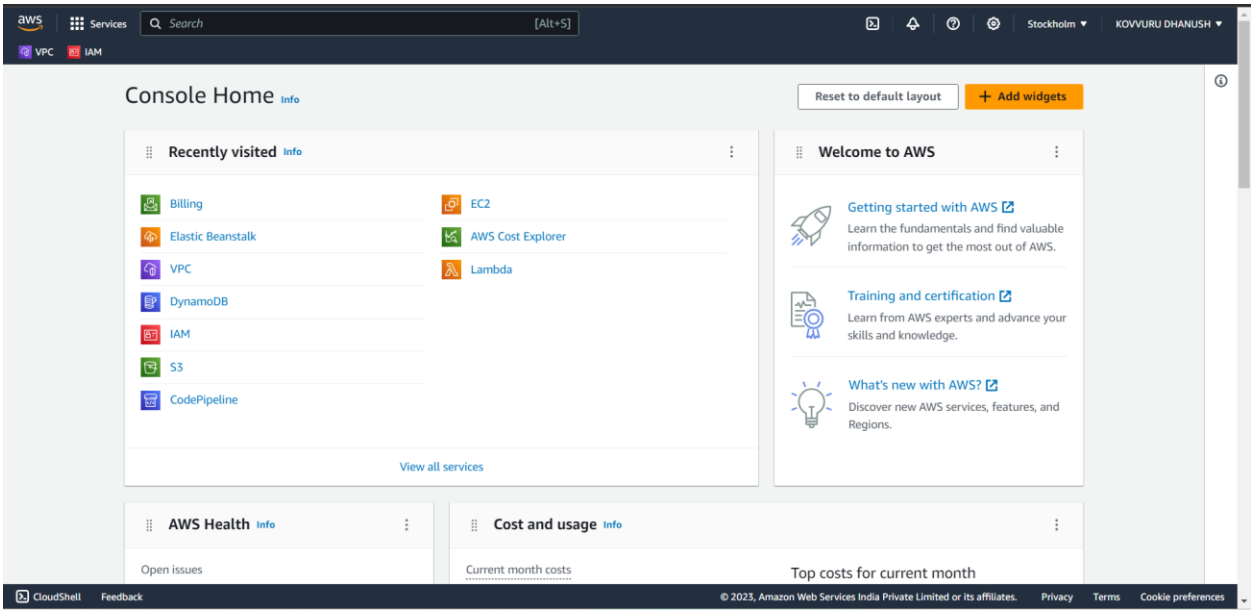
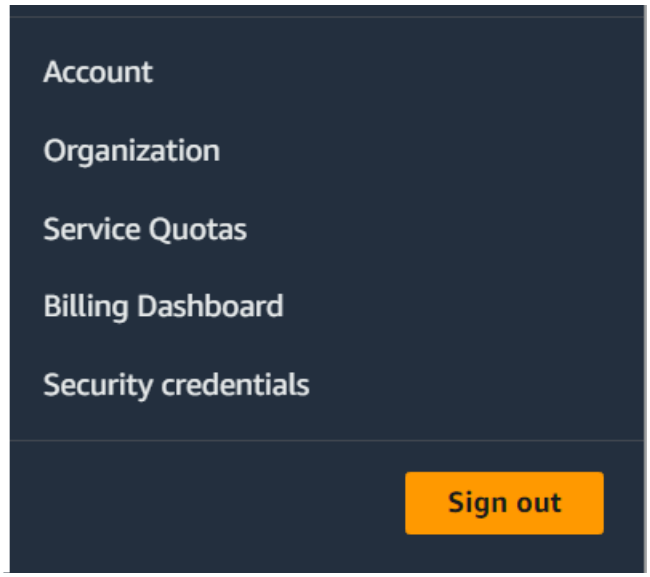
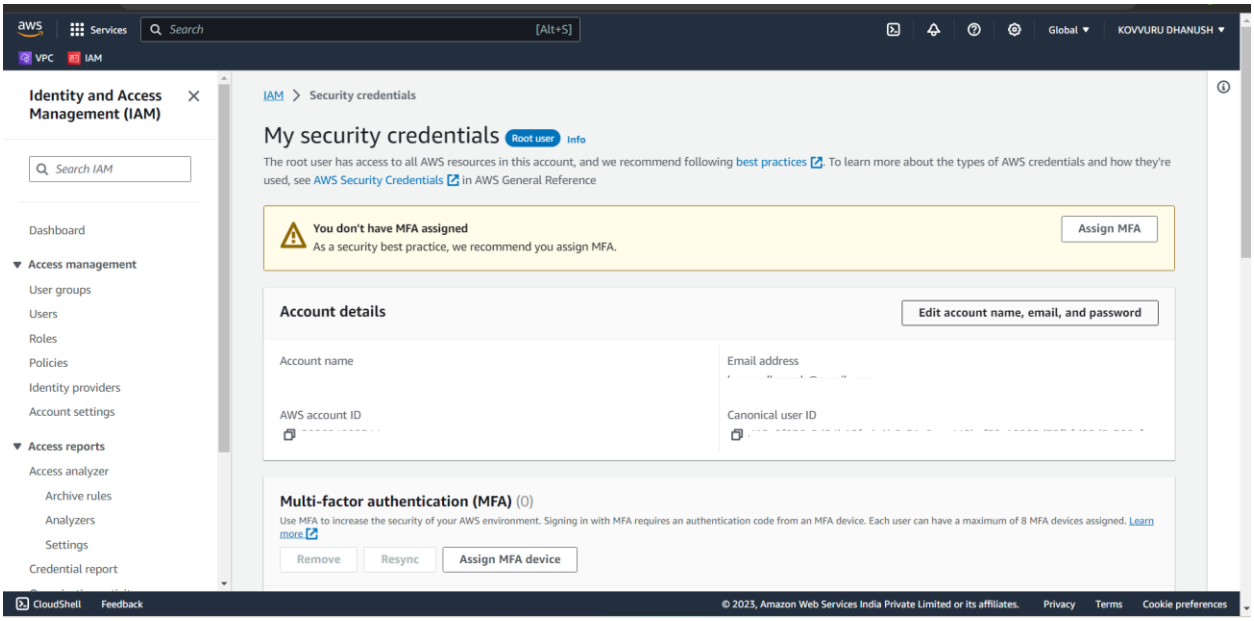
MFA AND ROLES

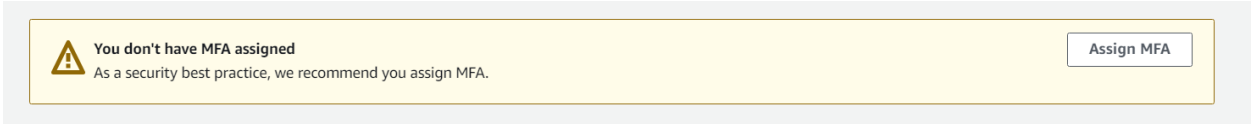


Login to your account.



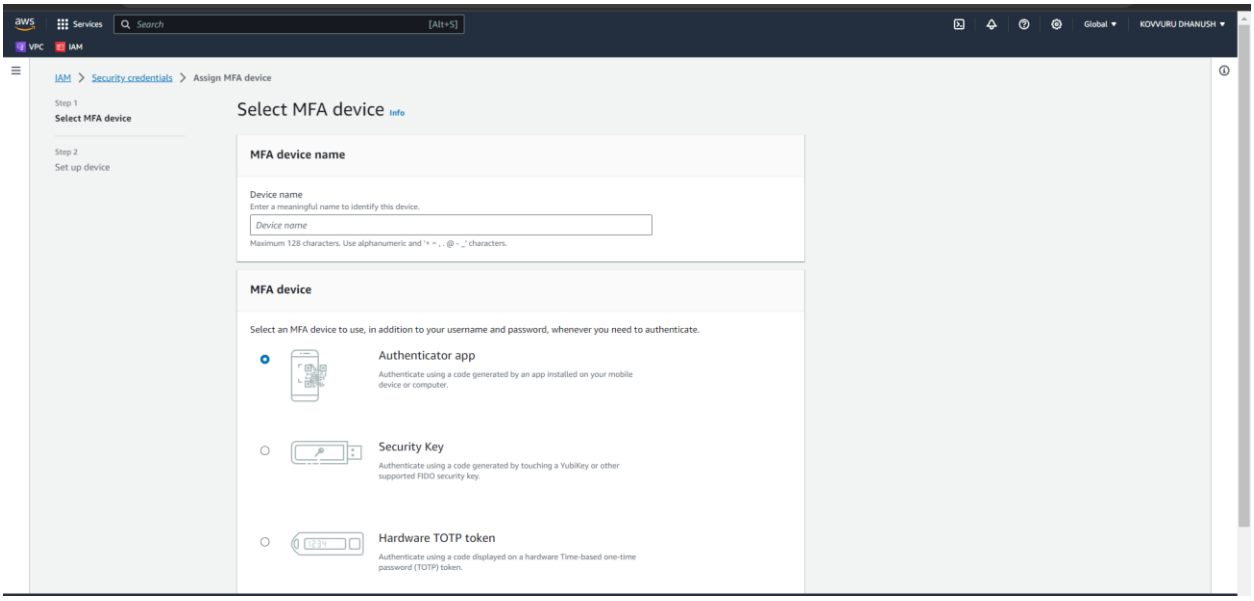
Click on security credentials.





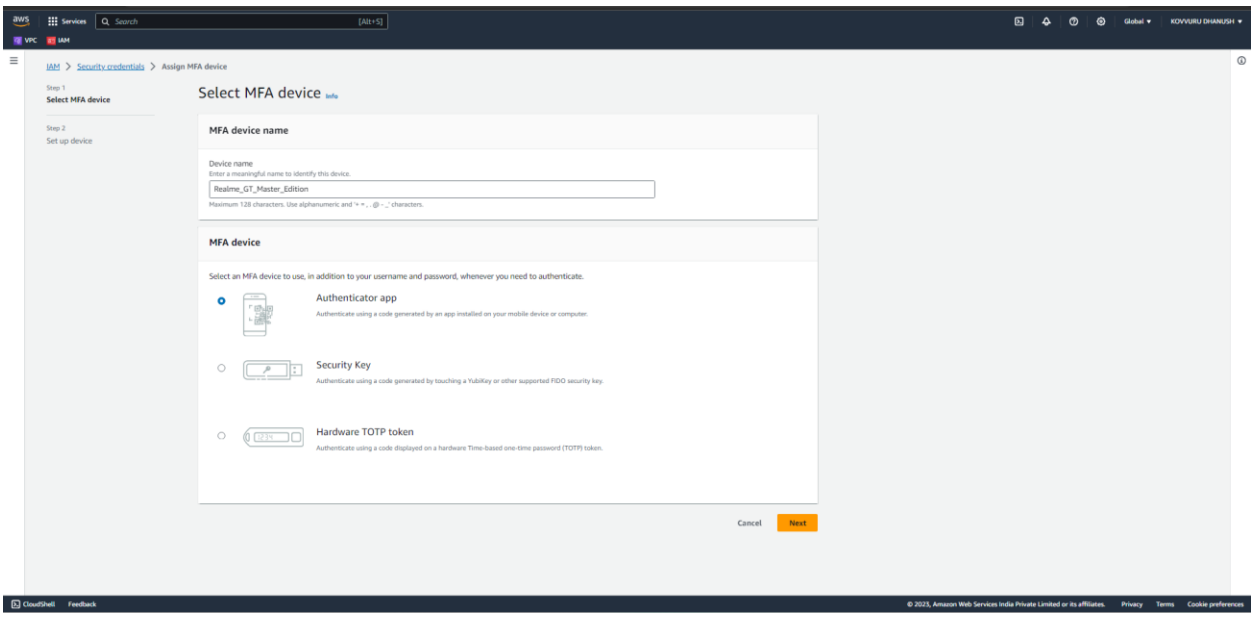
Check here it is asking us to assign MFA as we are root user as per AWS recommendations it Is asking us to ASSGIN MFA.

NOW Click on Assign MFA.

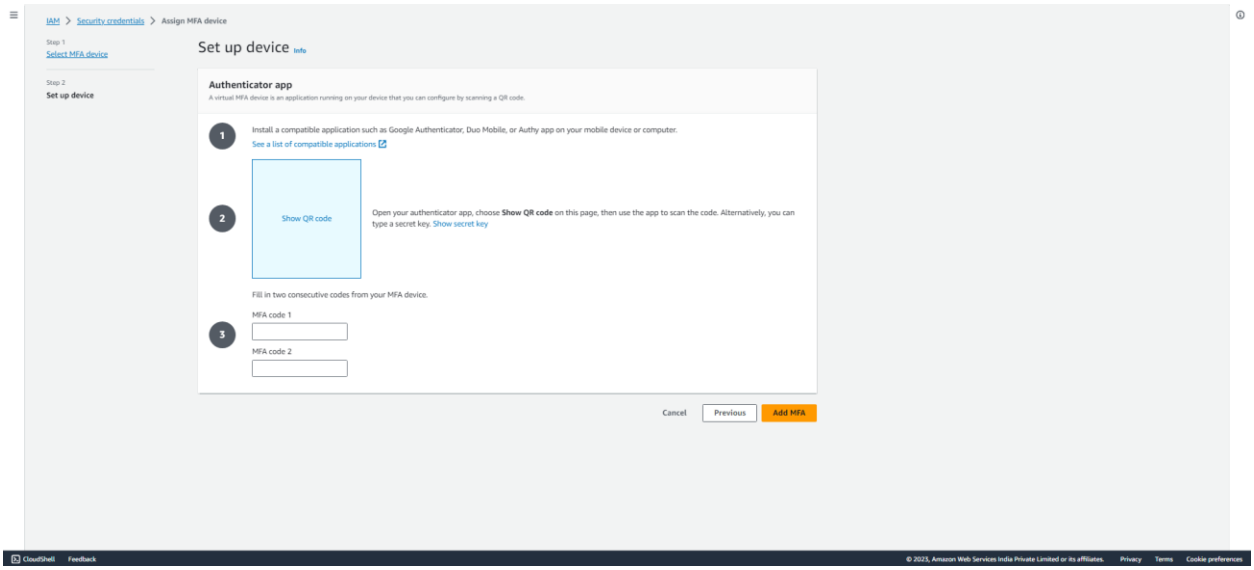


Then you will be landed on this page.

Here it is asking us to provide the device name, here in my case Realme GT Master Edition.



Now click on next.



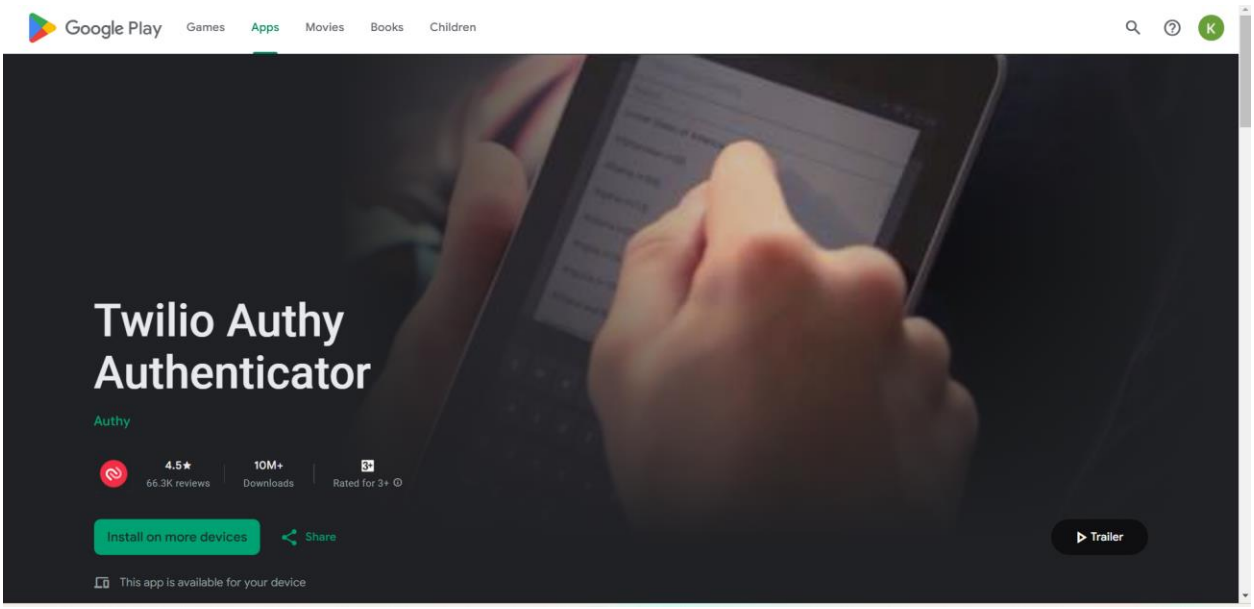
Click on see a list of compatible applications.

