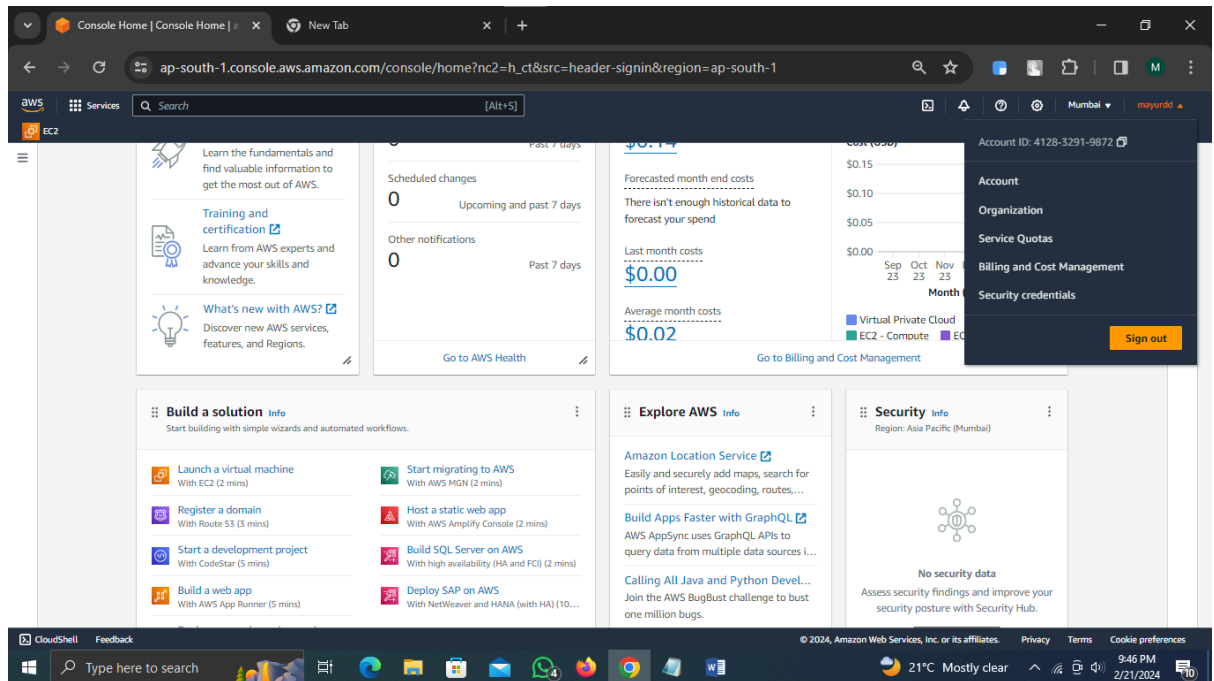
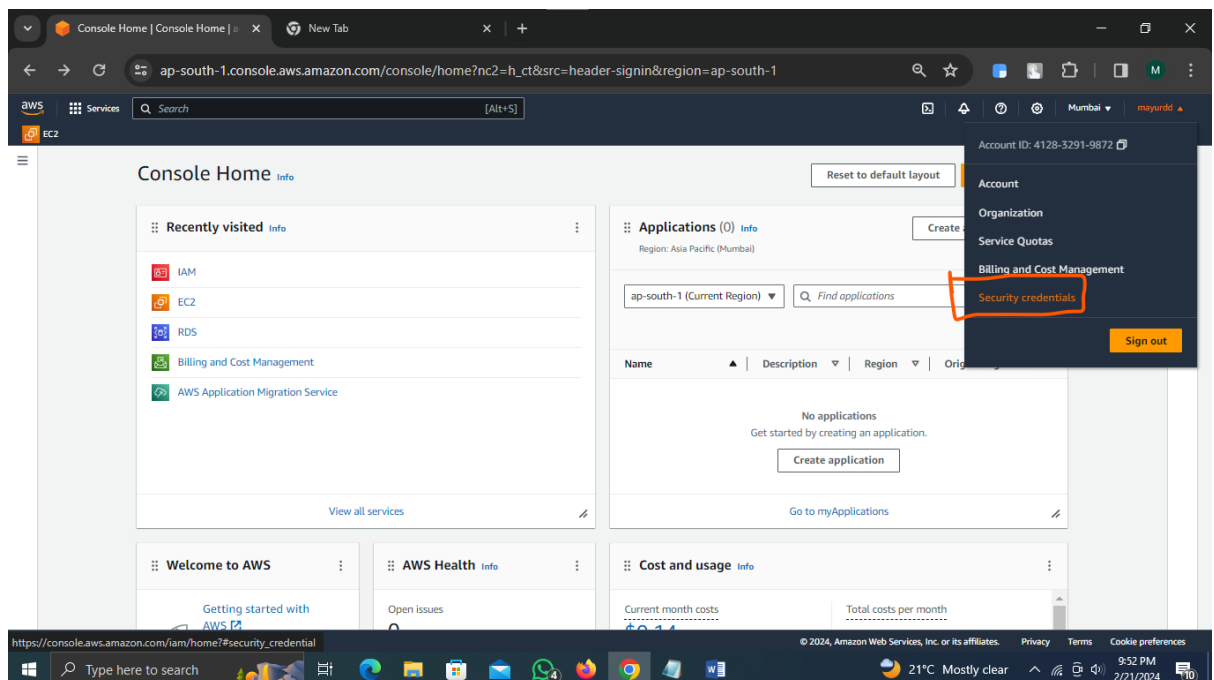


