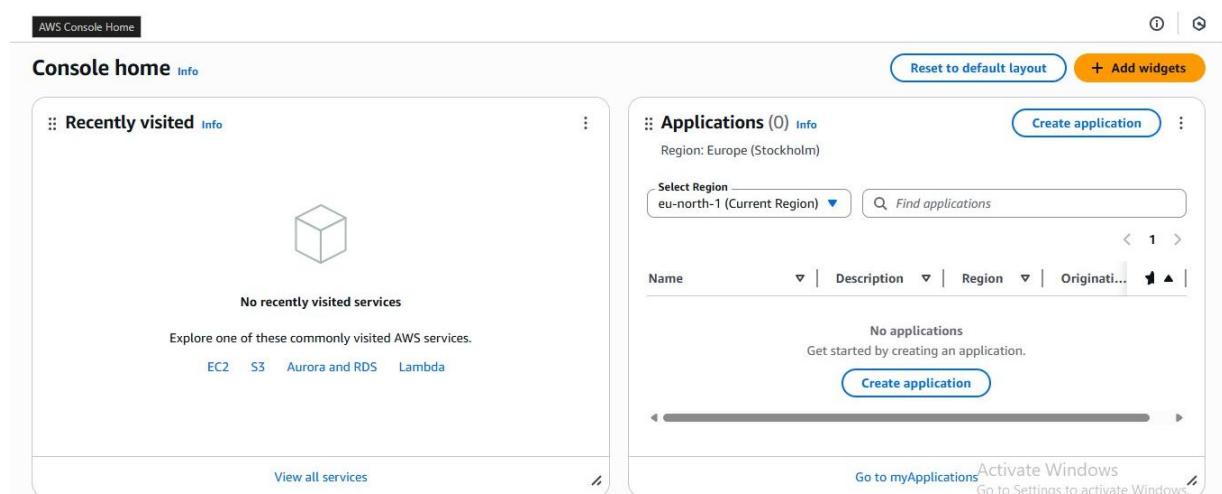


Practical :-6

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

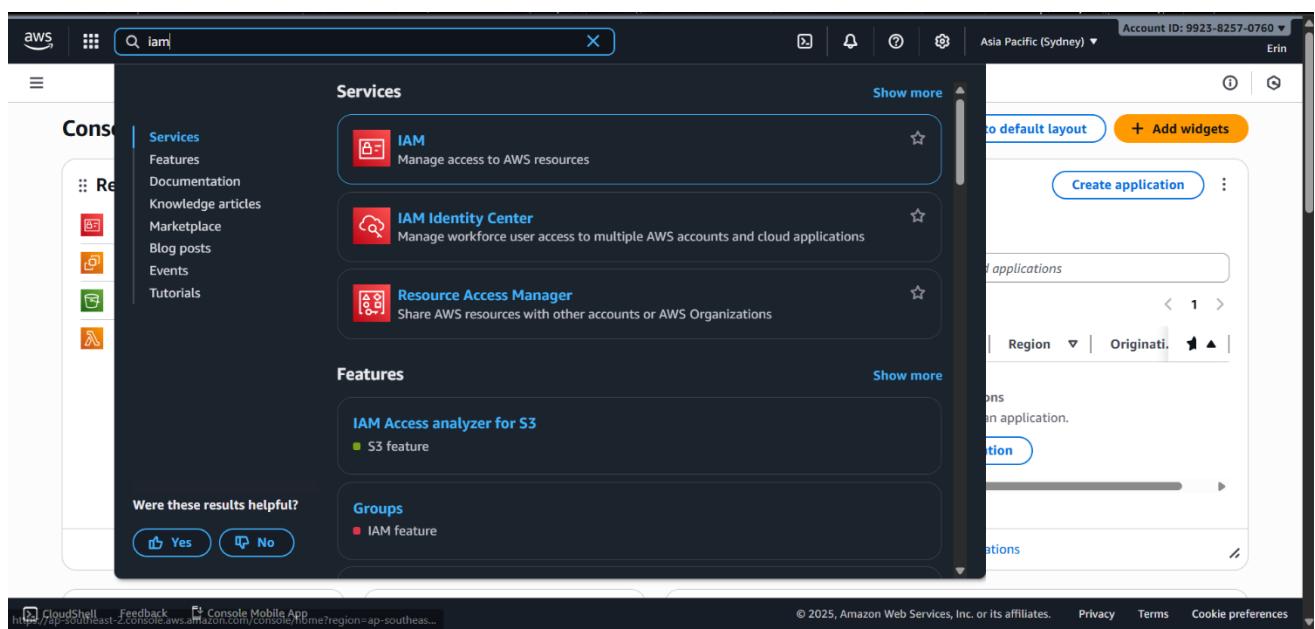
Step 1:- Sign in to AWS Management Console

- 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.

