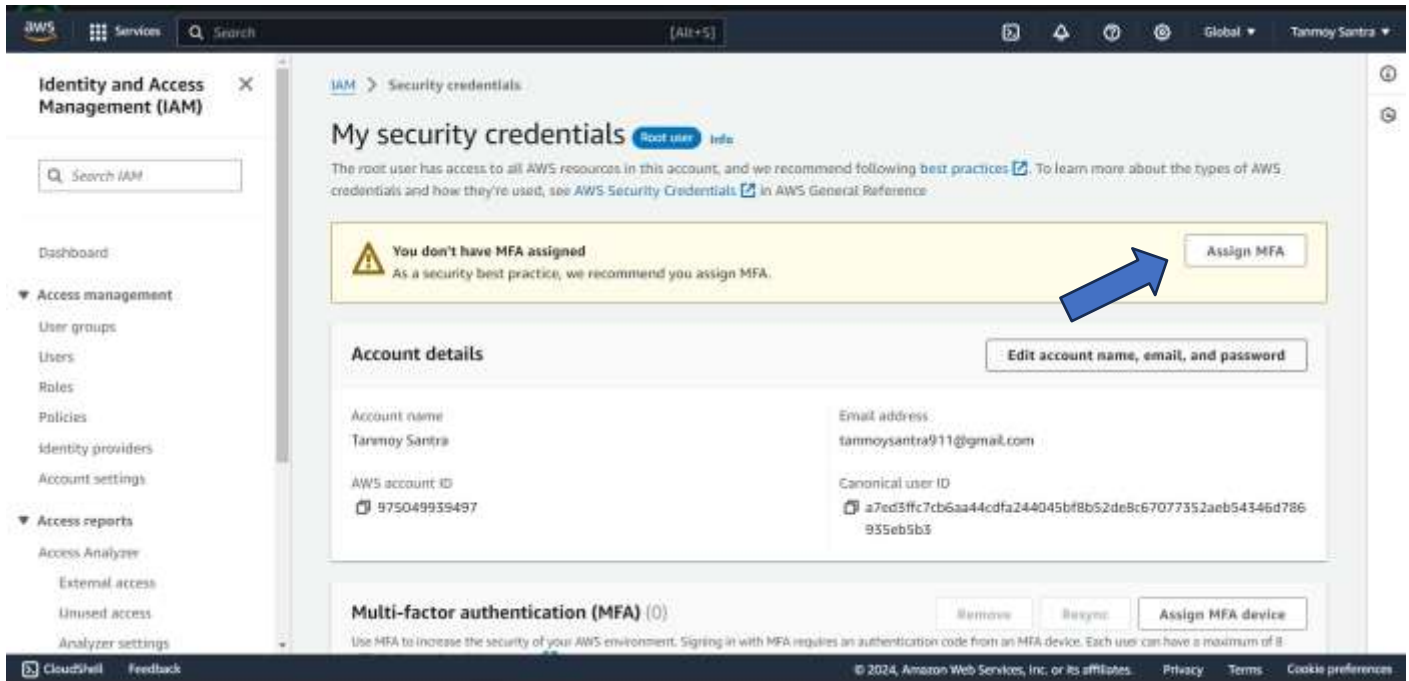
Step 1: Click on the name of the profile (i.e. top right of the screen).