Android	Twilio Authy Authenticator, Duo Mobile, Microsoft Authenticator, Google Authenticator, Symantec VIP
iOS	Twilio Authy Authenticator, Duo Mobile, Microsoft Authenticator, Google Authenticator, Symantec VIP

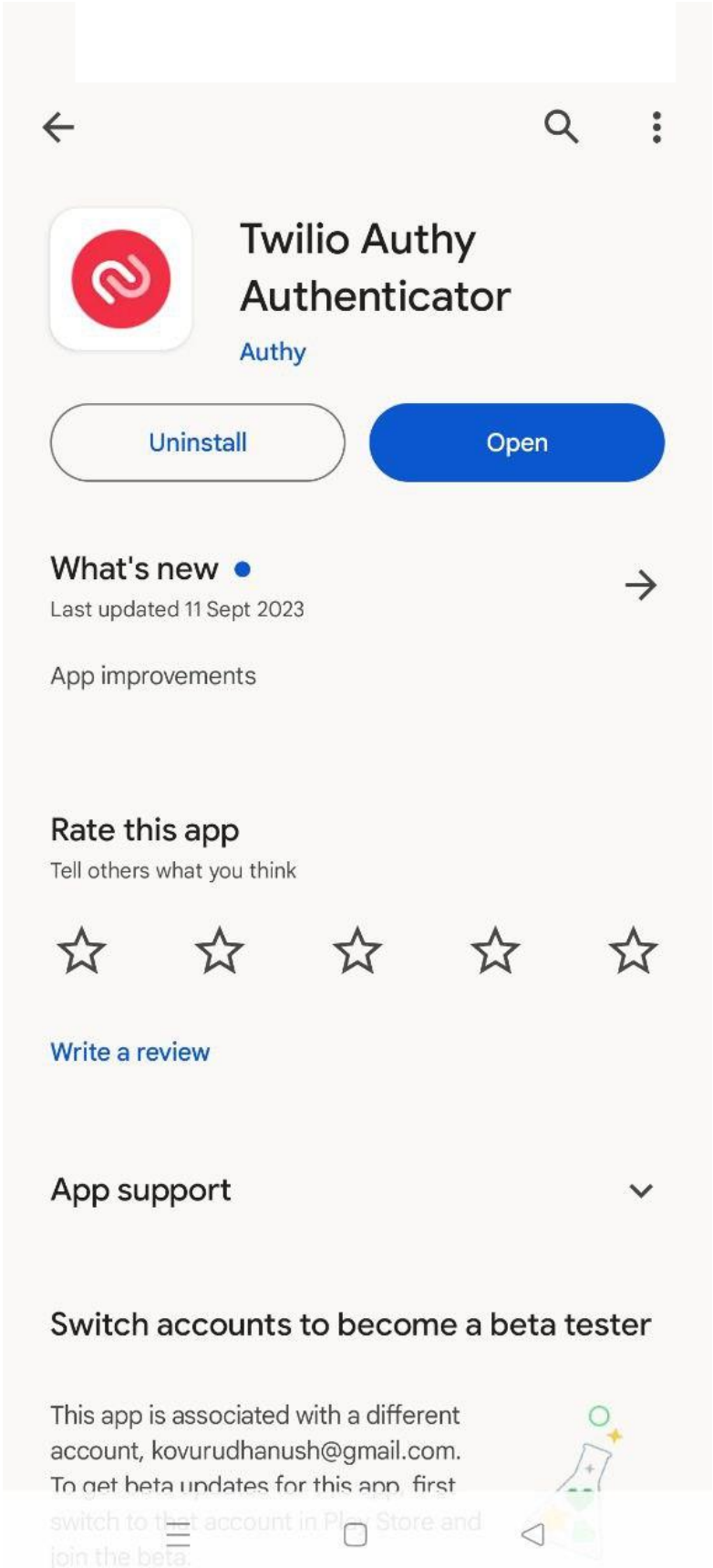
Here my device is Android, so these are the compatible applications if yours's IOS then download anyone.

Here I'm using Twilio Authy Authenticator.

So, click on Twilio Authy Authenticator.



Open your mobile and download the Authy Authenticator.

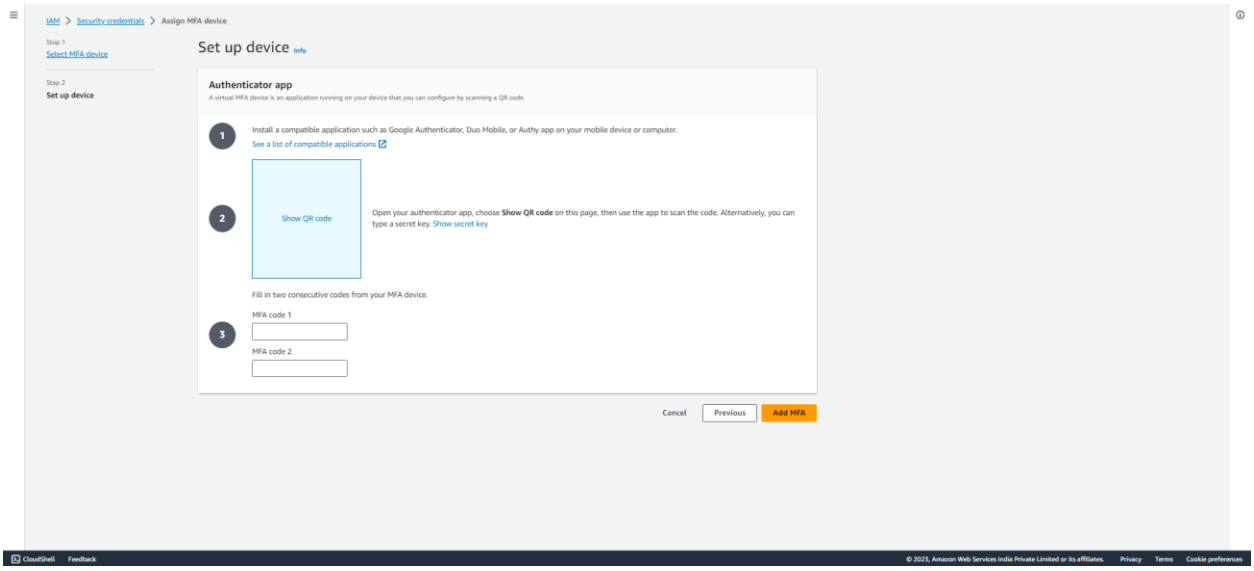

Twilio Authy Authenticator
Authy
Uninstall
Open
What's new
Last updated 11 Sept 2023
App improvements
Rate this app
Tell others what you think
Write a review
App support
Switch accounts to become a beta tester
This app is associated with a different account, kovurudhanush@gmail.com. To get beta updates for this app, first switch to that account in Play Store and join the beta.

here in my case, it is already installed.

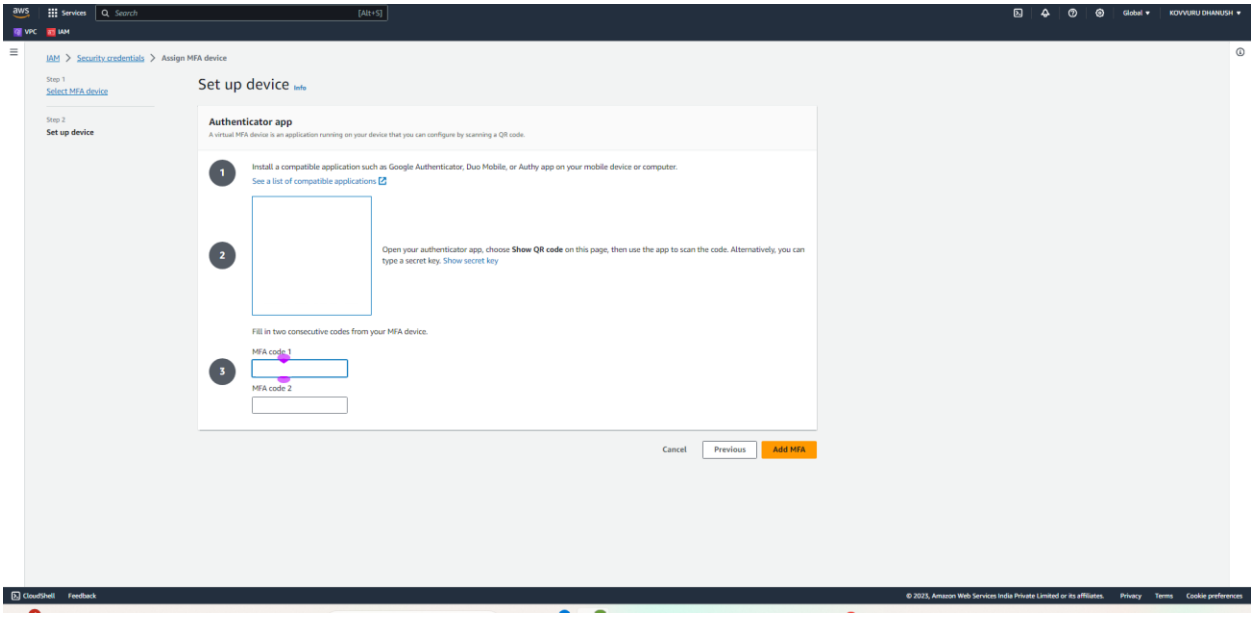
After the installation open the App.

Click on add Account.

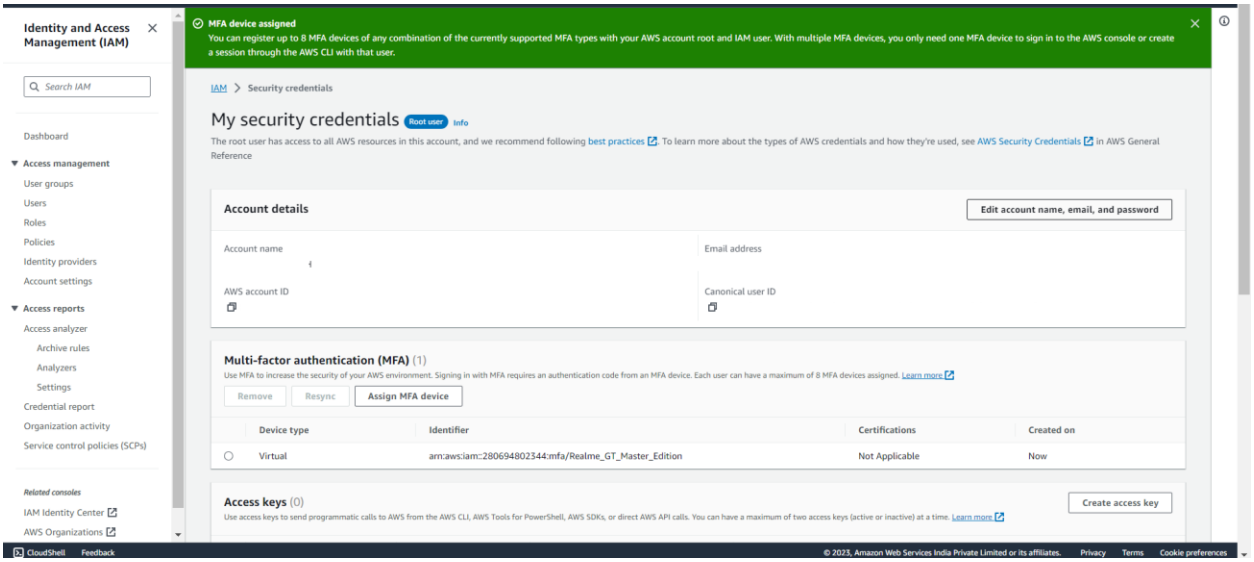
Next click on scan QR Code.



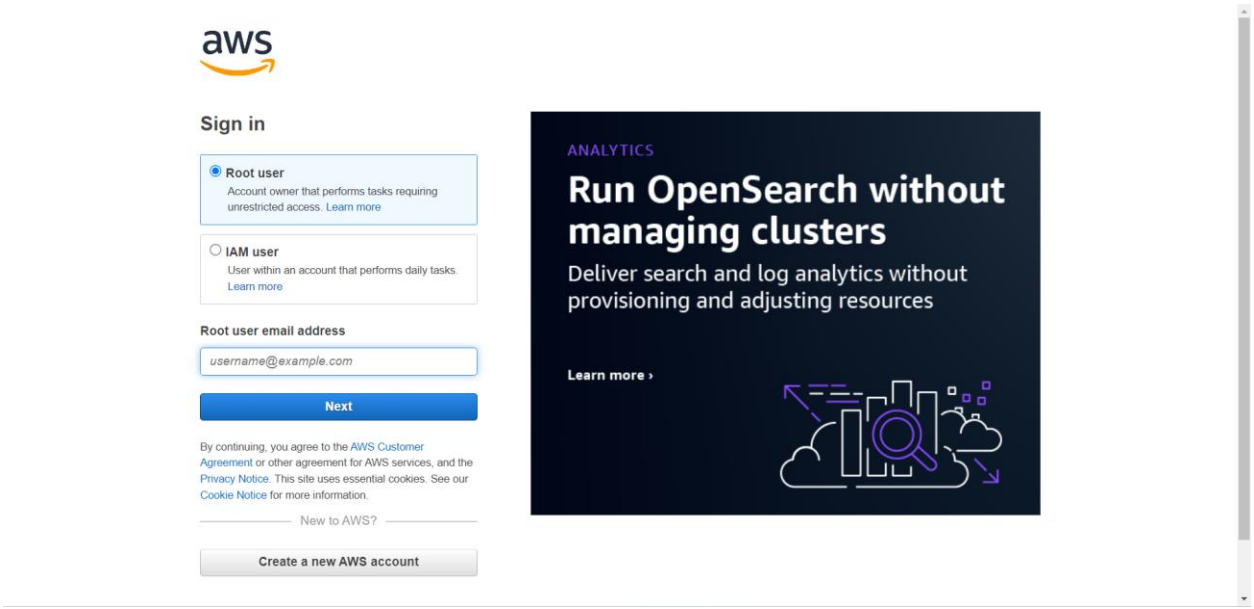
Click on show QR Code.