# 1) Assigning mfa to aws root account

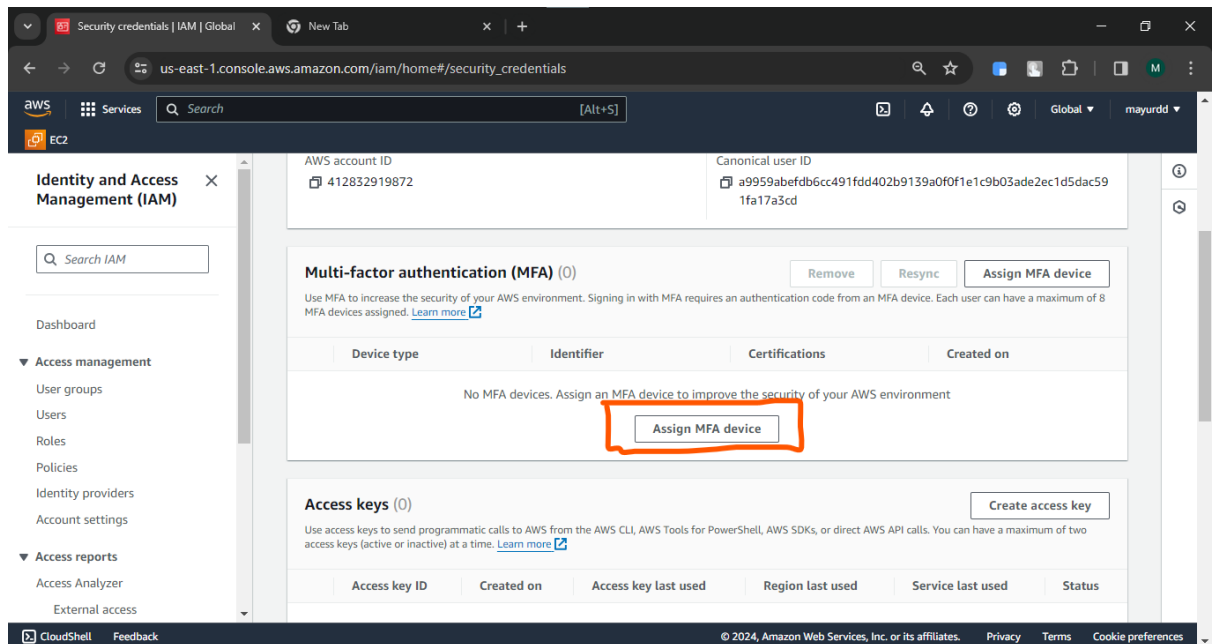
1. Click in right corner of aws dashboard security



