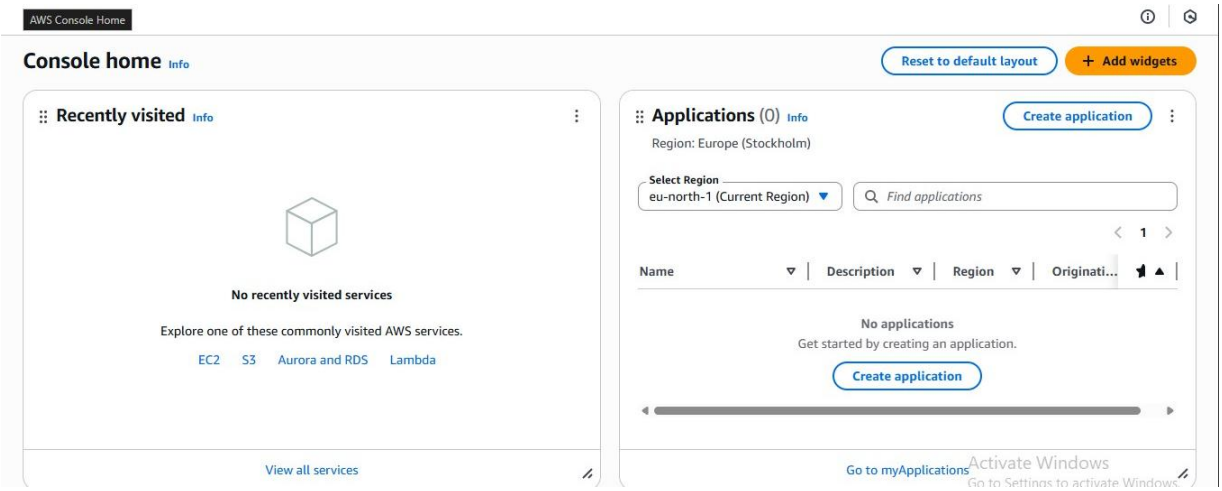
Practical :-6

Objective:- To secure an AWS IAM user account by enabling Multi-Factor Authentication (MFA), adding an extra verification step to prevent unauthorized access.

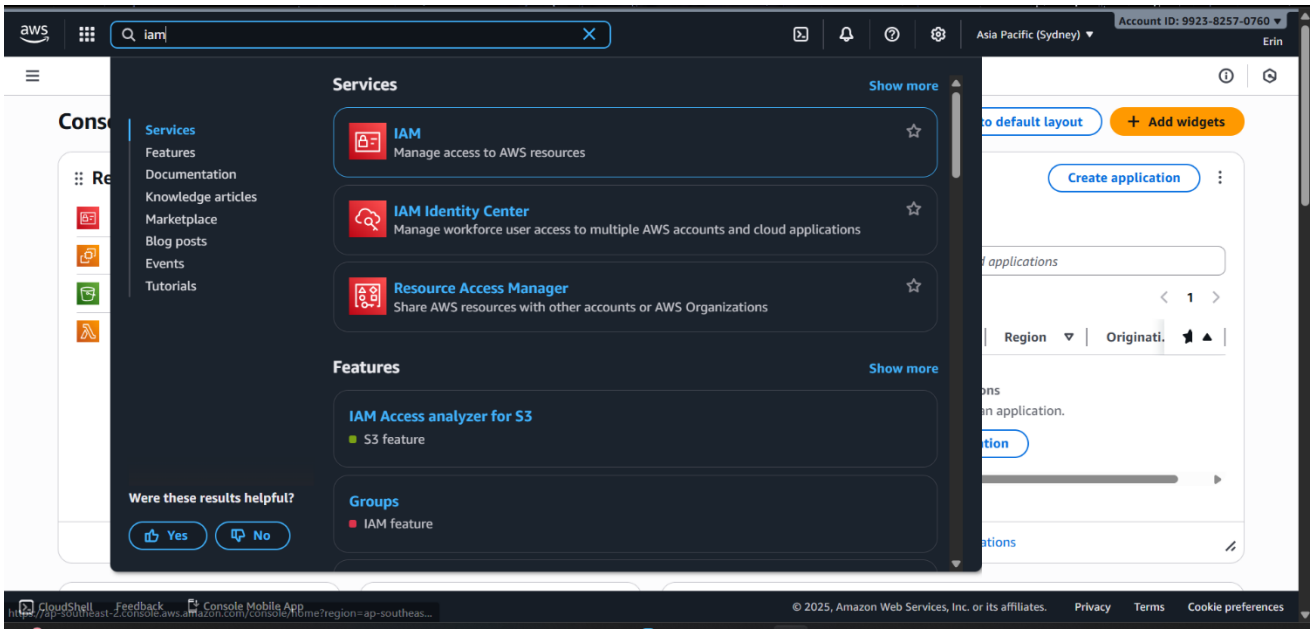
Step 1:- Sign in to AWS Management Console

- Log in using your **root account** or **IAM admin user**.
- Open the console.



