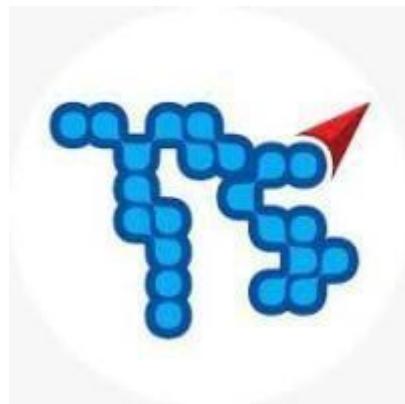


SOP0001 IAM & MFA CREATION

Document Version / Détails : Ver 0.1

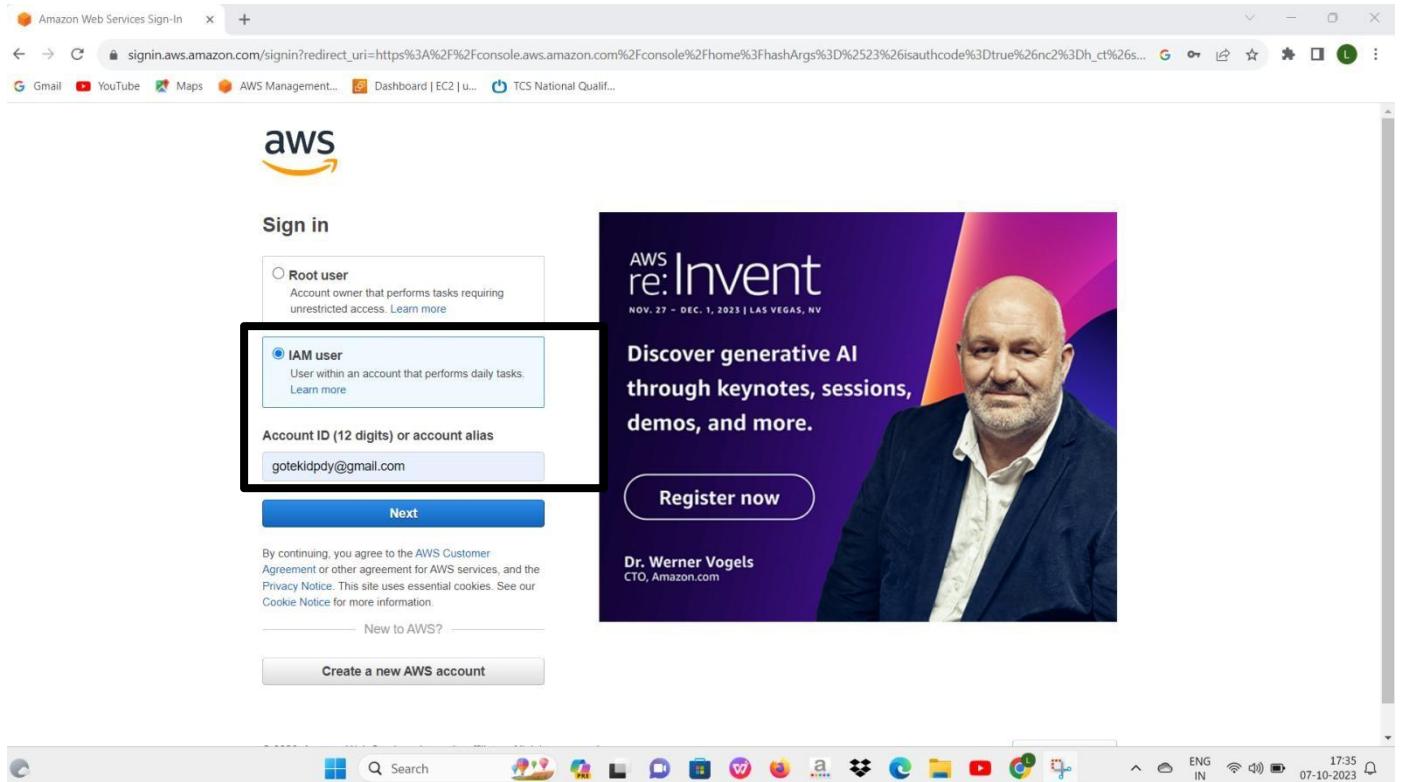


Record of Release

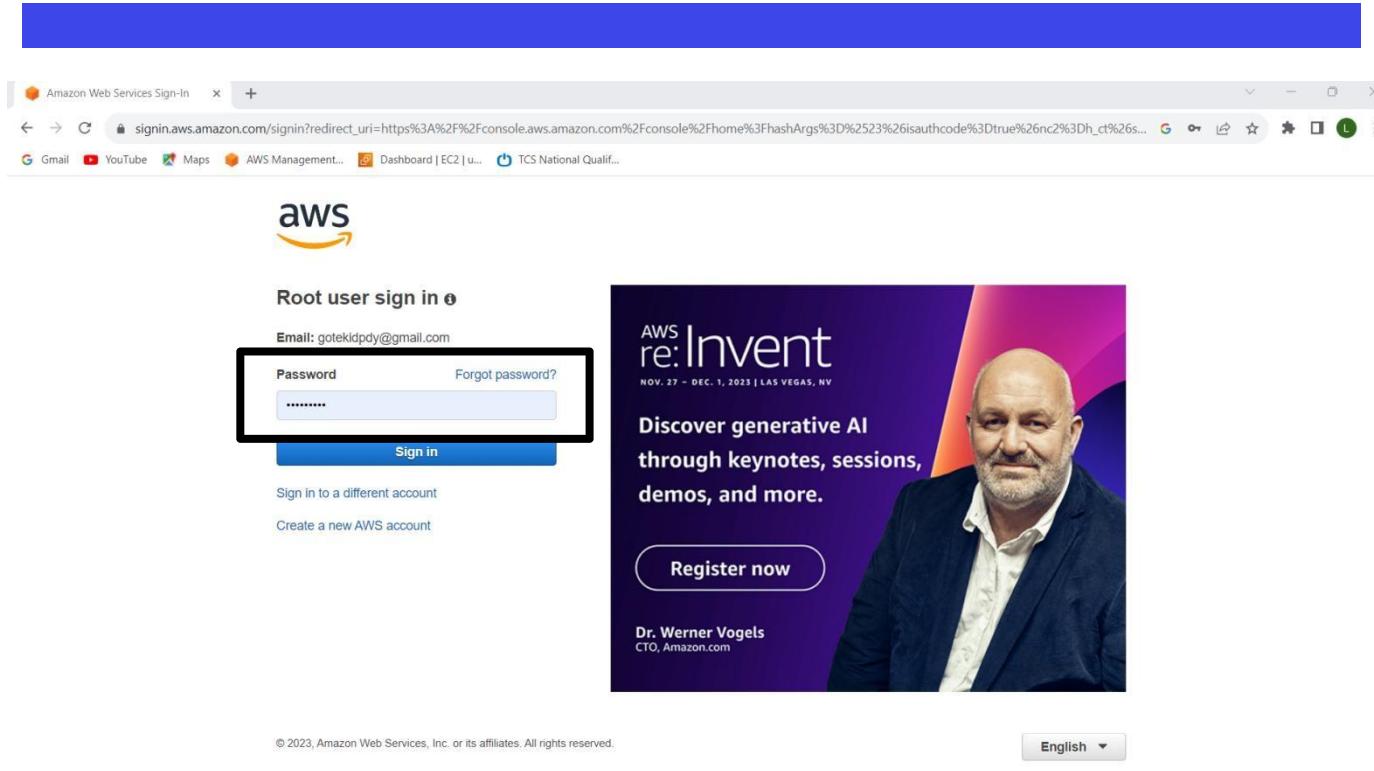
Version No.	Modified By	Reviewed By	Authorized By	Release Date	Modifications Done
0.1					Initial Version
1.0					
1.1					

1.0 Objective

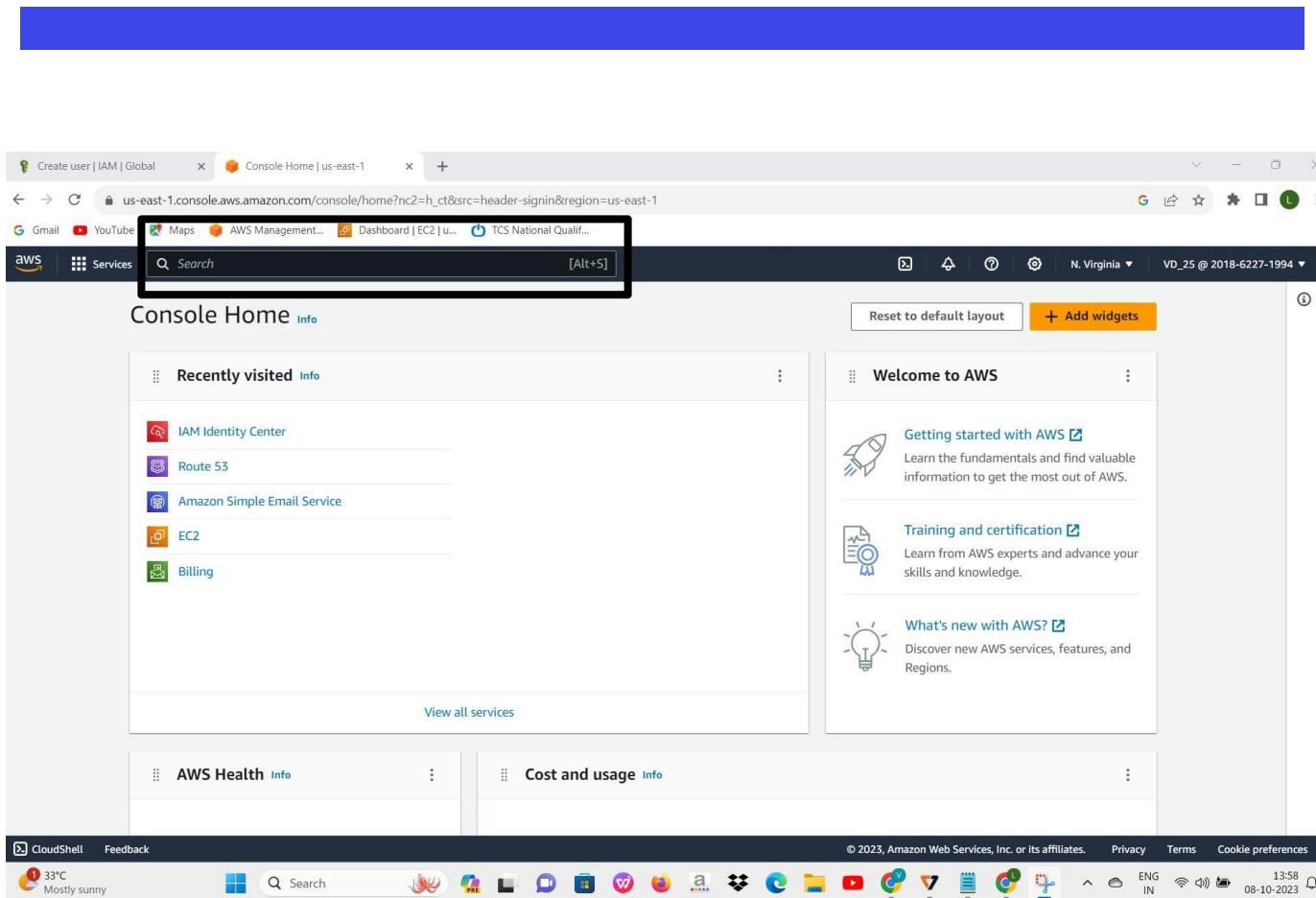
The objective of this document is to the IAM & MFA creation .



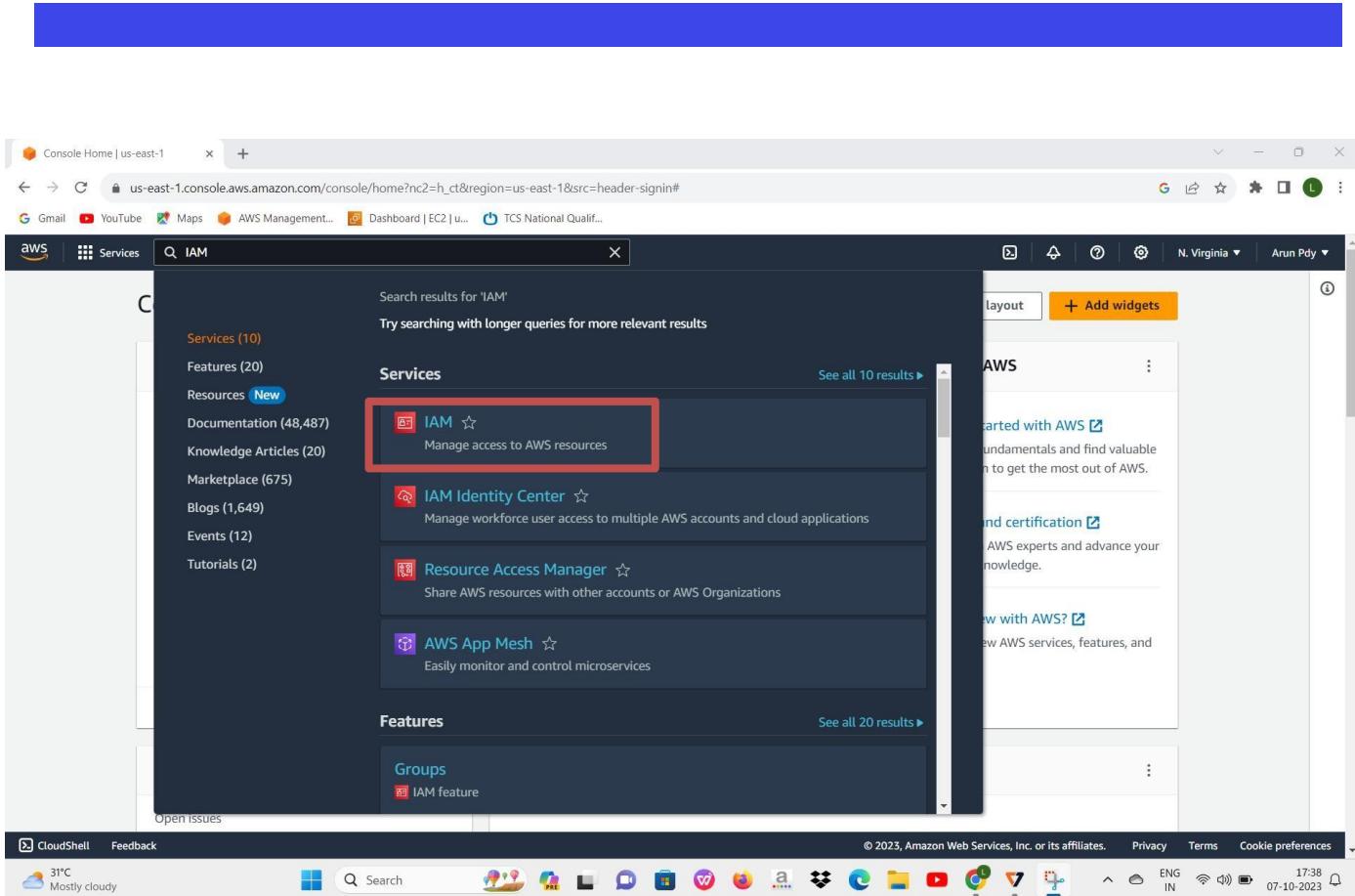
- Go with sign page .
<https://console.aws.amazon.com/ec2/>
- Sign with the root user .
- Enter your email id .



- Enter your password .
- Then sign up .



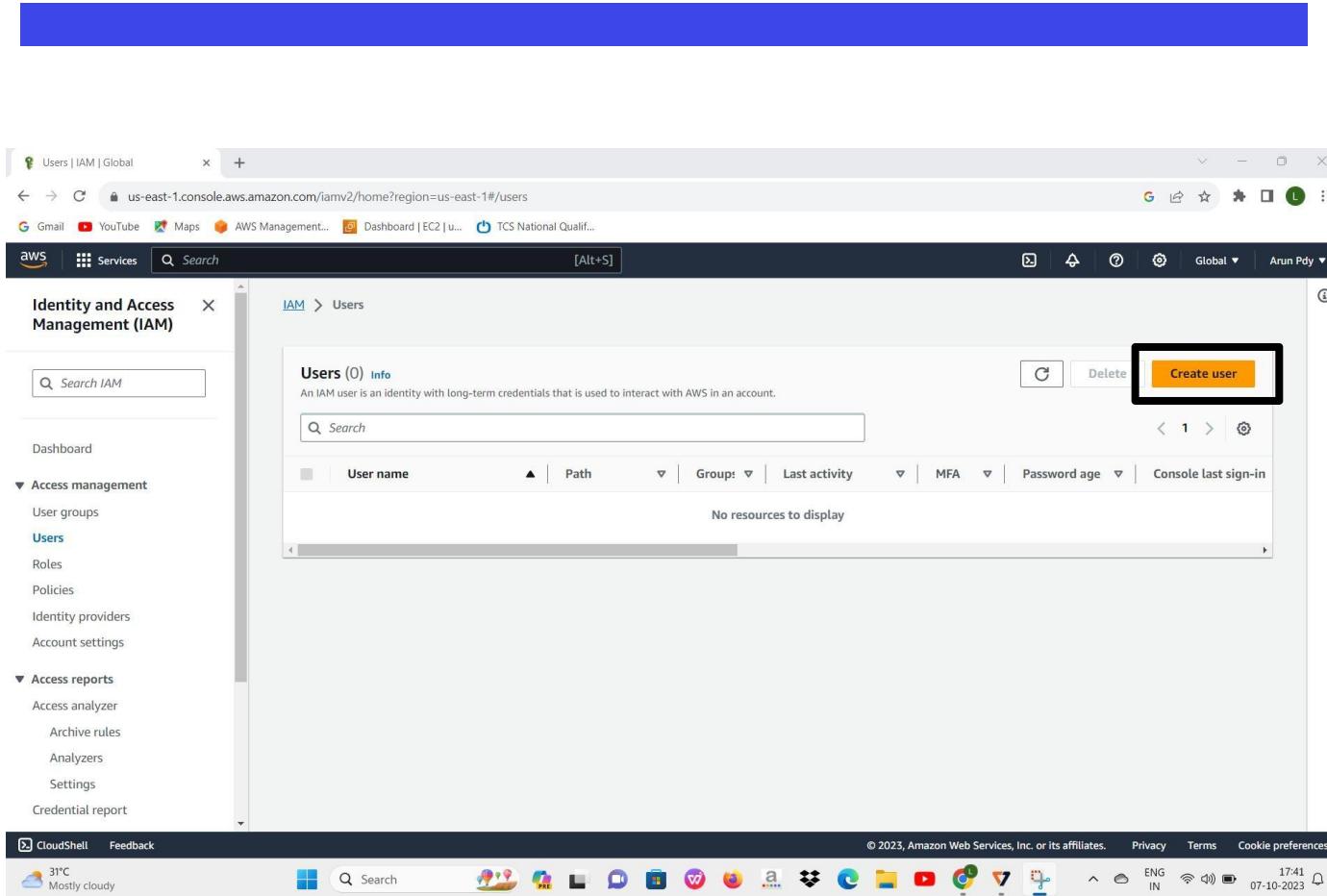
- In the Search box type IAM



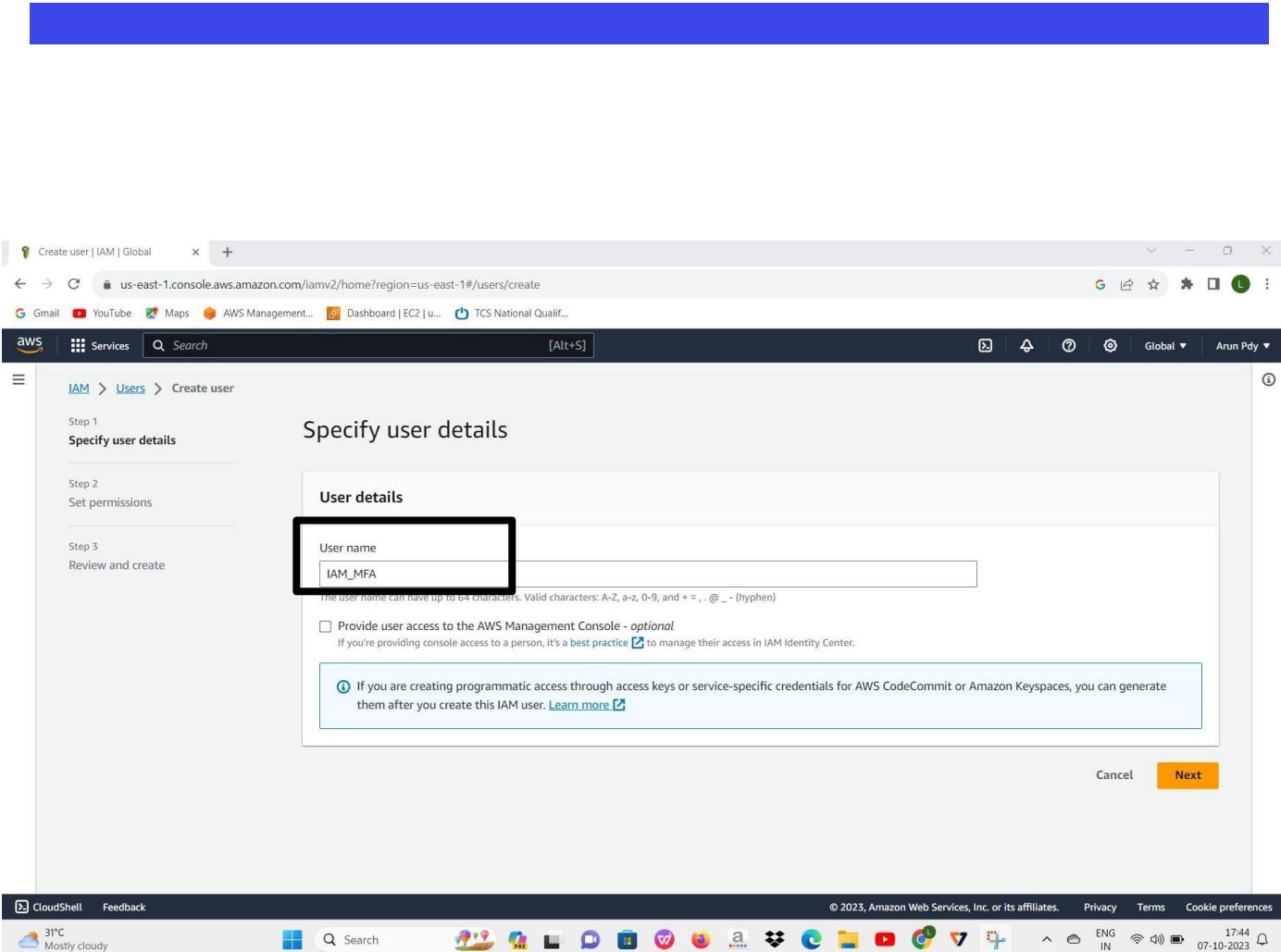
- Click the IAM .