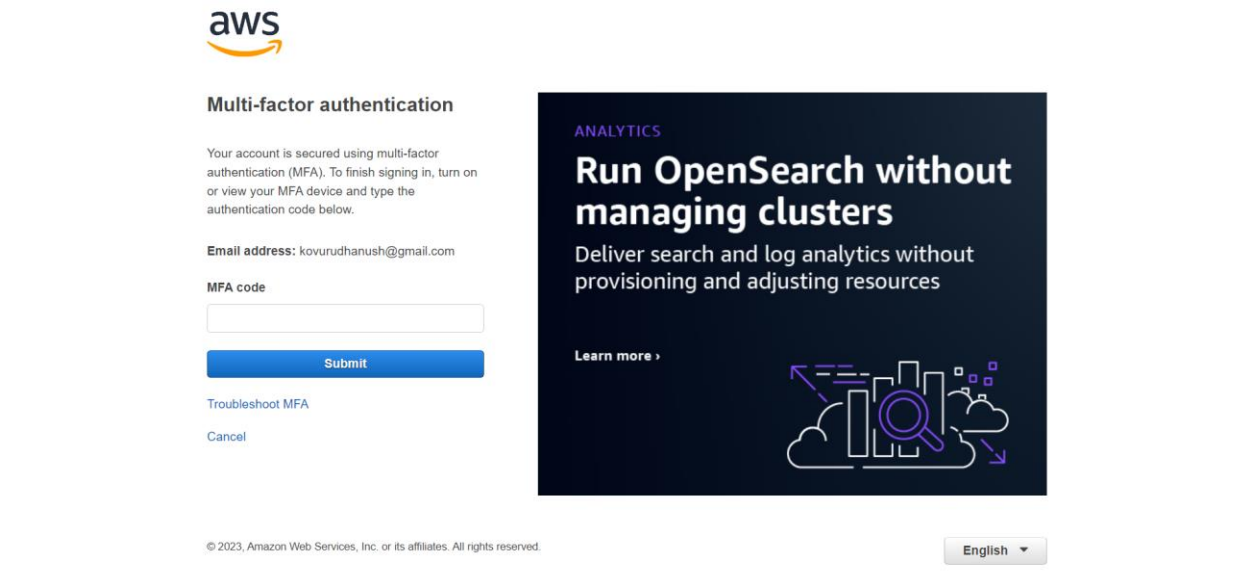
After scanning we need to add MFA Code 1,2 and click on Add MFA.

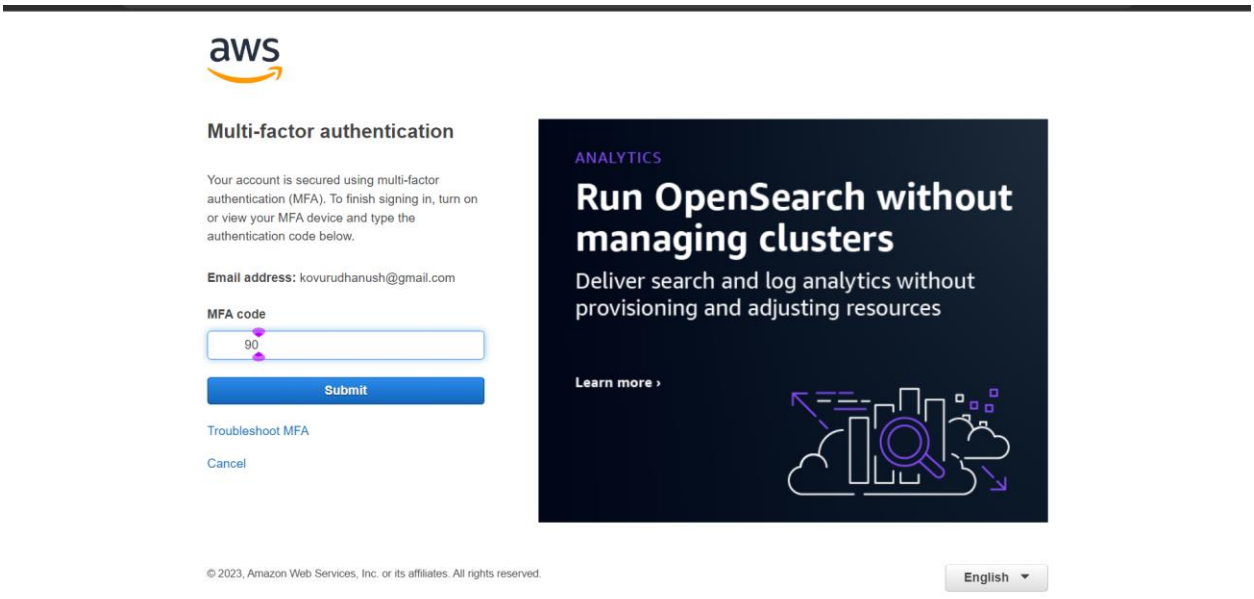


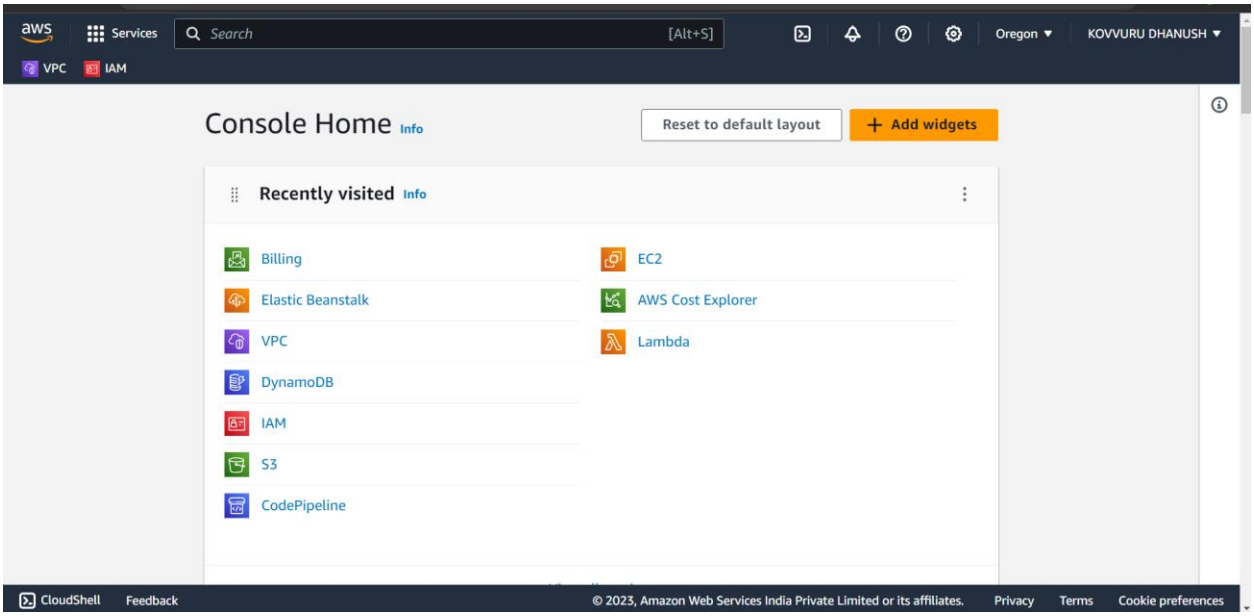
Here MFA is added successfully.



Enter your email.







Now I have log into my account successfully.

Google Authenticator

Google LLC

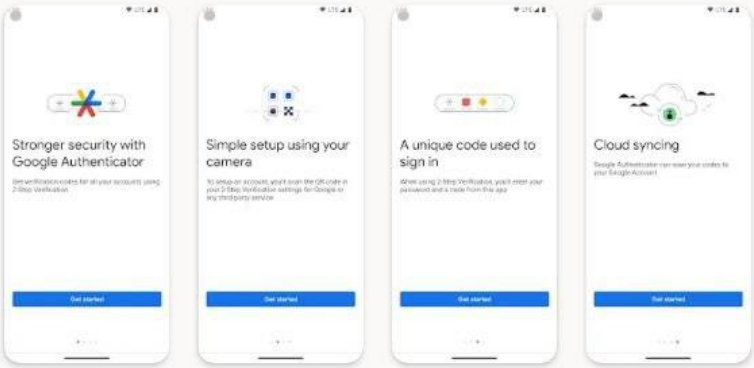
3.9★
452K reviews

7.0 MB

3+
Rated for 3+

Install

Install on phone. More devices available.



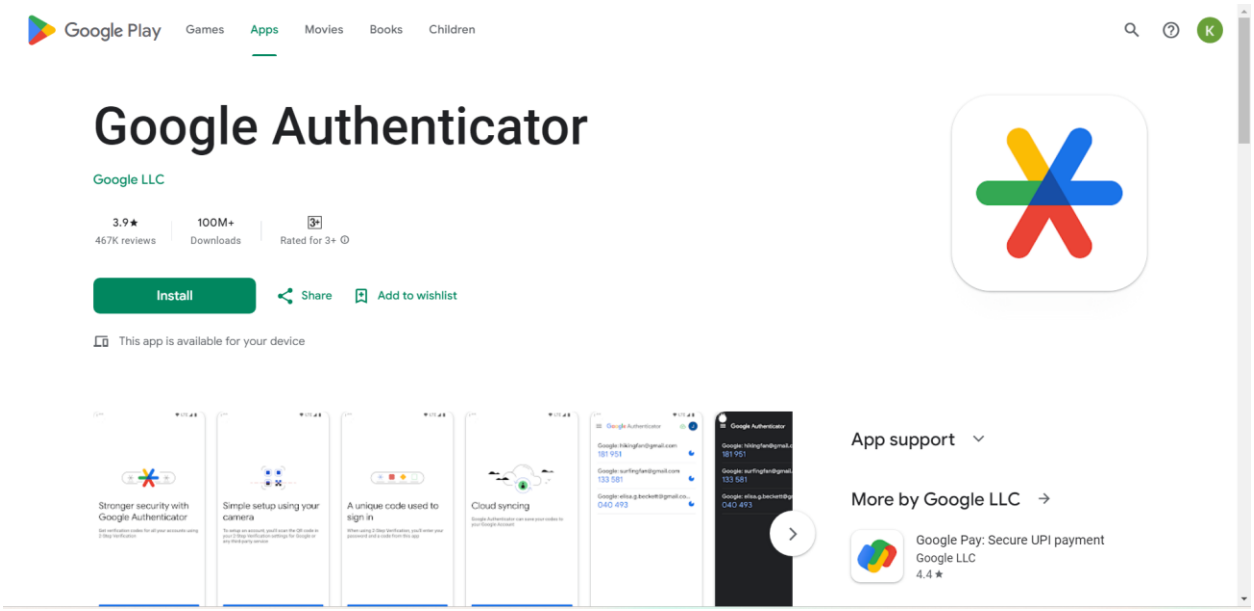
About this app

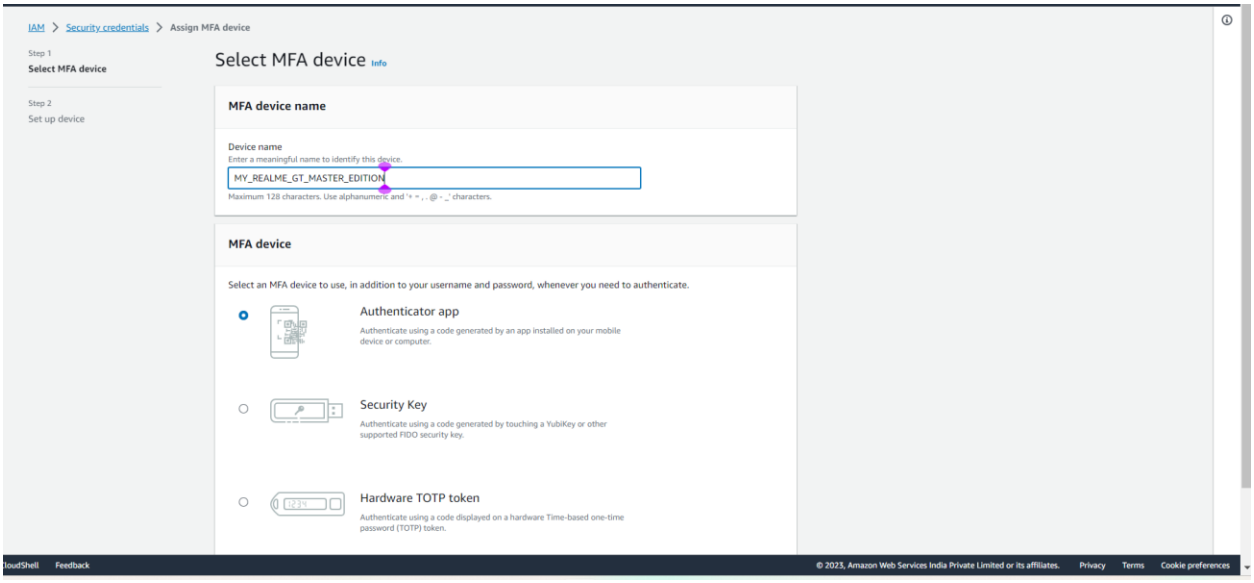
Enable 2-step verification to protect your account from hijacking.

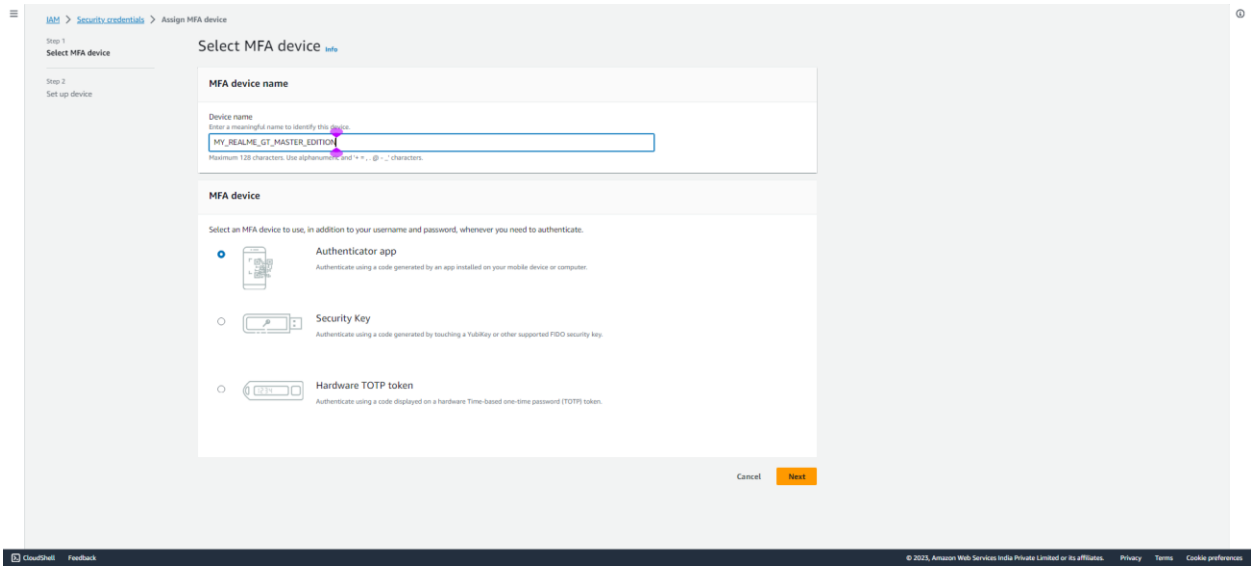
Tools

Data safety

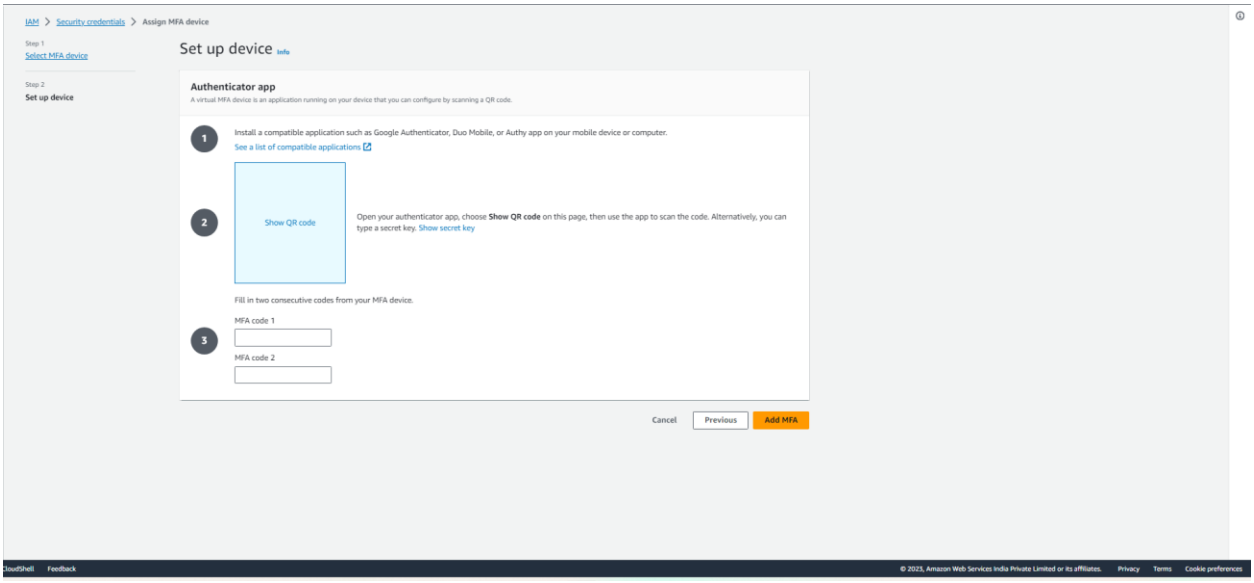
Safety starts with understanding how developers collect and share your data. Data privacy and security