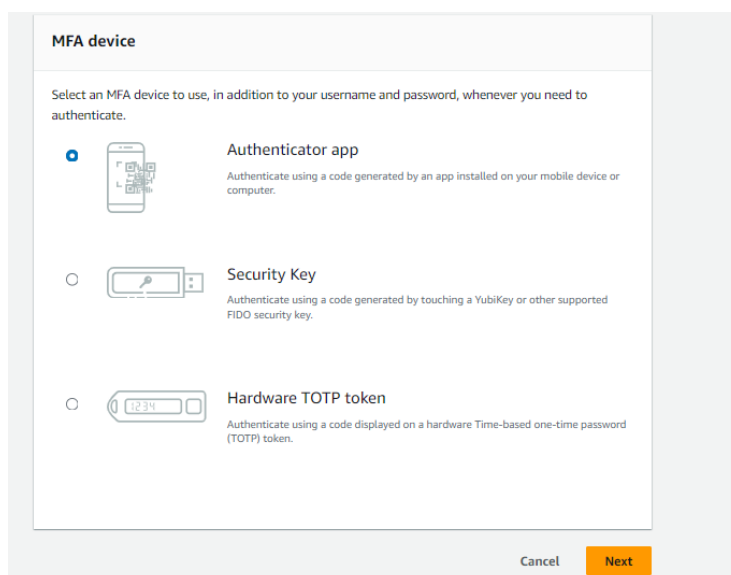
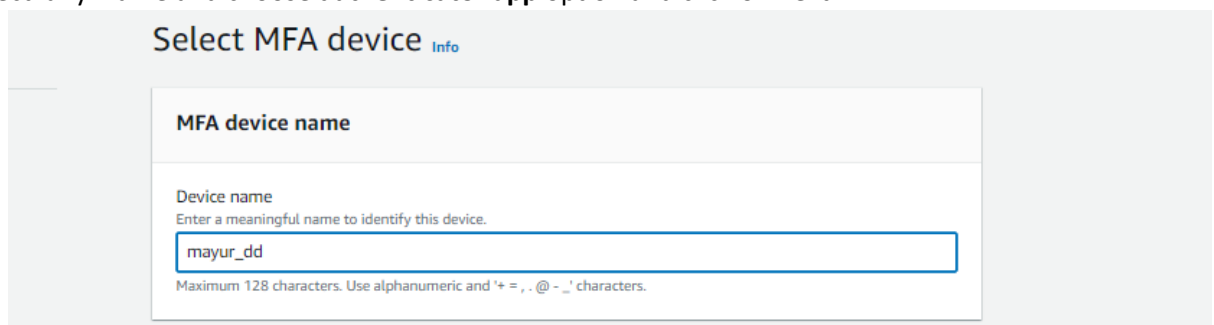
2. Click on security credentials



### 3. Click on Assign MFA device



### 4. Select any name and choose **authenticator app** option and click on next



5. Click on show QR code and enter MFA code (available in Google authenticator app)

IAM > Security credentials > Assign MFA device


Step 1  
[Select MFA device](#)

Step 2  
**Set up device**

## Set up device [Info](#)

### Authenticator app

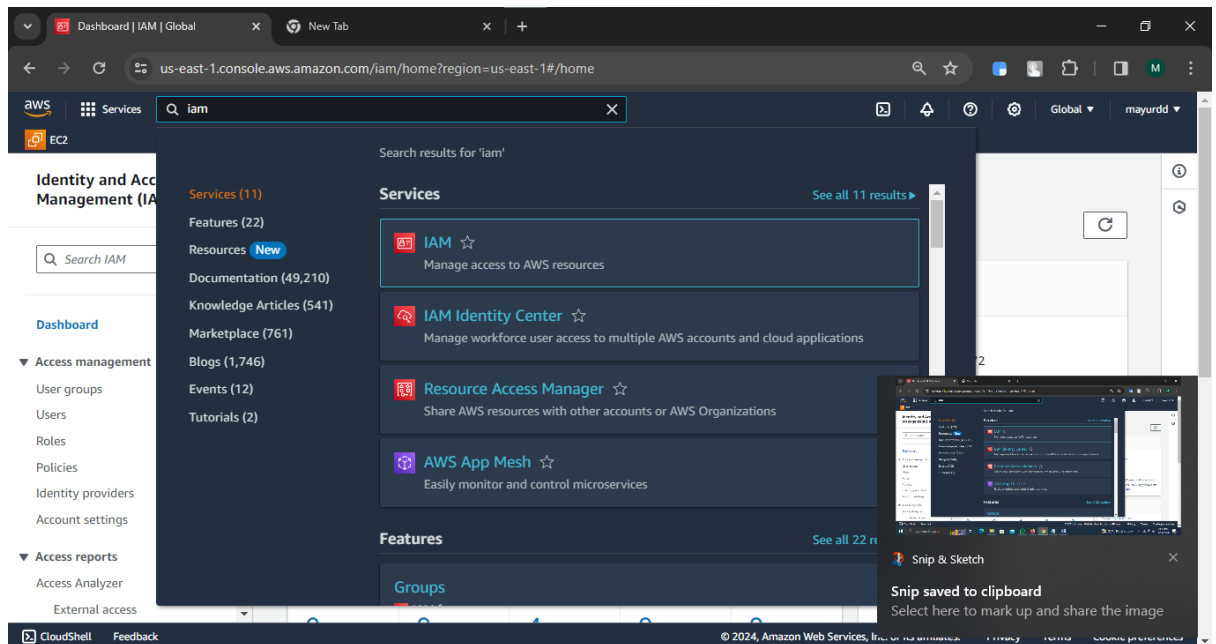
A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