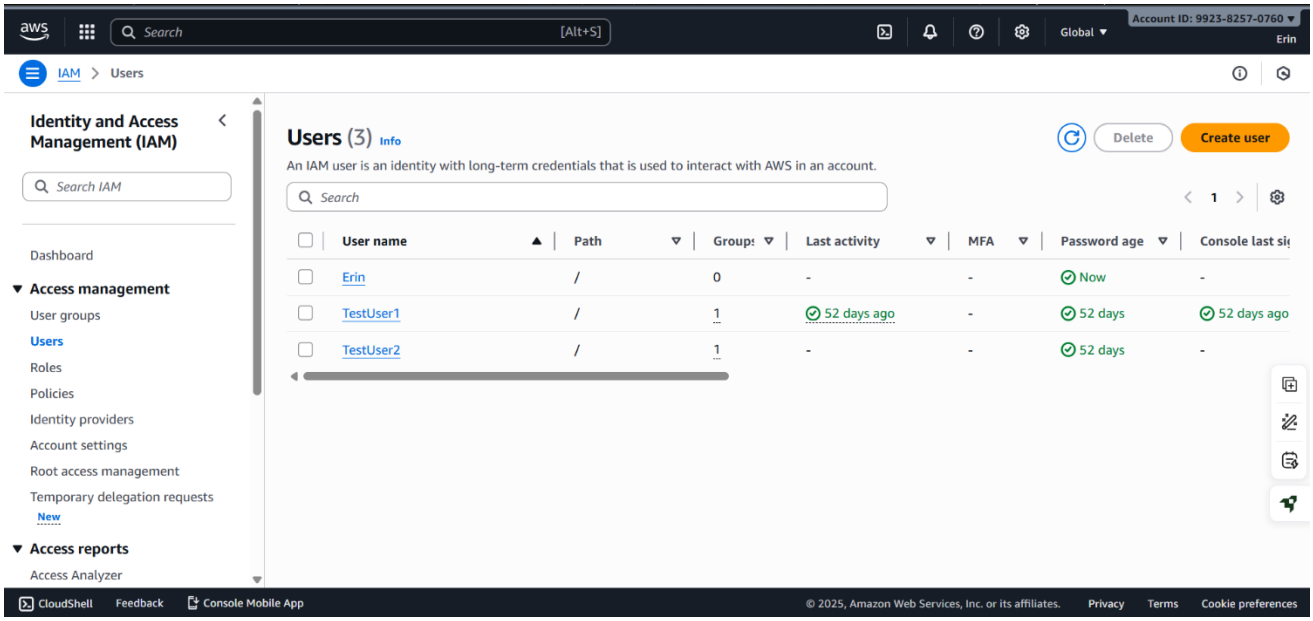
Step 2:- Go to IAM Service

- In the search bar, type **IAM**.
- Click **IAM (Identity and Access Management)**.



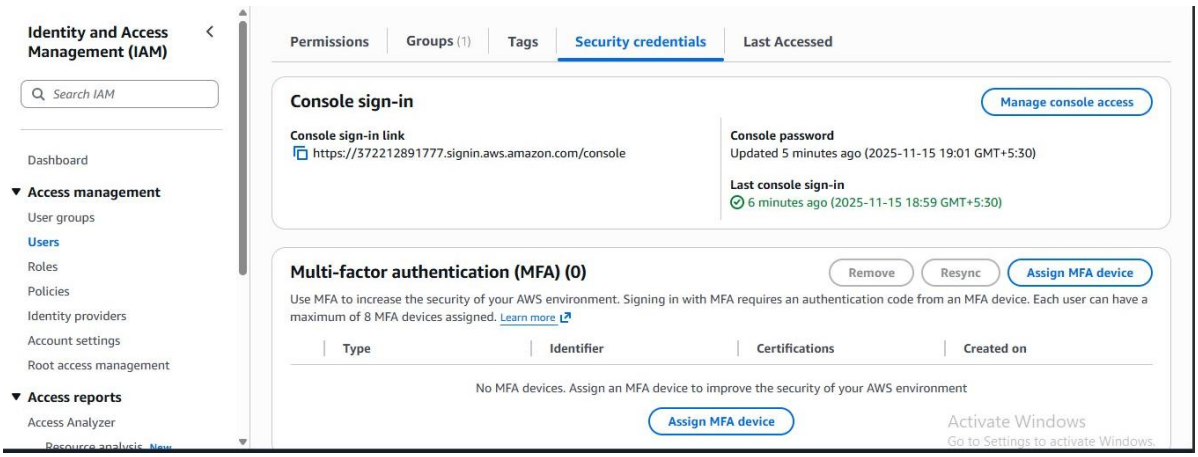
Step 3:-Open “Users”

- In the left navigation panel, select **Users**.
- Click the **username** for which you want to enable MFA.