Google Play
Games
Apps
Movies
Books
Children
Google Authenticator
Google LLC
3.9★
467K reviews
100M+
Downloads
3+
Rated for 3+
Install
Share
Add to wishlist
This app is available for your device
Stronger security with Google Authenticator
Simple setup using your camera
A unique code used to sign in
Cloud syncing
App support
More by Google LLC
Google Pay: Secure UPI payment
Google LLC
4.4★

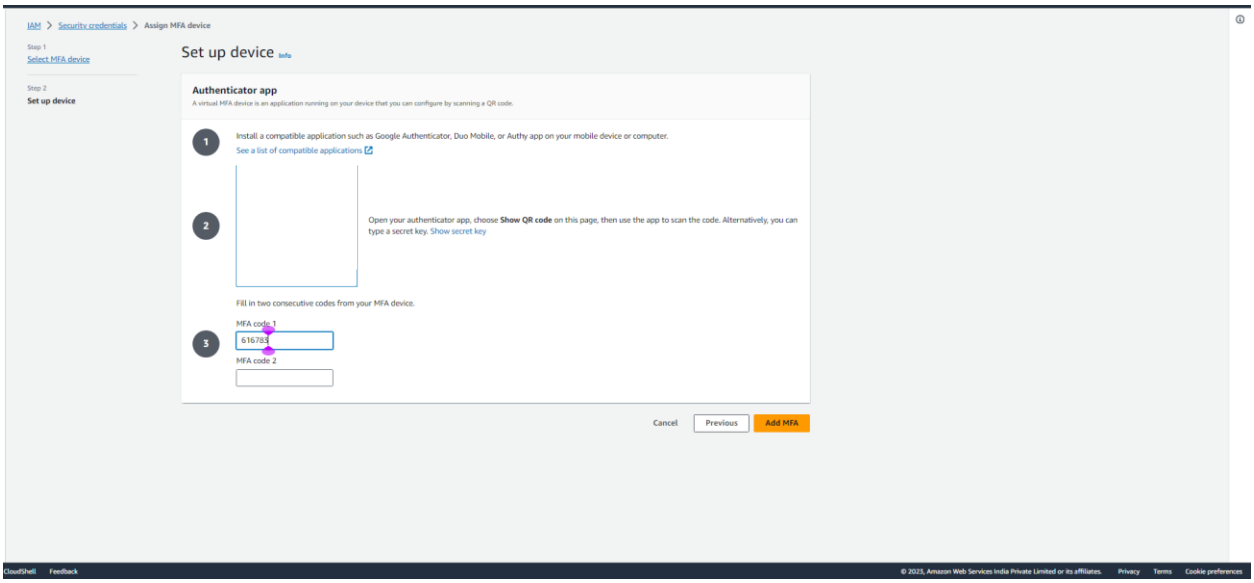

IAM
Security credentials
Assign MFA device
Step 1
Select MFA device
Step 2
Set up device
Select MFA device
Info
MFA device name
Device name
Enter a meaningful name to identify this device.
MY_REALME_GT_MASTER_EDITION
Maximum 128 characters. Use alphanumeric and '+ = , . @ - _' characters.
MFA device
Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.
Authenticator app
Authenticate using a code generated by an app installed on your mobile device or computer.
Security Key
Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.
Hardware TOTP token
Authenticate using a code displayed on a hardware Time-based one-time password (TOTP) token.
CloudShell
Feedback
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

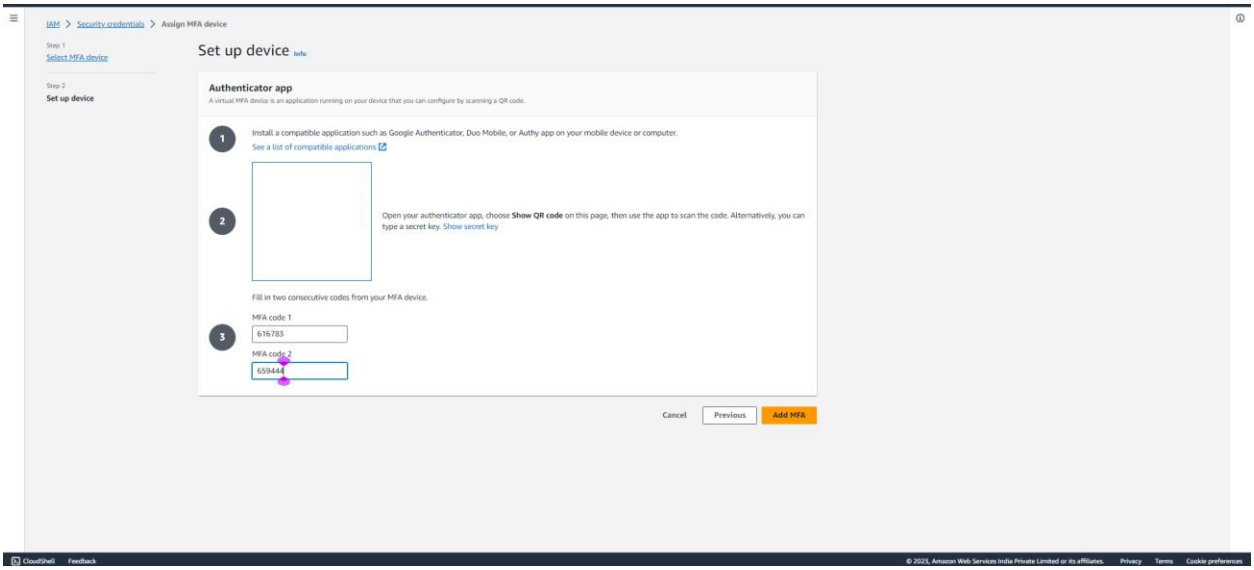


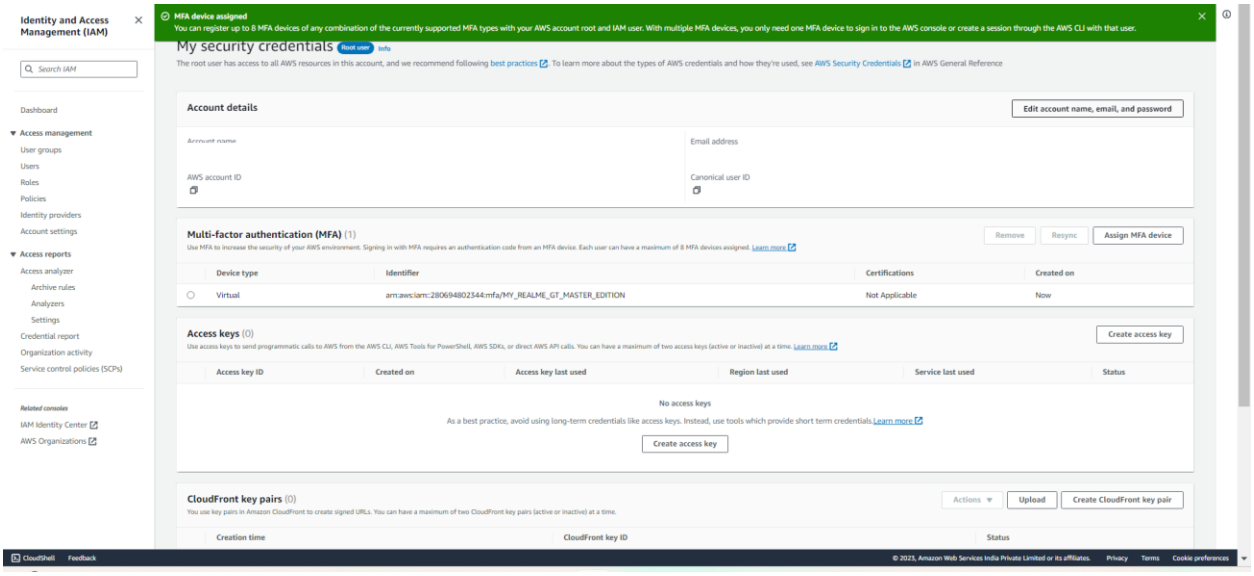
Click on next.



Now click on show QR Code and add MFA 1, 2 .

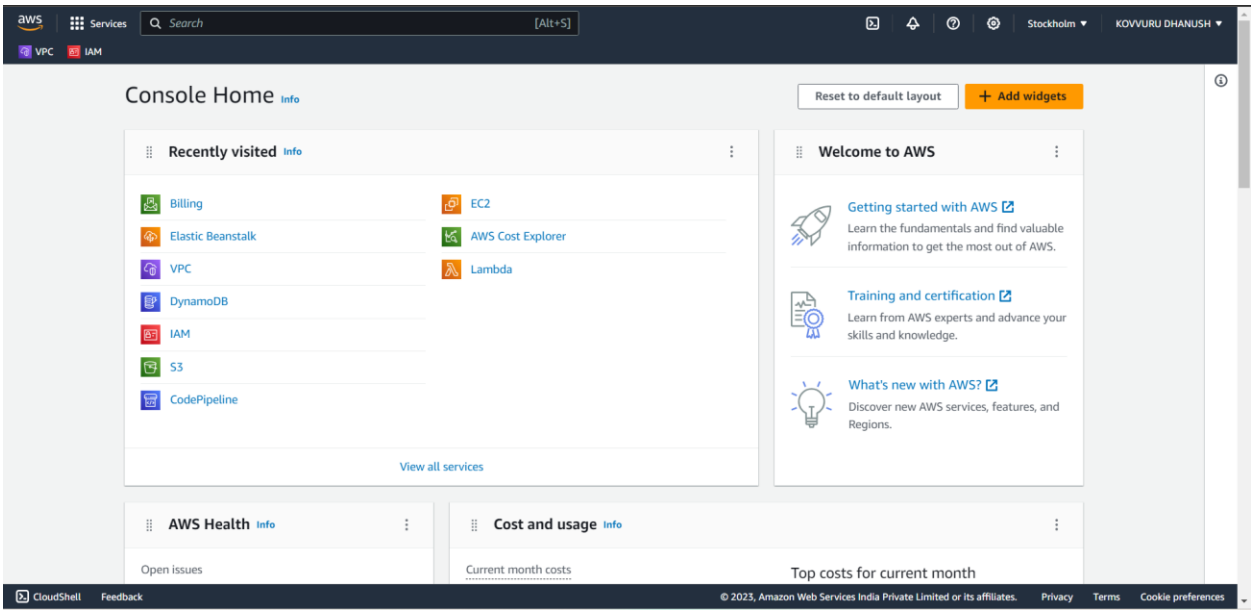

IAM > Security credentials > Assign MFA device
Step 1
Select MFA device
Step 2
Set up device
Set up device Info
Authenticator app
A virtual MFA device is an application running on your device that you can configure by scanning a QR code.
1
Install a compatible application such as Google Authenticator, 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
Fill in two consecutive codes from your MFA device.
3
MFA code 1
616783
MFA code 2
Cancel
Previous
Add MFA
CloudShell
Feedback
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences


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
Fill in two consecutive codes from your MFA device.
3
MFA code 1
616783
MFA code 2
659444
Cancel
Previous
Add MFA
CloudShell
Feedback
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

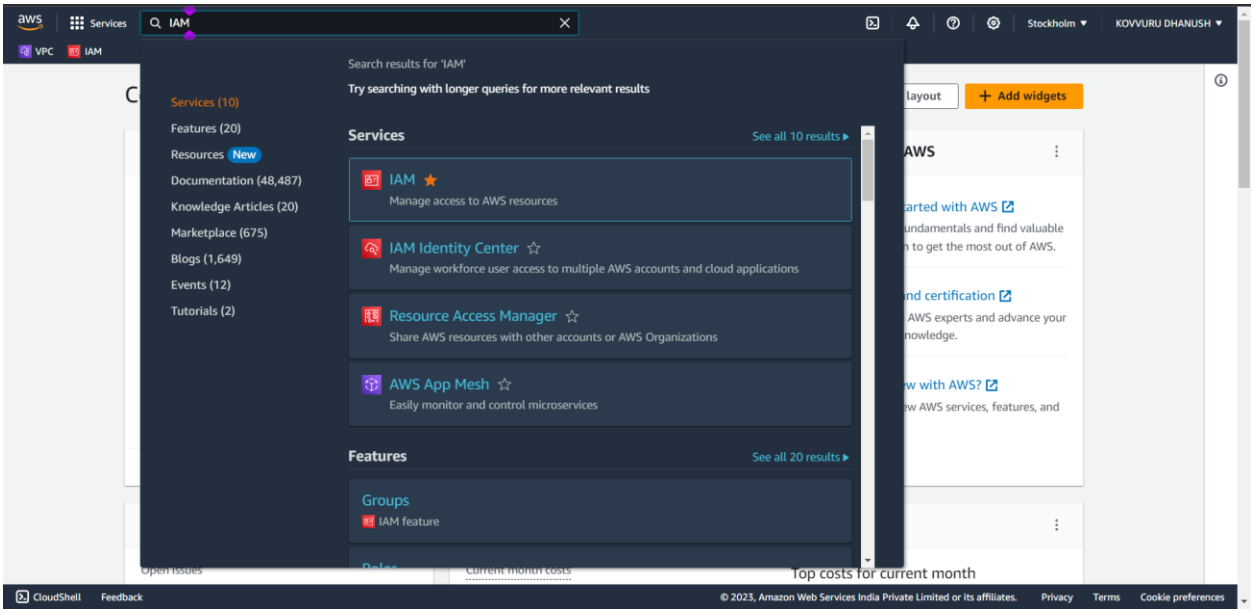


Now done.