The screenshot shows the AWS IAM service interface. The left sidebar is titled "Identity and Access Management (IAM)" and includes sections for Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management, Temporary delegation requests), and Access reports (Access Analyzer). The main content area is titled "Users (3) Info" and contains a table with the following data:

User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in
Erin	/	0	-	-	Now	-
TestUser1	/	1	52 days ago	-	52 days	52 days ago
TestUser2	/	1	-	-	52 days	-

At the bottom right of the main area, there are several icons for filtering, sorting, and other actions. The footer includes links for CloudShell, Feedback, Console Mobile App, and copyright information from 2025.

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)**.

This screenshot shows the "Security credentials" tab for the "Erin" user profile. The left sidebar is identical to the previous screenshot. The main content area has tabs for Permissions, Groups (1), Tags, Security credentials (which is selected and highlighted in blue), and Last Accessed. The "Security credentials" section contains the following information:

- Console sign-in:**
 - Console sign-in link: <https://372212891777.signin.aws.amazon.com/console>
 - Console password: Updated 5 minutes ago (2025-11-15 19:01 GMT+5:30)
 - Last console sign-in: 6 minutes ago (2025-11-15 18:59 GMT+5:30)
- Multi-factor authentication (MFA) (0):**

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](#)

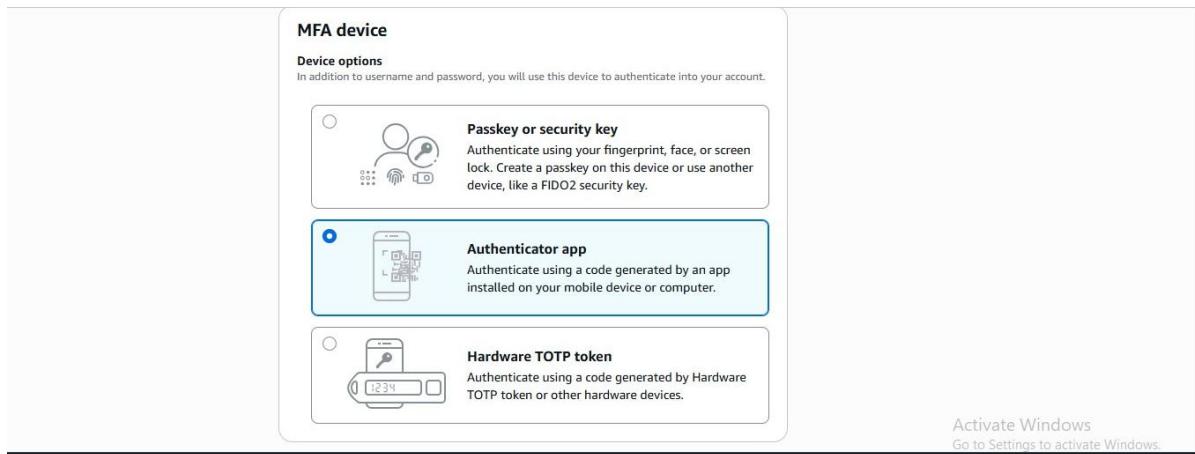
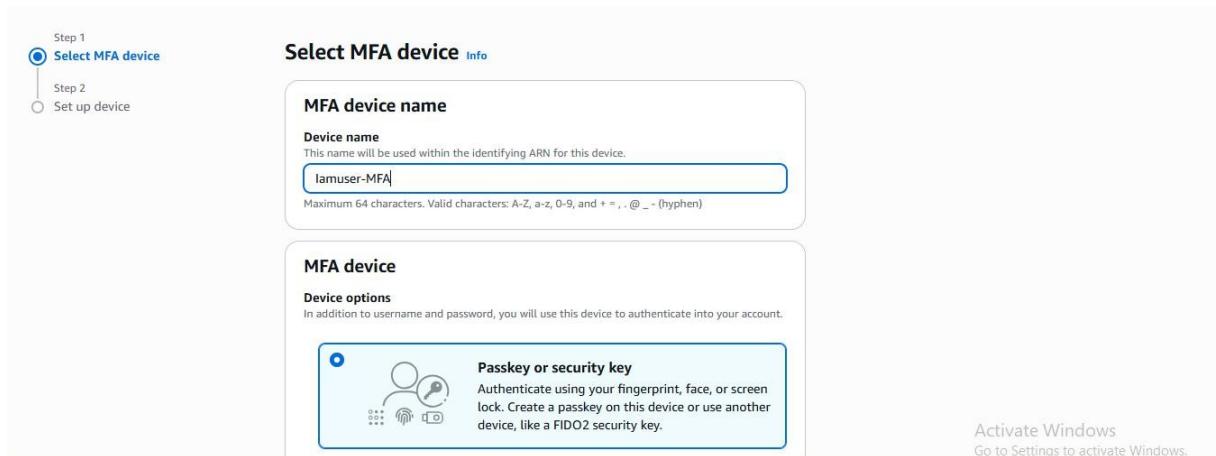
Type	Identifier	Certifications	Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment			

Buttons at the bottom of this section include "Assign MFA device" and "Activate Windows".

