# Module – 5 Security

Assignment 2: Setting up Custom Sign-in URL || MFA

**Custom URL** – To create sign-in URL with our company/organization name we can use account alias. It will replace the account ID from URL.

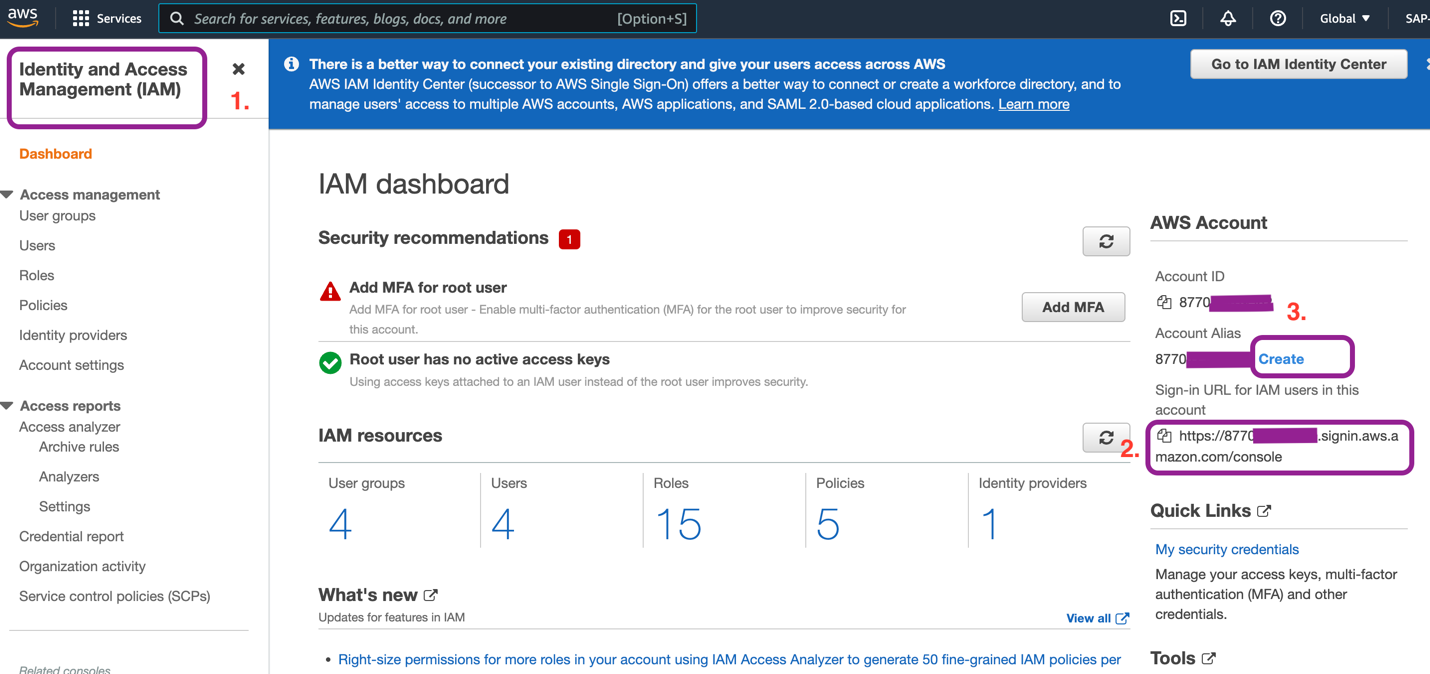
**MFA** – Multi-factor Authentication, to make account more secure and to authenticate the user sign in we can utilize MFA to authenticate user through multiple ways. Even user signed-in using username password, we can authenticate user through OTP/ access code etc.

