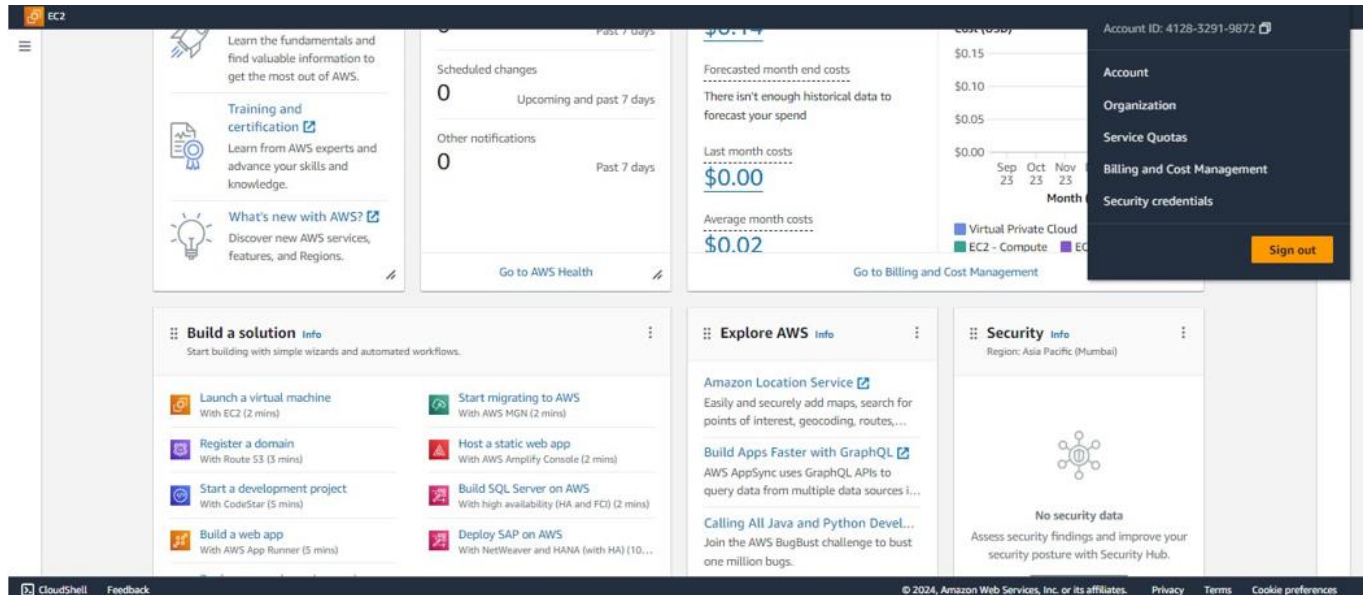
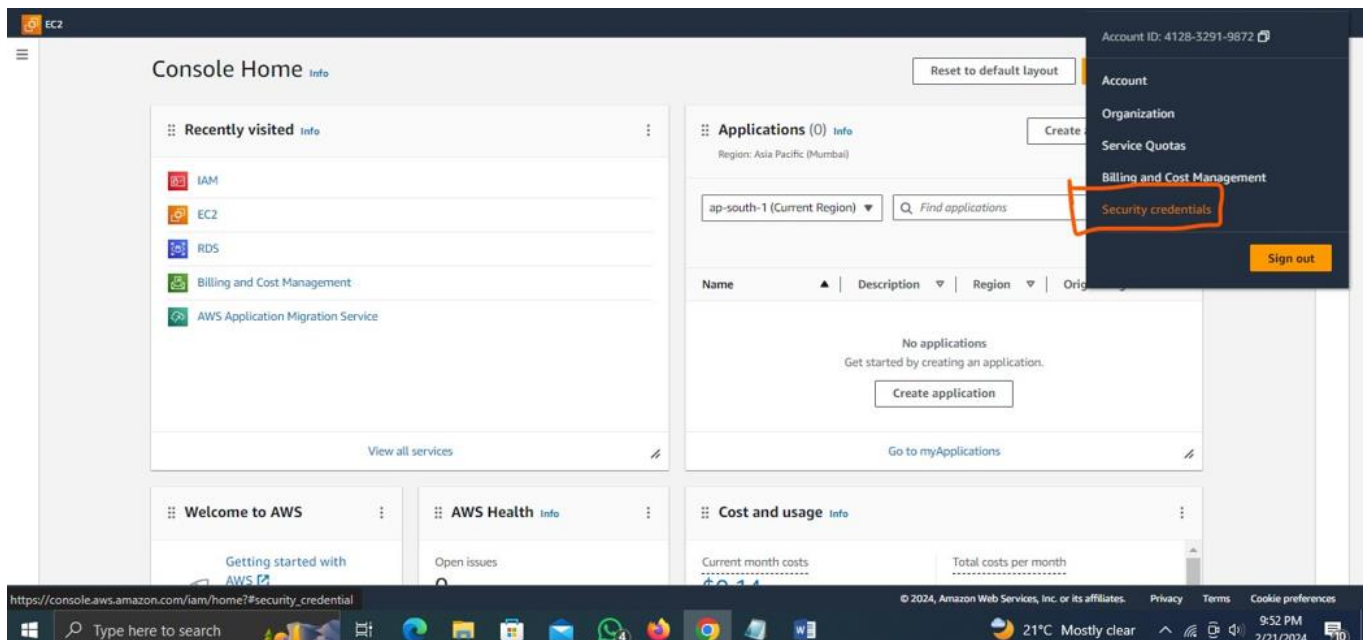