- 1 Install a compatible application such as Google Authenticator, Duo 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](#)
- 3 Fill in two consecutive codes from your MFA device.  
MFA code 1  
  
MFA code 2

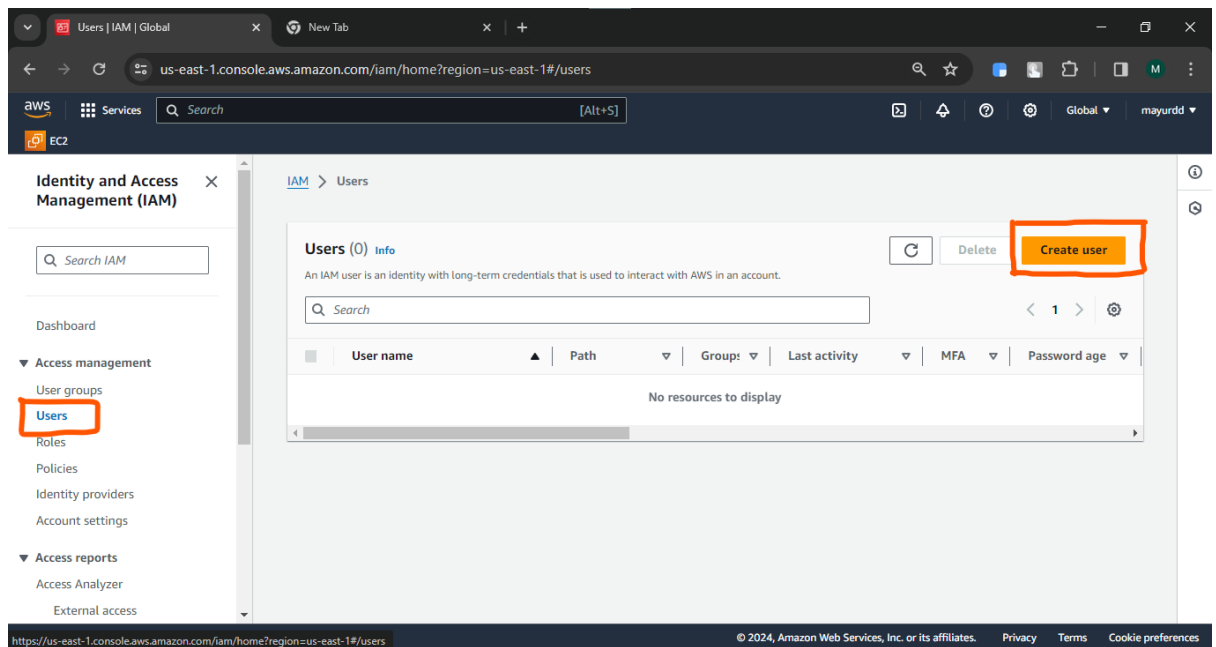
6. #Done

## 2) Creating IAM USER

1. Search IAM service and click on it



2. Click on **user** option and **create user** option



### 3. Enter any username as per your choice

The screenshot shows the 'Specify user details' step in the AWS IAM console. The breadcrumb navigation is 'IAM > Users > Create user'. The left sidebar shows three steps: 'Step 1 Specify user details' (active), 'Step 2 Set permissions', and 'Step 3 Review and create'. The main heading is 'Specify user details'. Under 'User details', the 'User name' field contains 'mayur\_temp'. A note below the field states: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ \_ - (hyphen)'. There is an unchecked checkbox for 'Provide user access to the AWS Management Console - optional' with a sub-note: 'If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.' A blue information box contains a note about generating access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, with a 'Learn more' link. At the bottom right are 'Cancel' and 'Next' buttons.