The screenshot shows the AWS IAM Dashboard. On the left, a sidebar menu includes 'Identity and Access Management (IAM)', 'Dashboard', 'Access management' (with 'Users' selected), 'Access reports', and 'Credential report'. The main content area displays 'Security recommendations' with two items: 'Add MFA for root user' (warning icon) and 'Root user has no active access keys' (info icon). Below this is a 'IAM resources' section with a table showing 0 User groups, 0 Users, 2 Roles, 0 Policies, and 0 Identity providers. To the right, there's a 'AWS Account' panel with account ID (201862271994), alias (Create), and sign-in URL (https://201862271994.signin.aws.amazon.com/console). A 'Quick Links' panel includes 'My security credentials' (Manage access keys, MFA, other credentials). The bottom navigation bar includes CloudShell, Feedback, a search bar, and various browser icons.

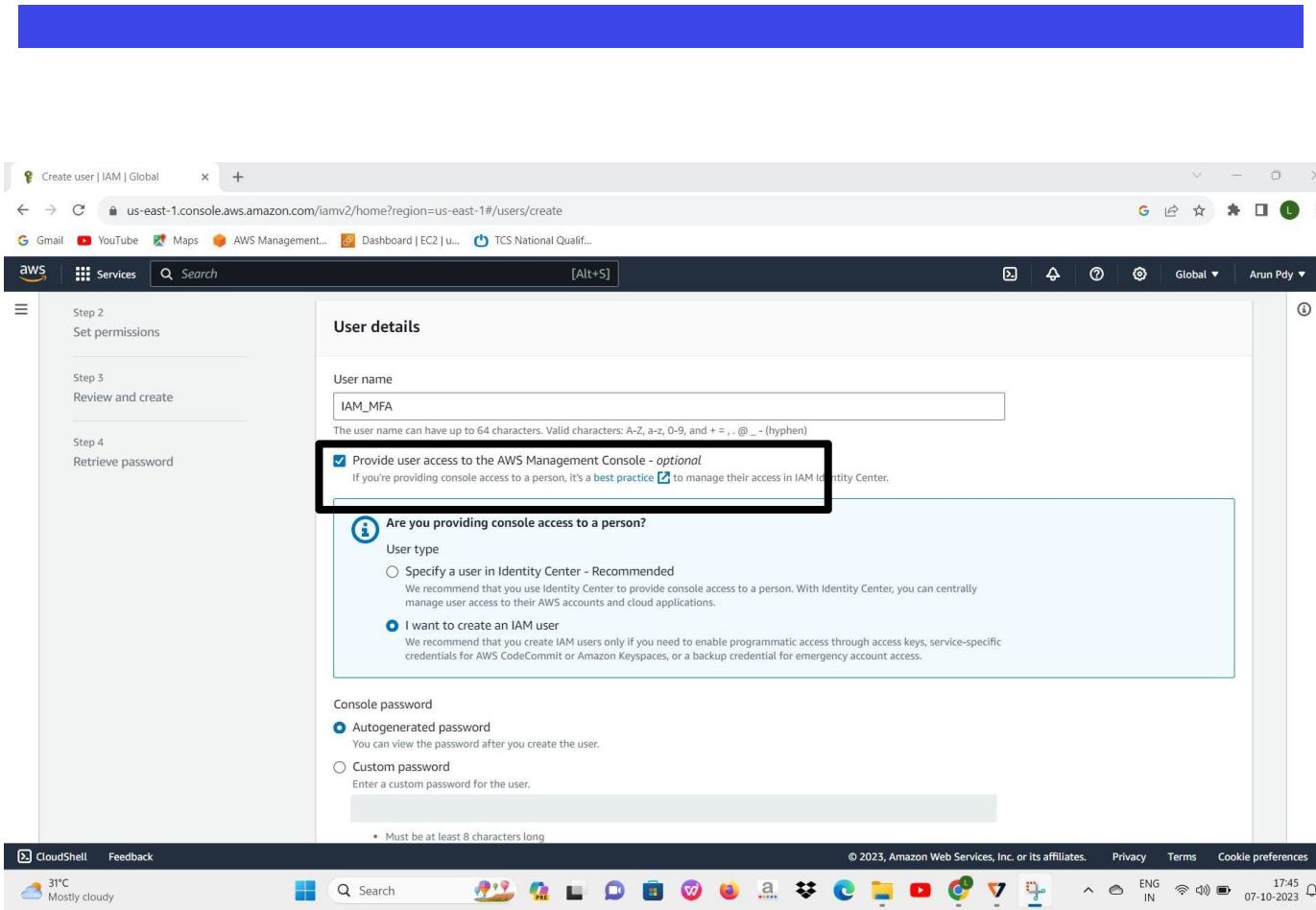
- Click The users.



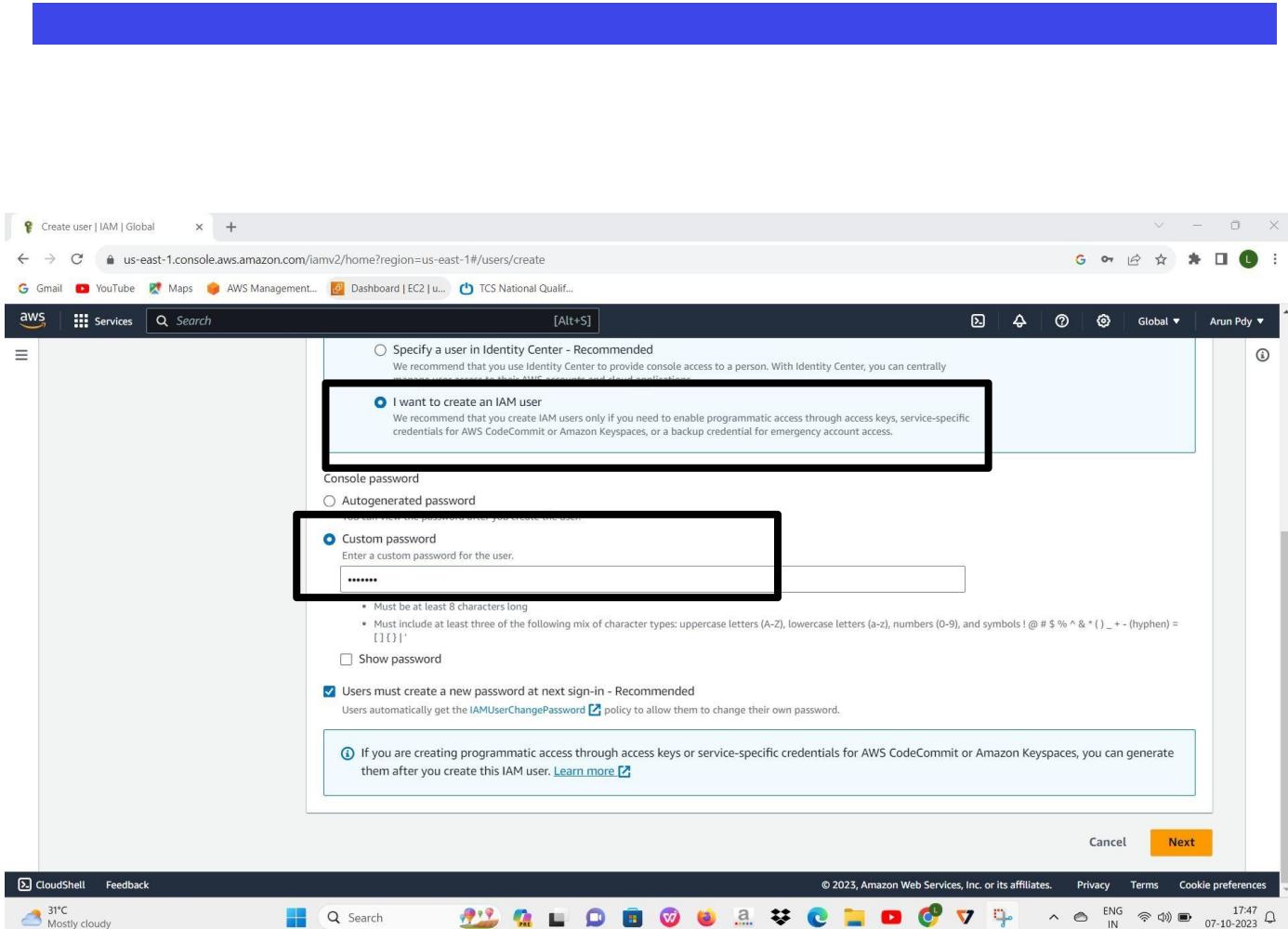
- Click the create user.



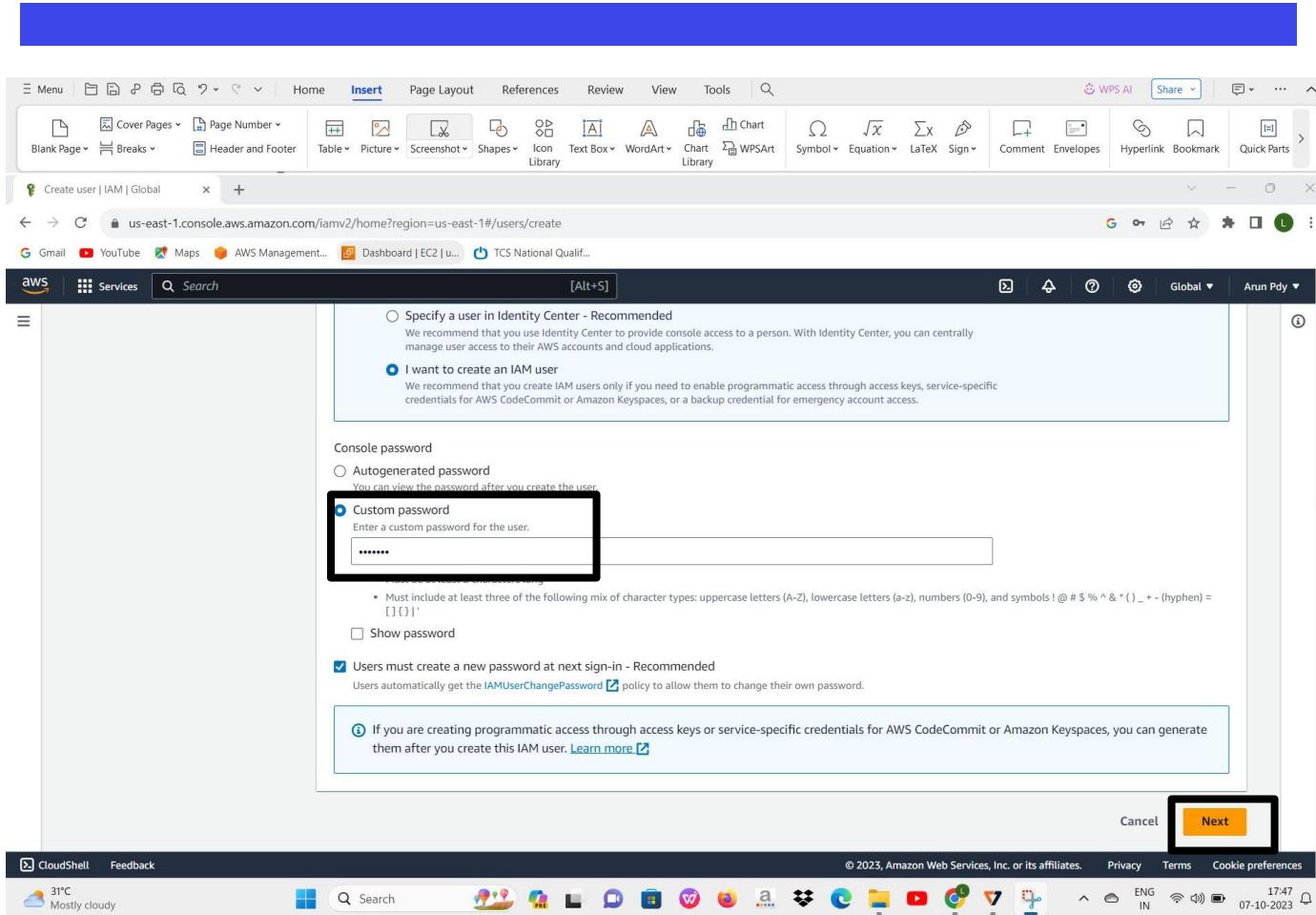
- Enter the user name.



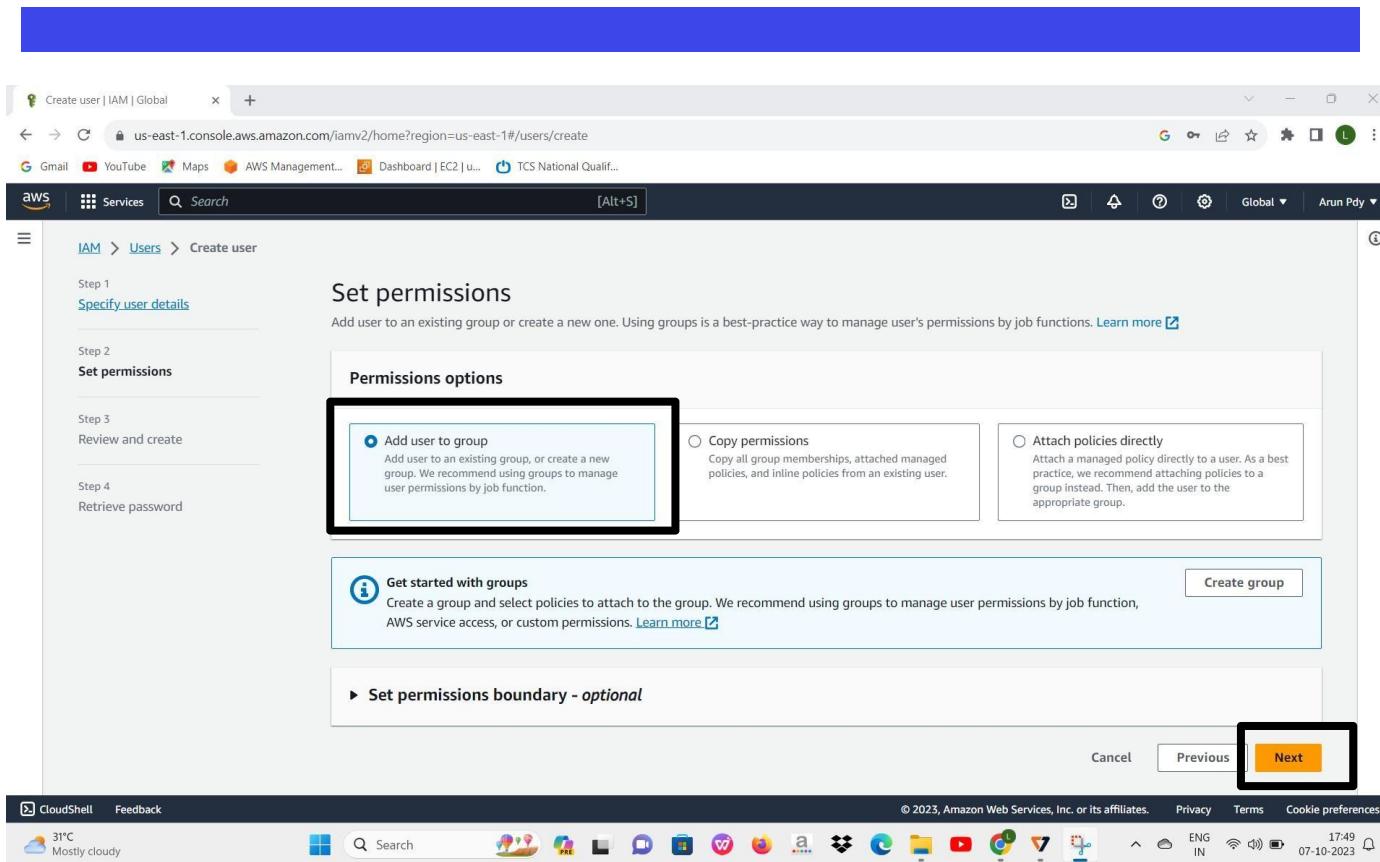
- select provide user access



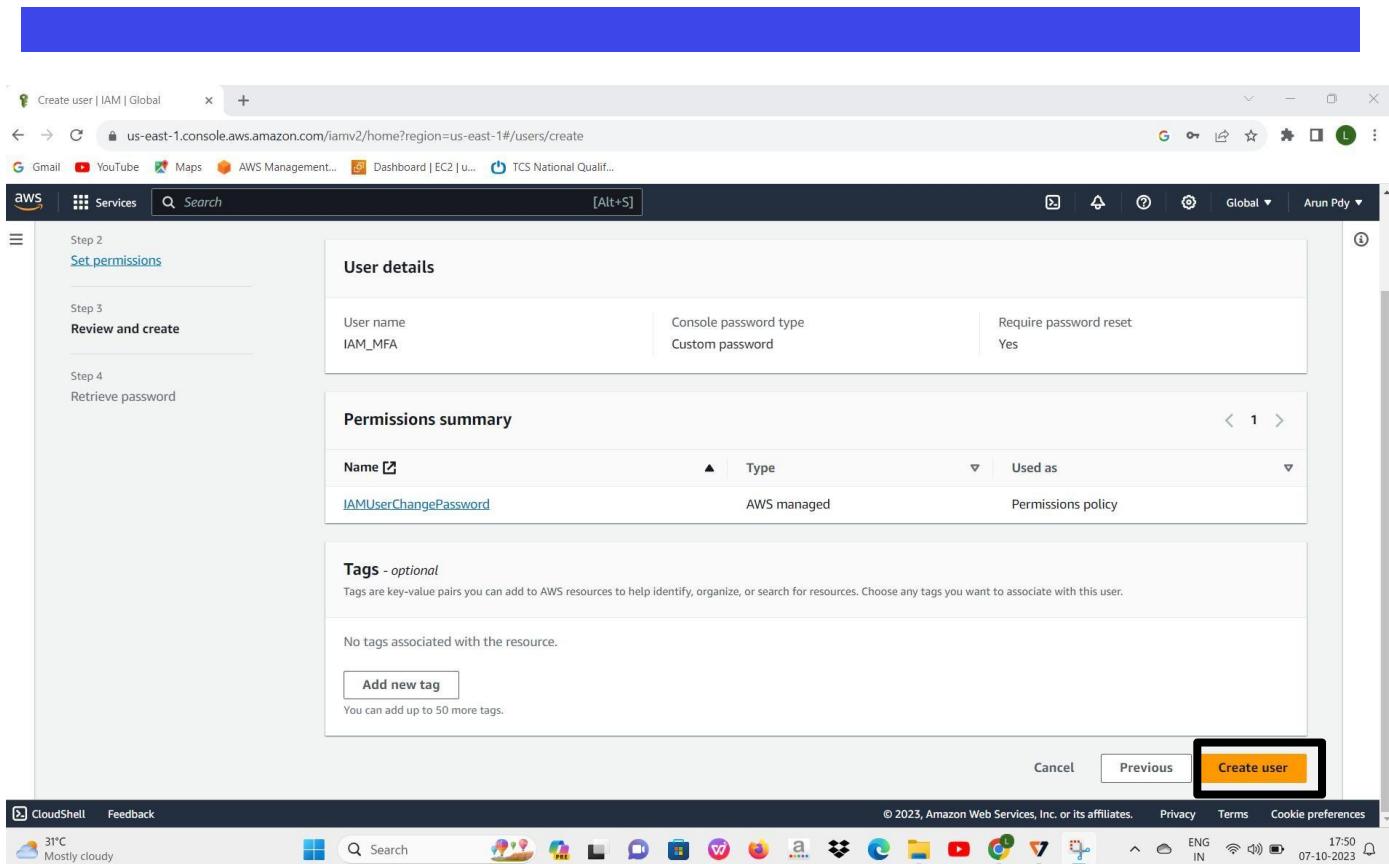
- select I want to create an IAM user.
- select custom password



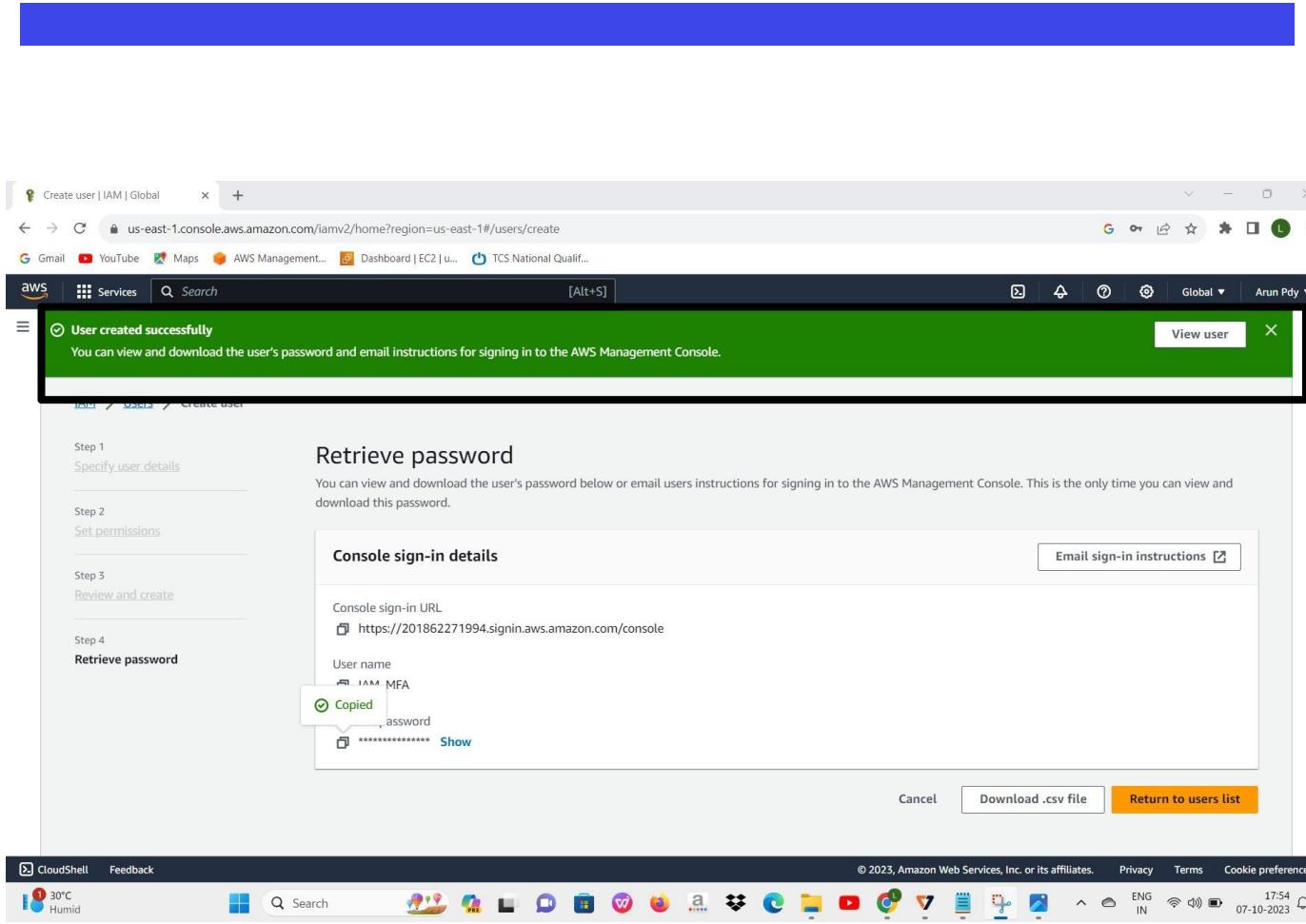
- Give your own password in custom password → disable recommended Tag.
- click next.