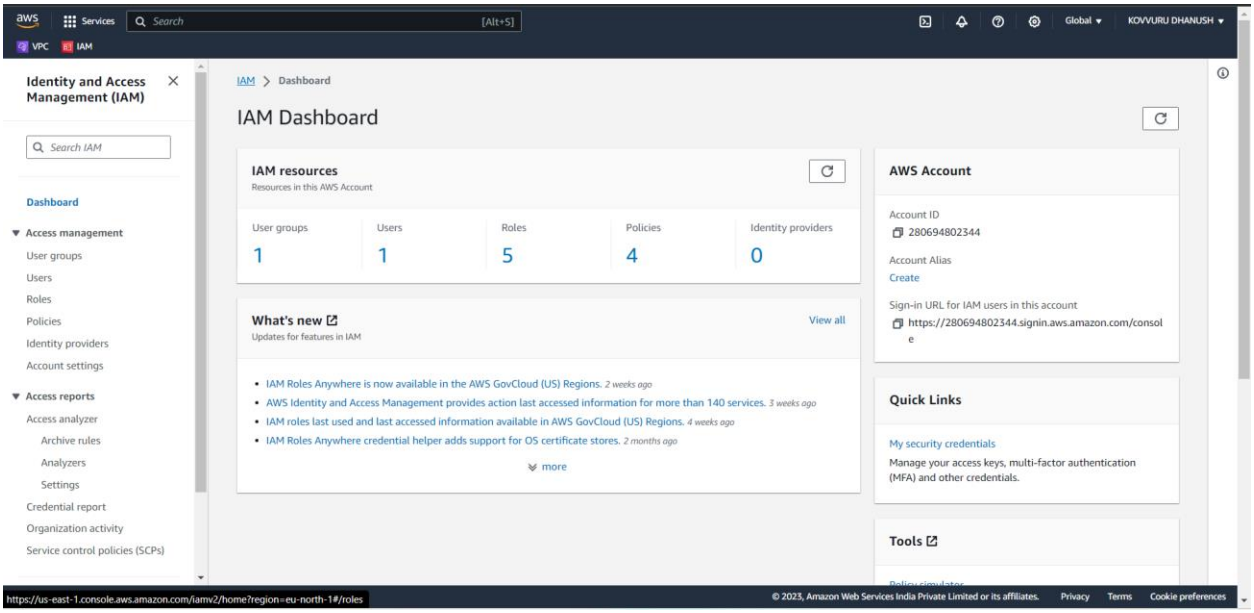
IAM ROLES



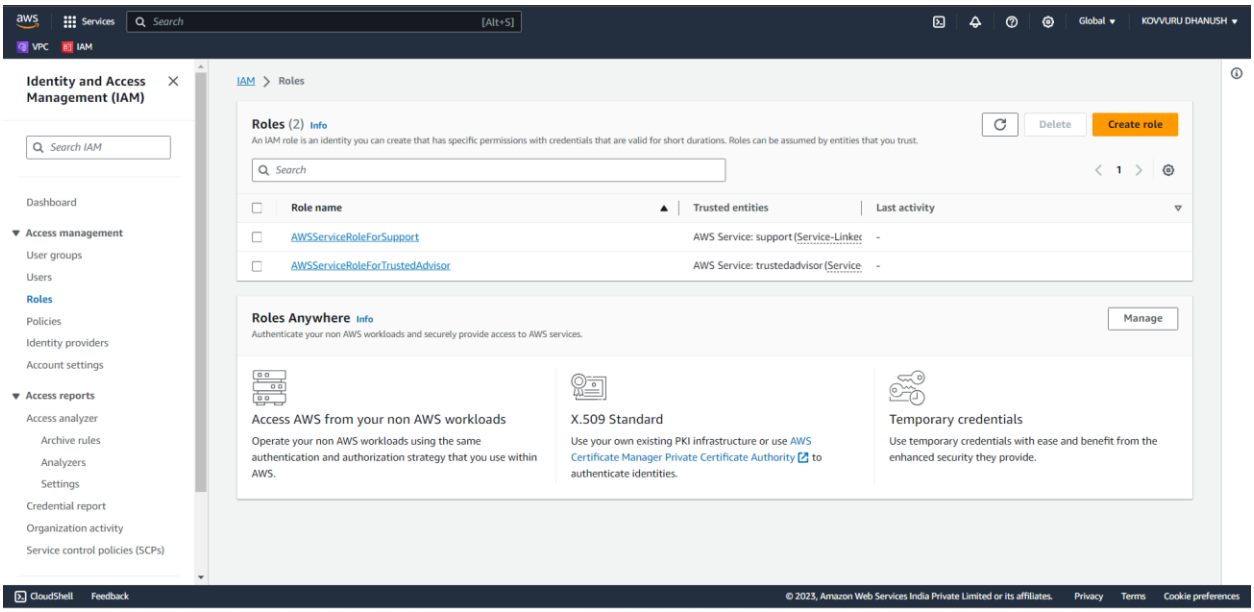
Login to your account.



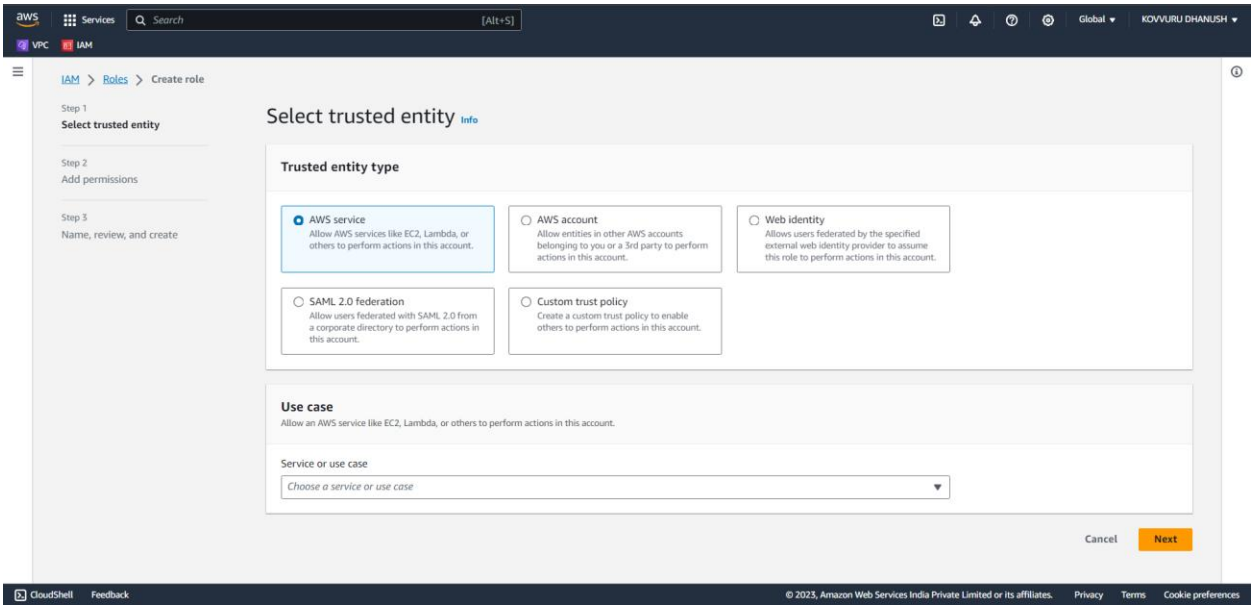
In Search bar type IAM.



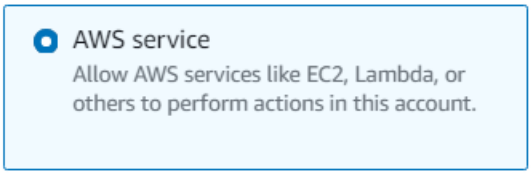
Click on Roles.



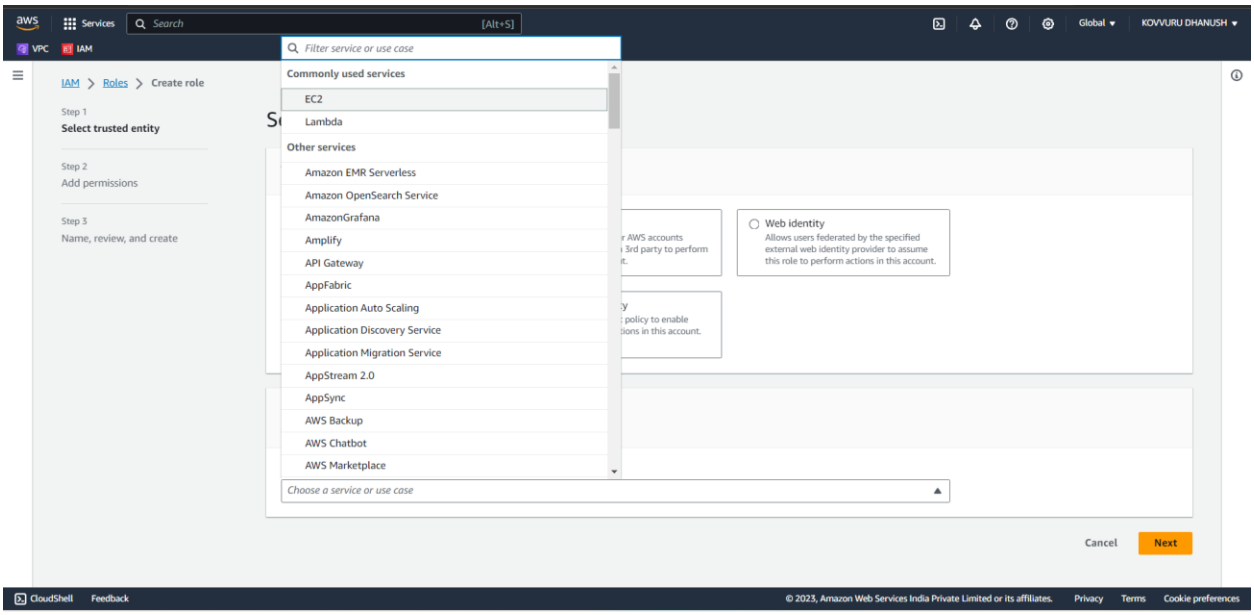
Click on create Role.



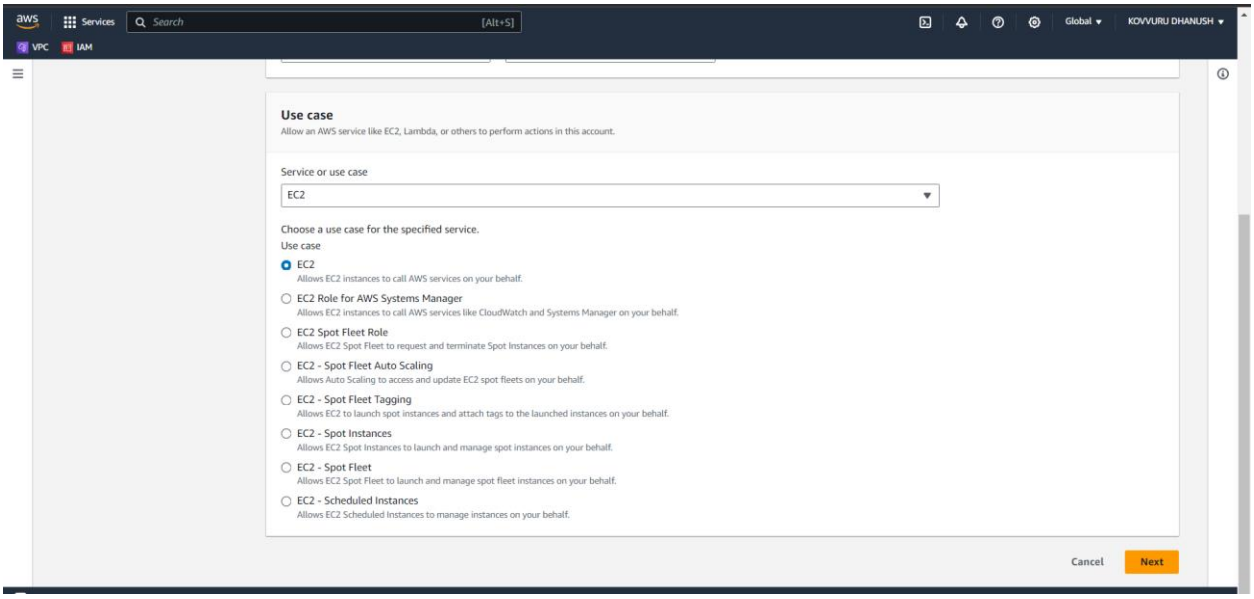
Click on AWS Service.



Read this.

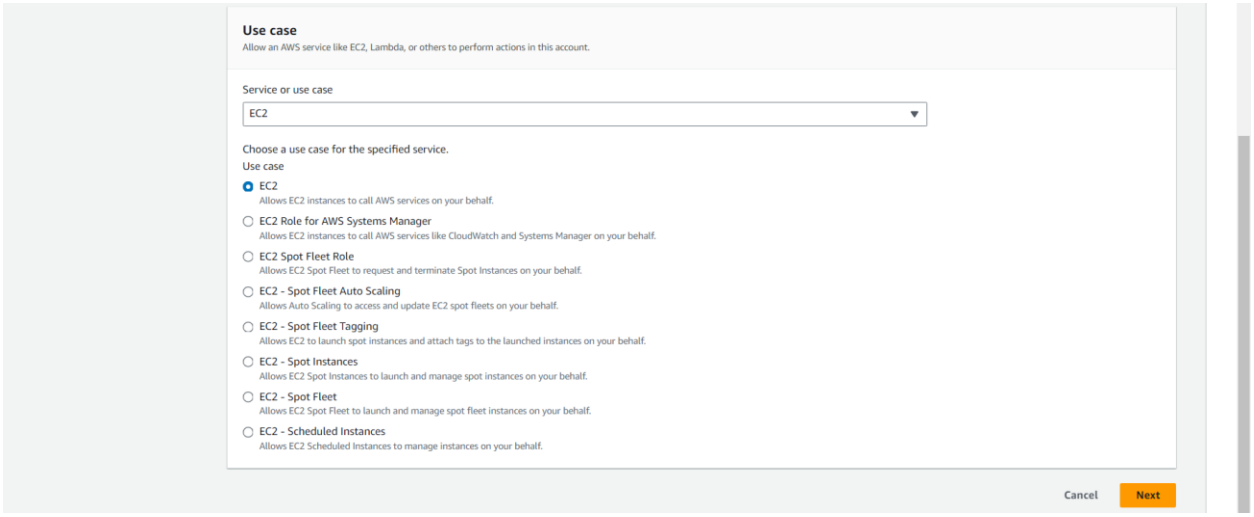


Here in the use case select EC2 .