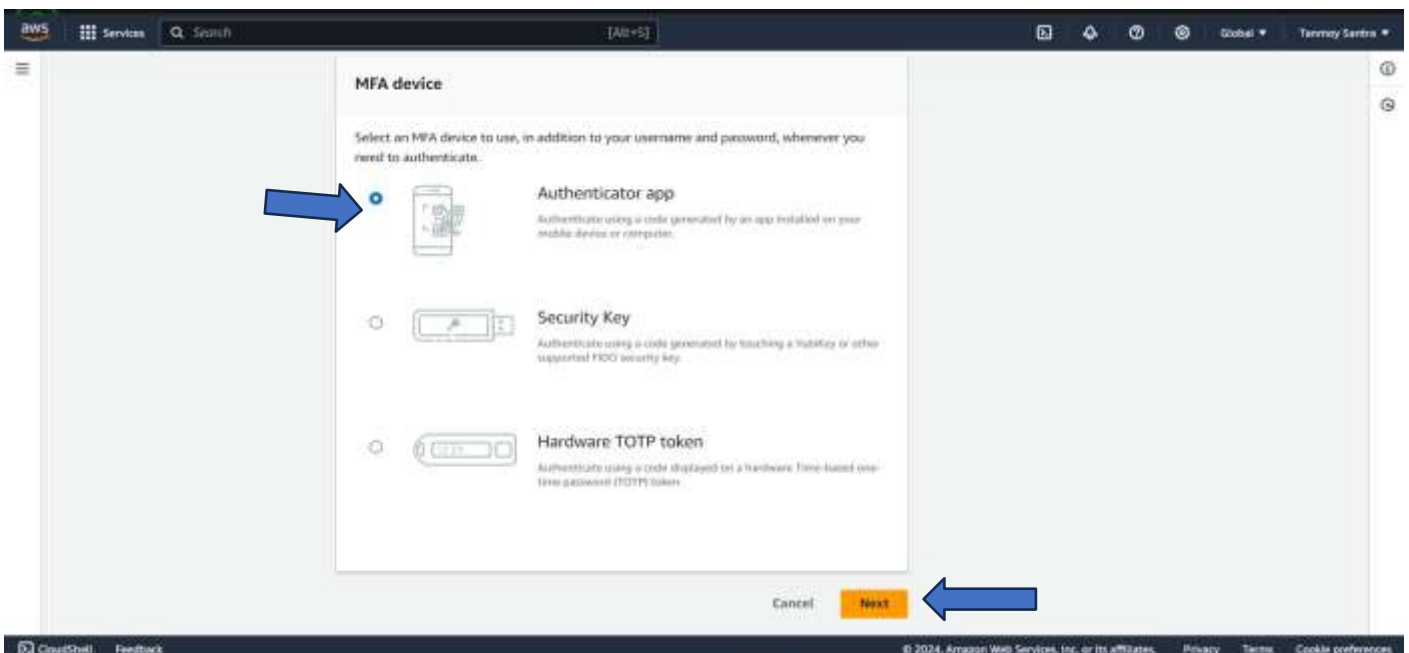
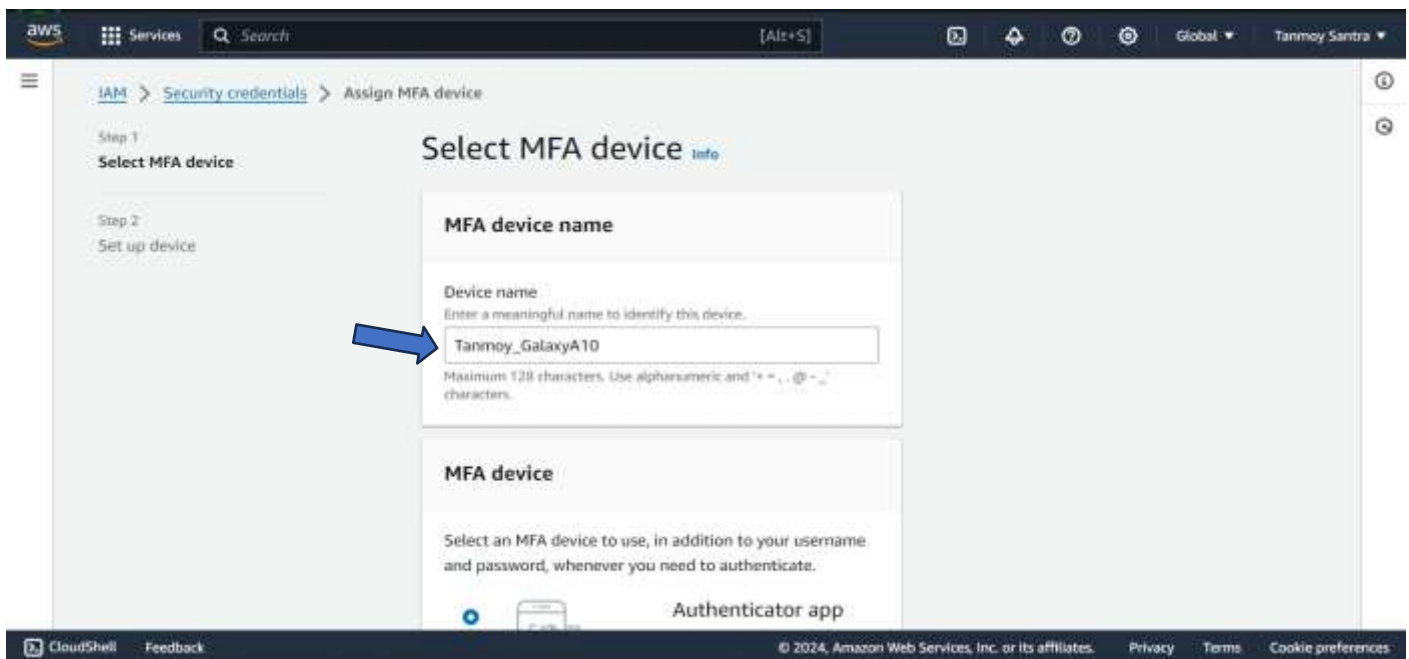
Step 2: Select “Security credentials” option.