- Click add user to group
- click next



- Click create user.



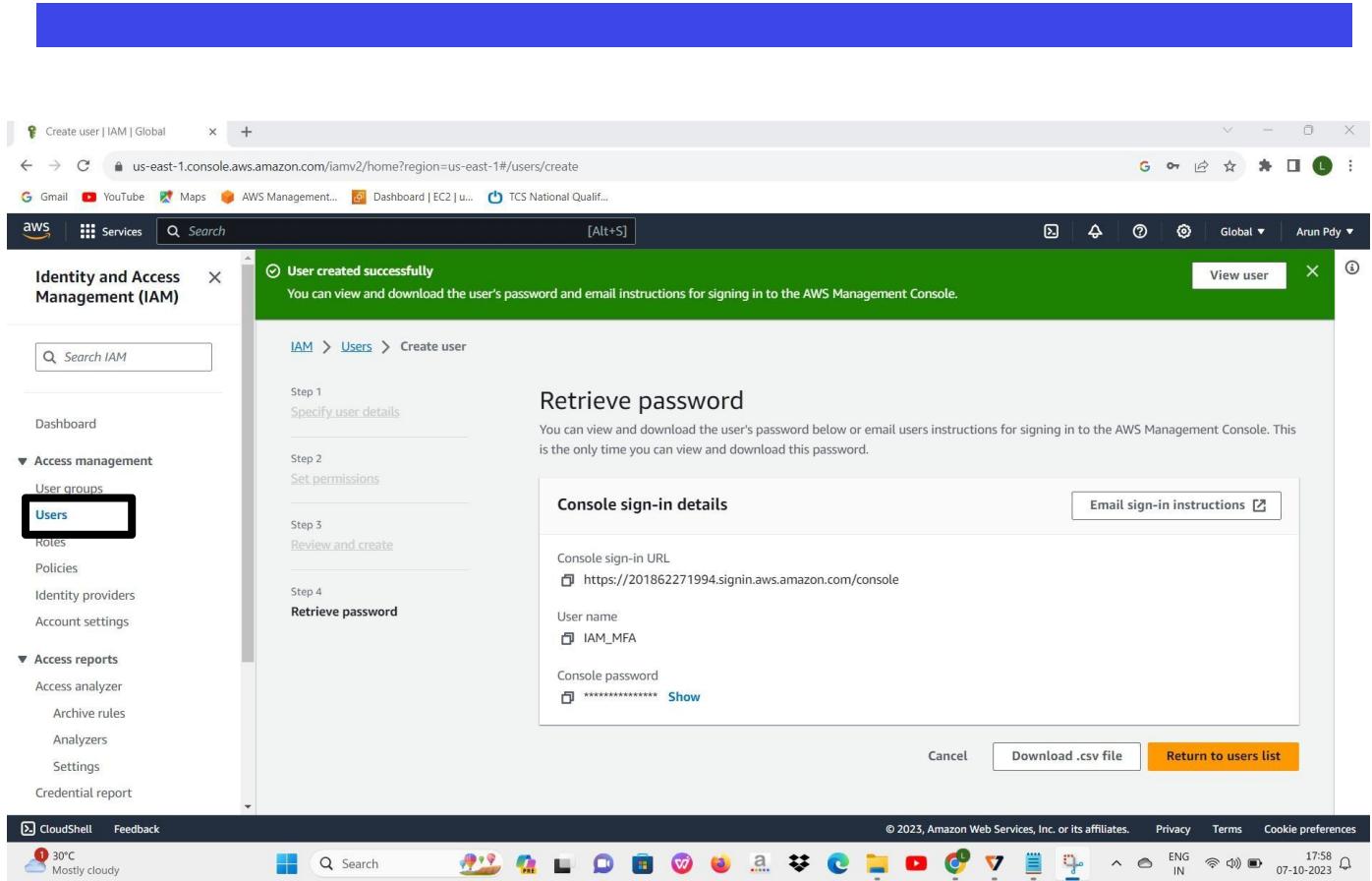
- The user has been created successfully.

The screenshot shows the AWS IAM 'Create user' process at Step 4: Retrieve password. A success message 'User created successfully' is displayed. The 'Console sign-in details' section is highlighted with a black box, showing the following information:

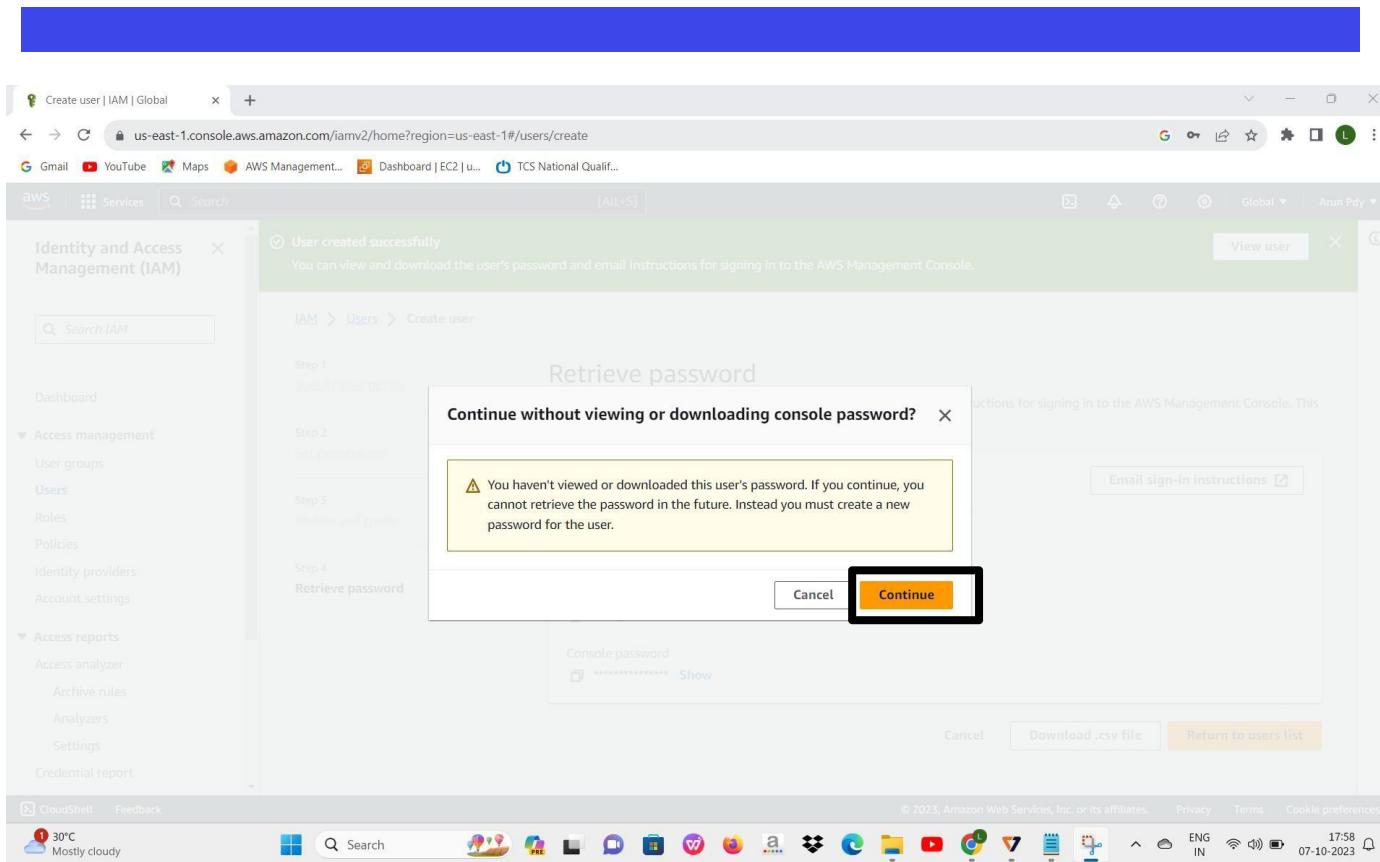
- Console sign-in URL: <https://201862271994.signin.aws.amazon.com/console>
- User name: IAM_MFA
- Console password: ***** (redacted)

Other visible elements include a 'View user' button, navigation links (IAM > Users > Create user), and standard browser controls.

- copy the url, username, password to notepad.



- tap the user



- tap the user.

The screenshot shows the AWS IAM Users page. At the top, a green banner displays the message: "User created successfully. You can view and download the user's password and email instructions for signing in to the AWS Management Console." Below the banner, the page title is "Users (1) Info". A sub-header states: "An IAM user is an identity with long-term credentials that is used to interact with AWS in an account." On the right, there are buttons for "View user" and "Create user". The main table lists one user: "IAM_MFA" (highlighted with a red box). The table columns include: User name, Path, Groups, Last activity, MFA, Password age, and Console last sign-in. The "User name" column shows "IAM_MFA". The "Last activity" column shows "12 minutes". The "Console last sign-in" column shows "-".

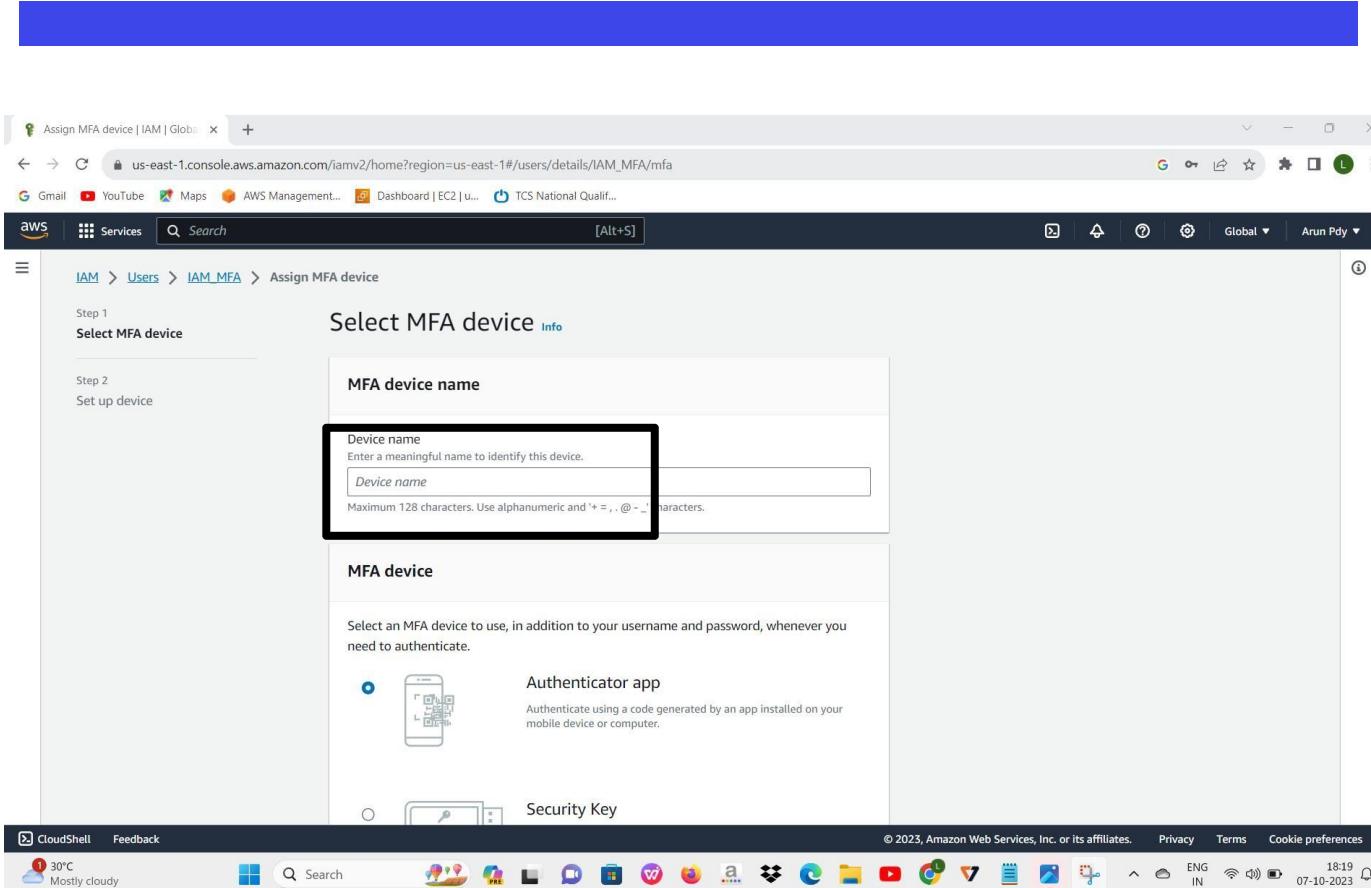
- click the user id.

The screenshot shows the AWS IAM console with the URL us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users/details/IAM_MFA?section=permissions. The left sidebar shows navigation options like Dashboard, Access management, and Access reports. The main content area displays the IAM_MFA user's summary, including ARN, creation date, and console access status. A yellow warning icon indicates 'Enabled without MFA'. Below this, the 'Permissions' tab is active, showing a single policy attached. The bottom of the screen shows the Windows taskbar with various pinned icons.

- here you can see enable MFA .

The screenshot shows the AWS IAM MFA configuration page. On the left, there's a sidebar with navigation links like Dashboard, Access management (with sub-links for User groups, Users, Roles, Policies, Identity providers, and Account settings), and Access reports (with sub-links for Access analyzer, Archive rules, Analyzers, Settings, and Credential report). The main content area has a breadcrumb trail: IAM > Users > IAM_MFA. It displays the 'IAM_MFA' user details. A tooltip is overlaid on the 'Console access' section, which says 'Enabled without MFA'. Below this, there's a button labeled 'Enable MFA'. The bottom section shows 'Permissions policies (1)' attached to the user.

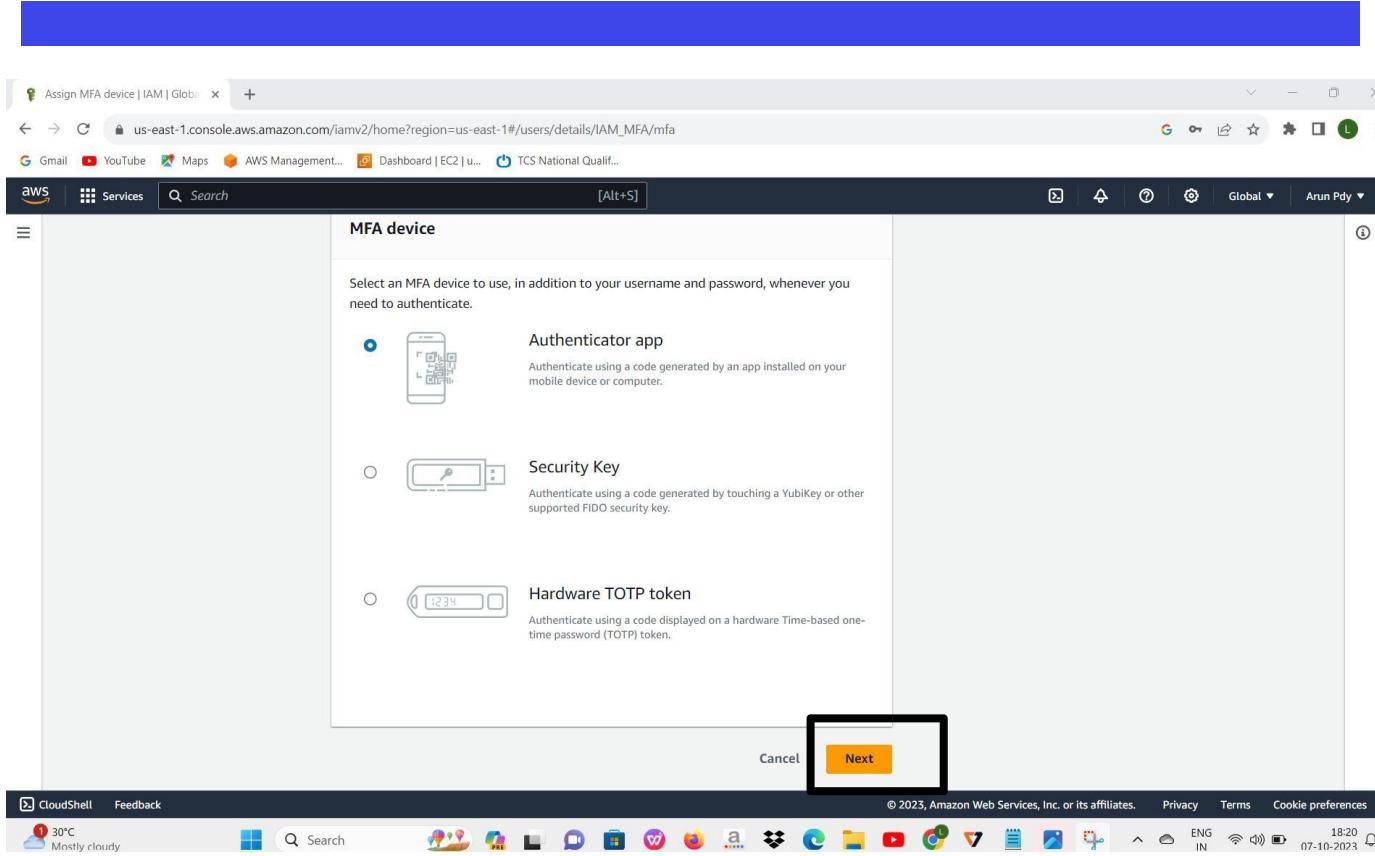
- click enable MFA.



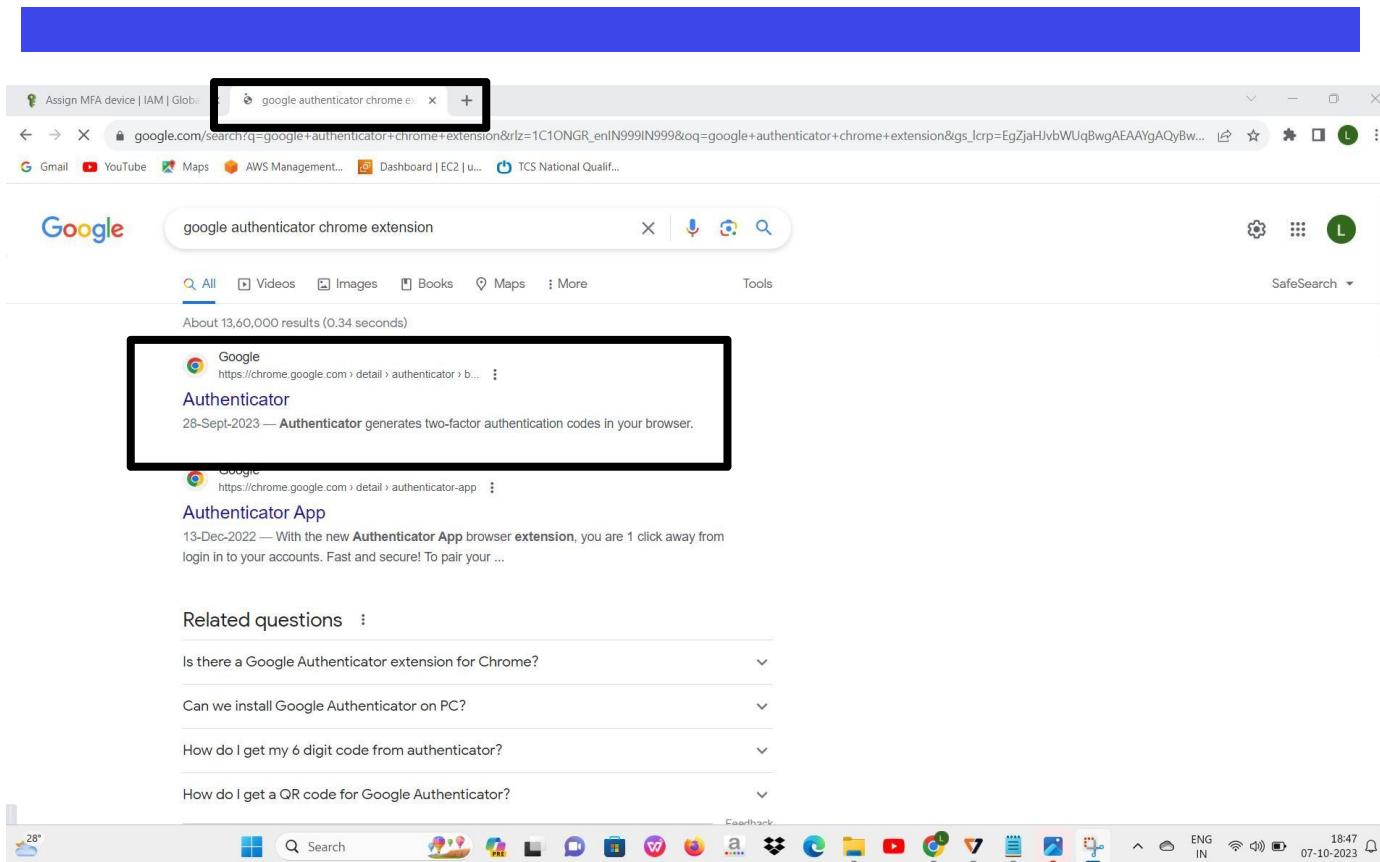
- Give name to the MFA.

The screenshot shows the AWS IAM 'Assign MFA device' process. The user is on Step 1, 'Select MFA device'. The left sidebar shows 'Step 1: Select MFA device' and 'Step 2: Set up device'. The main area has two sections: 'MFA device name' and 'MFA device'. In the 'MFA device name' section, a text input field contains 'Access'. In the 'MFA device' section, the 'Authenticator app' option is selected, indicated by a blue circle. Below it, there is a small icon of a smartphone displaying a QR code and the text 'Authenticator app'. The status bar at the bottom shows the date '07-10-2023' and time '18:20'.