# TASK 1

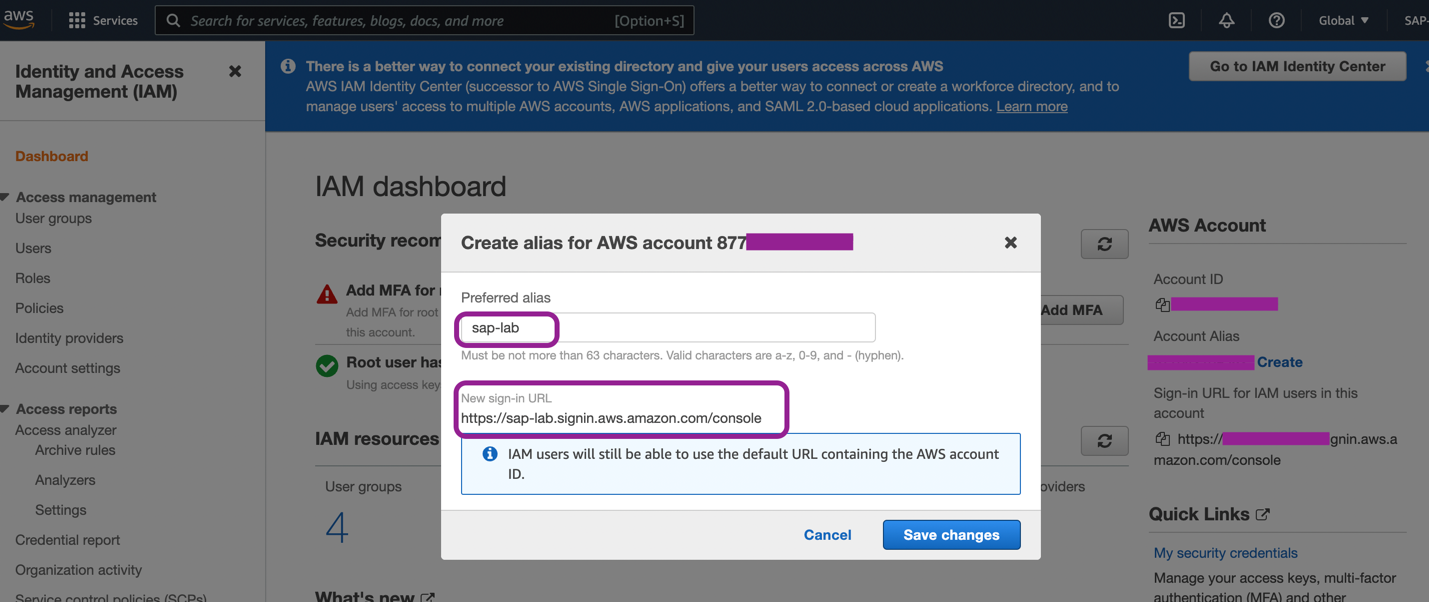
Practical Steps for **Custom URL**

Step 1: To setup Custom sign-in URL go to IAM Service. On IAM dashboard in right-side pane we can check account sign-in URL(marked point 2.) which contains account Id.

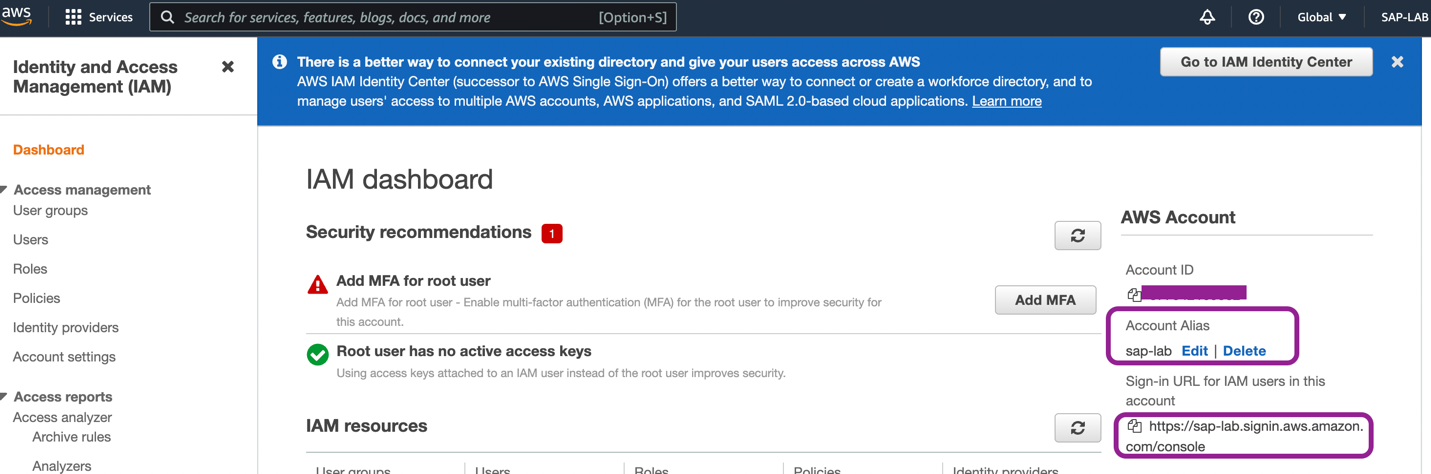
Step 2: Under ‘**Account Alias’** click on ‘**Create’ (**marked point 3.).