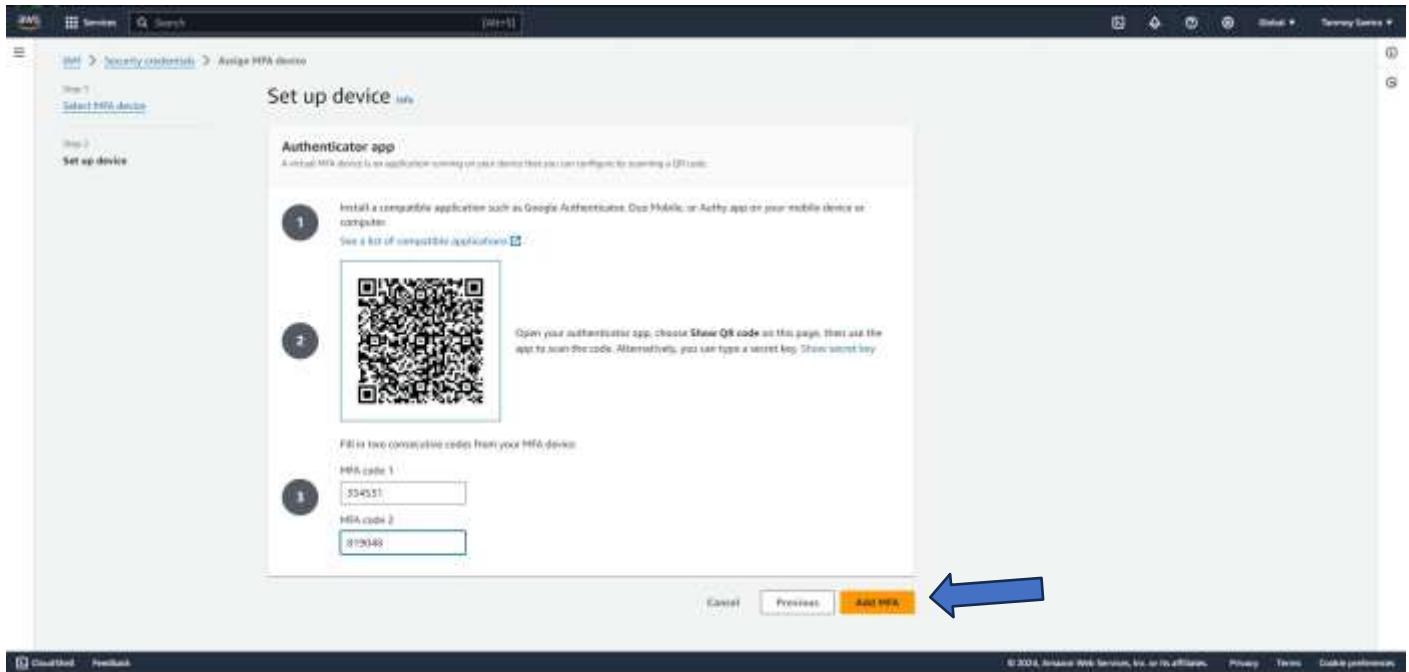
Step 3: Select “Assign MFA” option.



Step 4: Give device name (i.e. 'Tanmoy_GalaxyA10' in my case) & Select “Authenticator app” option then “Next”.



Step 5: Scan the QR code from the mobile phone using “Google Authenticator” app & provide the MFA code two time from the app then press “Add MFA”.



The screenshot shows the 'Set up device' page in the AWS IAM console. The page is titled 'Set up device' and has a sub-header 'Authenticator app'. It contains a QR code and instructions for scanning it with an authenticator app. Below the QR code, there are two input fields for 'MFA code 1' and 'MFA code 2'. The 'MFA code 1' field contains the value '334531' and the 'MFA code 2' field contains the value '819048'. At the bottom right of the page, there is a blue arrow pointing to the 'Add MFA' button.