Note :- providing aws console is optional

### 4. Set permission as shown in diagram

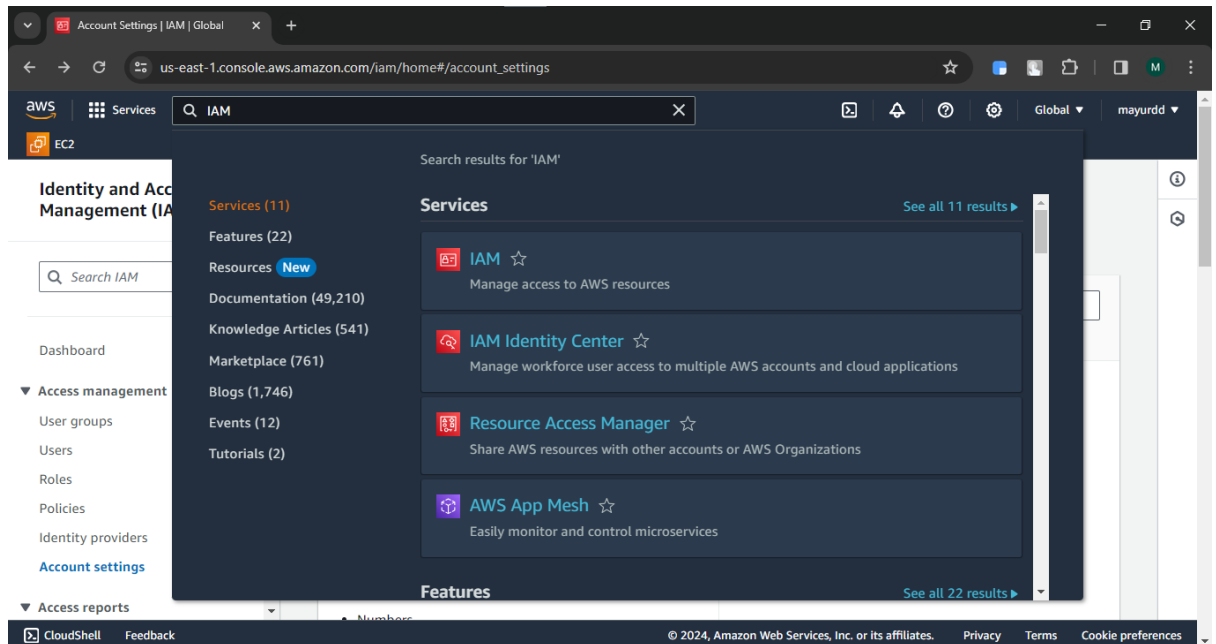
The screenshot shows the 'Set permissions' step in the AWS IAM console. The breadcrumb navigation is 'IAM > Users > Create user'. The left sidebar shows three steps: 'Step 1 Specify user details', 'Step 2 Set permissions' (active), and 'Step 3 Review and create'. The main heading is 'Set permissions'. A sub-heading reads: 'Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more'. Under 'Permissions options', there are three radio buttons: 'Add user to group' (selected), 'Copy permissions', and 'Attach policies directly'. The 'Add user to group' option has a sub-note: 'Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.' The 'Copy permissions' option has a sub-note: 'Copy all group memberships, attached managed policies, and inline policies from an existing user.' The 'Attach policies directly' option has a sub-note: 'Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.' Below these options is a blue information box with a 'Get started with groups' section, containing a note: 'Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more'. A 'Create group' button is next to this box. At the bottom is a section for 'Set permissions boundary - optional'. At the bottom right are 'Cancel', 'Previous', and 'Next' buttons.

