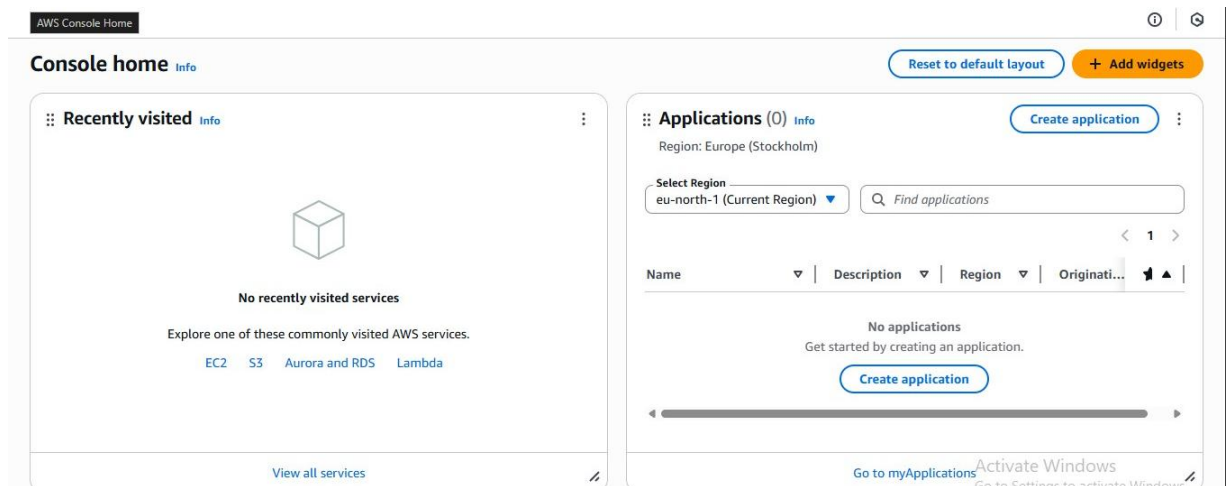


Practical :-6

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

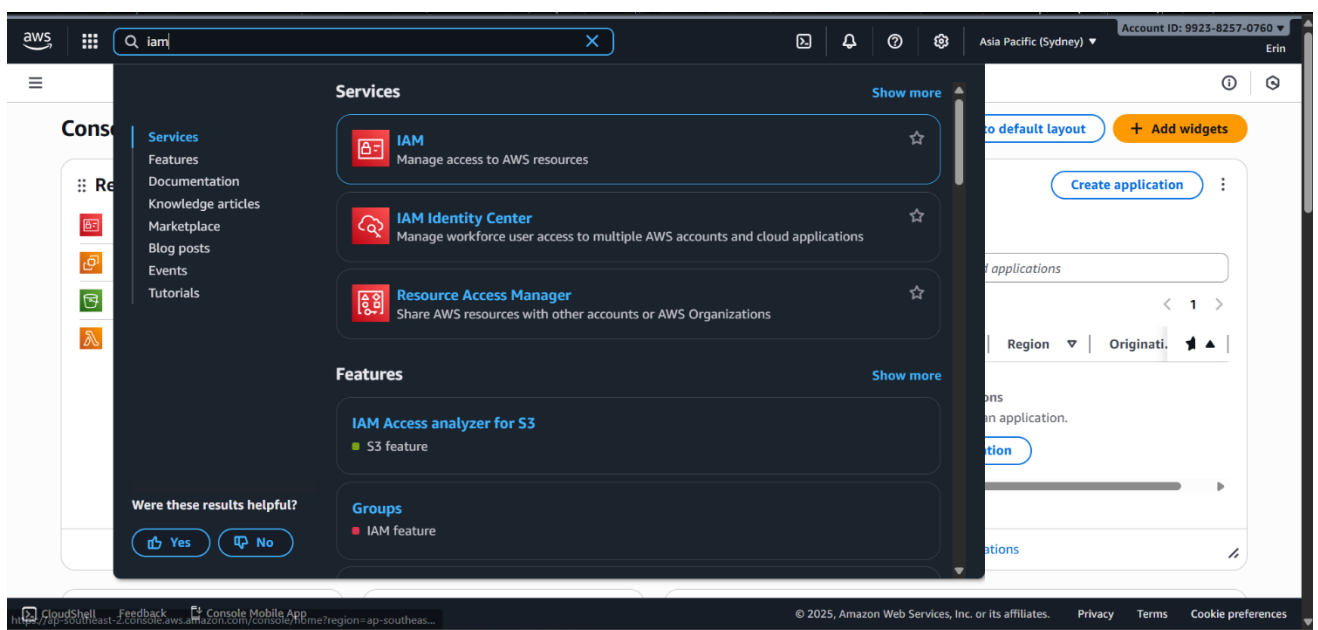
Step 1:- Sign in to AWS Management Console