Step 3: Put the desired alias name in ‘**Preferred alias**’ to use at the place of account id to create custom sign-in URL. Click on ‘**Save changes**’.



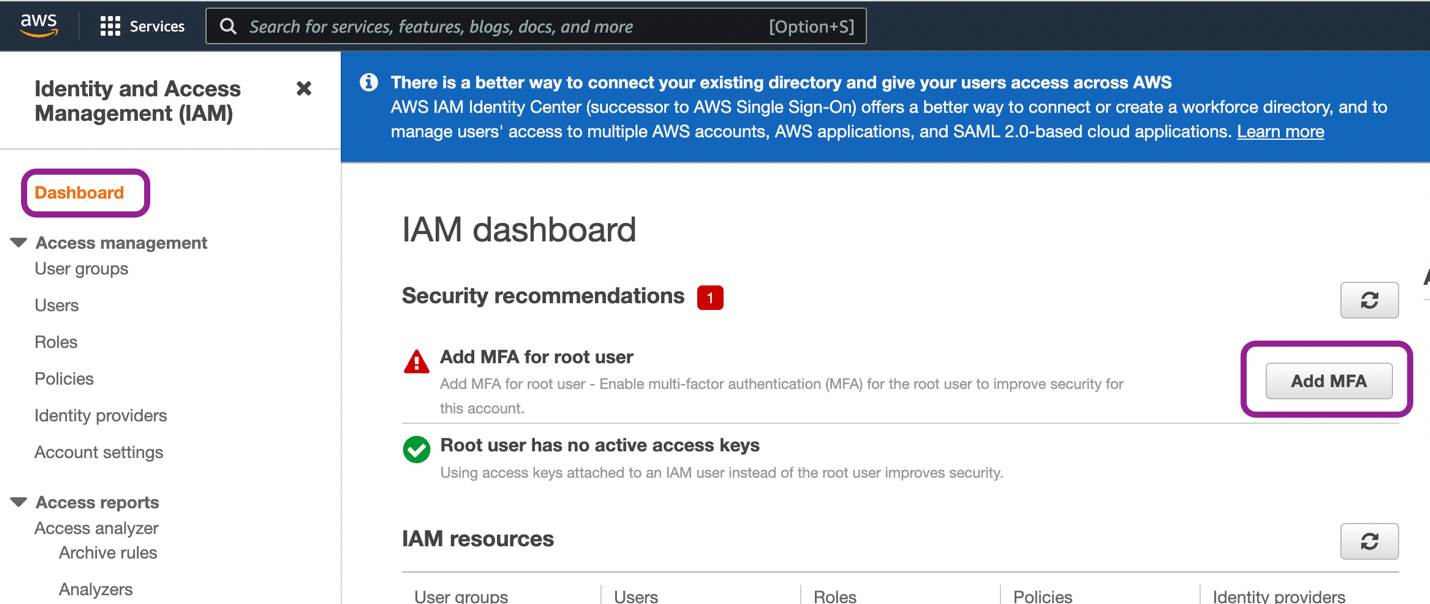
On IAM dashboard we can check the custom URL and edit if require.