### 5. Click on create user

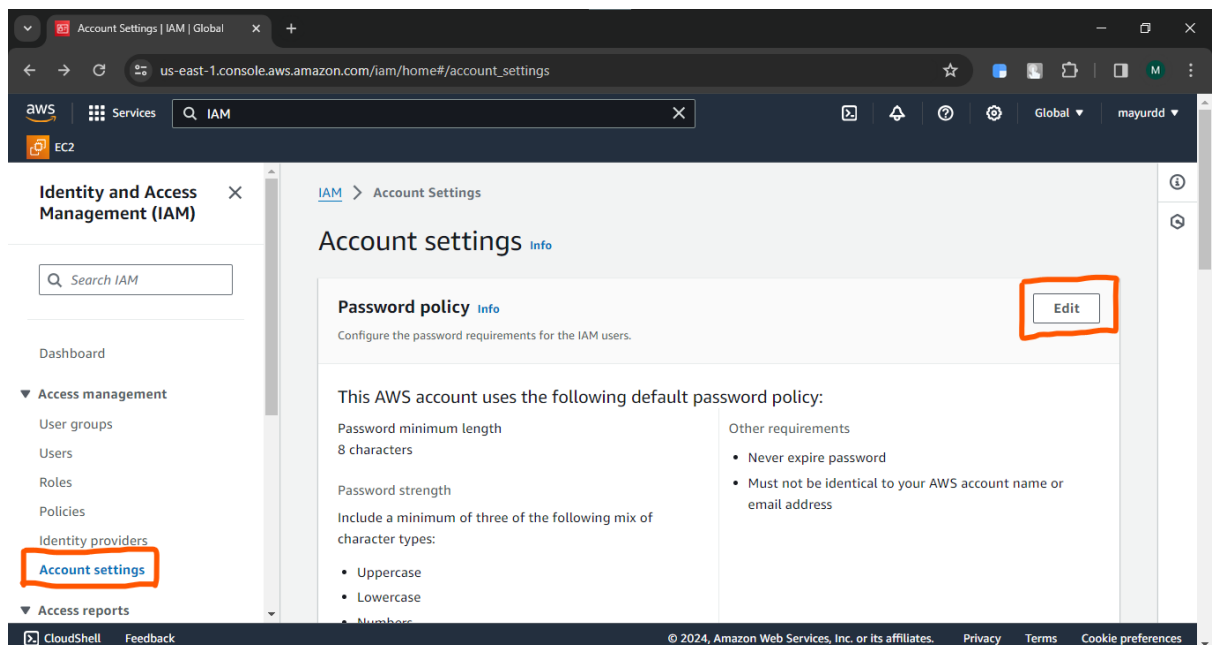
The screenshot shows the 'Review and create' step in the AWS IAM console. The breadcrumb navigation is 'IAM > Users > Create user'. The left sidebar shows three steps: 'Step 1 Specify user details', 'Step 2 Set permissions', and 'Step 3 Review and create' (active). The main heading is 'Review and create'. A sub-heading reads: 'Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.' Under 'User details', there are three fields: 'User name' (mayur\_temp), 'Console password type' (None), and 'Require password reset' (No). Under 'Permissions summary', there is a table with columns 'Name', 'Type', and 'Used as'. The table is empty, with a note 'No resources' below it. Under 'Tags - optional', there is a note: 'Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.' Below this note is a section for 'No tags associated with the resource.' and an 'Add new tag' button. At the bottom right are 'Cancel', 'Previous', and 'Create user' buttons.

### 3) Assigning Custom Password to IAM user

1. Search IAM service and click on it



2. Click on **Account settings** and also click on **edit** option



3. Click on **custom**

[IAM](#) > [Account Settings](#) > Edit password policy

## Edit password policy [Info](#)

**Password policy**

☐ IAM default  
Apply default password requirements.

☒ Custom  
Apply customized password requirements.

4. Select options as per your requirement and click on **Save changes**

☐ IAM default  
Apply default password requirements.

☒ Custom  
Apply customized password requirements.

**Password minimum length.**  
Enforce a minimum length of characters.

characters

Needs to be between 6 and 128.

**Password strength**

- ☒ Require at least one uppercase letter from the Latin alphabet (A-Z)
- ☒ Require at least one lowercase letter from the Latin alphabet (a-z)
- ☒ Require at least one number
- ☒ Require at least one non-alphanumeric character (!@#\$%^&\*()\_+-=[]{}|')

**Other requirements**

- ☒ Turn on password expiration
  - Expire password in  day(s)
  - Needs to be between 1 and 1095 days.
- ☒ Password expiration requires administrator reset
- ☒ Allow users to change their own password
- ☒ Prevent password reuse
  - Remember  password(s)
  - Needs to be between 1 and 24.

[Cancel](#) [Save changes](#)

5. #Done