Step 4:-Go to the “Security Credentials” Tab

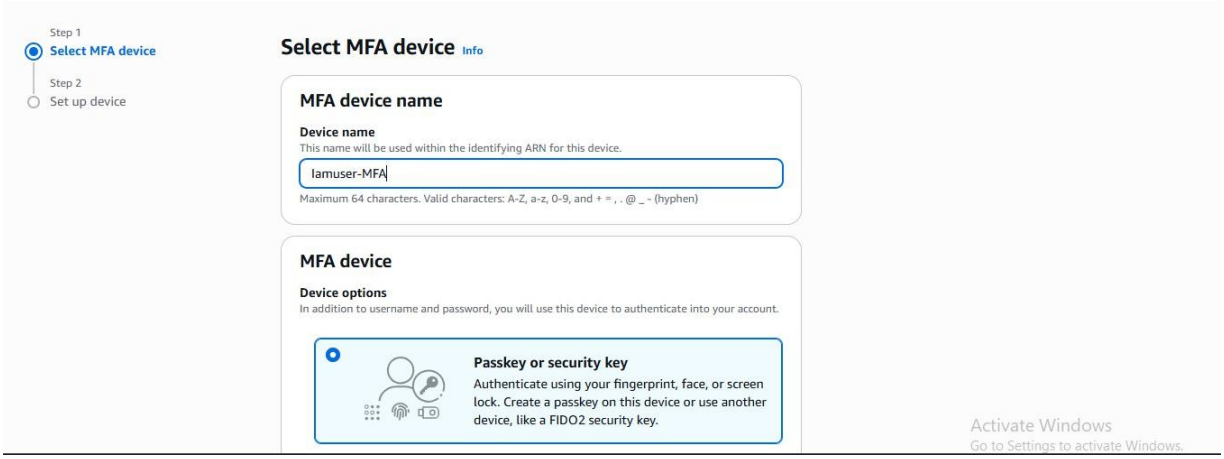
- After opening the user’s profile, click on **Security credentials**.
- Scroll down to the section **Multi-Factor Authentication (MFA)**.

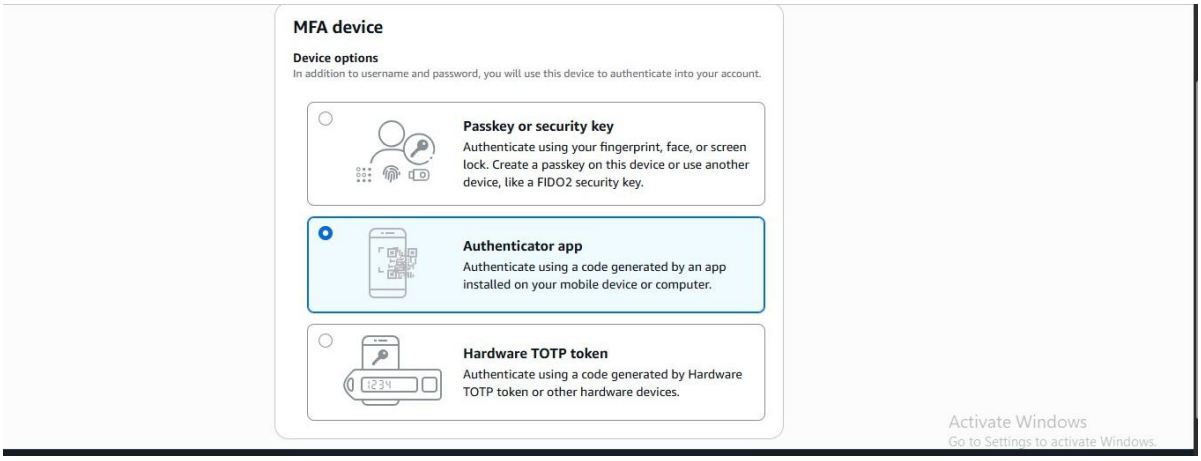


Step 5:-Click “Assign MFA Device”