Step 1: Select MFA device

Step 2: Set up device

Set up device

Authenticator app

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

1. Install a compatible application such as Google Authenticator. Open 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**

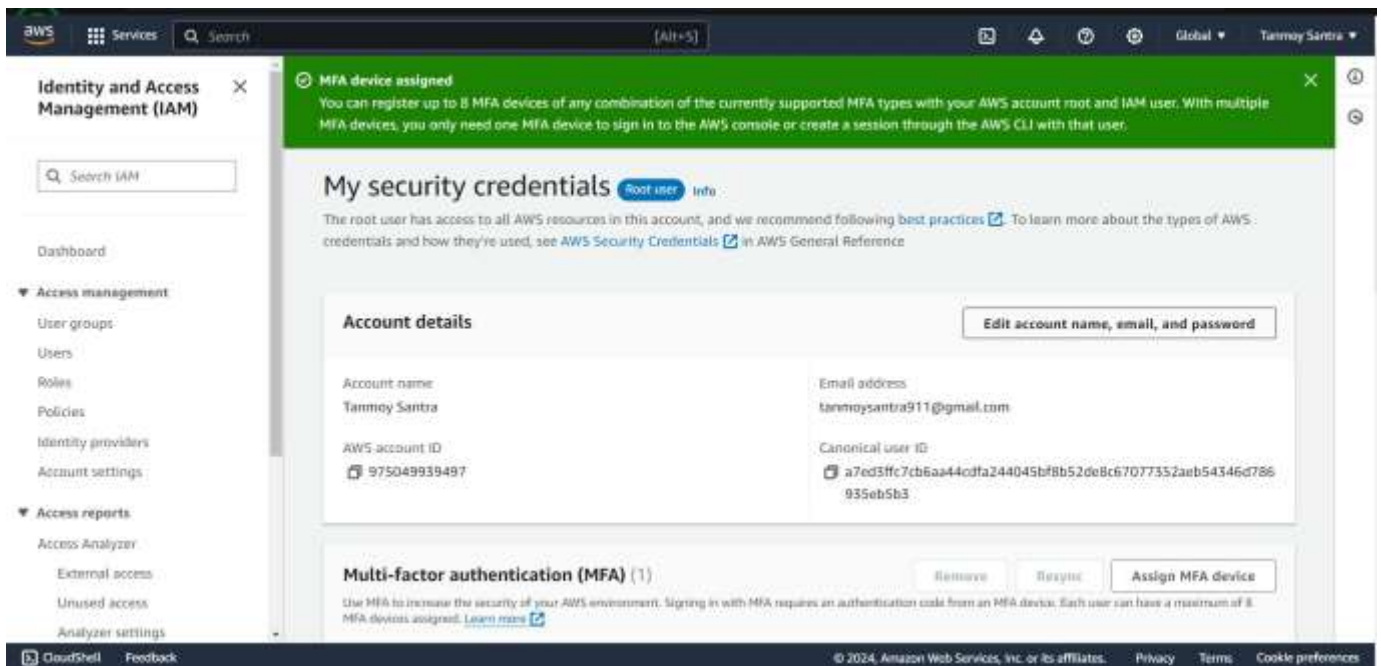
Fill in two consecutive codes from your MFA device:

MFA code 1: 334531

MFA code 2: 819048

Cancel Previous **Add MFA**

Step 6: MFA created successfully.



The screenshot shows the 'My security credentials' page in the AWS IAM console. The page is titled 'My security credentials' and has a sub-header 'Root user'. It displays account details and multi-factor authentication (MFA) settings. A green banner at the top indicates 'MFA device assigned'. The 'Account details' section shows the account name 'Tammy Santra', email address 'tammysantra911@gmail.com', AWS account ID '975049939487', and canonical user ID 'a7ed3ffc7cb6aa44cdfa244045bf8b52de8c67077352aeb54346d786935eb5b3'. The 'Multi-factor authentication (MFA)' section shows '1' device assigned and an 'Assign MFA device' button.

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

My security credentials (Root user)

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: Tammy Santra

Email address: tammysantra911@gmail.com

AWS account ID: 975049939487

Canonical user ID: a7ed3ffc7cb6aa44cdfa244045bf8b52de8c67077352aeb54346d786935eb5b3

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 Revoke **Assign MFA device**