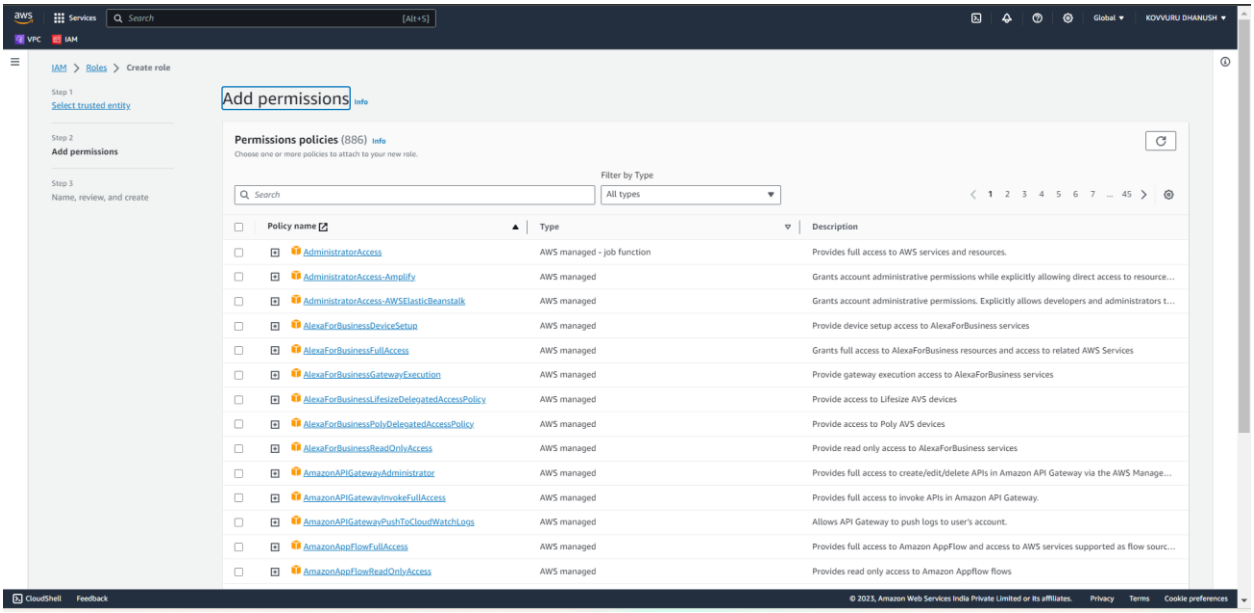


Here select EC2 ->Allows you to call AWS Services on your behalf.

Here while discussing EC2, I will share what is meant by Spot Fleet and spot instances and I will share minimum 6 posts on EC2 only in detailed and simple.

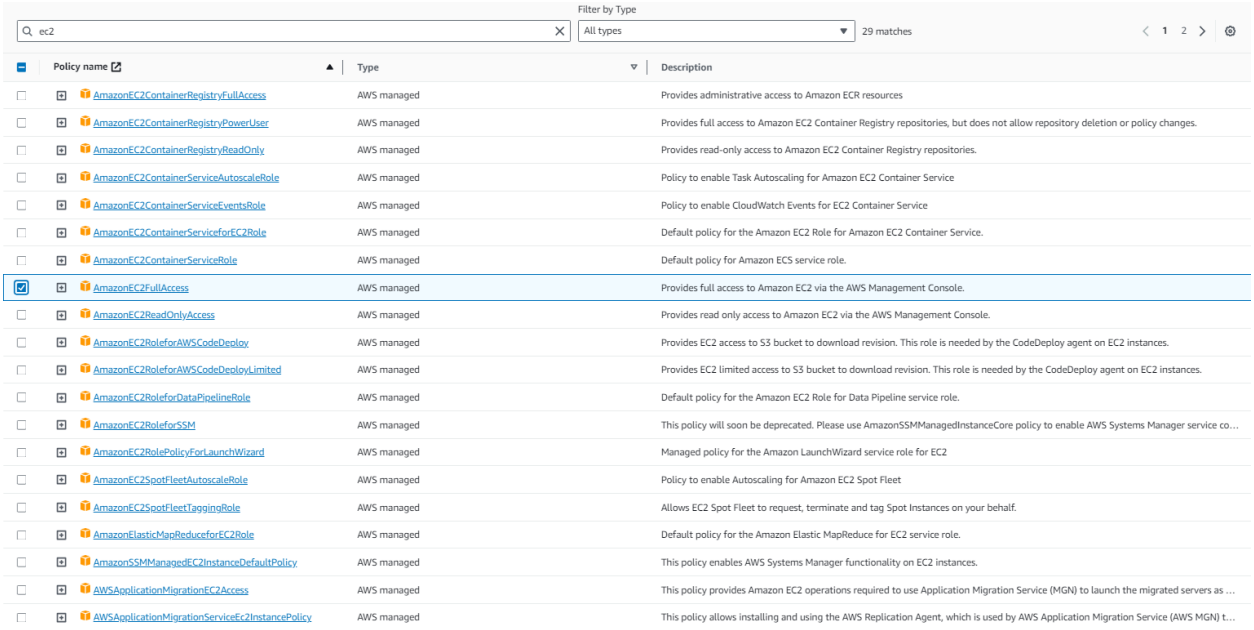


Click on next.

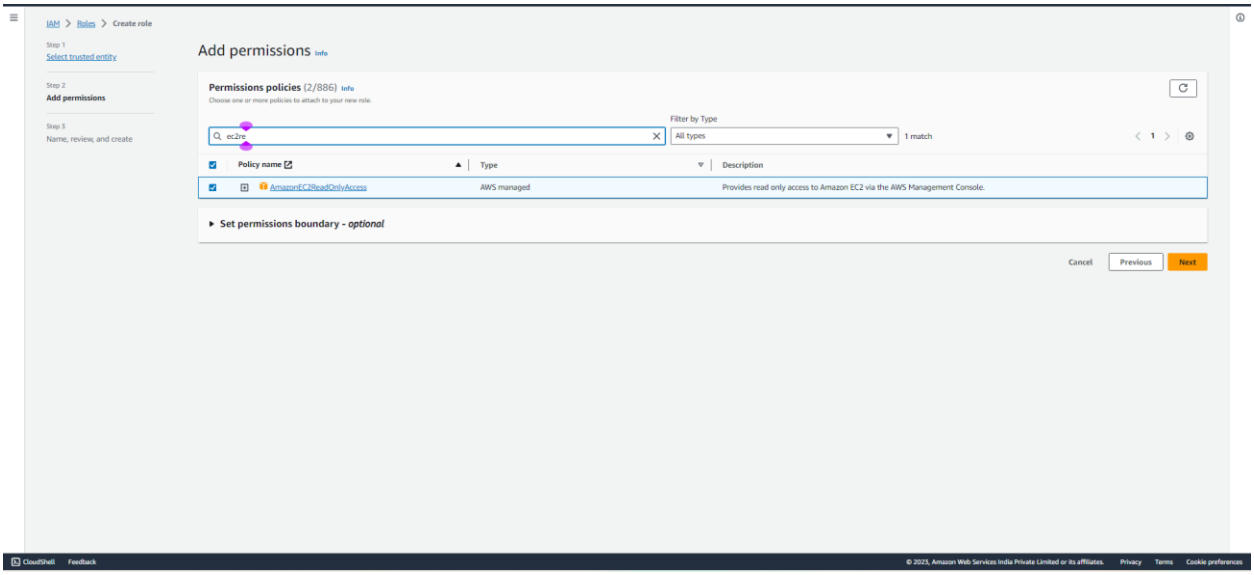


Here in permissions, we need to attach policy why this role and what to do.

Here we attach one policy for the roles.

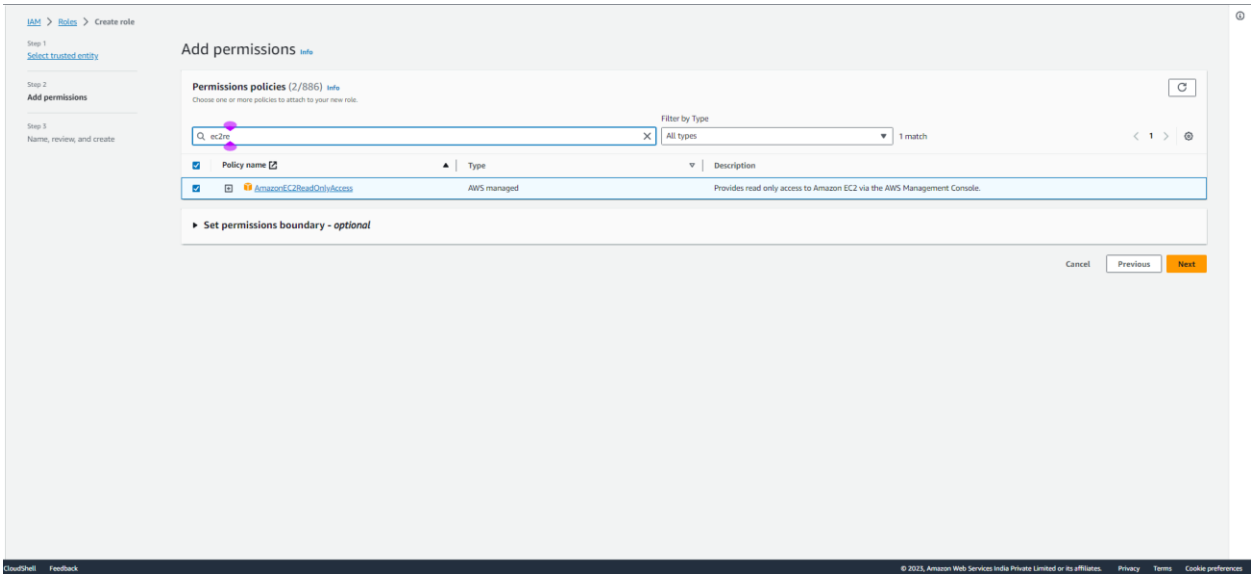


Here I gave full permission to EC2 mean EC2 Full Access.

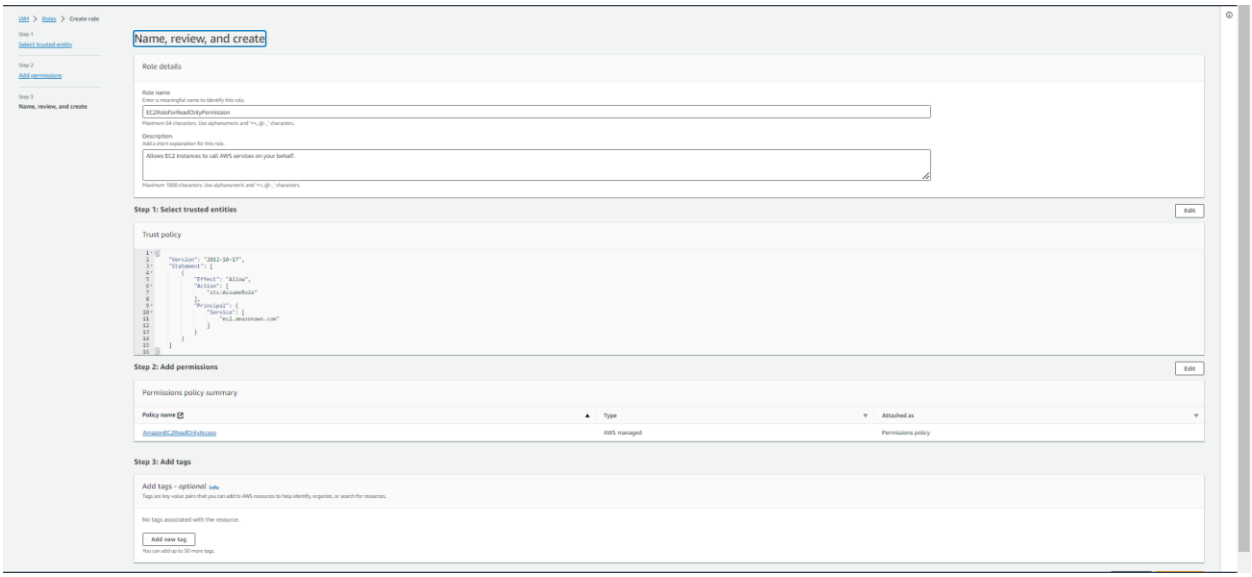


Here If I want to give read only Access, I can Give Access to just read mean I can't create the Instance or I can't do any changes I have permissions that is just to read.

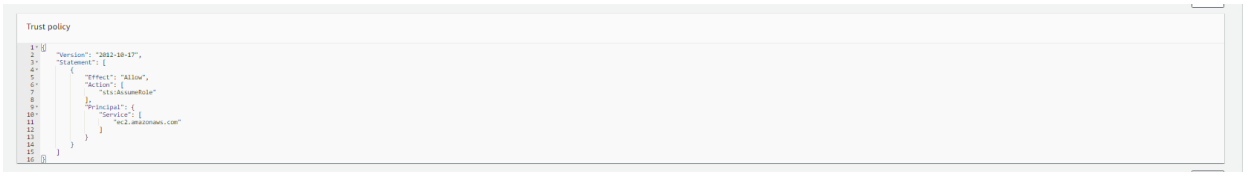
Here for security reasons, I'm giving only one permission that is just to read EC2 Instance.



So, select the permission and attach it to the role.



Here if you observer I gave permission to read EC2 Instances only.