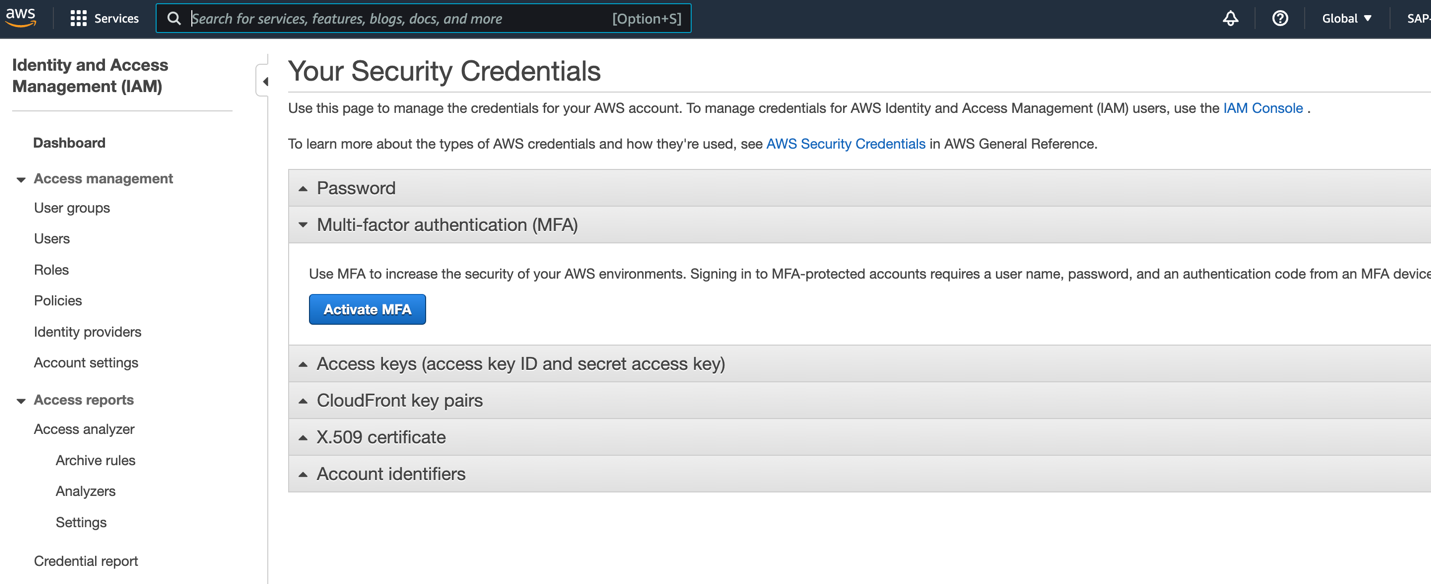
# TASK 2

Practical steps for **MFA**

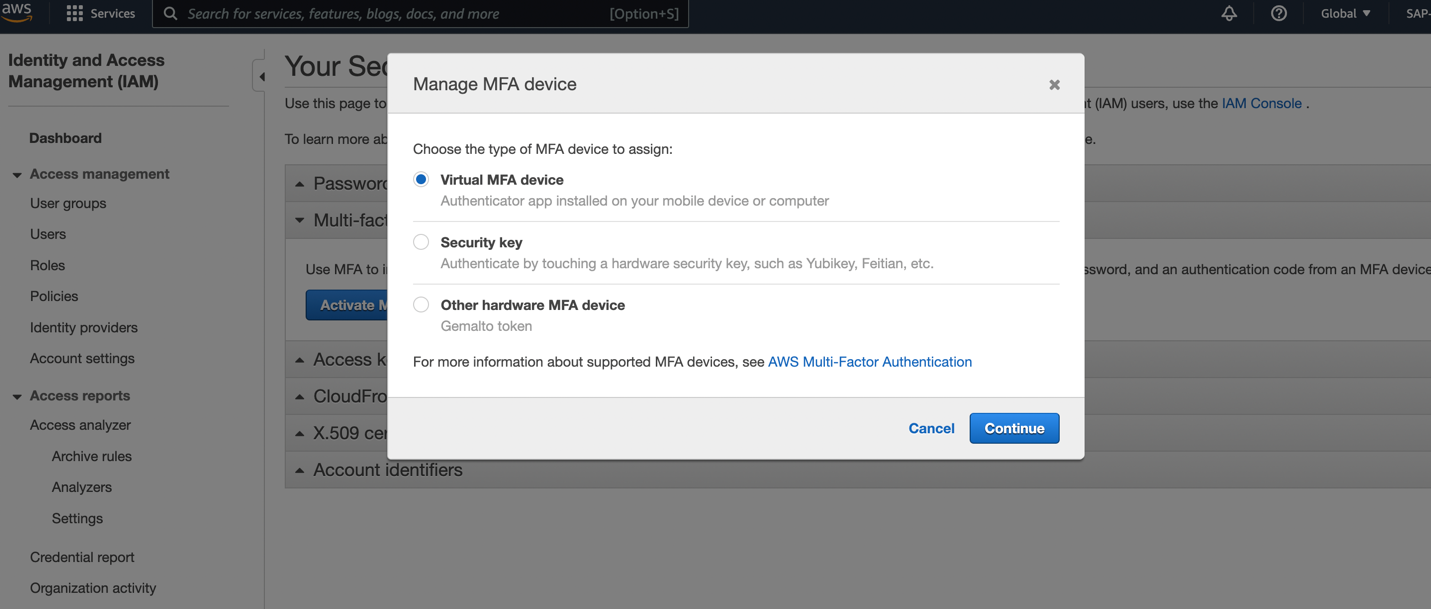
Step 1: Go to IAM dashboard, click on ‘**Add MFA**’.