1) Assigning mfa to aws root account

1. Click in right corner of aws dashboard security



2. Click on security credentials



3. Click on Assign MFA device

The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with 'Identity and Access Management (IAM)' selected. The main content area displays the 'Multi-factor authentication (MFA)' section for a user. It includes fields for 'AWS account ID' and 'Canonical user ID'. Below these, there's a section for MFA with buttons for 'Remove', 'Resync', and 'Assign MFA device'. A table below shows no existing MFA devices, with a message: 'No MFA devices. Assign an MFA device to improve the security of your AWS environment'. The 'Assign MFA device' button in this message is highlighted with an orange rectangle. Below the MFA section is the 'Access keys' section with a 'Create access key' button. The footer shows 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc.

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

The screenshot shows the 'Select MFA device' dialog box. It has a title 'Select MFA device' with an 'Info' link. Below the title is a section 'MFA device name'. Inside this section, there's a label 'Device name' and a prompt 'Enter a meaningful name to identify this device.' Below the prompt is a text input field containing the text 'mayur_dd'. At the bottom of the input field, there's a note: 'Maximum 128 characters. Use alphanumeric and '+', '=', '@', '-', '_' characters.'

The screenshot shows the 'MFA device' selection screen. It has a title 'MFA device'. Below the title is a prompt: 'Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.' There are three options, each with a radio button, an icon, and a description: 1. 'Authenticator app' (selected) with a smartphone icon and description: 'Authenticate using a code generated by an app installed on your mobile device or computer.' 2. 'Security Key' with a security key icon and description: 'Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.' 3. 'Hardware TOTP token' with a TOTP token icon and description: 'Authenticate using a code displayed on a hardware Time-based one-time password (TOTP) token.' At the bottom right are 'Cancel' and 'Next' buttons.

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

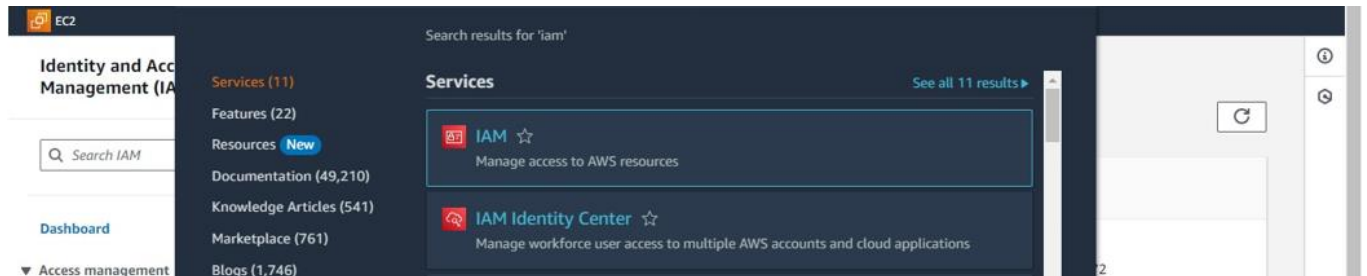
A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

- 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:

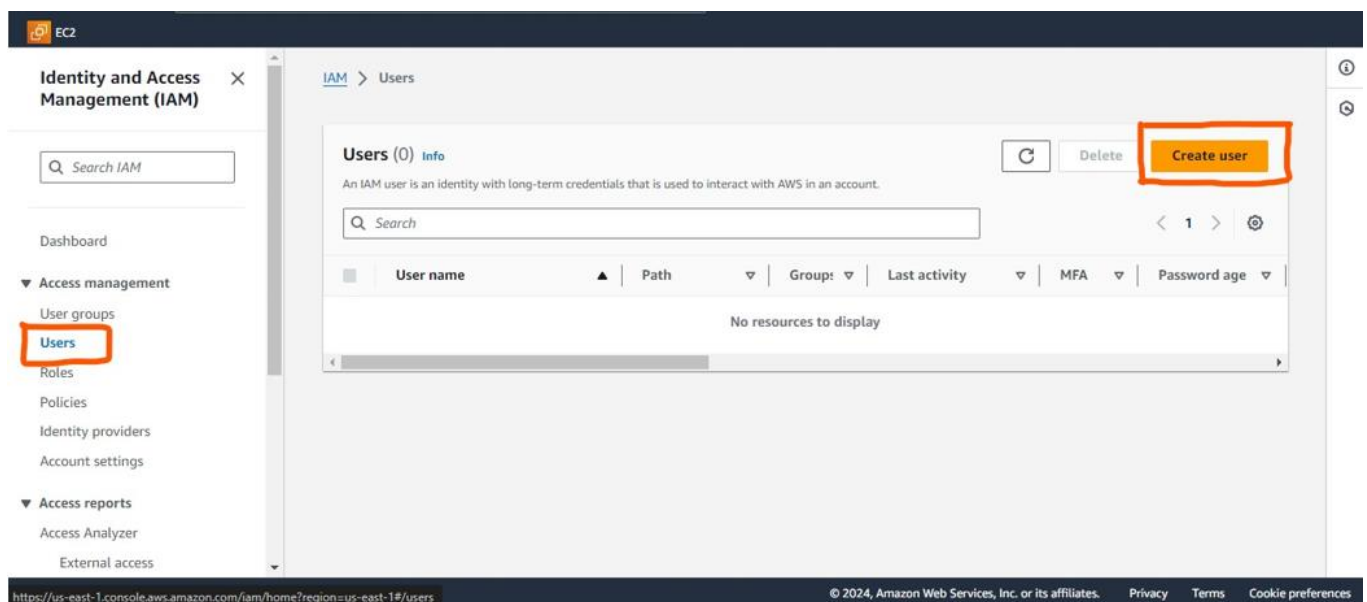
6. #Done

2) Creating IAM USER

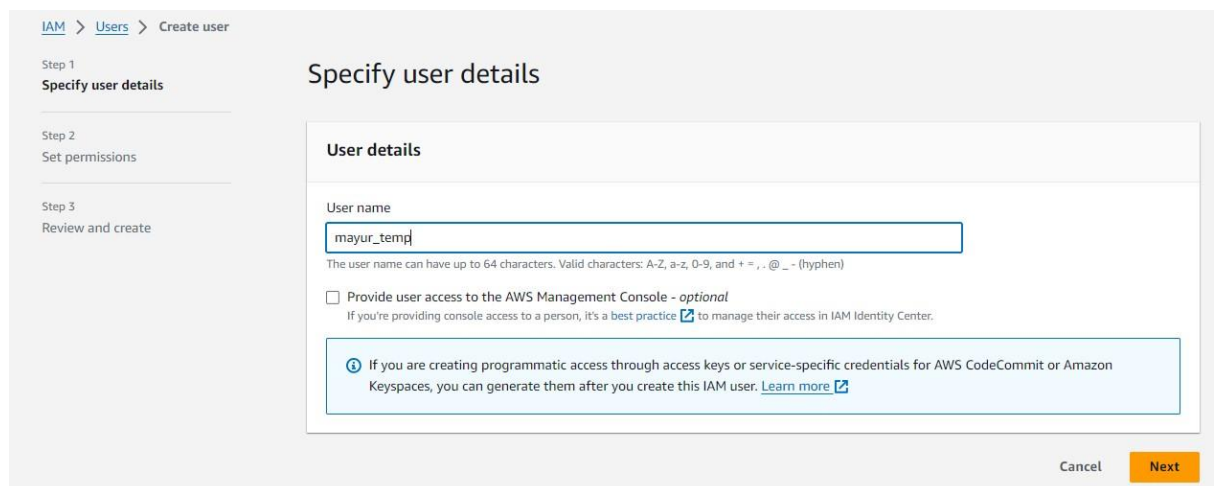
1. Search IAM service and click on it



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



3. Enter any username as per your choice



Note :- providing aws console is optional

4. Set permission as shown in diagram

The screenshot shows the 'Set permissions' step of the AWS IAM 'Create user' wizard. The breadcrumb navigation at the top reads 'IAM > Users > Create user'. On the left, a sidebar indicates the current step: 'Step 2 Set permissions'. The main heading is 'Set permissions', followed by a subtext: '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](#)'. Below this, there are three radio button options under the heading 'Permissions options':

- Add user to group** (selected): 'Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.'
- Copy permissions**: 'Copy all group memberships, attached managed policies, and inline policies from an existing user.'
- Attach policies directly**: '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 box with an information icon and the heading 'Get started with groups'. It contains the text: '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](#)'. To