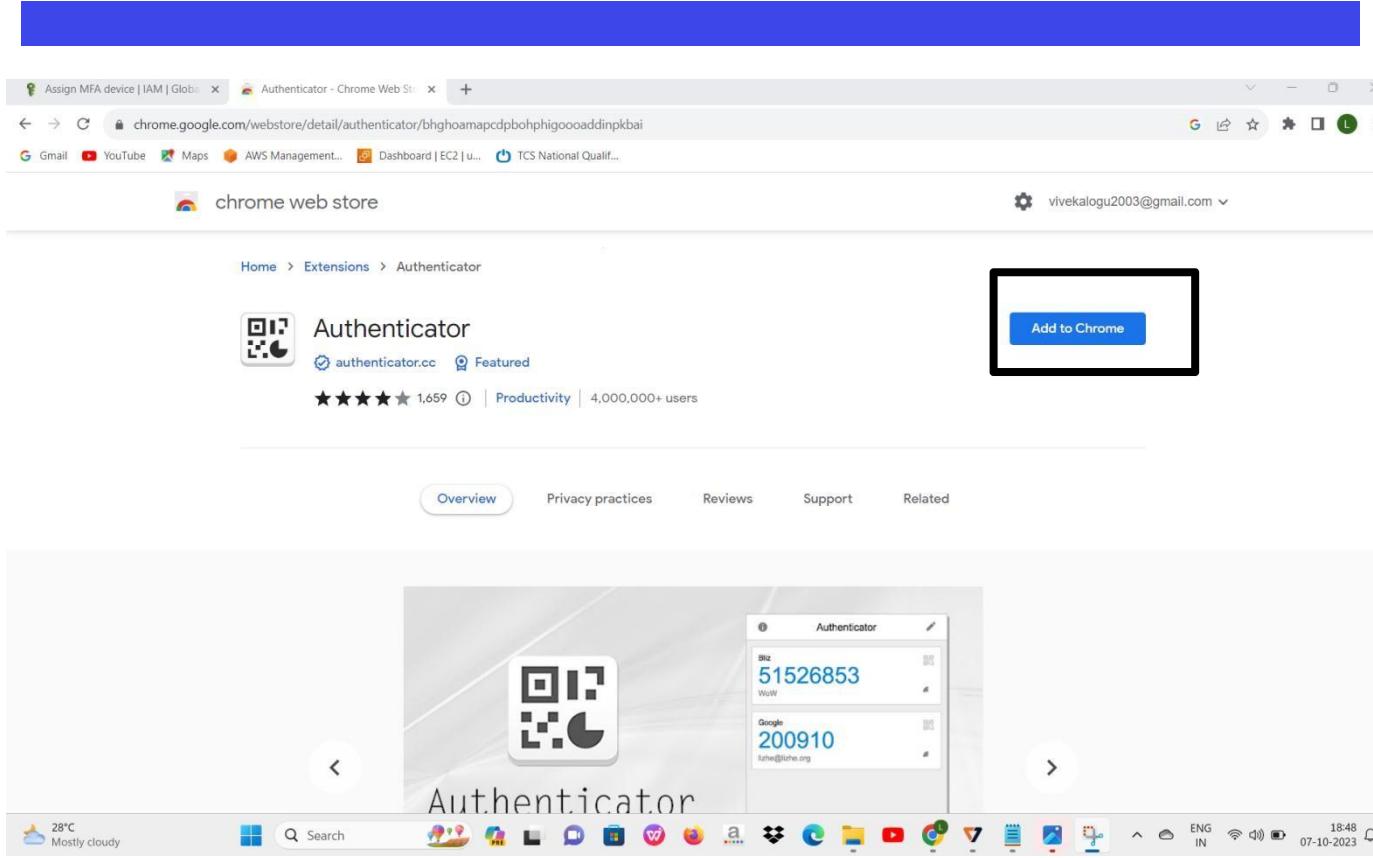
- Give name to MFA(eg.access).
- Select the 1st option authenticator app,



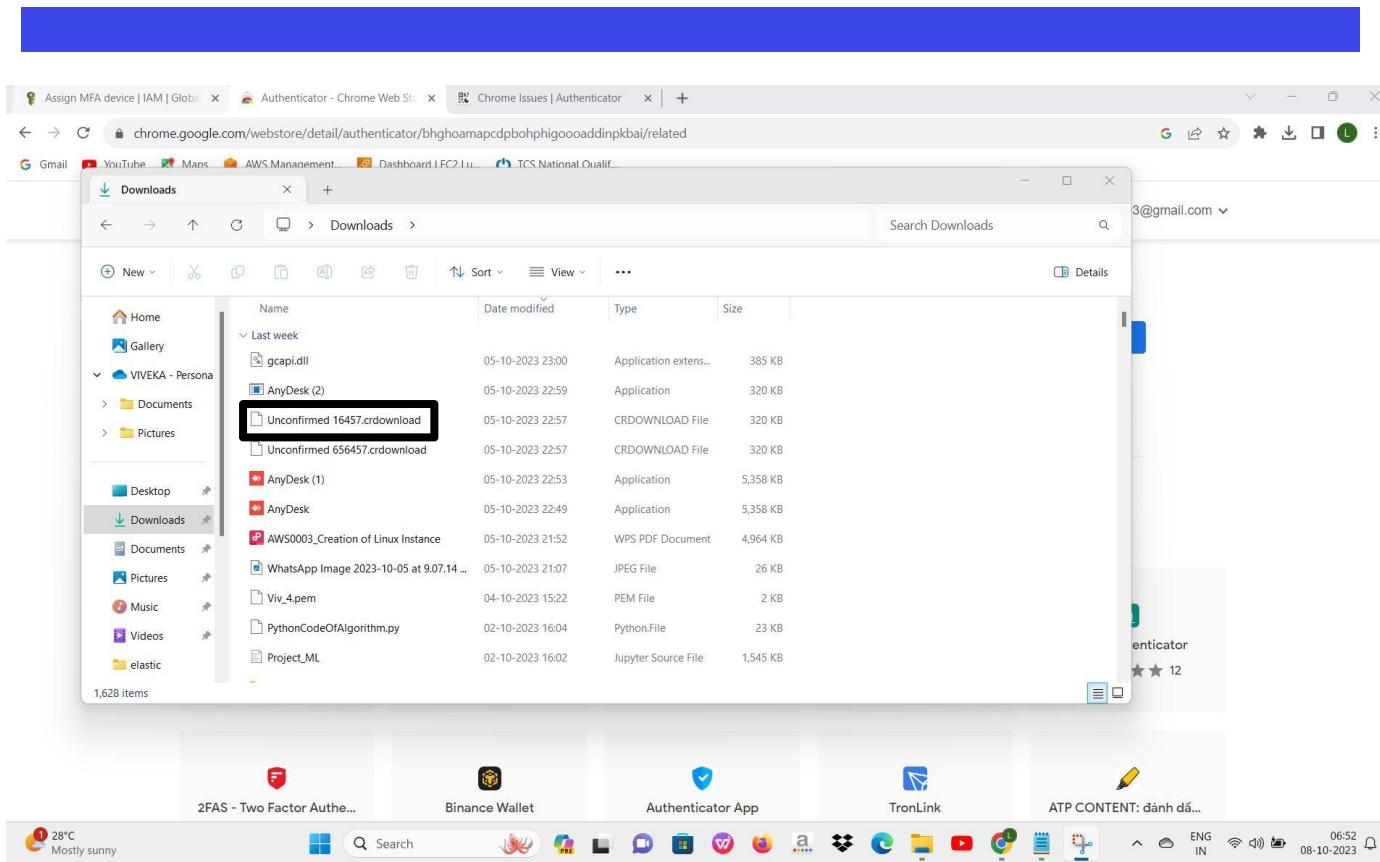
- click next.



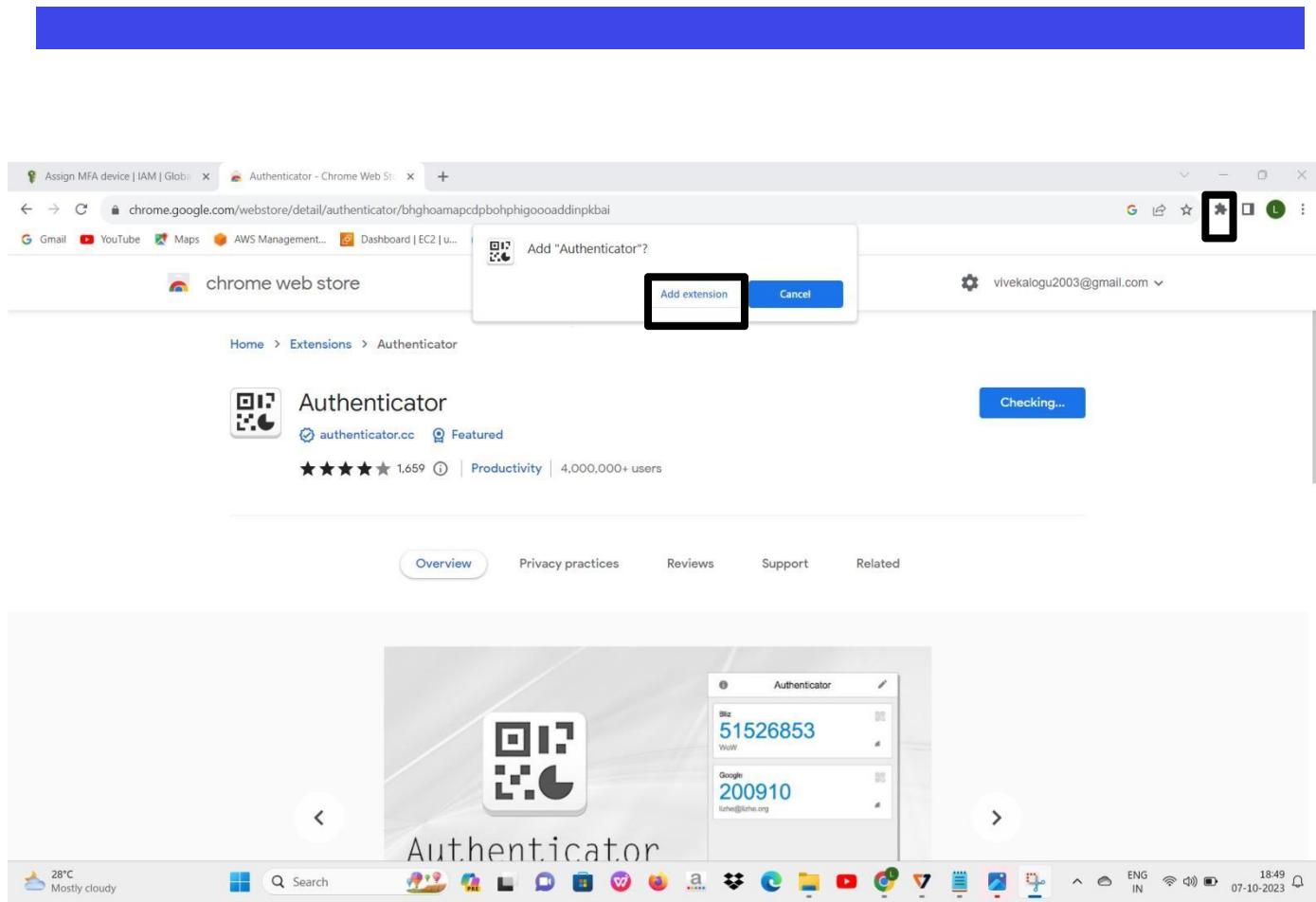
- Open a new tab search for google authenticator as an chrome extension.



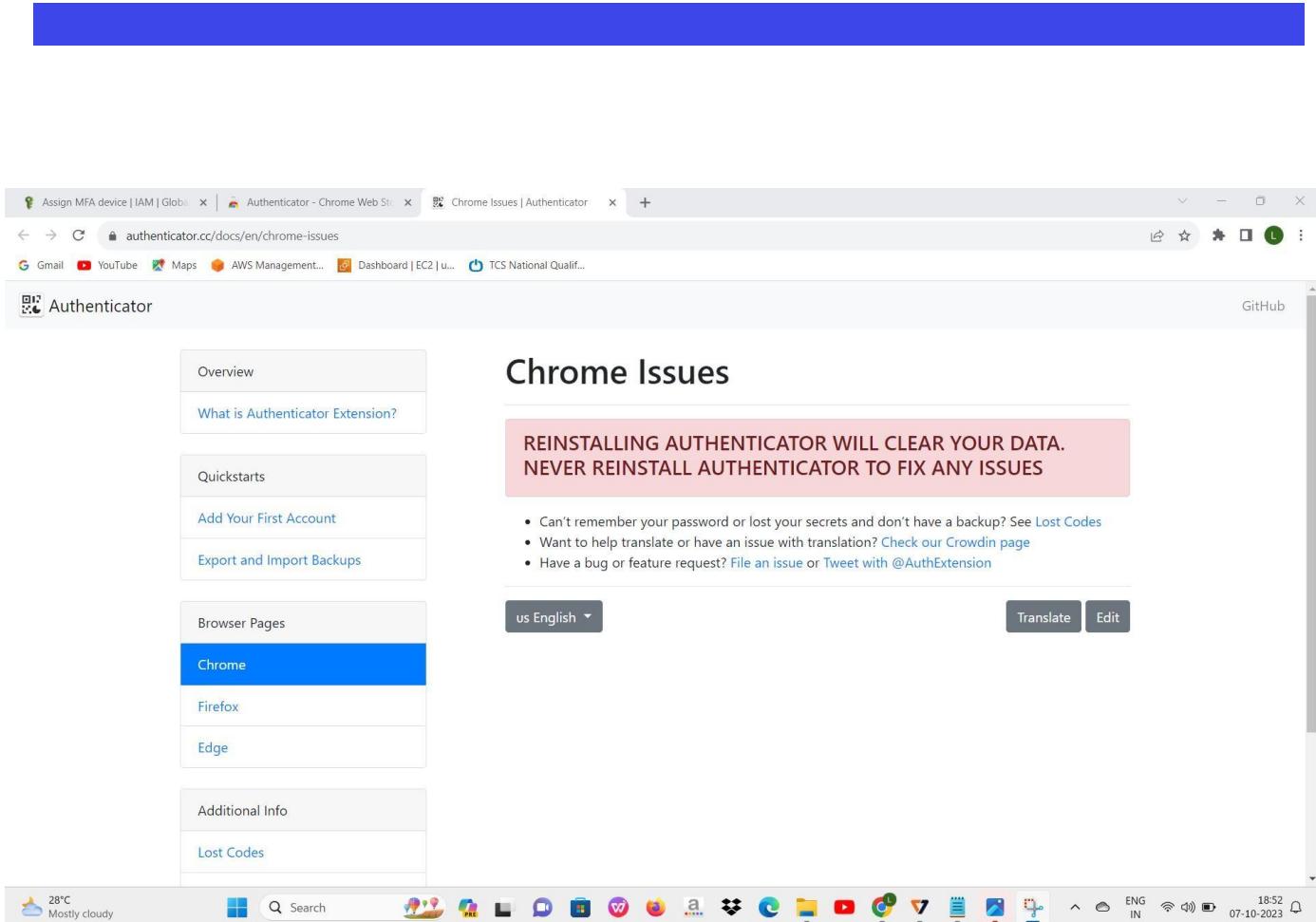
- Click add to chrome.



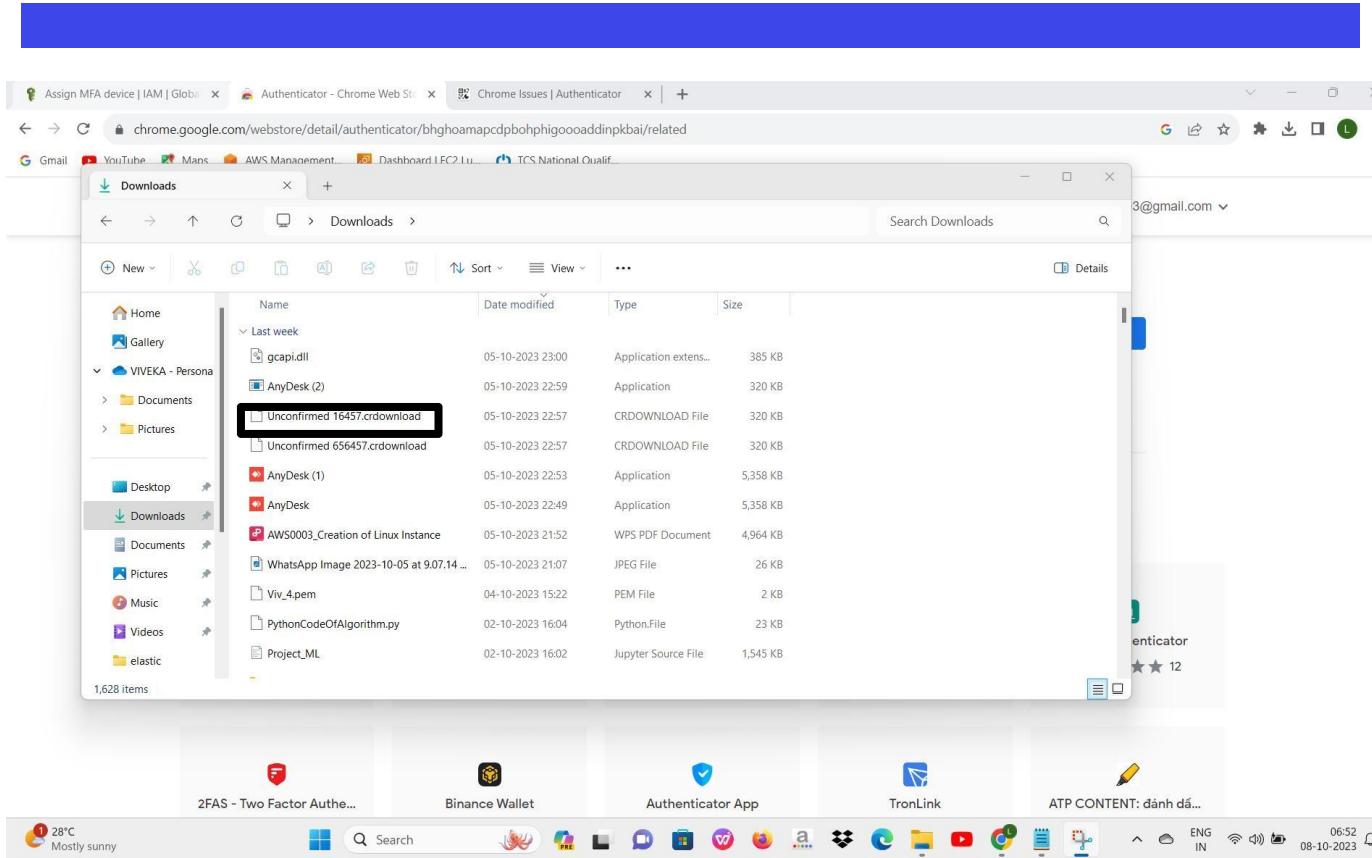
- Next the extension file is downloaded .we can see it on the downloads.



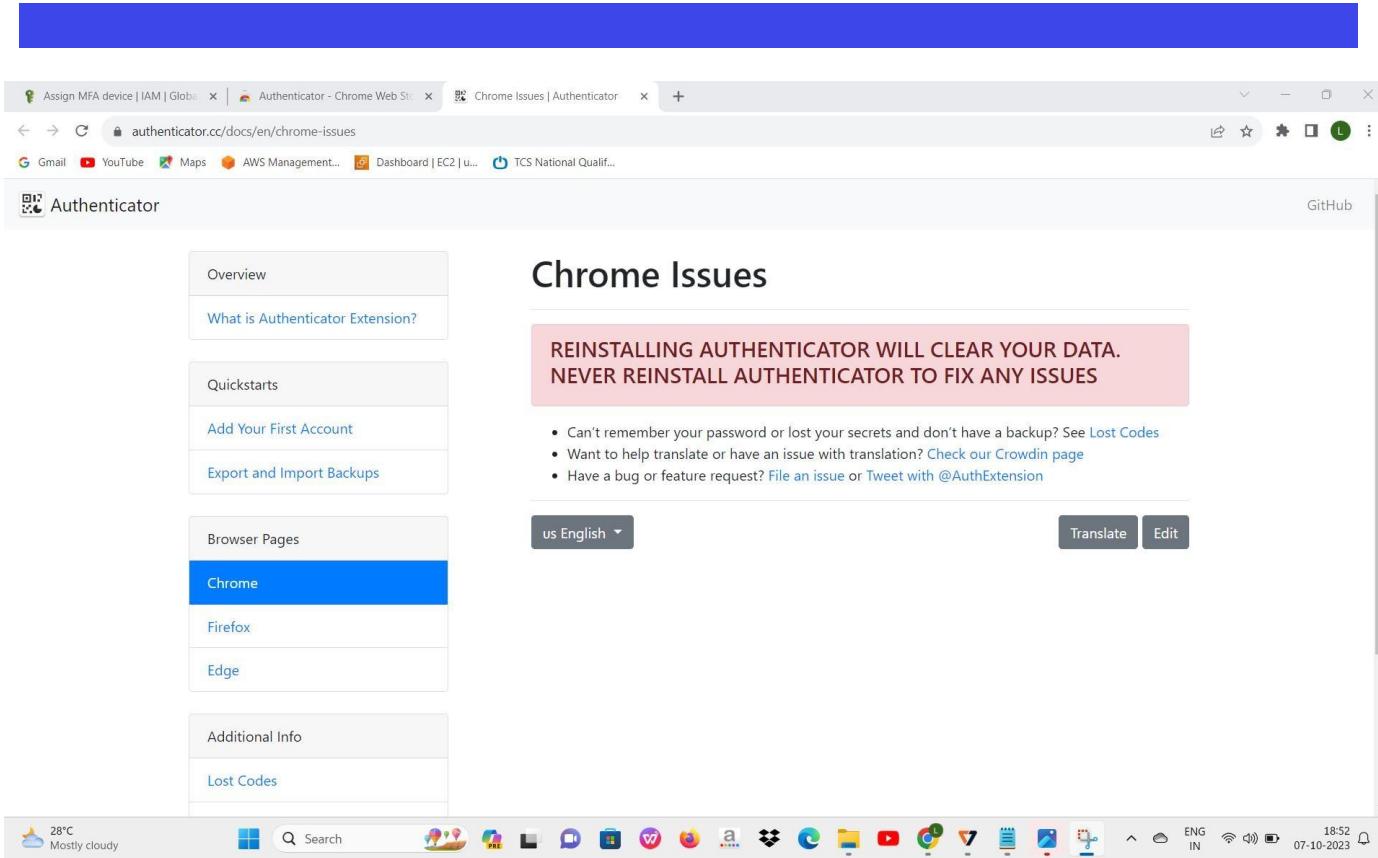
- In order to view the extension, click the menu icon.
- Click the extension.
- Then the pop message is show.
- Then click the Add extension.