Step 2: Click on ‘**Activate MFA**’

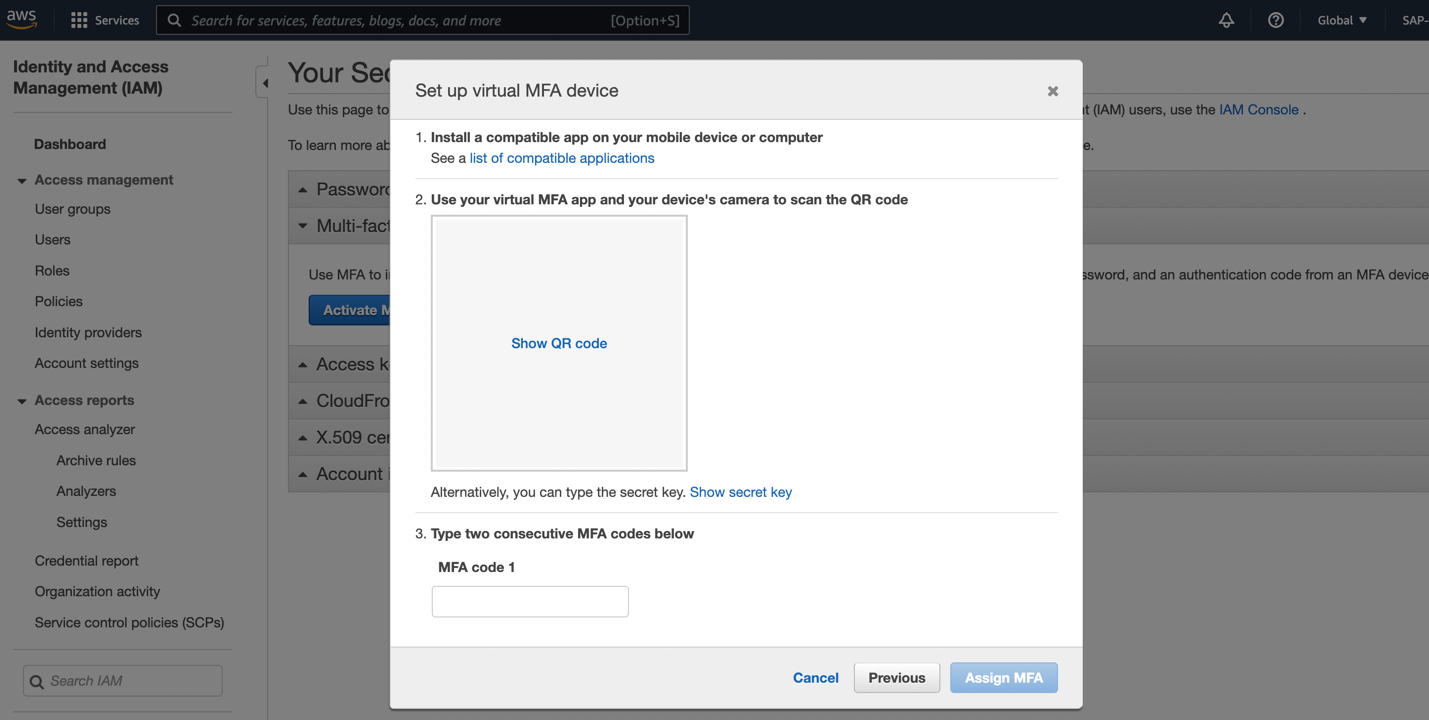


Step 3: MFA can be setup with Virtual/Physical devices. There will be 3 options to choose to proceed for MFA setup as shown in below screen. I selected ‘**Virtual MFA’** device and installed ‘**Microsoft Authenticator’** app in mobile.

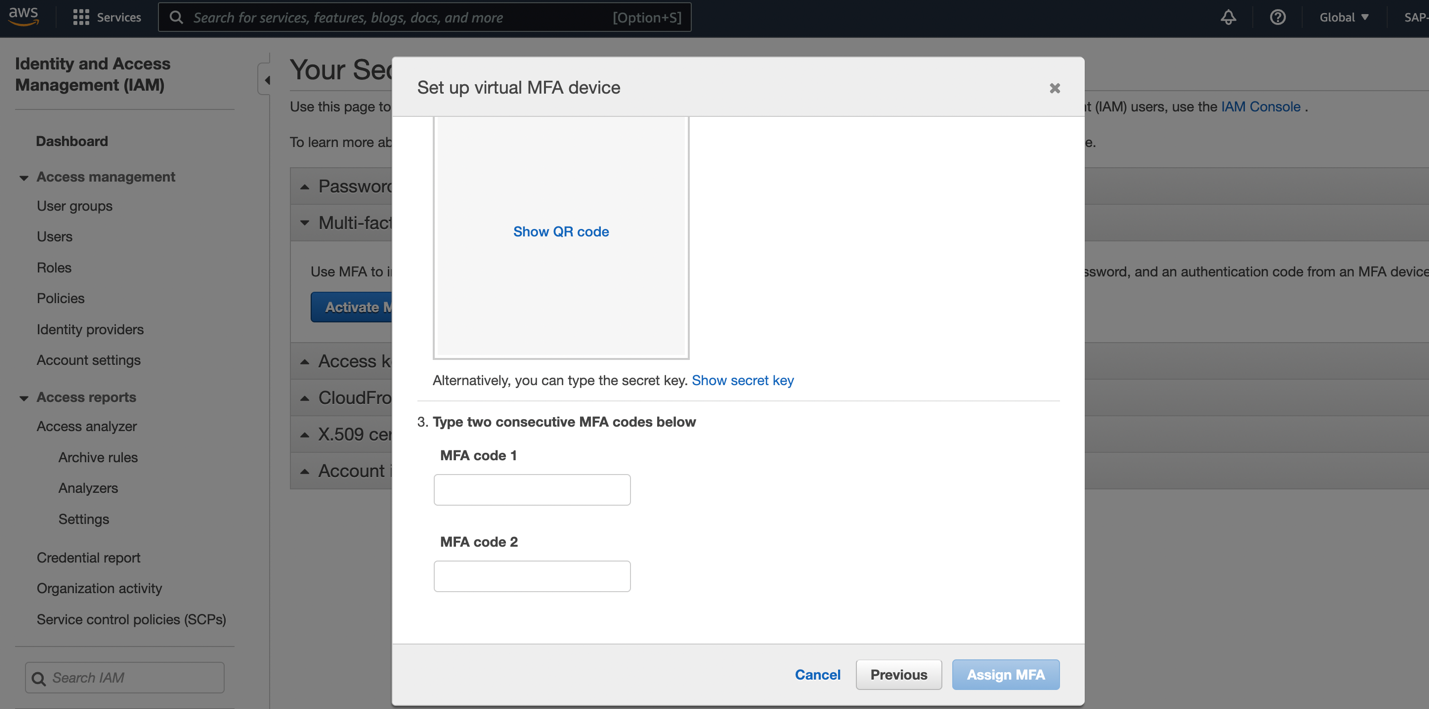


Step 4: After installing the Authenticator app click on ‘**Kebab menu’** (3 vertical dots menu) in the app at top right corner. From the available options choose ‘**+ Add account**’, then click on **personal** or **work** or **other account**. After account selection choose option ‘**Scan a QR code’** from pop-up window.