the right of this box is a 'Create group' button. At the bottom of the main content area, there is a link: '► Set permissions boundary - optional'. At the bottom right of the page are three buttons: 'Cancel', 'Previous', and 'Next'.

5. Click on create user

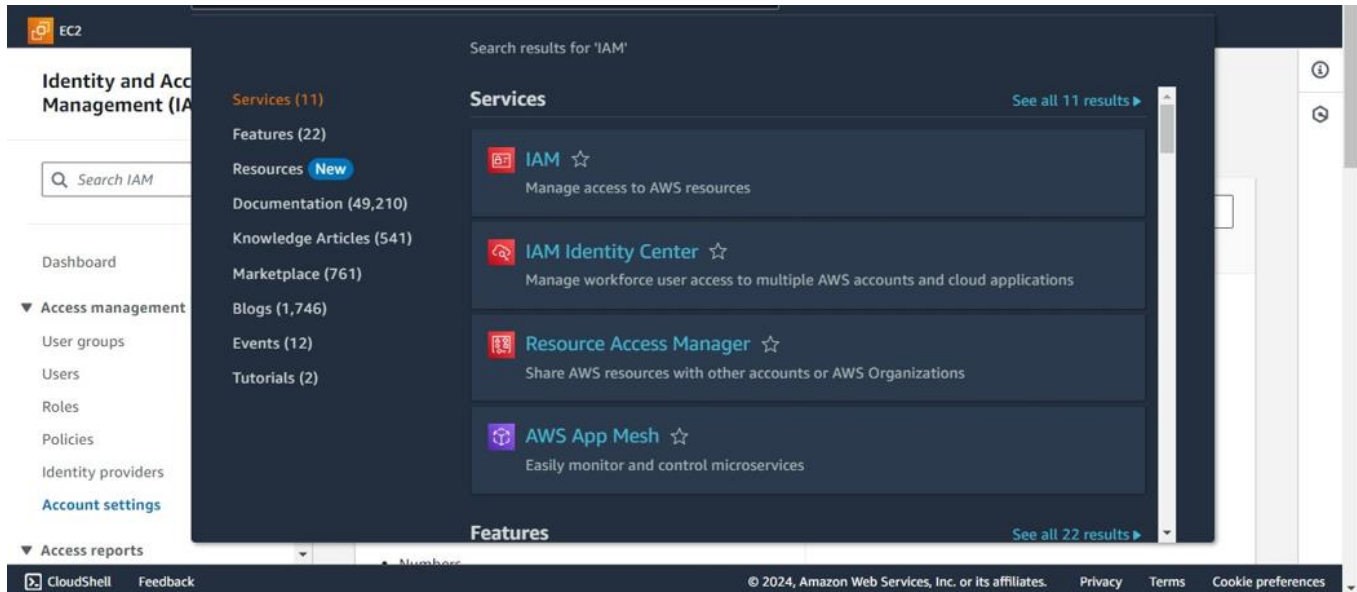
The screenshot shows the 'Review and create' step of the AWS IAM 'Create user' wizard. The breadcrumb navigation at the top reads 'IAM > Users > Create user'. On the left, a sidebar indicates the current step: 'Step 3 Review and create'. The main heading is 'Review and create', followed by a subtext: 'Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.' Below this, there are three sections:

- User details**: A table with three columns: 'User name' (value: 'magyar_temp'), 'Console password type' (value: 'None'), and 'Require password reset' (value: 'No').
- Permissions summary**: A table with three columns: 'Name', 'Type', and 'Used as'. The table is currently empty, with the text 'No resources' displayed below it.
- Tags - optional**: A section with the text: '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 text is a button labeled 'Add new tag' and a note: 'You can add up to 50 more tags.'