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



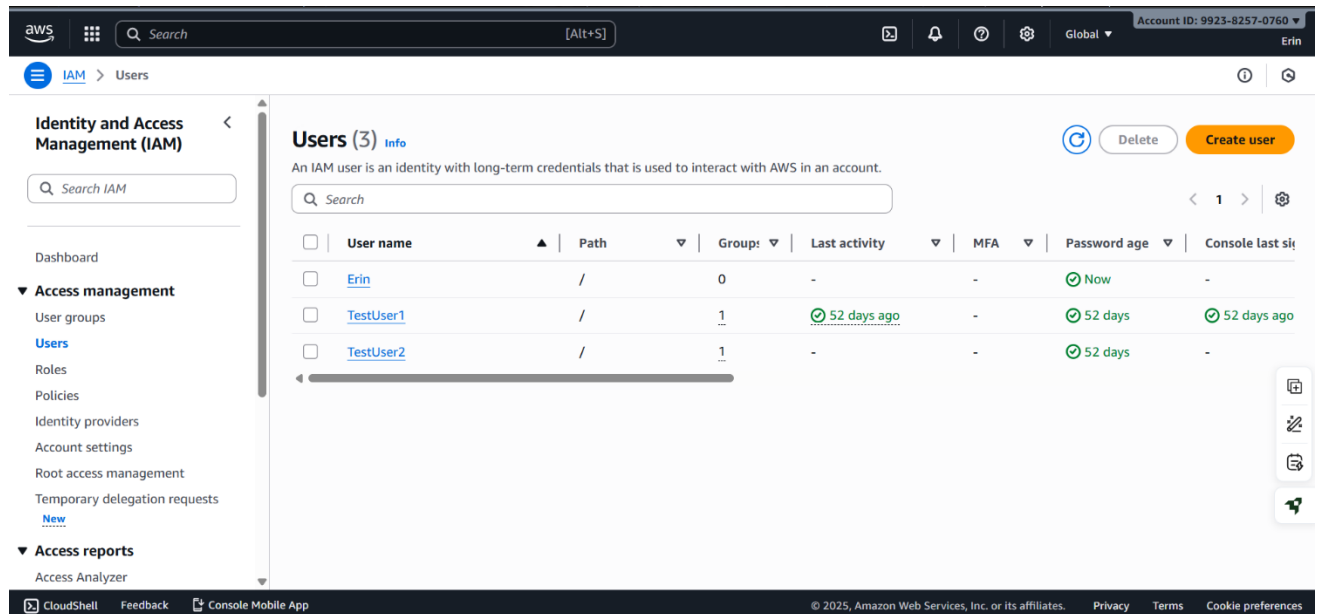
Step 2:- Go to IAM Service

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



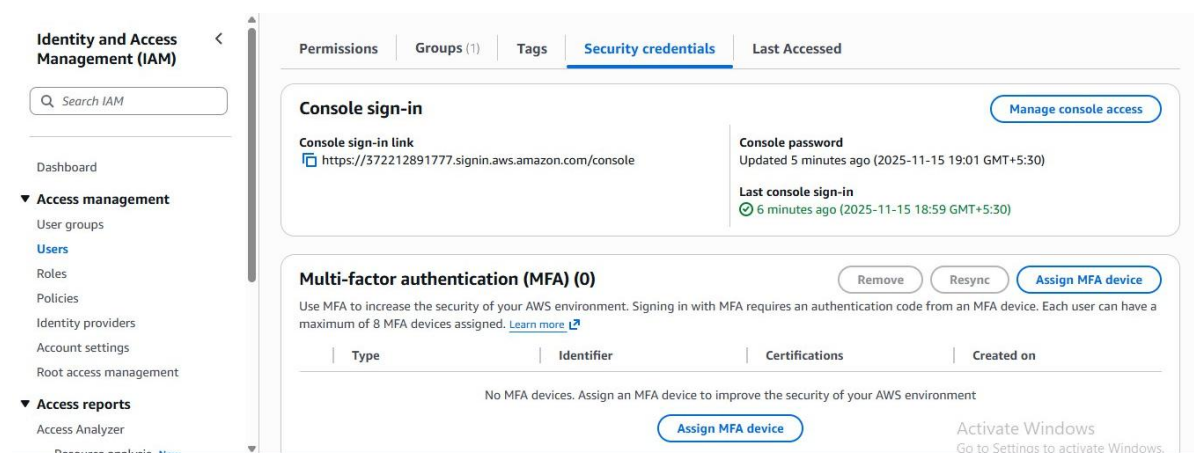
Step 3:-Open “Users”

- 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 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.

Maximum 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

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.