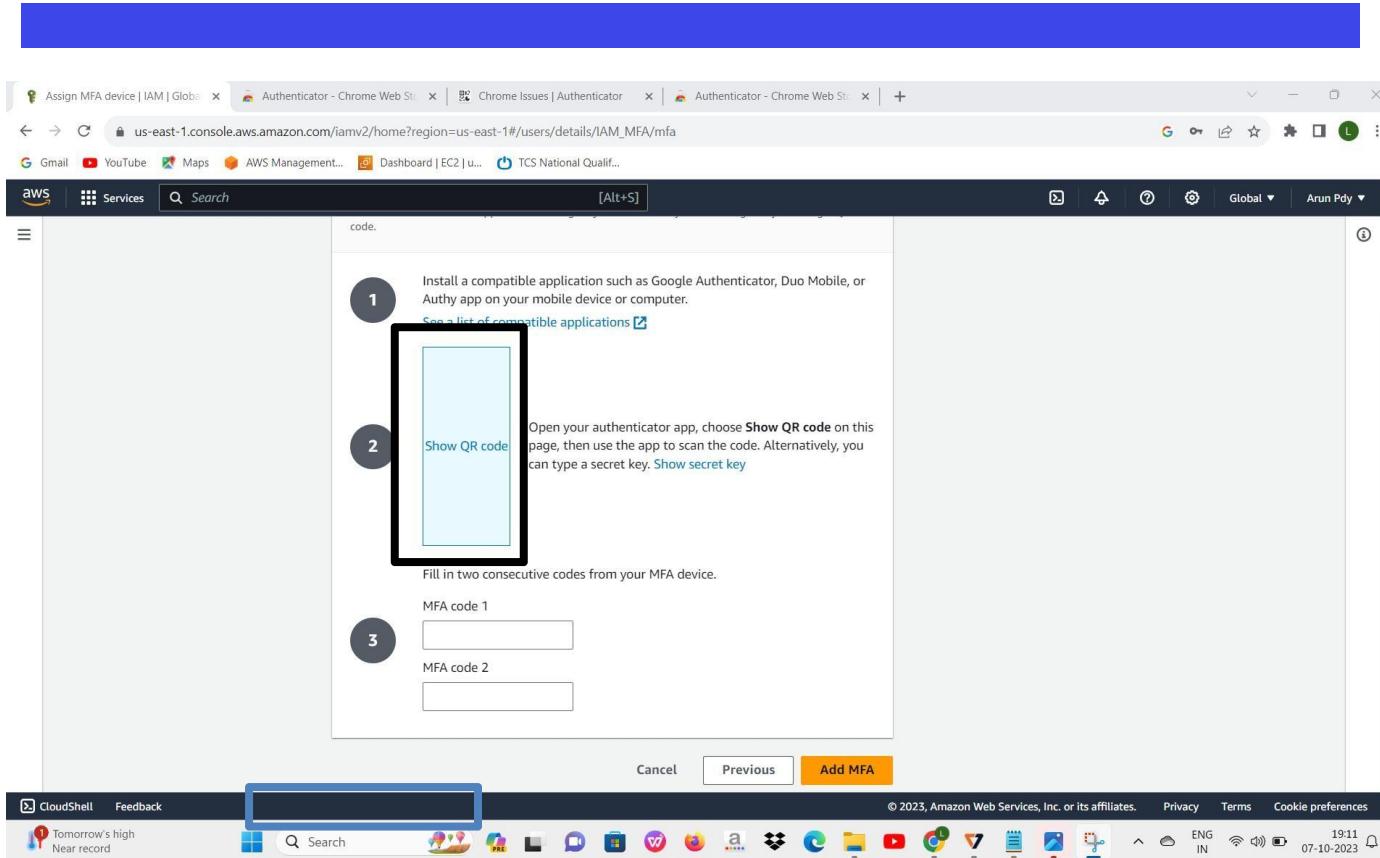
- Next you can automatically direct to the new tab.



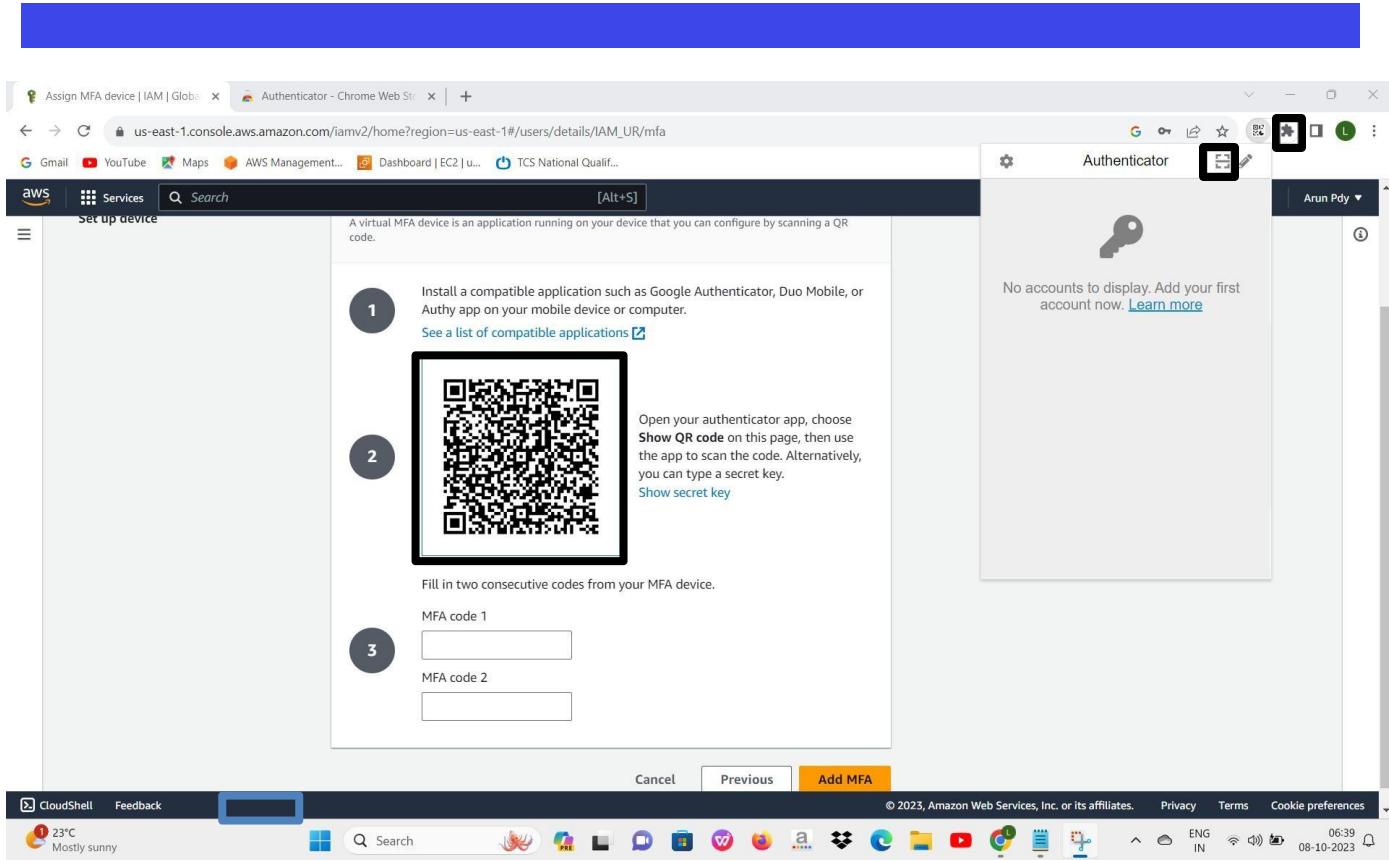
- Next the extension file is downloaded .we can see it on the downloads.



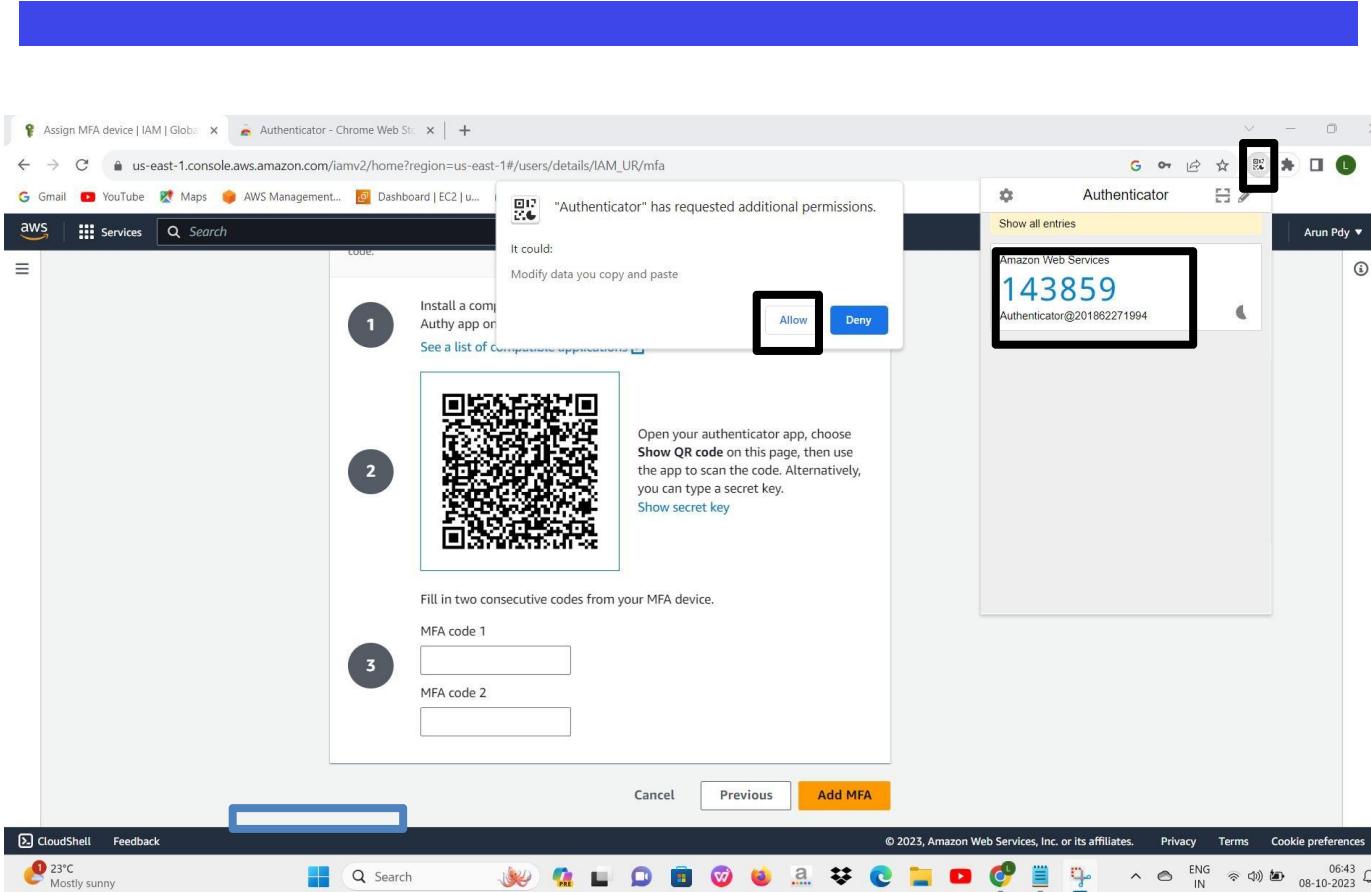
- Next it automatically direct to the new tab.



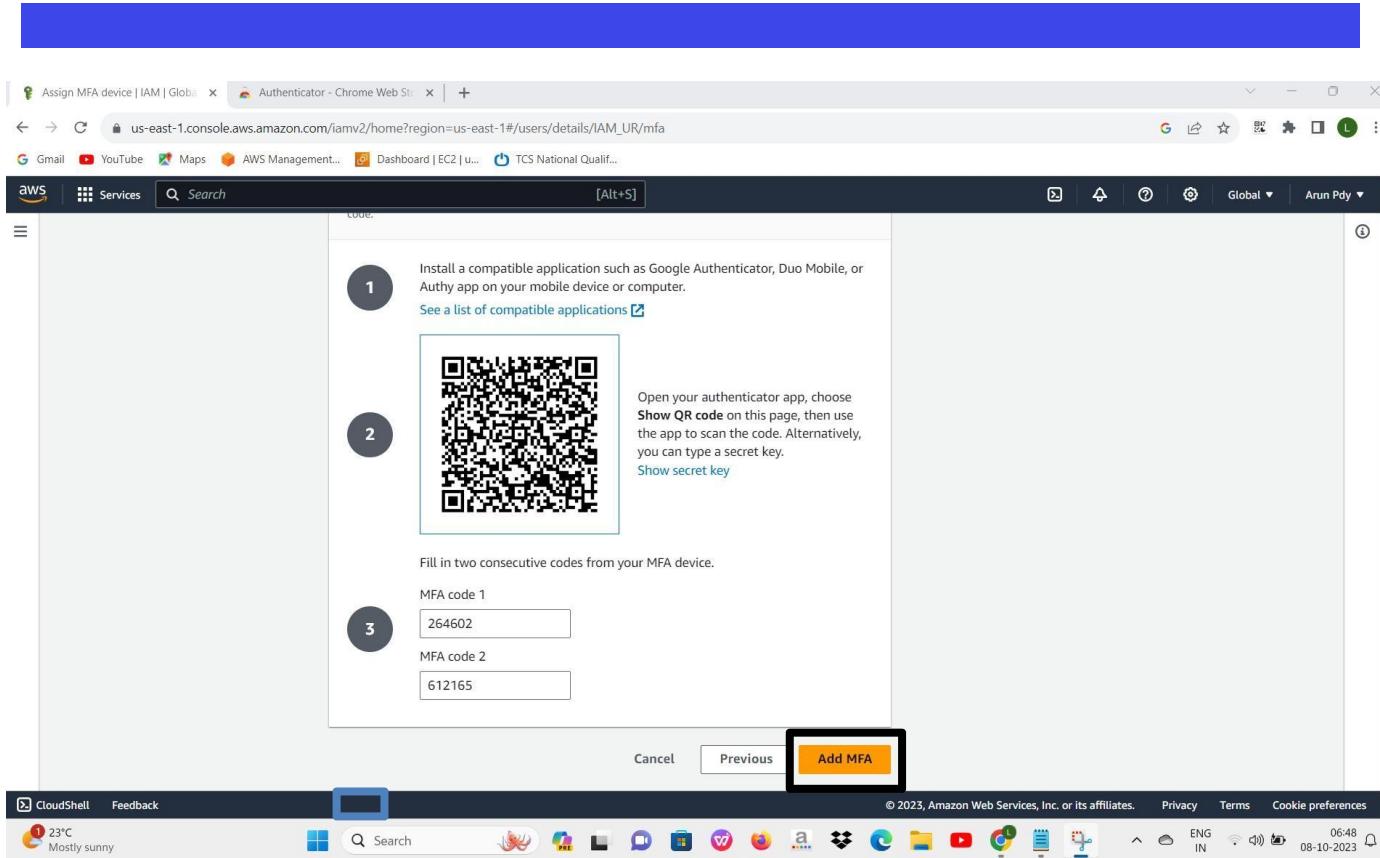
- Get back to aws iam.
- click show QR code.



- You can view the QR code we gonna to scan the code using authenticator extension.



- Click on the extension.
- You can see the pop message.
- Click Allow.
- you can see the authenticator icon
- click on it.
- copy the code and paste it in MFA code 1 and refresh it then paste the second code in MFA code 2.



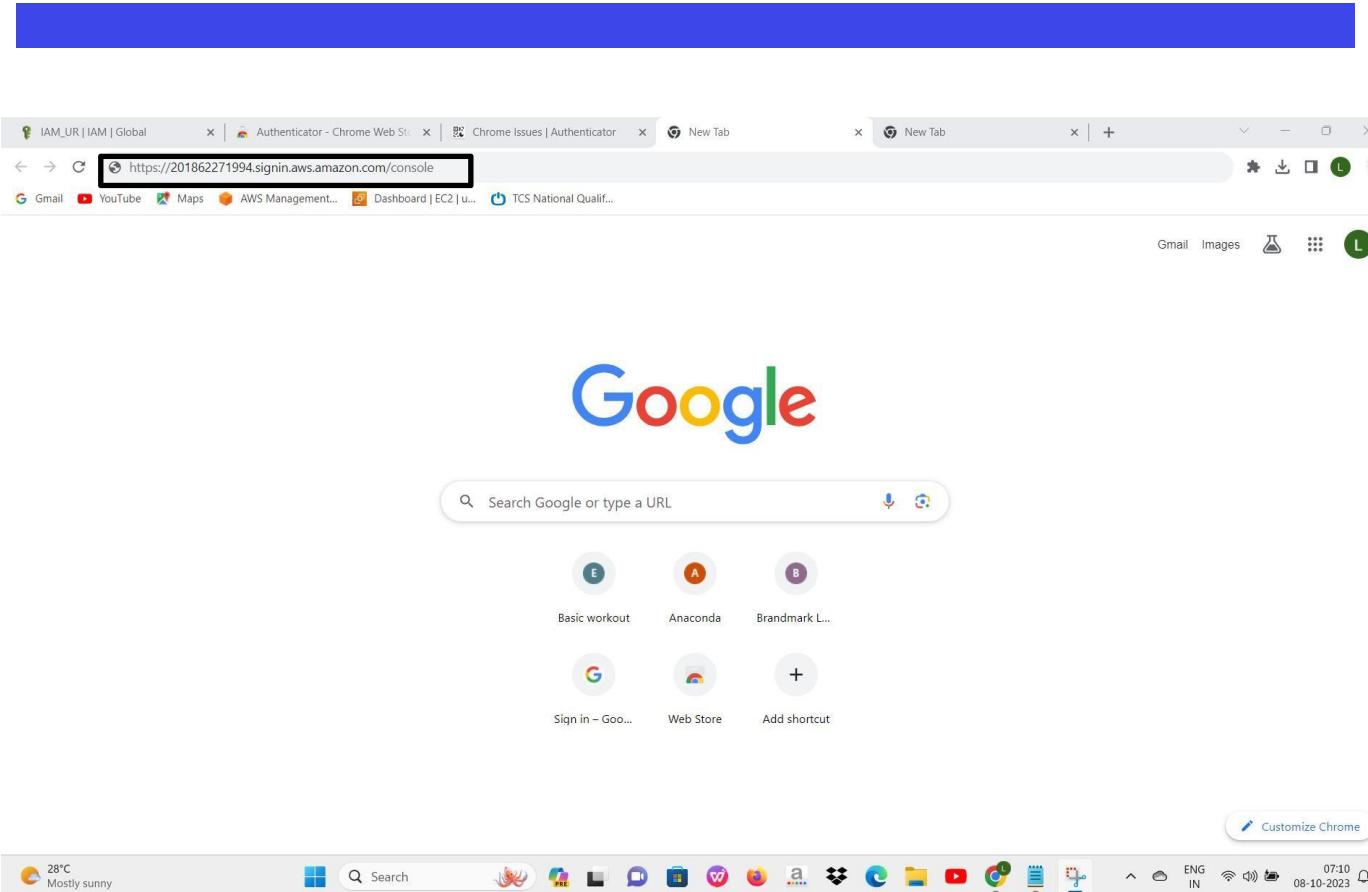
- Once you pasted the code click add MFA.

The screenshot shows the AWS Identity and Access Management (IAM) console. A specific user named 'IAM_UR' is selected. The 'Security credentials' tab is active, showing that 'Console access' is 'Enabled with MFA'. Other tabs include 'Permissions', 'Groups', 'Tags', and 'Access Advisor'. Below the tabs, there's a 'Console sign-in' section with a link to the sign-in page and information about the last sign-in. At the bottom, there's a note about Multi-factor authentication (MFA). The browser interface at the top includes tabs for 'Authenticator - Chrome Web St...', 'Chrome Issues | Authenticator', and 'New Tab', along with various system icons.

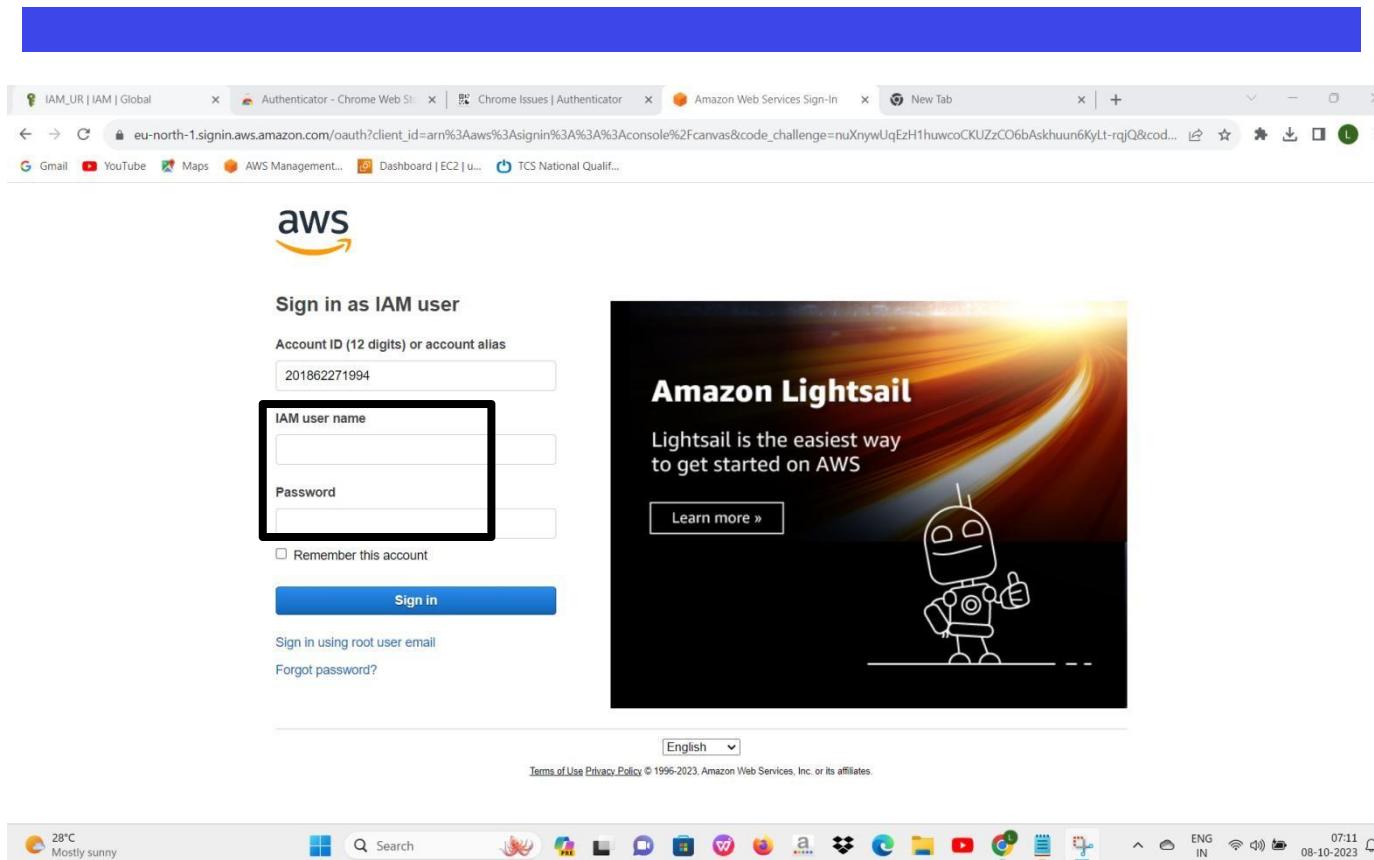
- MFA has been added successfully.