Here this is called JSON Policy we will see what is meant by version, Statement, Effect, Action and Service in simple.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "sts:AssumeRole"
         ],
         "Principal": {
            "Service": [
               "ec2.amazonaws.com"
            ]
         }
      }
   ]
}
```

Here we will look into this Syntax and what it is meant in detailed.

Version:

This specifies the version of the policy language being used. In this case, it's using the version released on October 17, 2012.

Statement:

This is an array of statements. Each statement defines a single permission or rule.

Effect:

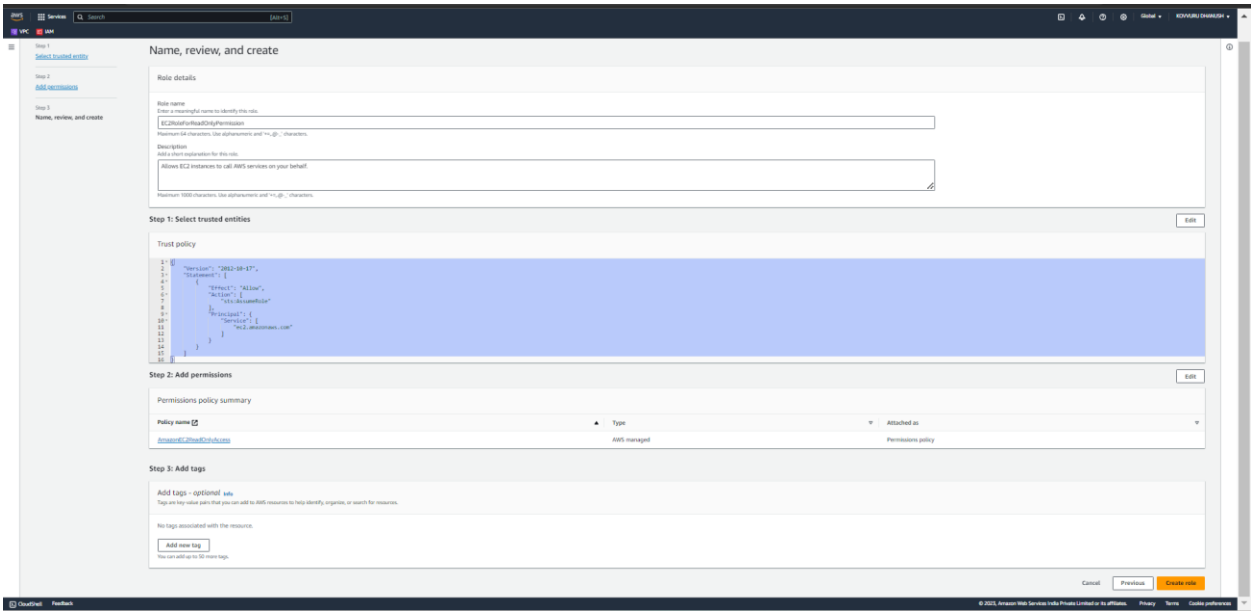
This determines whether the permissions are granted or denied. In this case, it's set to "Allow", which means it allows the specified action.

Action:

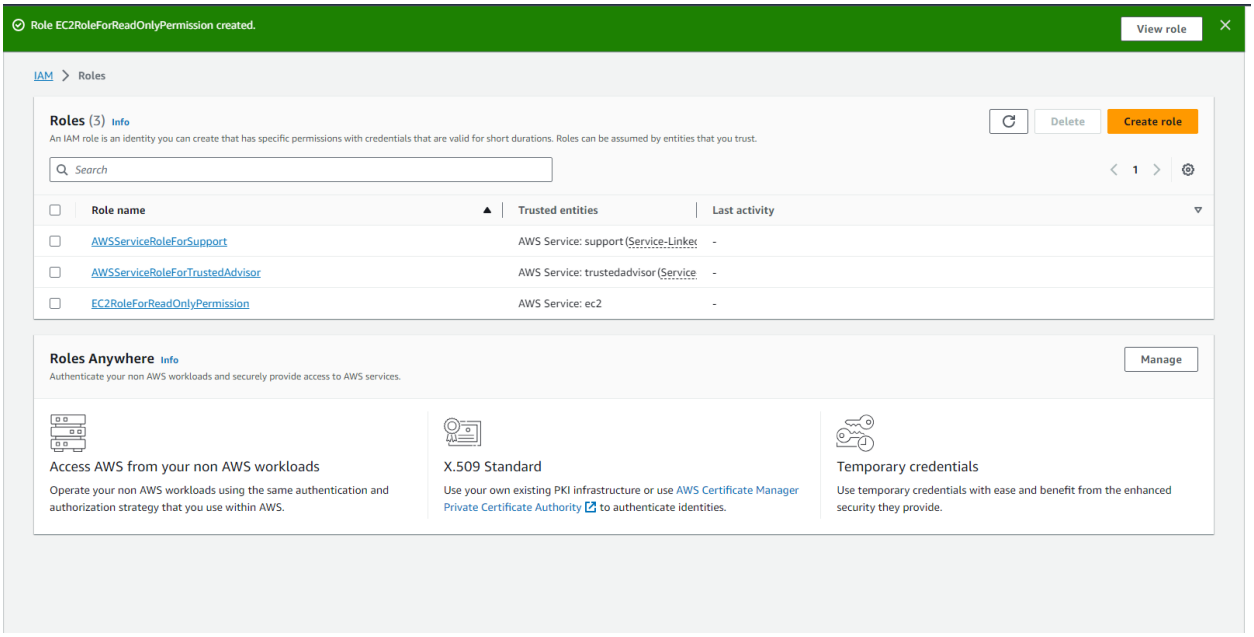
This specifies the action or actions that are allowed. In this case, it allows the action "sts:AssumeRole". This action allows an entity (in this case, an EC2 instance) to assume a specified IAM role.

Principal:

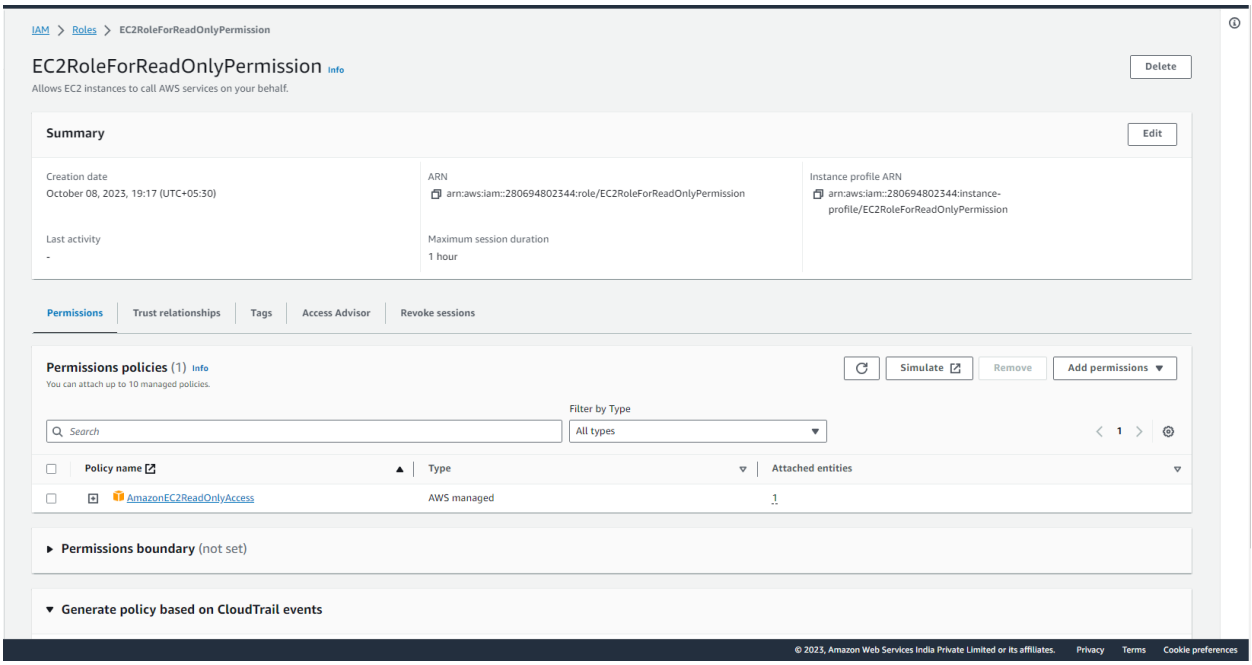
Think like this policy applies to EC2 instances.



Click on create Role.



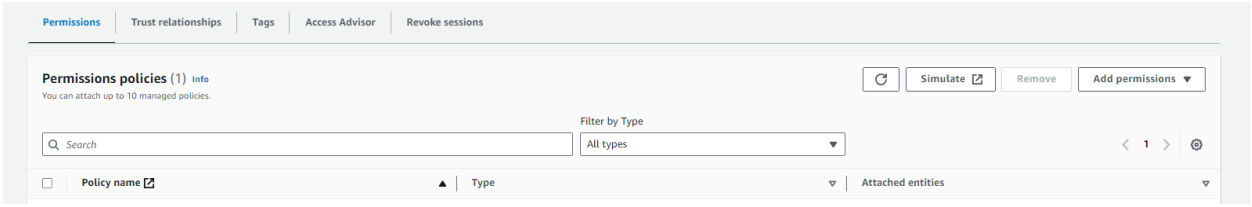
Now role has created successfully.



Here check the permission policies.

Check this below link for further information.

https://docs.aws.amazon.com/aws-managed-policy/latest/reference/AmazonEC2ReadOnlyAccess.html