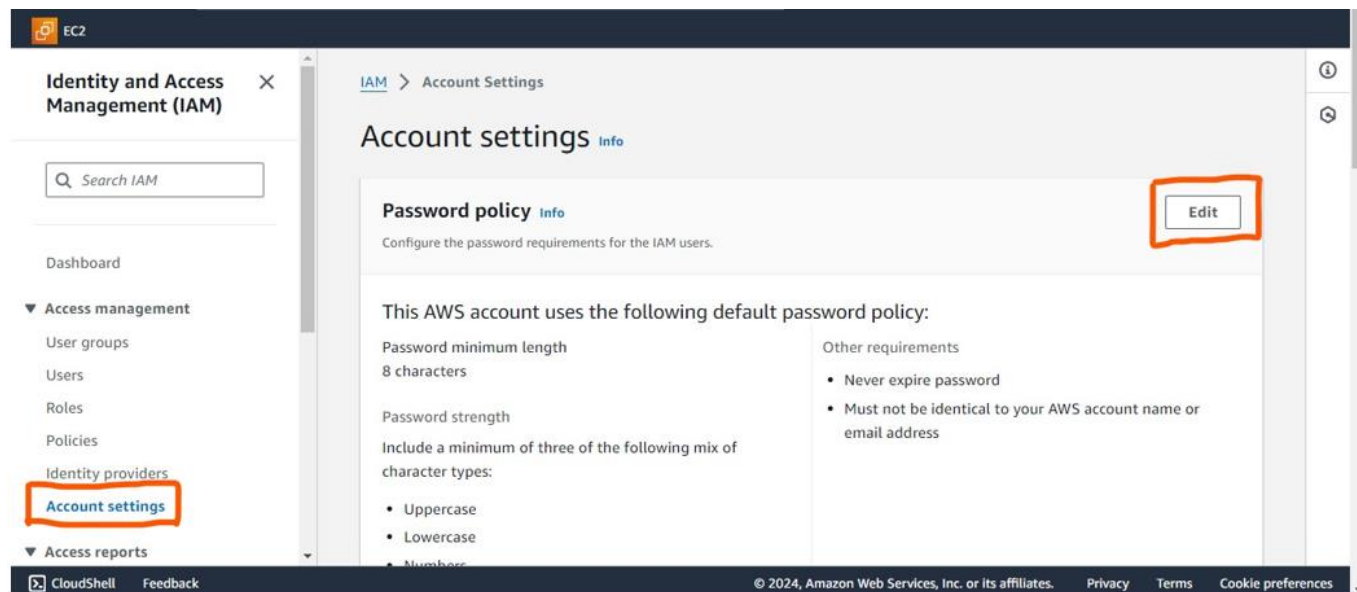
At the bottom right of the page are three buttons: 'Cancel', 'Previous', and 'Create user'.

3) Assigning Custom Password to IAM user

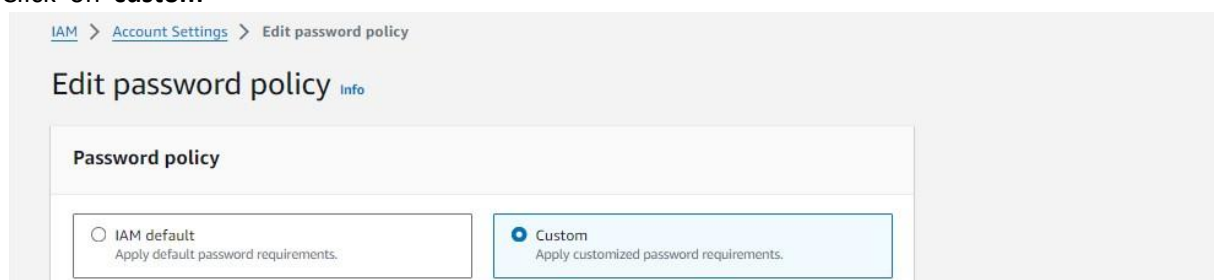
1. Search **IAM** service and click on it



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



3. Click on **custom**



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