The screenshot shows the AWS Identity and Access Management (IAM) console. The left sidebar is collapsed, and the main area displays the 'Summary' tab for a user named 'IAM_UR'. The 'Security credentials' tab is selected. A modal window is open over the 'Console sign-in' section, indicating that the link has been copied. The copied URL is displayed in the modal: <https://201862271994.signin.aws.amazon.com/console>. The right sidebar contains information about IAM users and links to learn more.

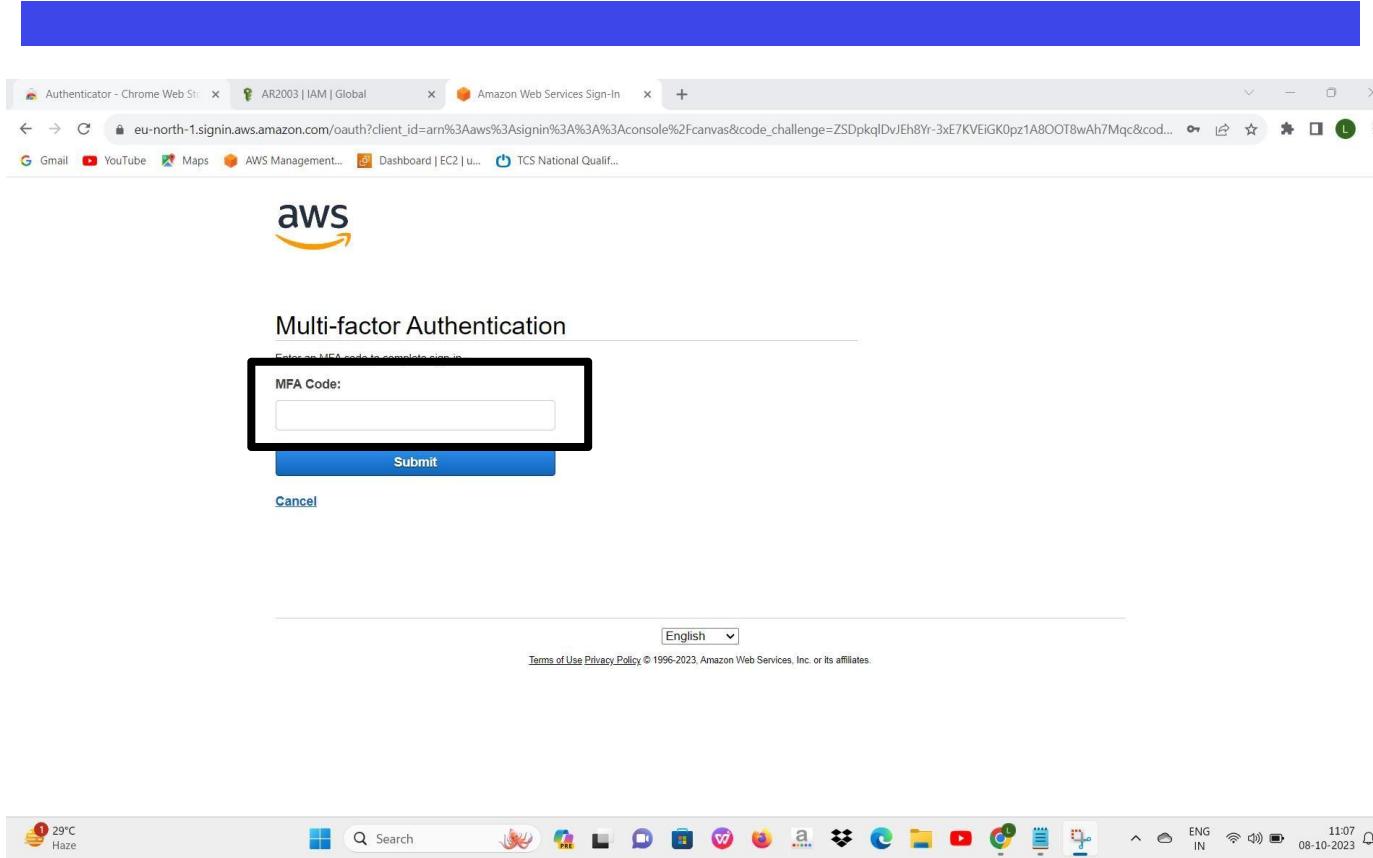
- Now copy the console sign-in-link.



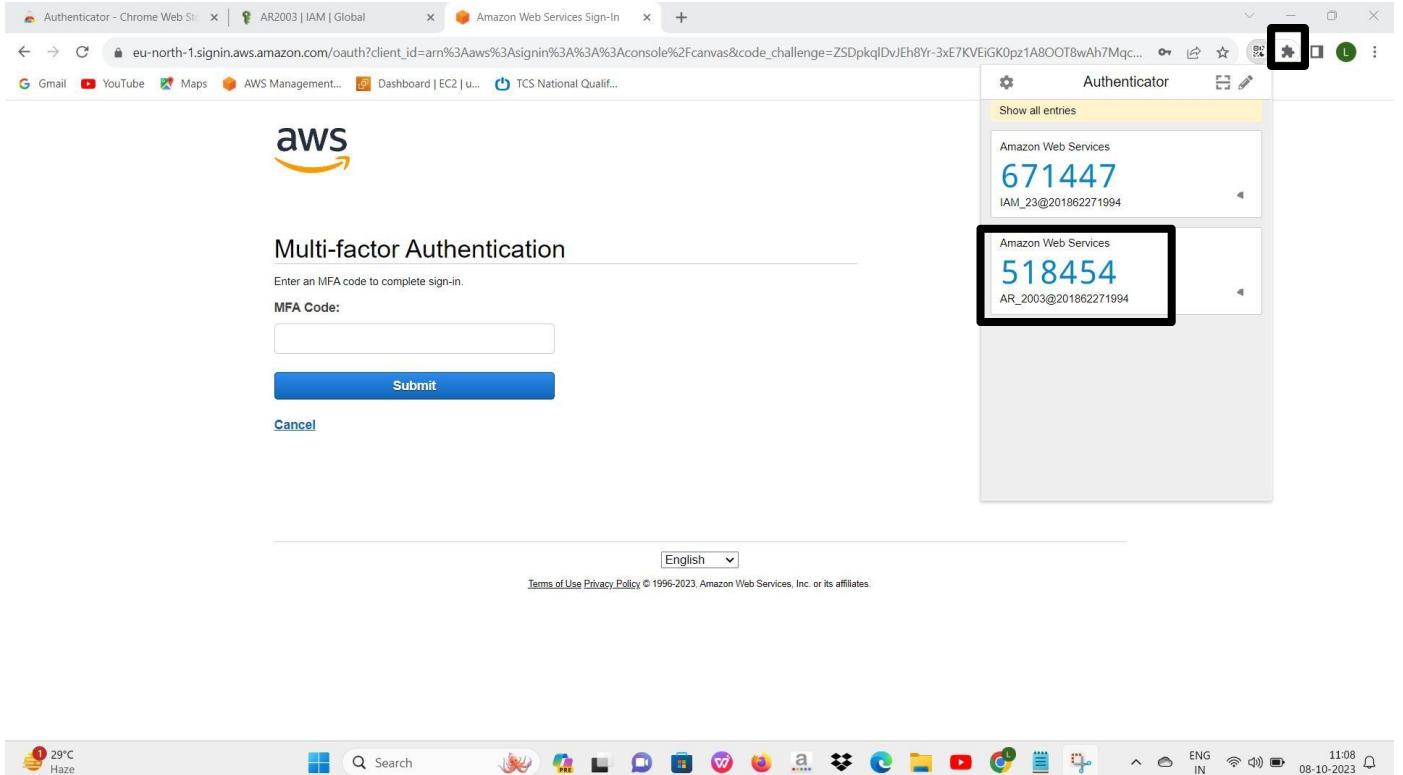
- Now paste the copied url in new tab chrome.



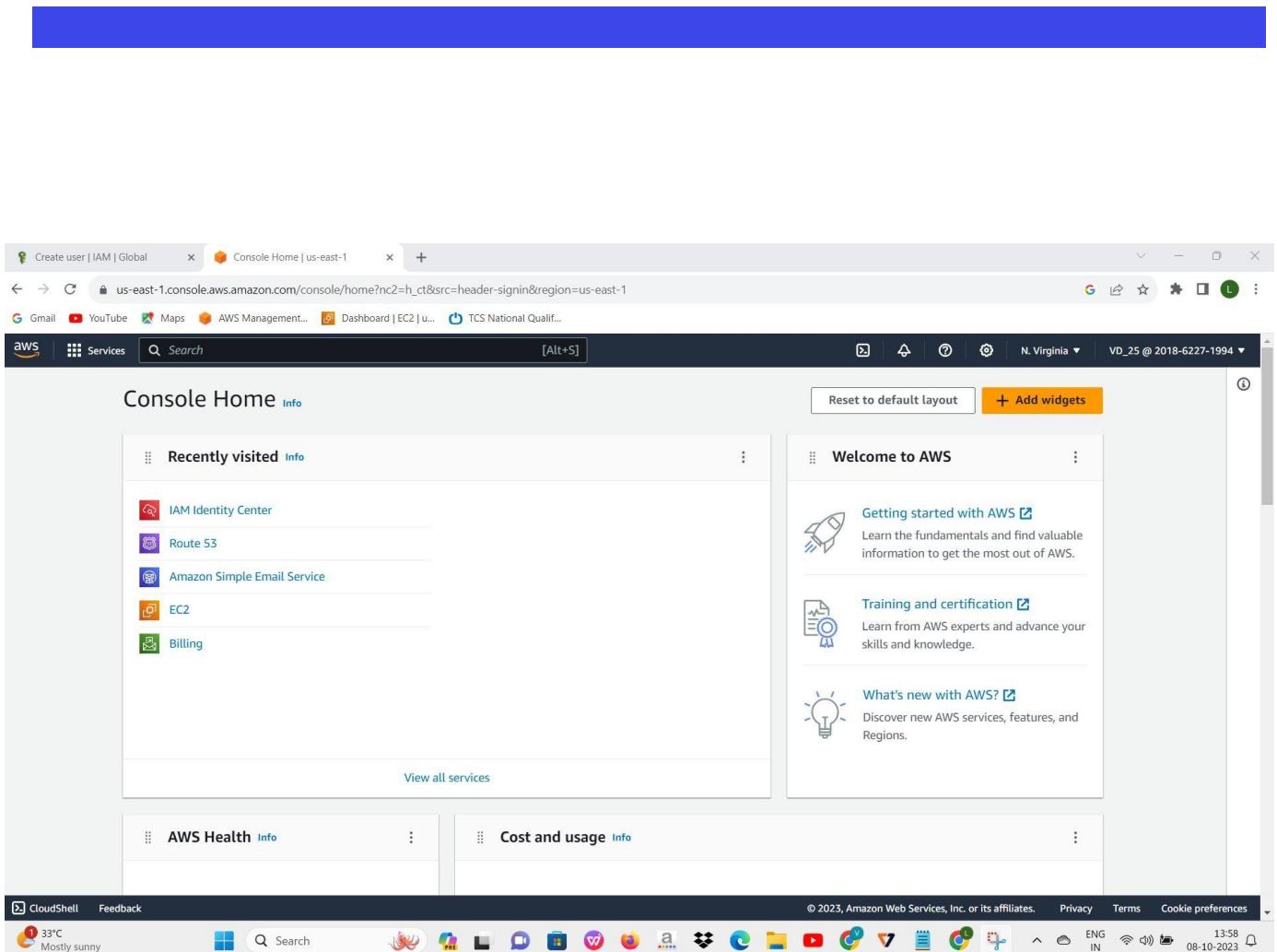
- Sign in with your user name and password.



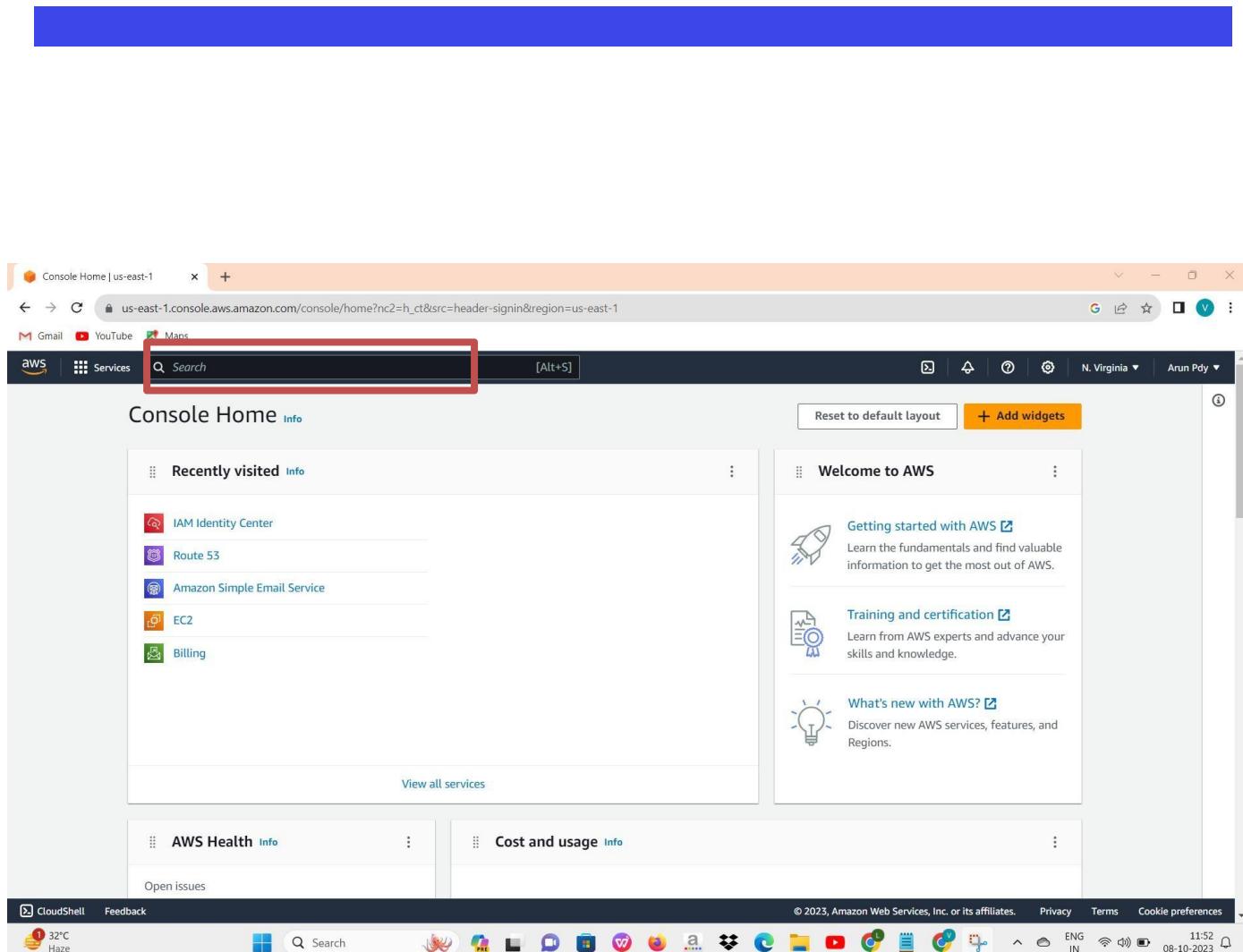
- Here you can see it asking for authentication,



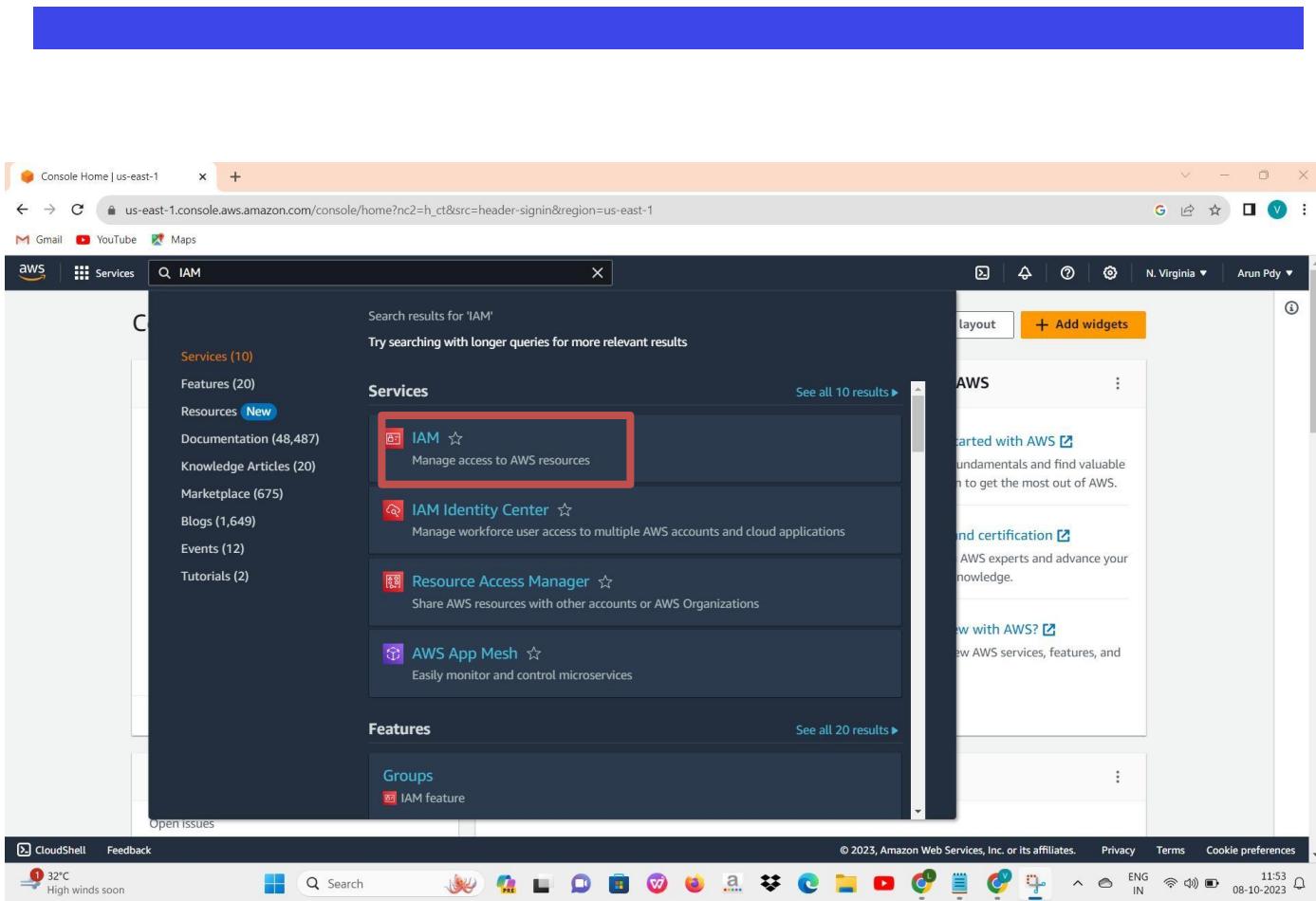
- In order to sing in paste the code get from extension.



- The user get successfully signined.



- search bar type IAM and search.



- Click the IAM.

The screenshot shows the AWS IAM Dashboard. On the left sidebar, under 'Access management', the 'Policies' option is selected and highlighted with a red box. The main content area displays the 'IAM resources' summary with counts: 0 User groups, 1 User, 4 Roles, 0 Policies, and 0 Identity providers. Below this, the 'What's new' section lists recent updates:

- IAM Roles Anywhere is now available in the AWS GovCloud (US) Regions. 2 weeks ago
- AWS Identity and Access Management provides action last accessed information for more than 140 services. 3 weeks ago
- IAM roles last used and last accessed information available in AWS GovCloud (US) Regions. 4 weeks ago
- IAM Roles Anywhere credential helper adds support for OS certificate stores. 2 months ago

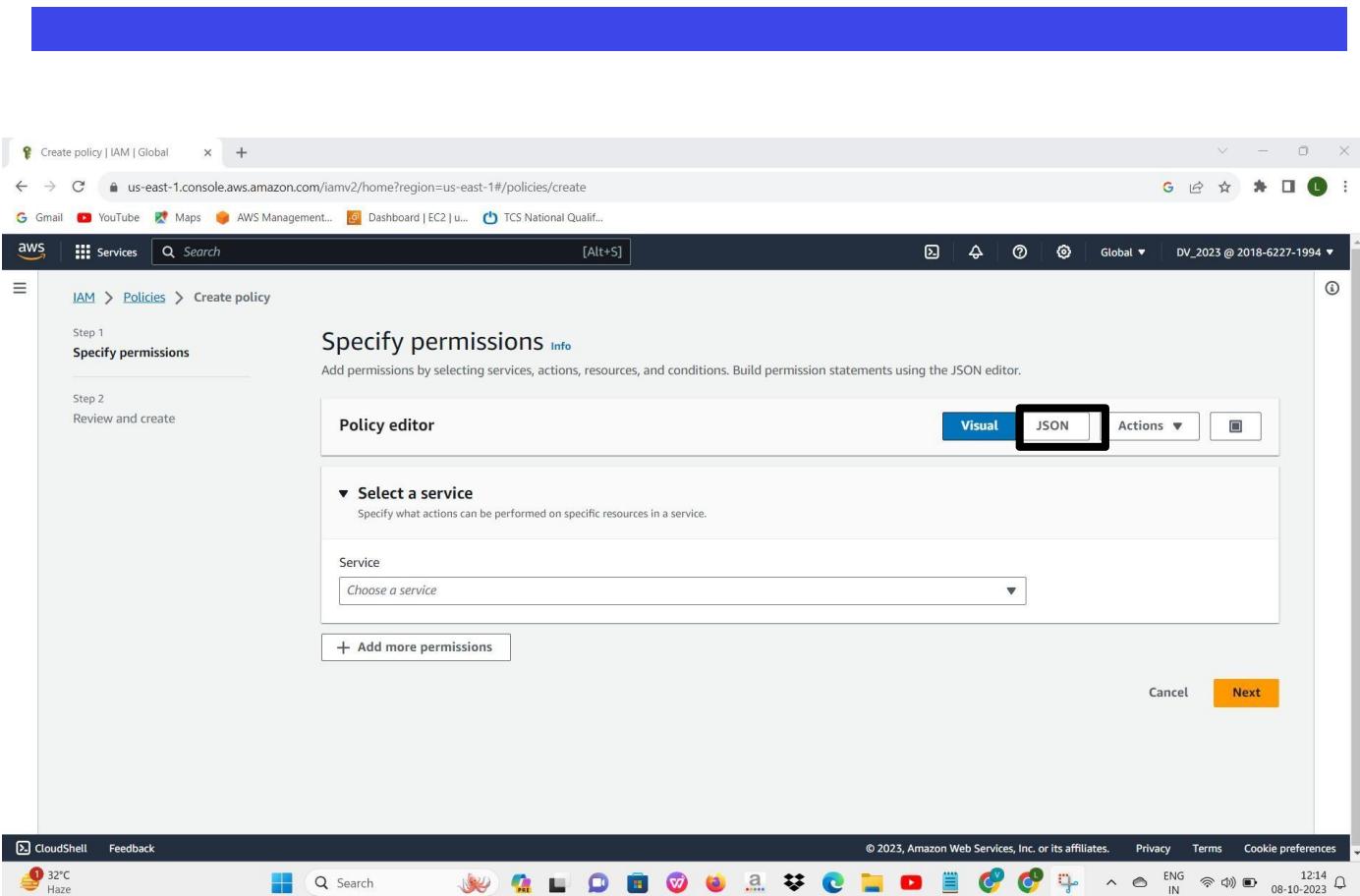
On the right side, there are 'Quick Links' for 'My security credentials' and 'Tools' for 'Policy simulator' and 'Web identity federation playground'. The top navigation bar shows the URL as us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/home.