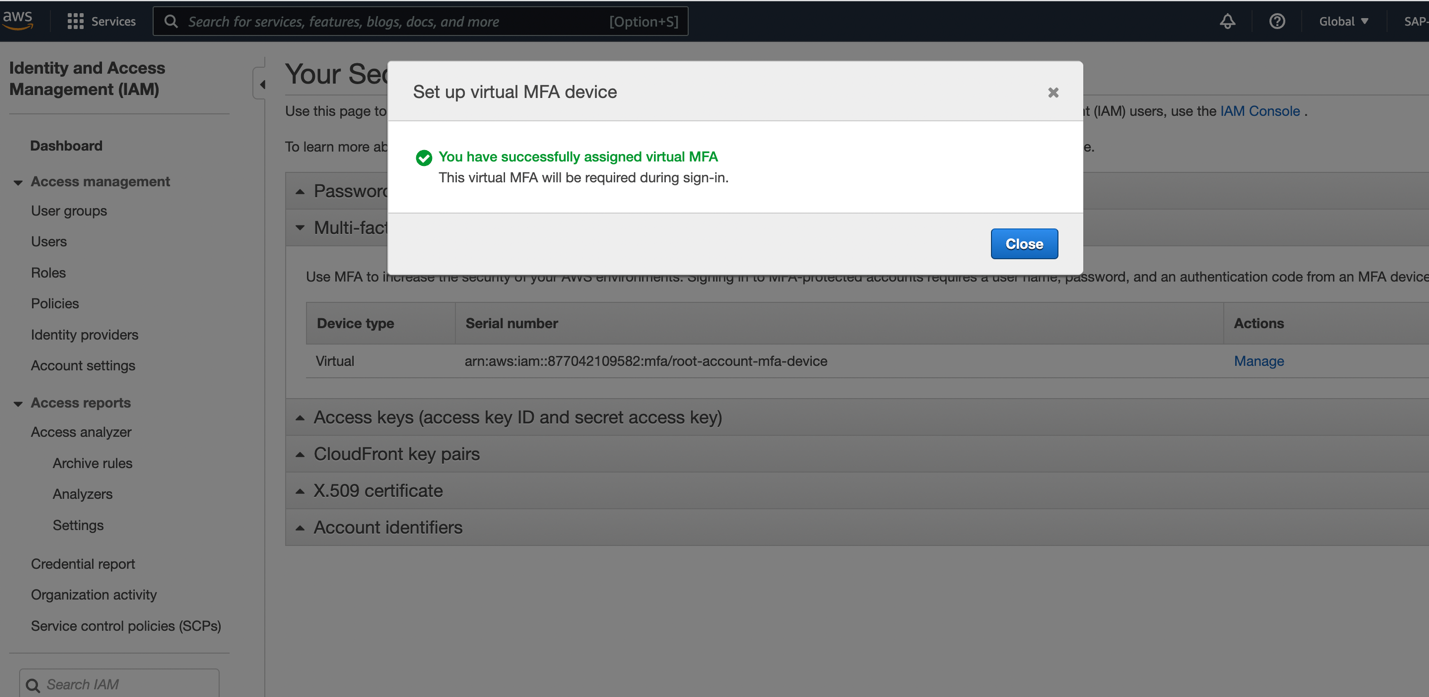
Step 5: Click on the **show QR code** on AWS console screen. Scan the QR code from mobile. After scanning , you will be able to see account alias name/ID in your authenticator app. Click on the AWS account name/ID in app.



Step 6: After every specific duration a code generates in app. We need to put 2 consecutive code in the marked box in below screen ( in 3. Type two consecutive MFA codes below). And click on **‘Assign MFA**’.



After successful setup we will receive ‘Set up virtual MFA device’ message.



Go to IAM dashboard and check ‘**Root user(IAM user if it’s not root account) has MFA’** should have green tick.

After setting up MFA, now whenever user will login to account, user needs to provide MFA from the authenticator App where we have scanned our account QR code.