Activate Windows
Go to Settings to activate Windows.

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.

☒



Authenticator app
Authenticate using a code generated by an app installed on your mobile device or computer.

☐

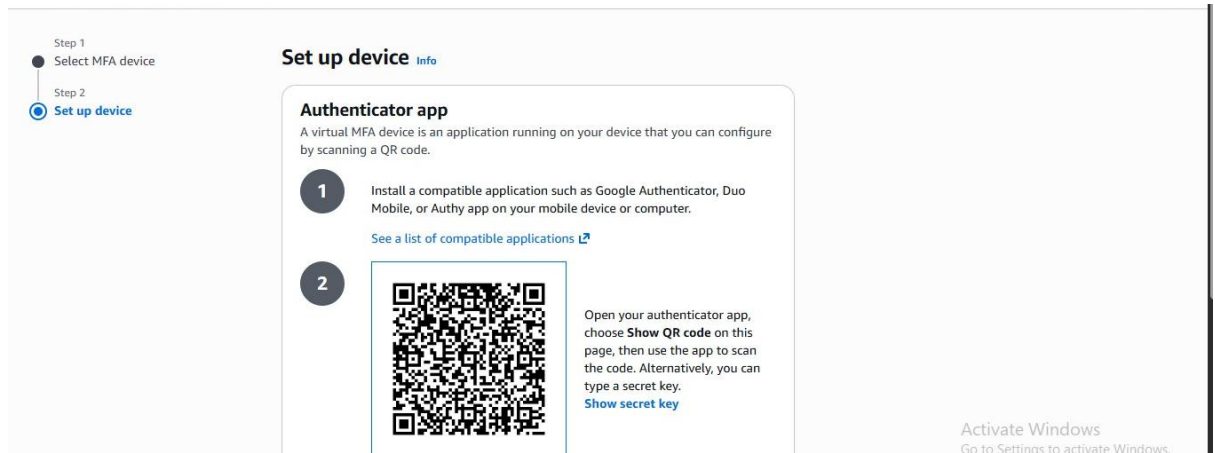


Hardware TOTP token
Authenticate using a code generated by Hardware TOTP token or other hardware devices.

Activate Windows
Go to Settings to activate Windows.

Step 6:-Select “Authenticator App” and Continue

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



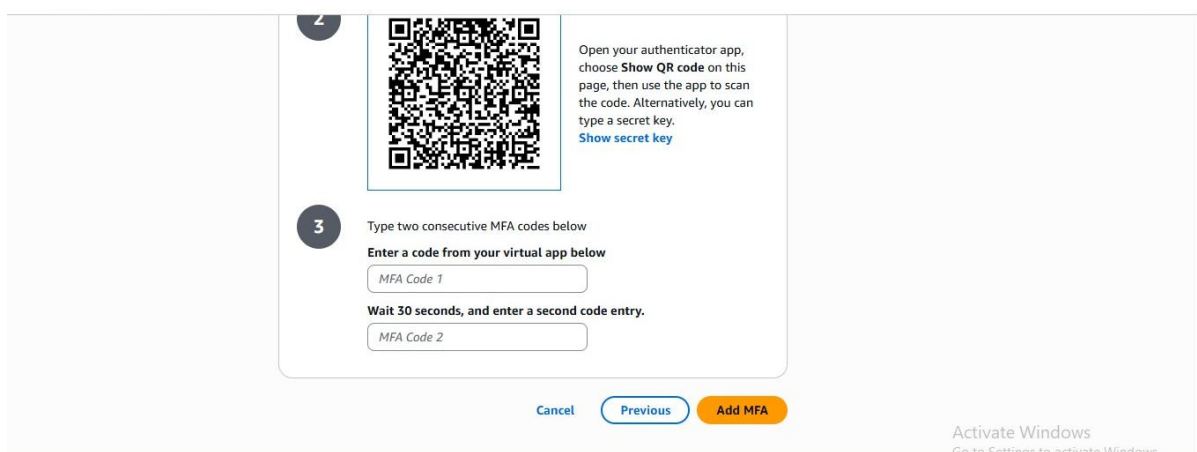
Step 7:-Open your Authenticator App

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”

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

▼ Access reports

Access Analyzer

Resource analysis New

Summary

ARN

am:aws:iam::372212891777:user/srishti2

Created

November 08, 2025, 11:58 (UTC+05:30)

Console access

Enabled with MFA

Last console sign-in

Today

Access key 1

Create access key

Permissions

Groups (1)

Tags

Security credentials

Last Accessed

Console sign-in

Console sign-in link

https://372212891777.signin.aws.amazon.com/console

Console password

Updated 21 minutes ago (2025-11-15 19:01 GMT+5:30)

Manage console access

Activate Windows

Go to Settings to activate Windows.