- Click the policy.

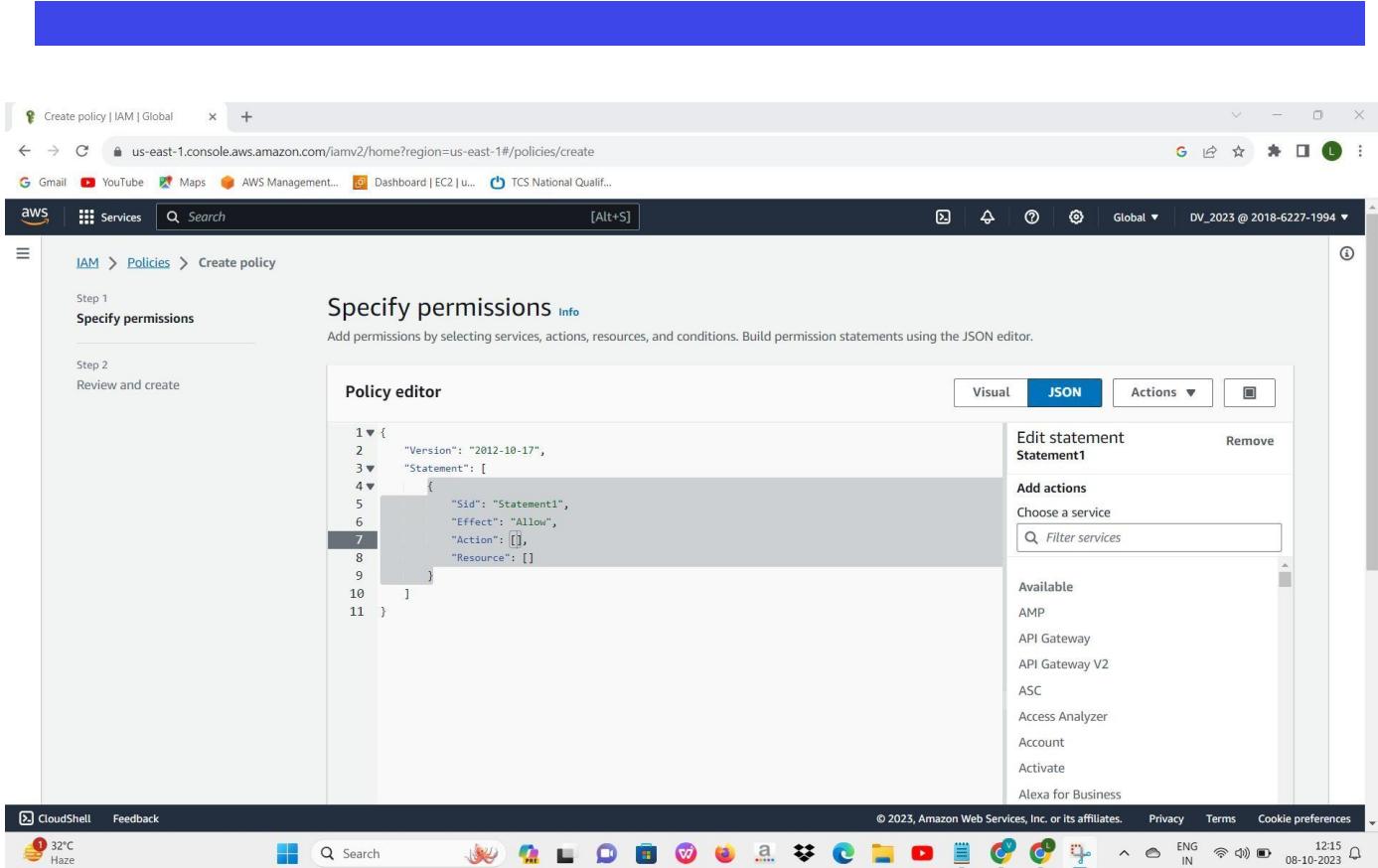
The screenshot shows the AWS Identity and Access Management (IAM) Policies page. The left sidebar includes links for Identity and Access Management (IAM), Access management, Access reports, and CloudShell. The main content area displays a table of existing policies, each with a name, type (AWS managed or AWS managed - job function), usage status (None), and a brief description. A search bar and filter options are at the top of the table. At the top right, there are 'Actions', 'Delete', and a large orange 'Create policy' button.

Policy name	Type	Used as	Description
AccessAnalyzerService...	AWS managed	None	Allow Access Analyzer to analyze resou...
AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
AdministratorAccess-...	AWS managed	None	Grants account administrative permissi...
AdministratorAccess-...	AWS managed	None	Grants account administrative permissi...
AlexaForBusinessDevi...	AWS managed	None	Provide device setup access to AlexaFo...
AlexaForBusinessFullA...	AWS managed	None	Grants full access to AlexaForBusiness ...
AlexaForBusinessGate...	AWS managed	None	Provide gateway execution access to A...
AlexaForBusinessLifes...	AWS managed	None	Provide access to Lifesize AVS devices
AlexaForBusinessNet...	AWS managed	None	This policy enables Alexa for Business ...
AlexaForBusinessPoly...	AWS managed	None	Provide access to Poly AVS devices

- click create policies.

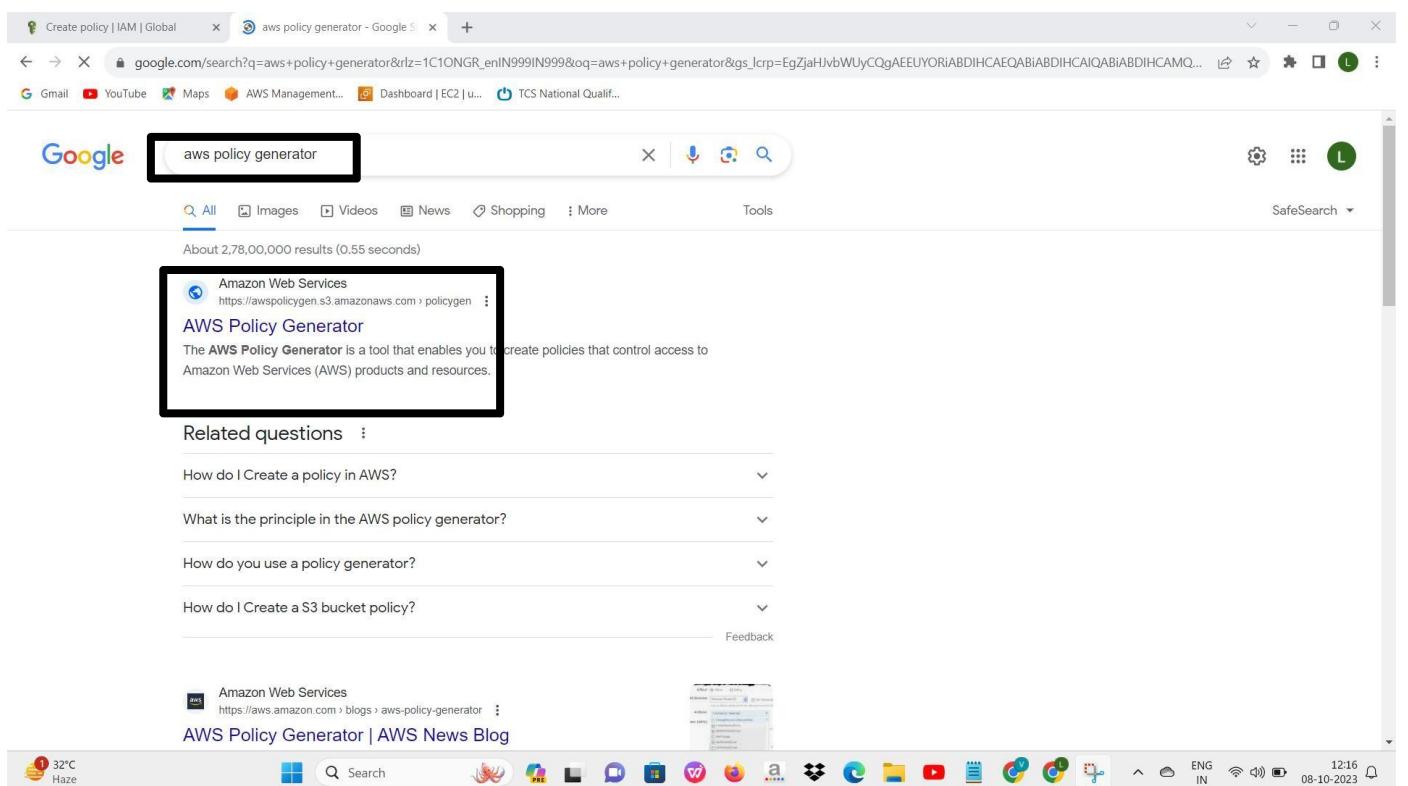


- Click json



- The policy editor window will get open.

- Now open a new tab search for aws policy generator



- Click the aws policy generator.

The screenshot shows the AWS Policy Generator interface. It consists of three main sections:

- Step 1: Select Policy Type**: A dropdown menu is set to "IAM Policy".
- Step 2: Add Statement(s)**:
 - Effect: Allow (radio button selected)
 - AWS Service: Amazon EC2 (dropdown menu)
 - Actions: 5 Action(s) Selected (dropdown menu)
 - Amazon Resource Name (ARN): (*) (input field)
- Step 3: Generate Policy**: A note says "Add one or more statements above to generate a policy."

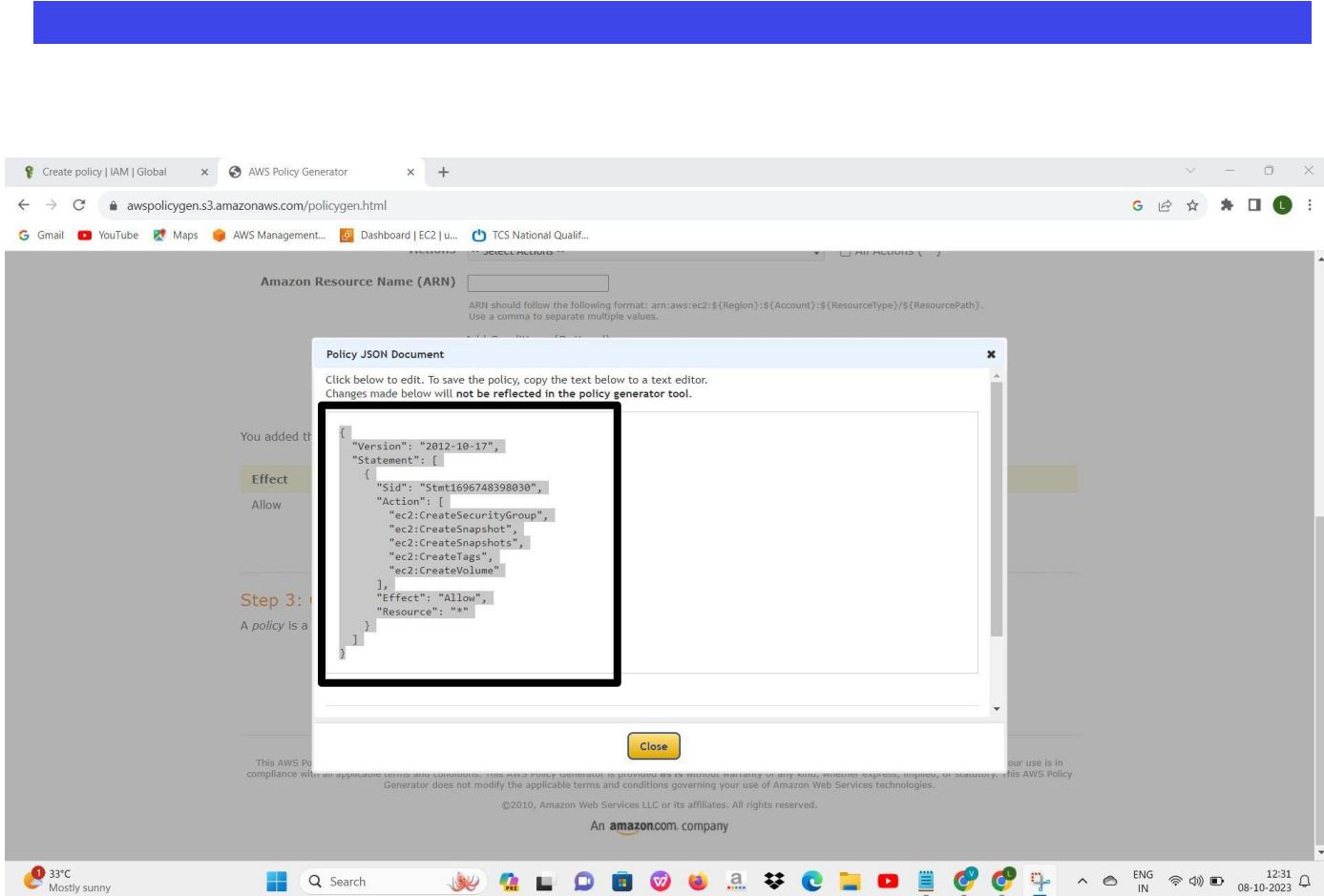
- Choose type as IAM policy.
- effect-allow.
- aws service-amazon EC2
- In actions
- I have selected ,creation of instance,volume,snapshots,etc→you can choose according to your choice.
- Amazon resource name-enter * symbol.
- click add statement.

The screenshot shows the AWS Policy Generator interface. At the top, there's a navigation bar with links like 'Create policy | IAM | Global' and 'AWS Policy Generator'. Below the navigation is a search bar with the URL 'awspolicygen.s3.amazonaws.com/policygen.html'. The main area has several sections:

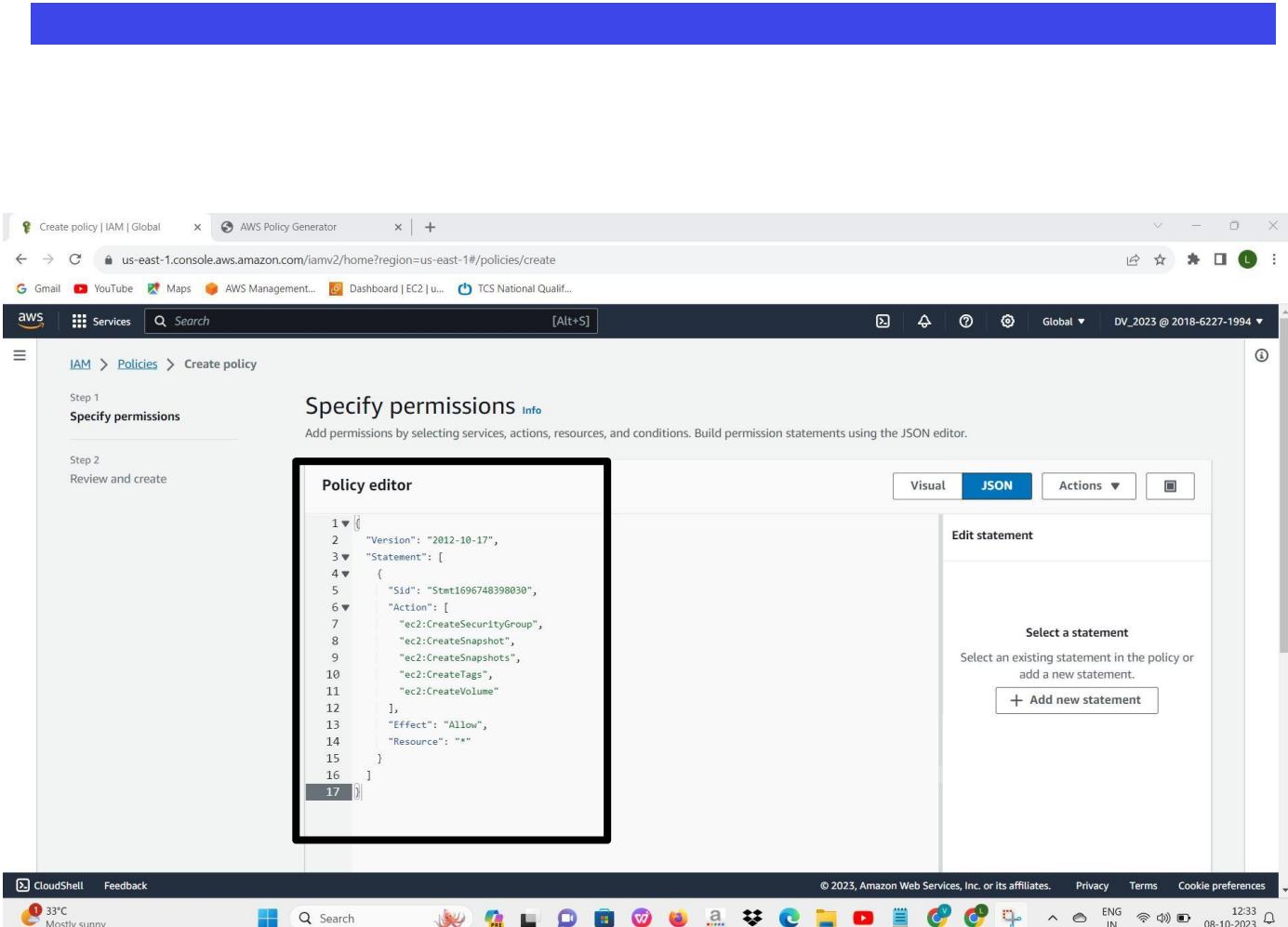
- Amazon Resource Name (ARN)**: A text input field with placeholder text: "ARN should follow the following format: arn:aws:ec2:\${Region}:\${Account}:\${ResourceType}/\${ResourcePath}. Use a comma to separate multiple values."
- Add Conditions (Optional)**: A section with a 'Add Statement' button and a message: "No Action selected. You must select at least one Action".
- A message: "You added the following statements. Click the button below to Generate a policy."
- A table showing the policy statements:

Effect	Action	Resource	Conditions
Allow	<ul style="list-style-type: none">ec2:CreateSecurityGroupec2:CreateSnapshotec2:CreateSnapshotsec2:CreateTagsec2:CreateVolume	*	None
- Step 3: Generate Policy**: A section describing what a policy is and providing a 'Generate Policy' button.
- Footnotes and copyright information at the bottom.
- The taskbar at the bottom shows various application icons and system status.

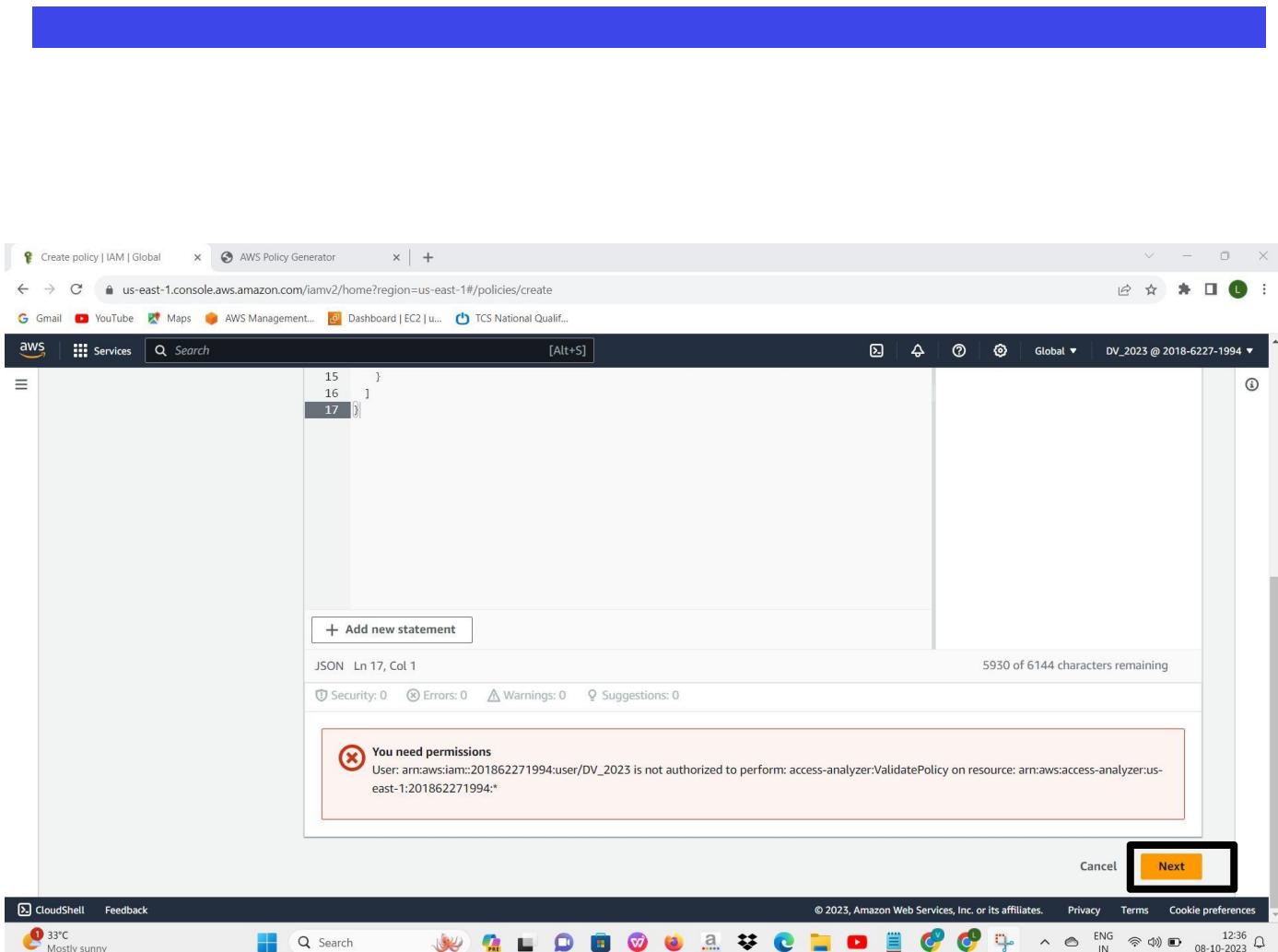
- Click generate policy.