- A popup will open with 3 options:
    1. **FIDO2 Security Key**
    2. **Authenticator App** (Google Authenticator / Authy / Microsoft Authenticator)
    3. **Hardware TOTP Device**

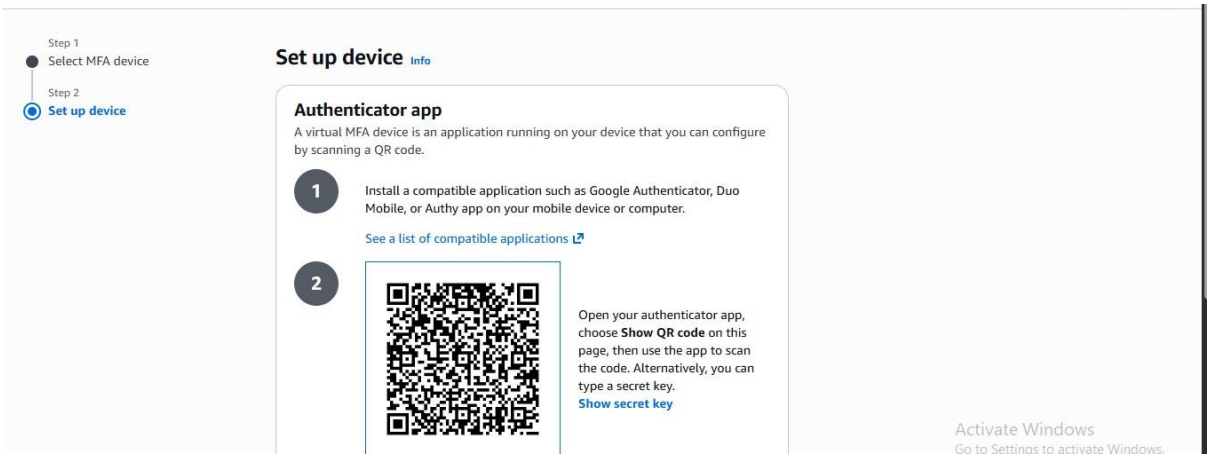
For most labs, choose **Authenticator App**.





Step 6:-Select “Authenticator App” and Continue

- Click **Continue**.
- AWS will show a **QR code** for MFA enrollment.



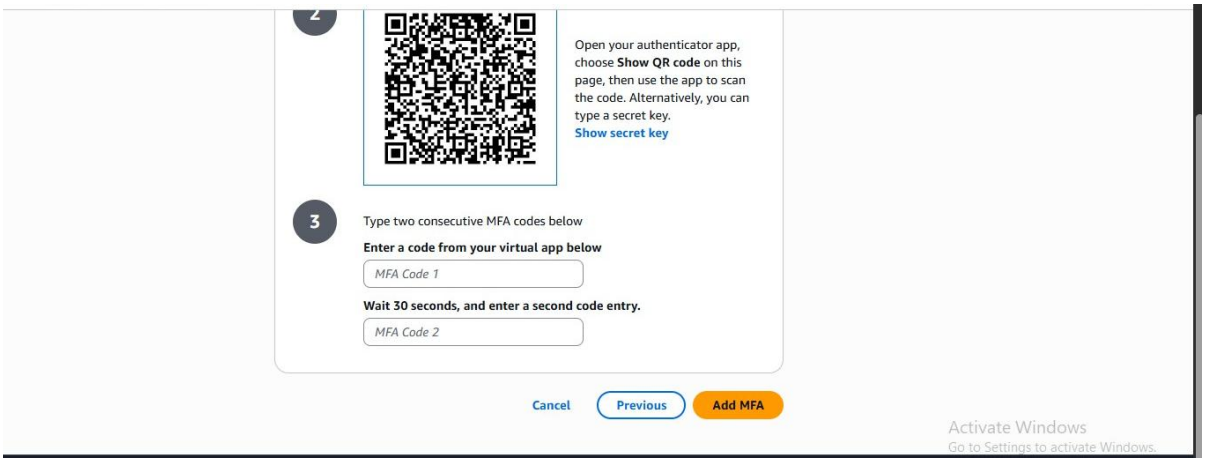
Step 7:-Open your Authenticator App

You can use any app:

- Google Authenticator
- Authy
- Microsoft Authenticator
- LastPass Authenticator

Click **Add Account → Scan QR Code**.

The app will generate a **6-digit one-time password (OTP)** that refreshes every 30 seconds.



Step 8:-MFA Successfully Enabled

“MFA device assigned successfully”