Step 5:-Click “Assign MFA Device”

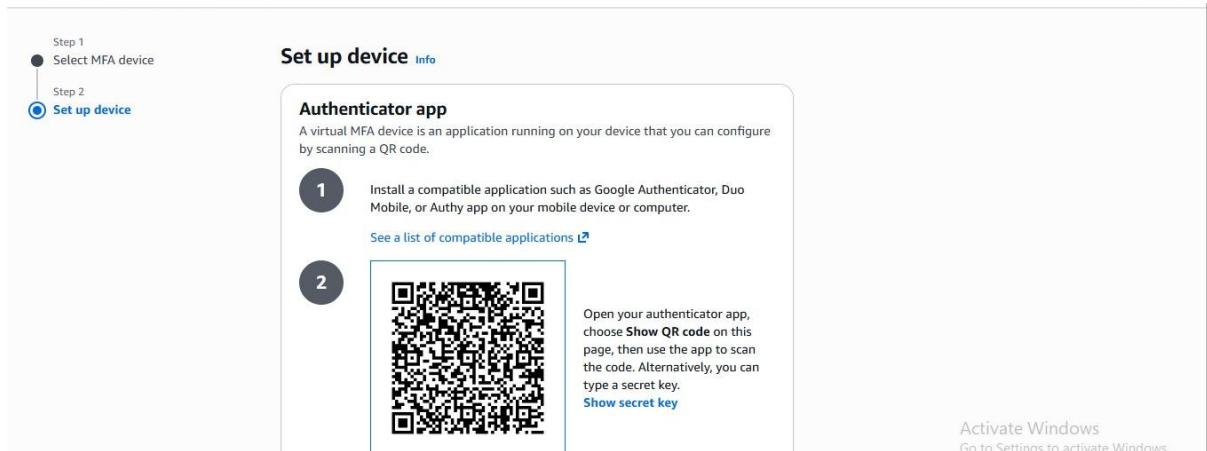
- A popup will open with 3 options:
 1. **FIDO2 Security Key**
 2. **Authenticator App** (Google Authenticator / Authy / Microsoft Authenticator)
 3. **Hardware TOTP Device**

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



Step 6:-Select “Authenticator App” and Continue

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



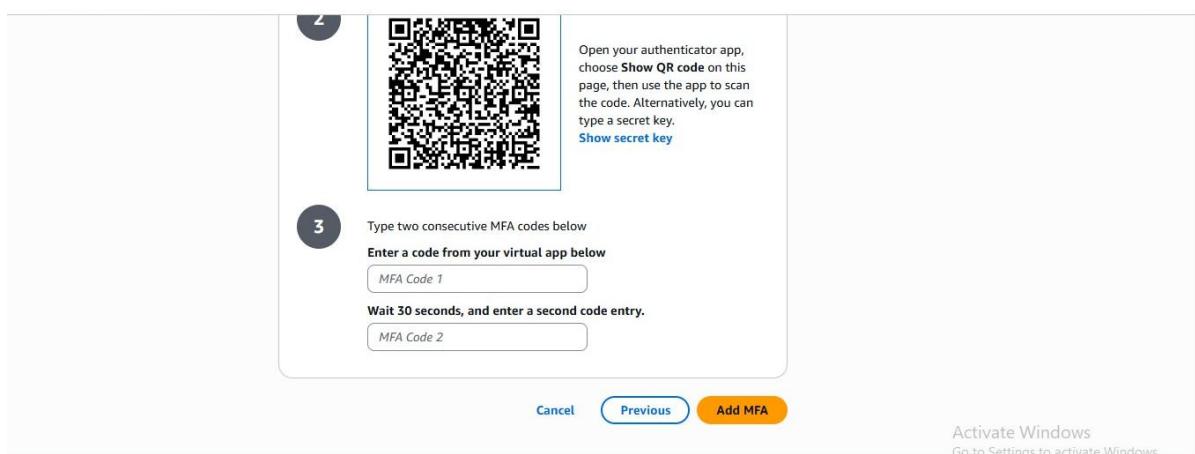
Step 7:-Open your Authenticator App

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”

The screenshot shows the AWS IAM User Summary page for a user named 'srishti2'. The 'Security credentials' tab is selected. Key details shown include:

- ARN:** arn:aws:iam::372212891777:user/srishti2
- Console access:** Enabled with MFA
- Created:** November 08, 2025, 11:58 (UTC+05:30)
- Last console sign-in:** Today
- Access key 1:** Create access key

Below the summary, the 'Console sign-in' section displays a 'Console sign-in link' (https://372212891777.signin.aws.amazon.com/console) and a 'Console password' (Updated 21 minutes ago / 2025-11-15 19:01 GMT+05:30). There are 'Manage console access' and 'Activate Windows' buttons.

On the left sidebar, the 'Users' section is expanded, showing options like User groups, Roles, Policies, Identity providers, Account settings, and Root access management. Other sections like 'Access management' and 'Access reports' are also listed.