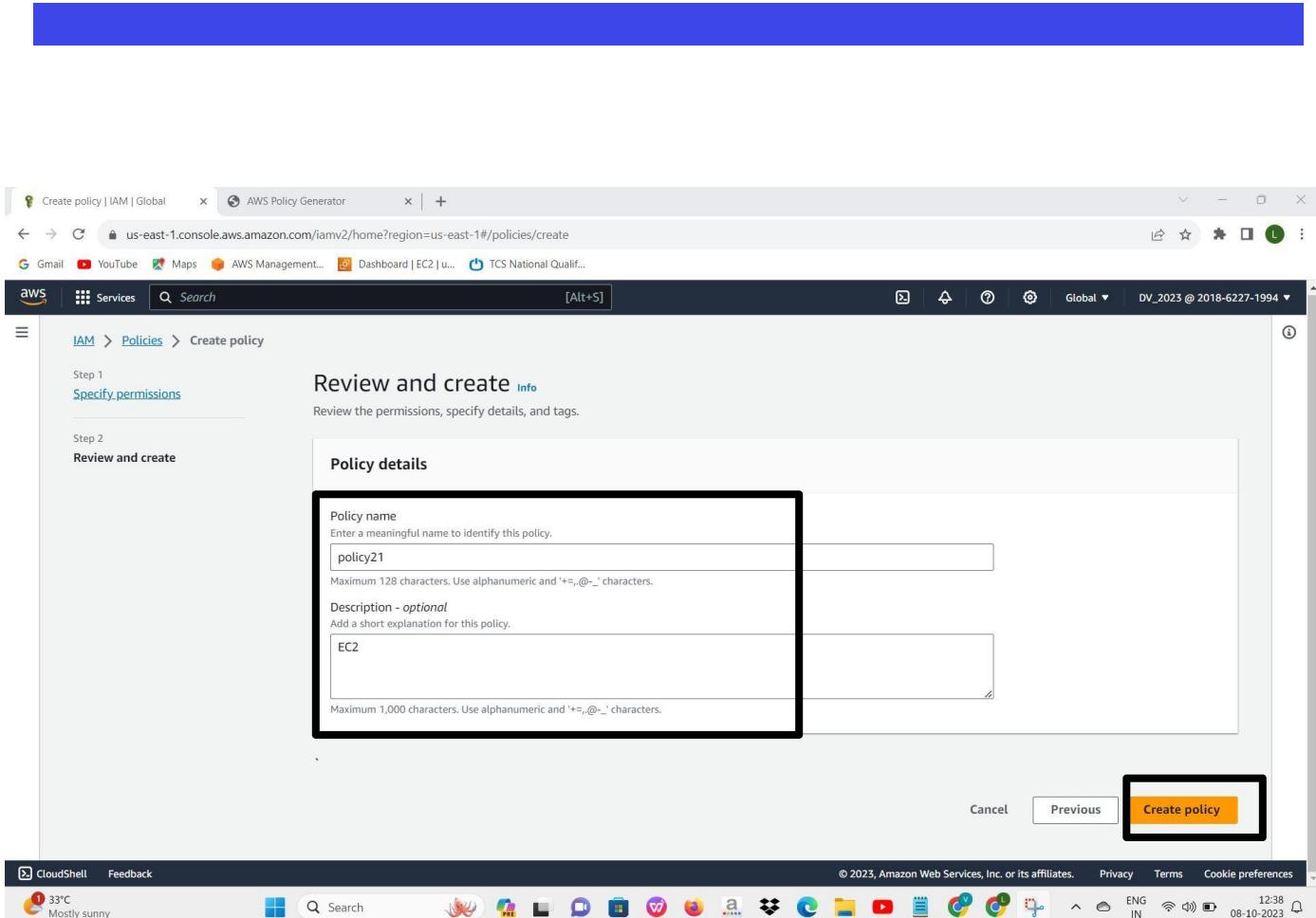
- The policy has been generated successfully. copy it.



- Back to aws.
- paste it in the policy editor.



- click next.



- Give name.
- Click create policy.

The screenshot shows the AWS Identity and Access Management (IAM) Policies page. On the left, there's a navigation sidebar with links like 'Identity and Access Management (IAM)', 'Dashboard', 'Access management', 'Policies', and 'Access reports'. The main content area is titled 'Policies (1085)' and contains a table of existing policies. A new policy, '001_policy', has just been created and is highlighted with a black border. The table columns include 'Policy name', 'Type', 'Used as', and 'Description'. The 'Description' column for '001_policy' states 'policy creation'. At the bottom of the page, there are links for 'CloudShell', 'Feedback', 'Language', and copyright information: '© 2023, Amazon Web Services, Inc. or its affiliates.' followed by 'Privacy', 'Terms', and 'Cookie preferences'.

Policy name	Type	Used as	Description
001_policy	Customer managed	None	policy creation
s3cr_for_s3versbucket_49b6be	Customer managed	Permissions policy (1)	
AdministratorAccess	AWS managed - j...	None	Provides full access to Al...
PowerUserAccess	AWS managed - j...	None	Provides full access to Al...
ReadOnlyAccess	AWS managed - j...	None	Provides read-only acces...
AWSCloudFormationReadOnlyAccess	AWS managed	None	Provides access to AWS...
CloudFrontFullAccess	AWS managed	None	Provides full access to th...

- The policy has been created successfully

The screenshot shows the AWS Identity and Access Management (IAM) service interface. The left sidebar is titled 'Identity and Access Management (IAM)' and includes sections for 'Dashboard', 'Access management' (with 'User groups', 'Users' selected, and 'Roles', 'Policies', 'Identity providers', 'Account settings'), and 'Access reports' (with 'Access analyzer', 'Archive rules', 'Analyzers', 'Settings', 'Credential report'). The main content area is titled 'IAM > Users'. A banner at the top says 'Ready to streamline human access to AWS and cloud apps?' with a 'Dismiss' button and a 'Manage workforce users' link. Below the banner, it says 'Identity Center is enabled. We recommend managing workforce users' access to AWS accounts and cloud applications in Identity Center.' with 'Learn more' and 'Watch how it works' links. The 'Users' table lists one item: 'VD_25'. The table has columns for 'User name', 'Path', 'Group', 'Last activity', 'MFA', 'Password age', and 'Console last sign-in'. At the bottom of the page, there's a 'Feedback' section with a weather icon (33°C, Mostly sunny), a search bar, and various browser icons. The status bar at the bottom right shows 'ENG IN', '13:46', '08-10-2023', and a battery icon.

- Go to users.
- click the user name.

The screenshot shows the AWS IAM Permissions page for a user named 'VD_25'. The left sidebar has 'Identity and Access Management (IAM)' selected. The main content area shows a table for 'Permissions policies (1)'. The table has one row with the following details:

Policy name	Type	Attached via
IAMUserChangePassword	AWS managed	Directly

Below the table, there's a section for 'Permissions boundary (not set)' and a 'Generate policy based on CloudTrail events' section with a 'Generate policy' button.

- Here you can see permission .
- Click the dropdown

The screenshot shows the AWS Identity and Access Management (IAM) service interface. The left sidebar is titled 'Identity and Access Management (IAM)' and includes sections for Dashboard, Access management (with sub-options like User groups, Users, Roles, Policies, Identity providers, Account settings), and Access reports (with sub-options like Access analyzer, Archive rules, Analyzers, Settings, Credential report). The main content area is titled 'Permissions' and shows a table of permissions policies. One policy is listed: 'IAMUserChangePassword' (Type: AWS managed, Attached via Directly). There is also a section for 'Generate policy based on CloudTrail events' with a 'Generate policy' button. The top navigation bar shows the URL 'us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users/details/VD_25?section=permissions'. The browser taskbar at the bottom shows various open tabs and system icons.

- click add permissions.

The screenshot shows the AWS IAM Policy Generator interface. At the top, there are three tabs: 'Add permissions | IAM | Global', 'AWS Policy Generator', and a third tab which is partially visible. Below the tabs, the URL is 'us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users/details/VD_25/add-permissions'. The main content area has a dark header bar with the AWS logo, 'Services', a search bar, and various global settings. The main panel is titled 'Permissions options' and contains three radio button options:

- Add user to group: 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, inline policies, and any existing permissions boundaries 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 this is a section titled 'Permissions policies (1132)' with a 'Filter by Type' dropdown set to 'All types'. A table lists several AWS managed policies:

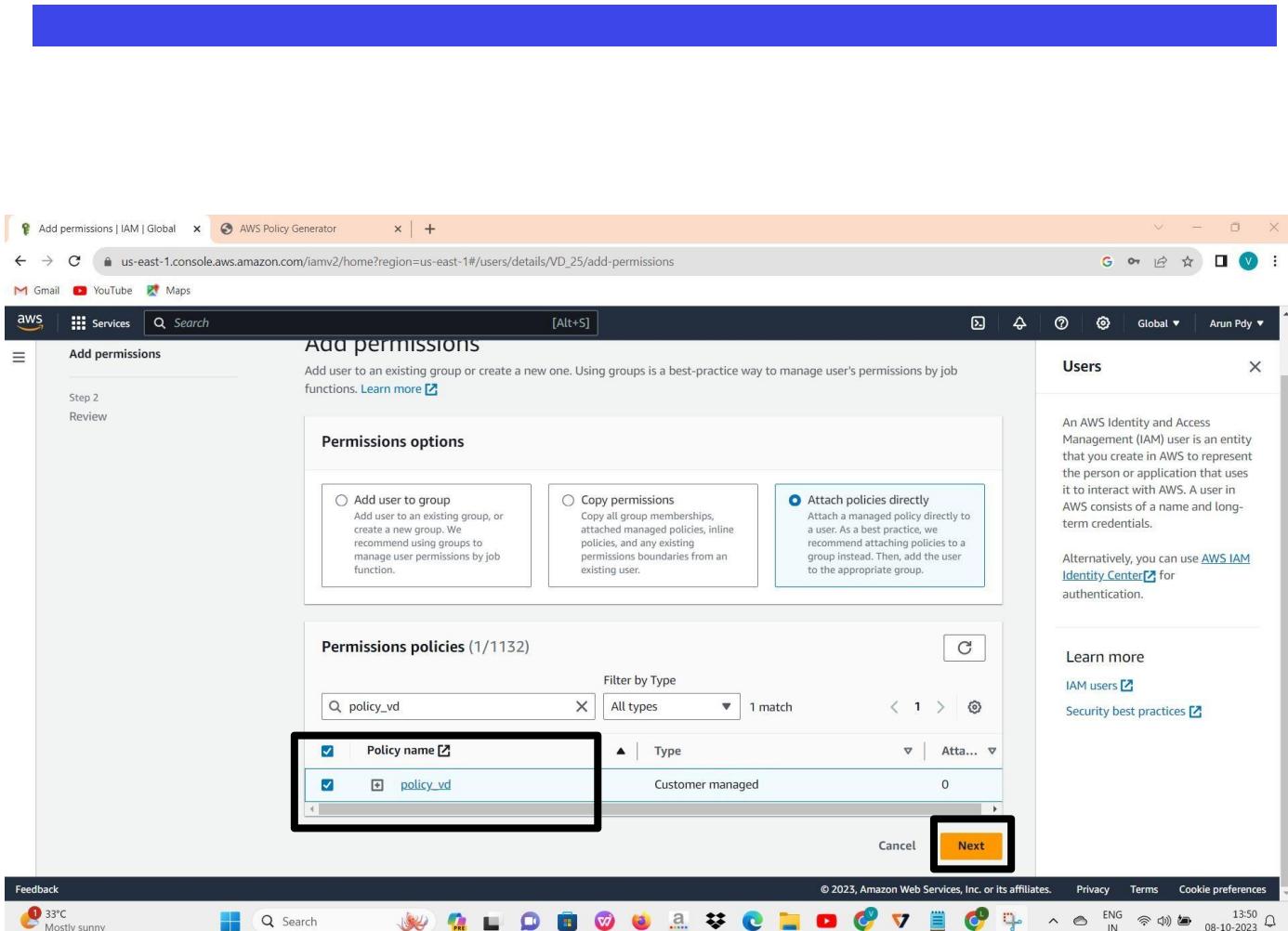
Policy name	Type	Attachments
AccessAnalyzerServiceRolePolicy	AWS managed	0
AdministratorAccess	AWS managed - job function	0
AdministratorAccess-Amplify	AWS managed	0
AdministratorAccess-AWSElasticBea...	AWS managed	0
AlexaForBusinessDeviceSetup	AWS managed	0

On the right side of the screen, there is a sidebar titled 'Users' with the following content:

- An introduction: 'An AWS Identity and Access Management (IAM) user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user in AWS consists of a name and long-term credentials.'
- A note: 'Alternatively, you can use [AWS IAM Identity Center](#) for authentication.'
- A 'Learn more' section with links to 'IAM users' and 'Security best practices'.

At the bottom of the browser window, there is a toolbar with icons for weather, search, and various system functions, along with the date and time (08-10-2023).

- Select attach policies directly.



- Here you can see the policy that we created.
- choose tit.
- Click the next.

The screenshot shows the AWS IAM console interface. The user is in the 'Add permissions' step for a user named 'VD_25'. The 'User details' section shows the user name 'VD_25'. The 'Permissions summary' table lists one policy: 'policy_vd' (Customer managed, Used as Permissions policy). The 'Add permissions' button is highlighted with a yellow box.

Name	Type	Used as
policy_vd	Customer managed	Permissions policy

- Click add permissions.

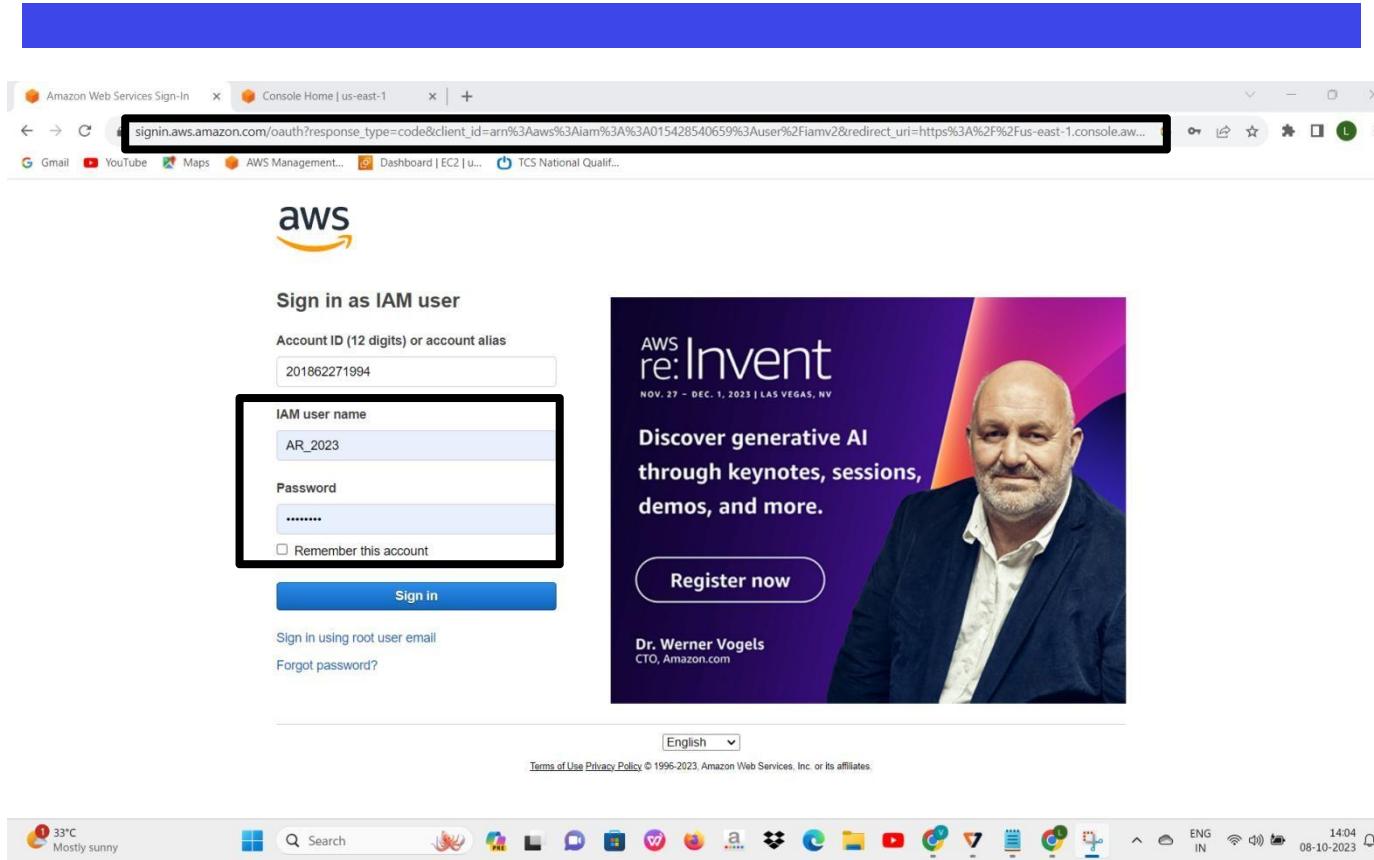
The screenshot shows the AWS IAM Policy Generator interface. At the top, there's a blue header bar. Below it, the browser title bar displays "us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users/details/VD_25?section=permissions". The main content area has a dark header with tabs: "Permissions", "Groups", "Tags", "Security credentials", and "Access Advisor". A green banner at the top of the content area says "1 policy added". Below this, the "Permissions policies (2)" section is visible, listing two policies: "IAMUserChangePassword" (AWS managed, Directly) and "policy_vd" (Customer managed, Directly). There are also sections for "Permissions boundary (not set)" and "Generate policy based on CloudTrail events". The left sidebar contains navigation links for IAM: Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), Access reports (Access analyzer, Archive rules, Analyzers, Settings, Credential report), and Feedback. The bottom of the screen shows the Windows taskbar with various pinned icons and system status.

The policy has been added successfully

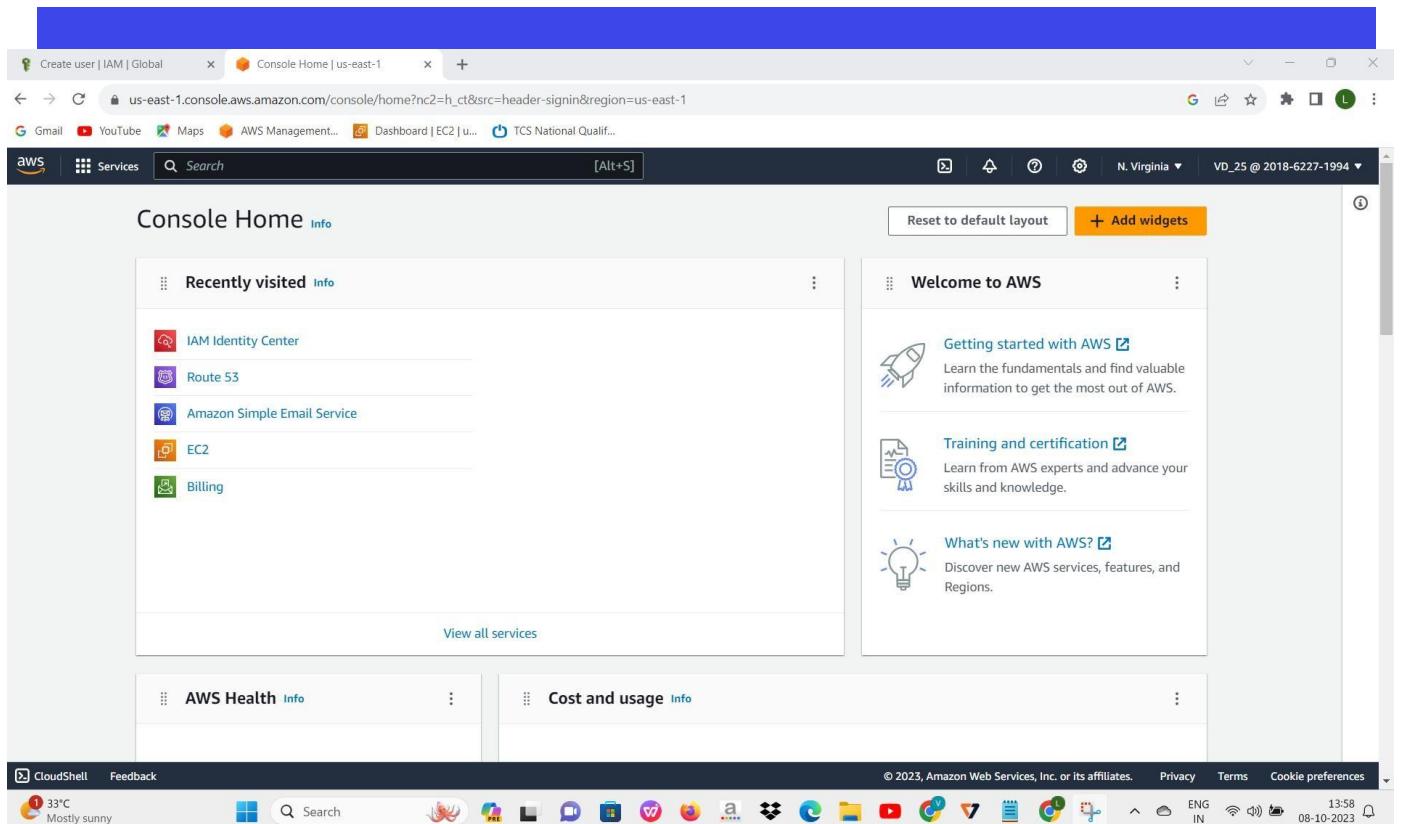


The screenshot shows the AWS Identity and Access Management (IAM) console. A green banner at the top indicates "1 policy added". The "Security credentials" tab is selected. In the "Console sign-in" section, a message says "Console sign-in link copied" with a green checkmark icon. Below it is a URL: <https://201862271994.signin.aws.amazon.com/console>. To the right, there are fields for "Console password" (updated 37 minutes ago), "Last console sign-in" (Never), and a note about MFA. The left sidebar shows navigation links for Identity and Access Management (IAM), Access management, Access reports, and Feedback.

- Now go to security credentials.
- copy the url.
- paste in new tab.



- Now login with the username and password.



- The user has been successfully logged In.
- you can now able to access only the resources according to policy.
- The resources not attached to the policies will not be accessed.



THANK YOU