Here if we want further permissions, we can edit the permissions mean we can add permissions.

Now role has created successfully.

AWS CLI and Console Access

Use this link to download CLI.

Download and run the AWS CLI MSI installer for Windows (64-bit):

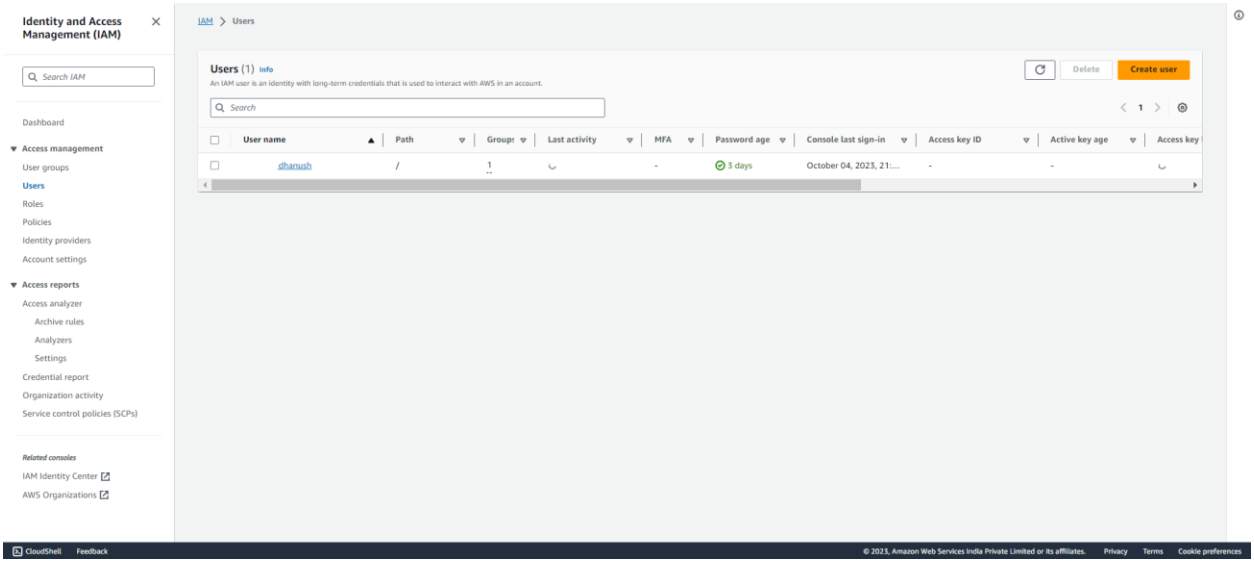
https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html

https://awscli.amazonaws.com/AWSCLIV2.msi

After Downloading successfully.

To check if it is downloaded successfully or not.

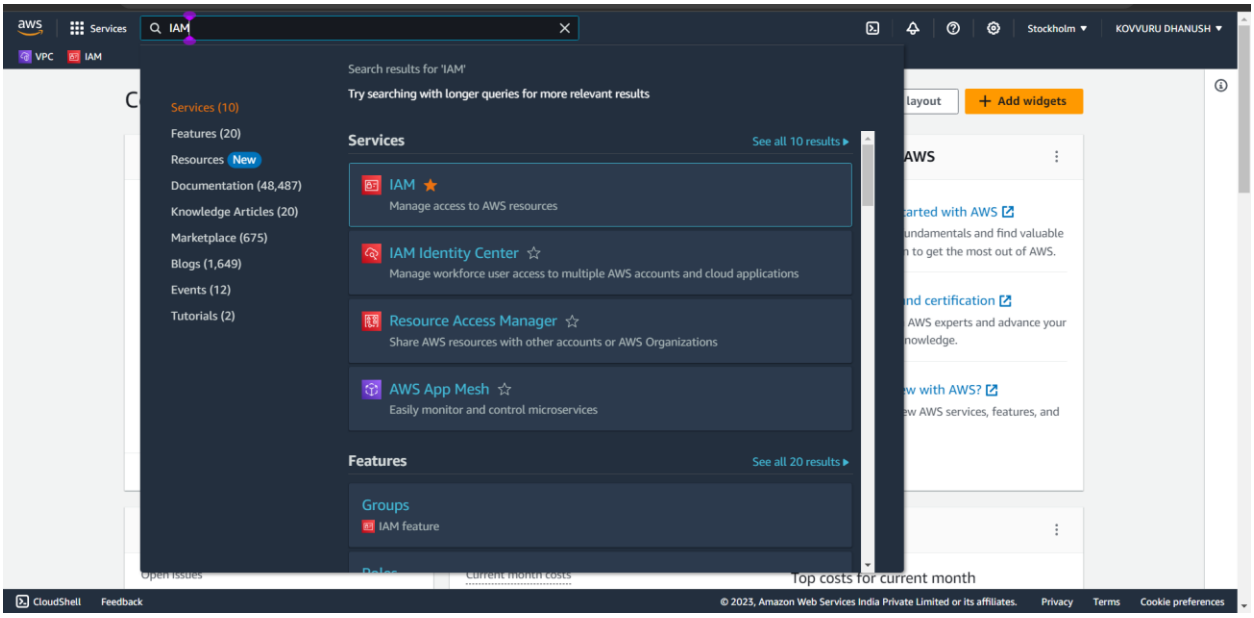
Here in my case, it is downloaded successfully.



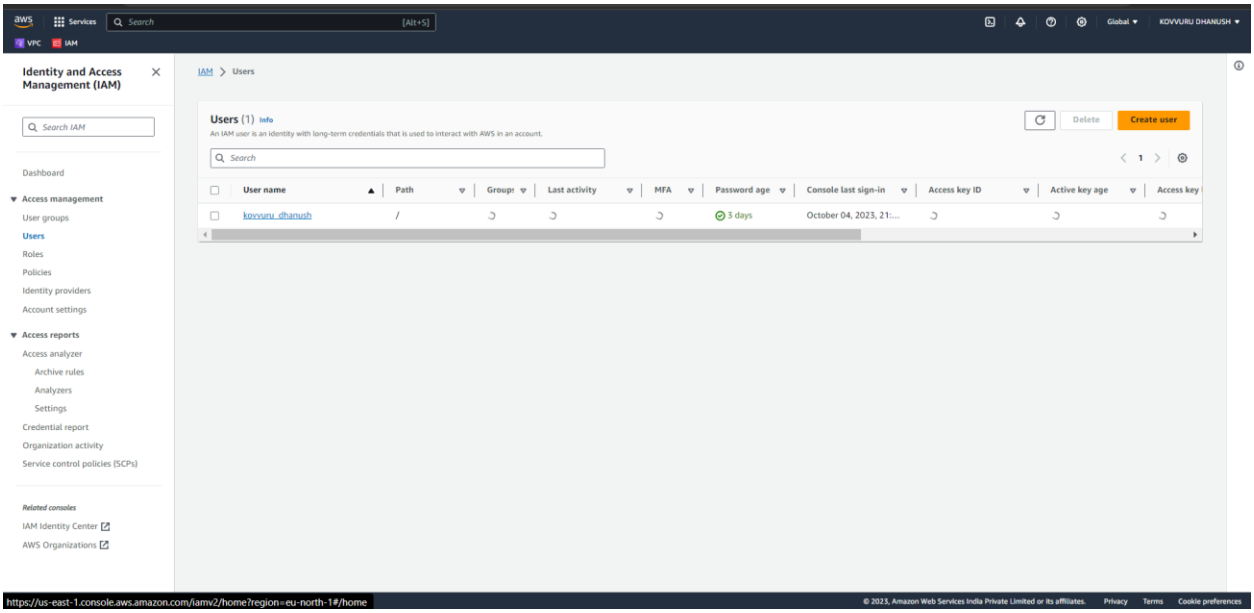
Here if you remember in my previous post, I created IAM User, and we gave permission Administrator Access right so by using CLI we will create S3 bucket via CLI when I'm sharing posts regarding S3 .

But now we will see via CLI how many users that are present in my account.

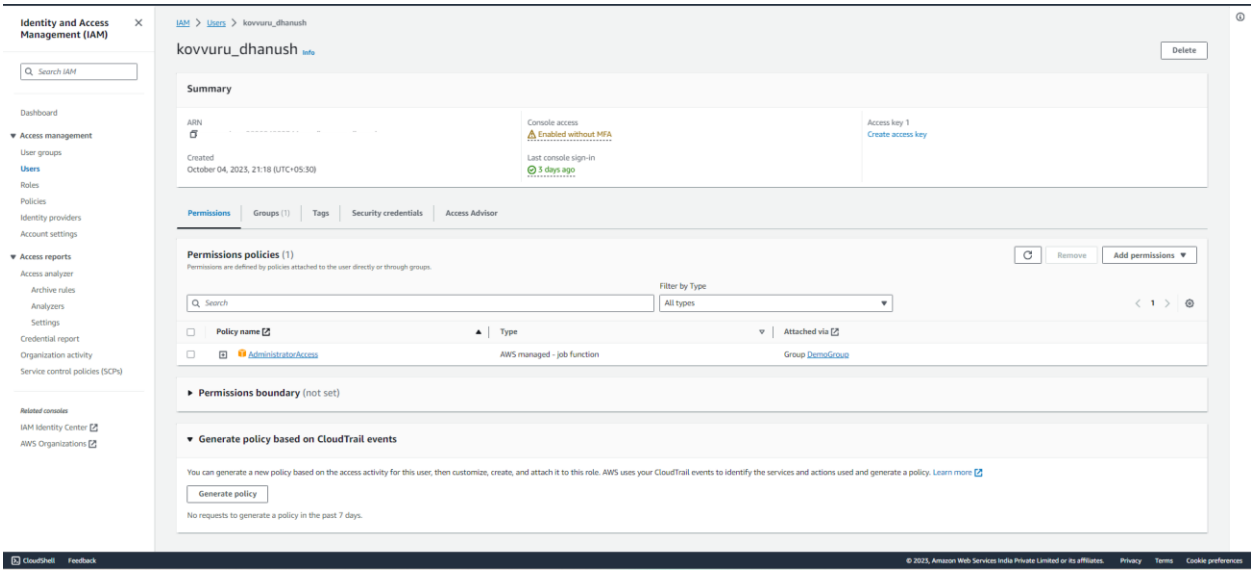
So, here we need the Access key and Secret Access key.

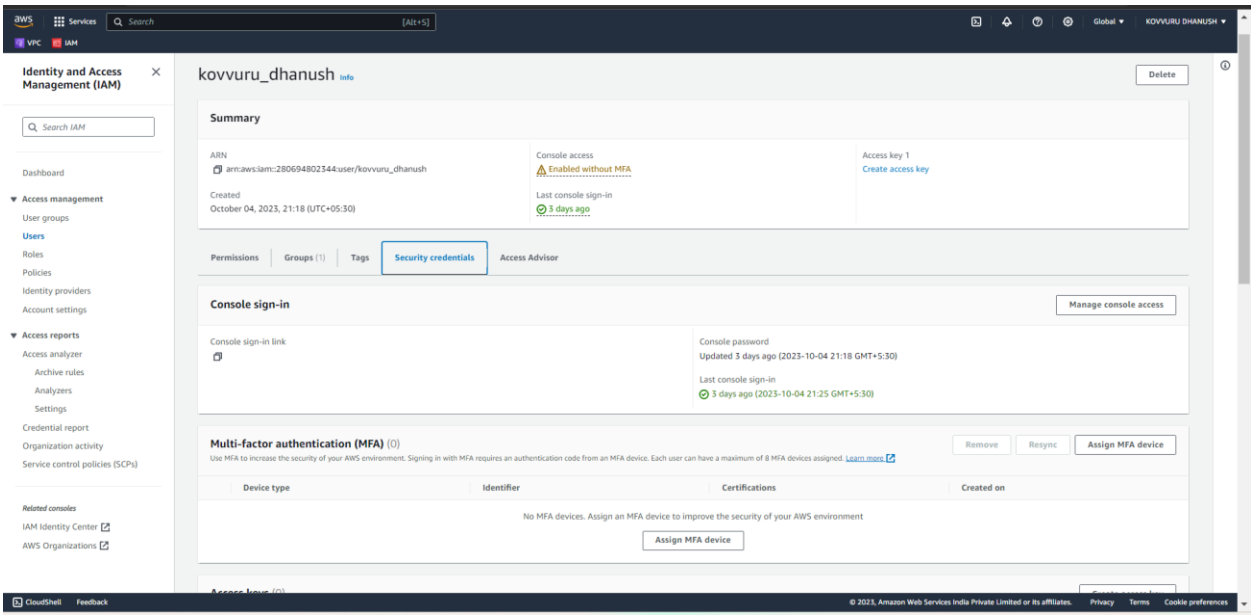


In search bar type IAM.

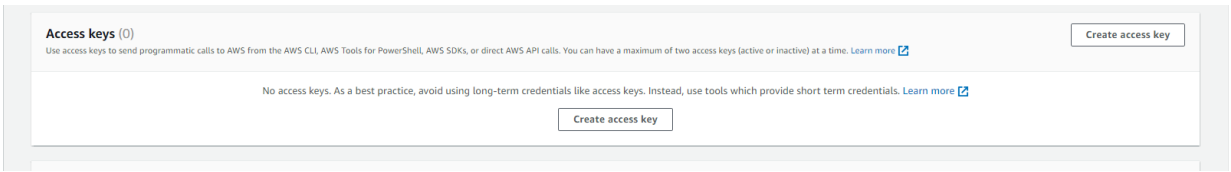


Come to the Users section.

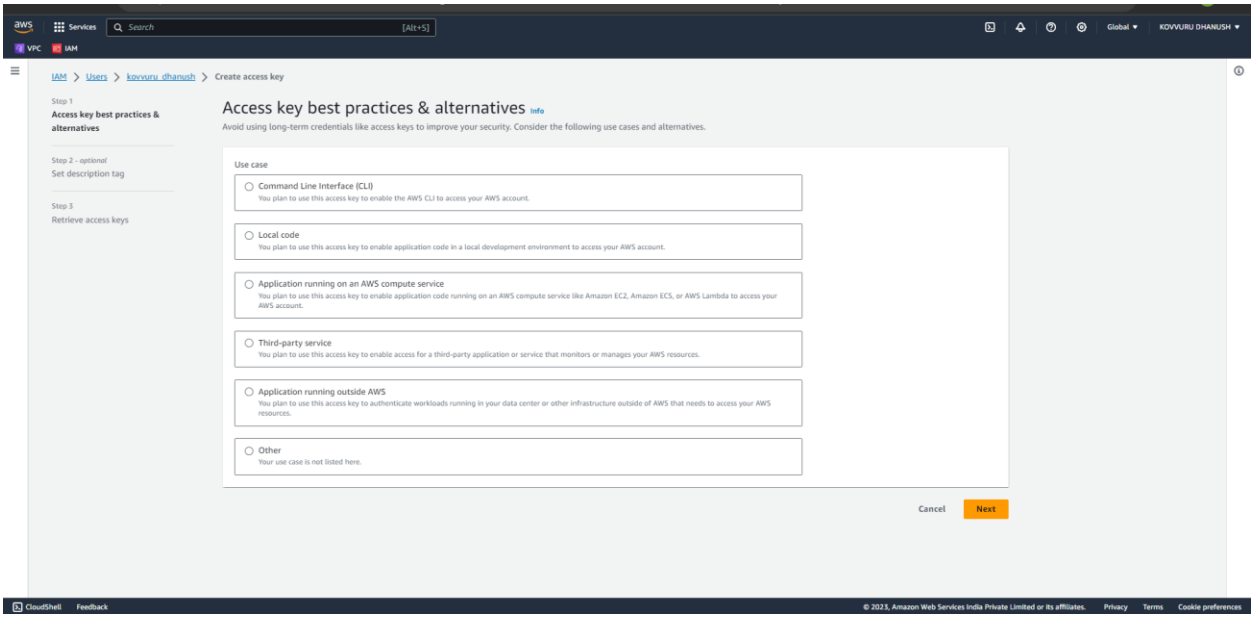




Click on security credentials.

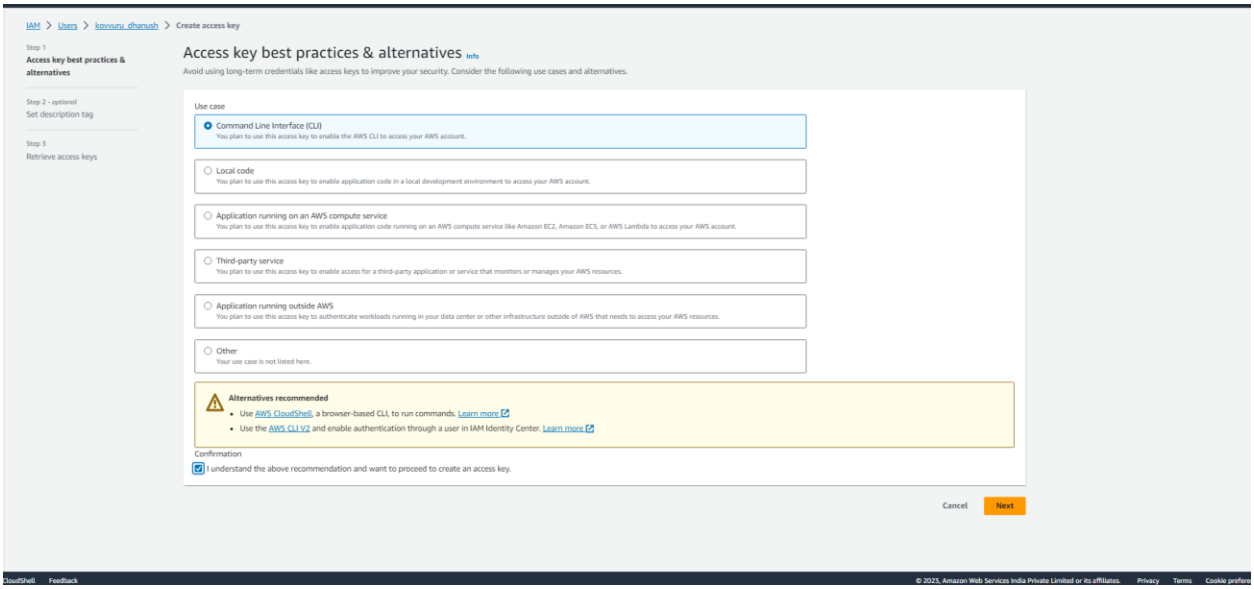


Click on the create Access key.

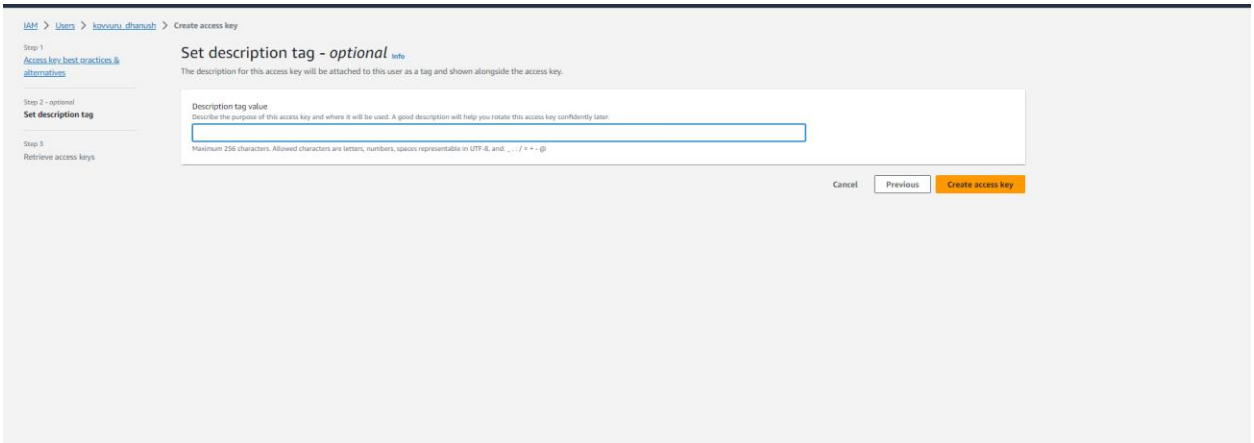


Here we need to access via CLI.

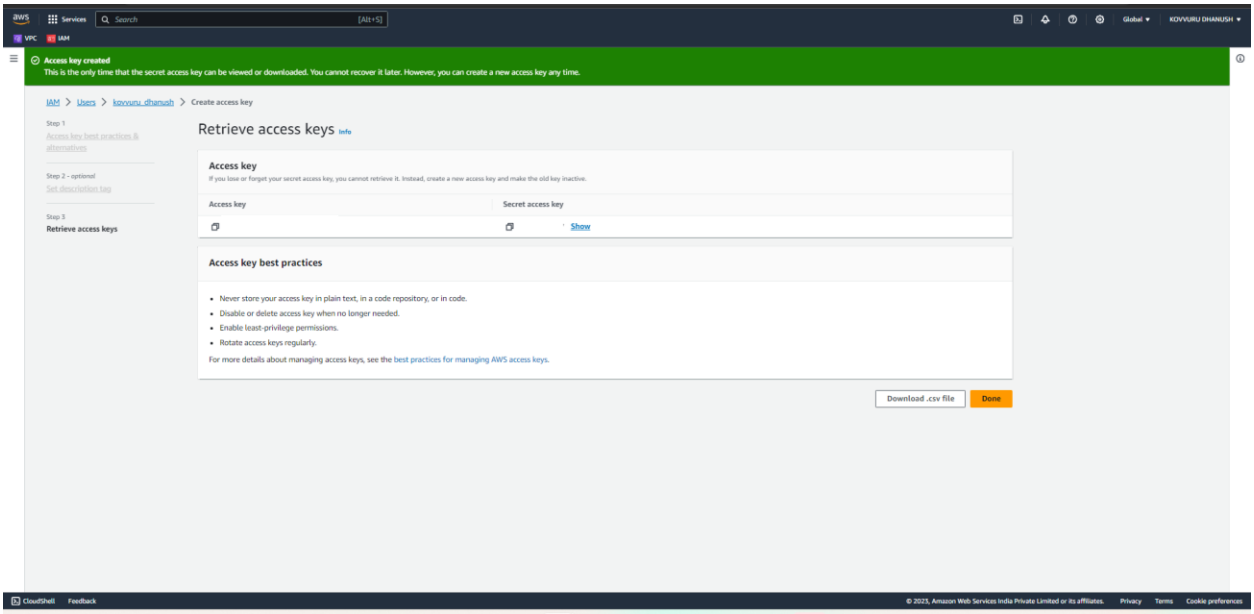
So, select CLI(Command Line Interface).



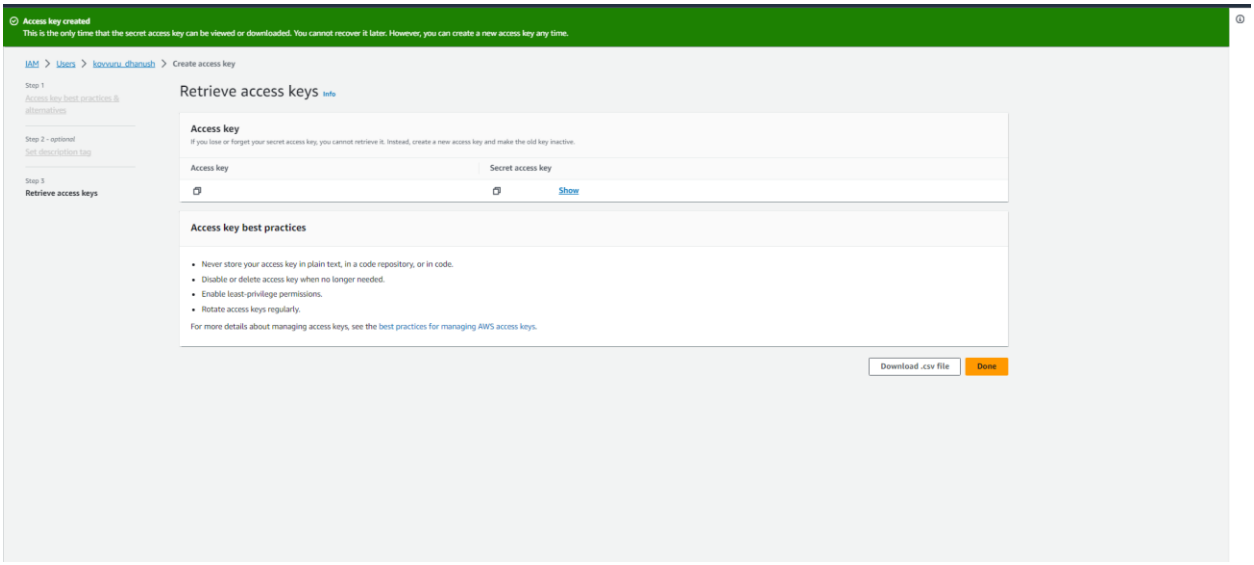
Now click on next.



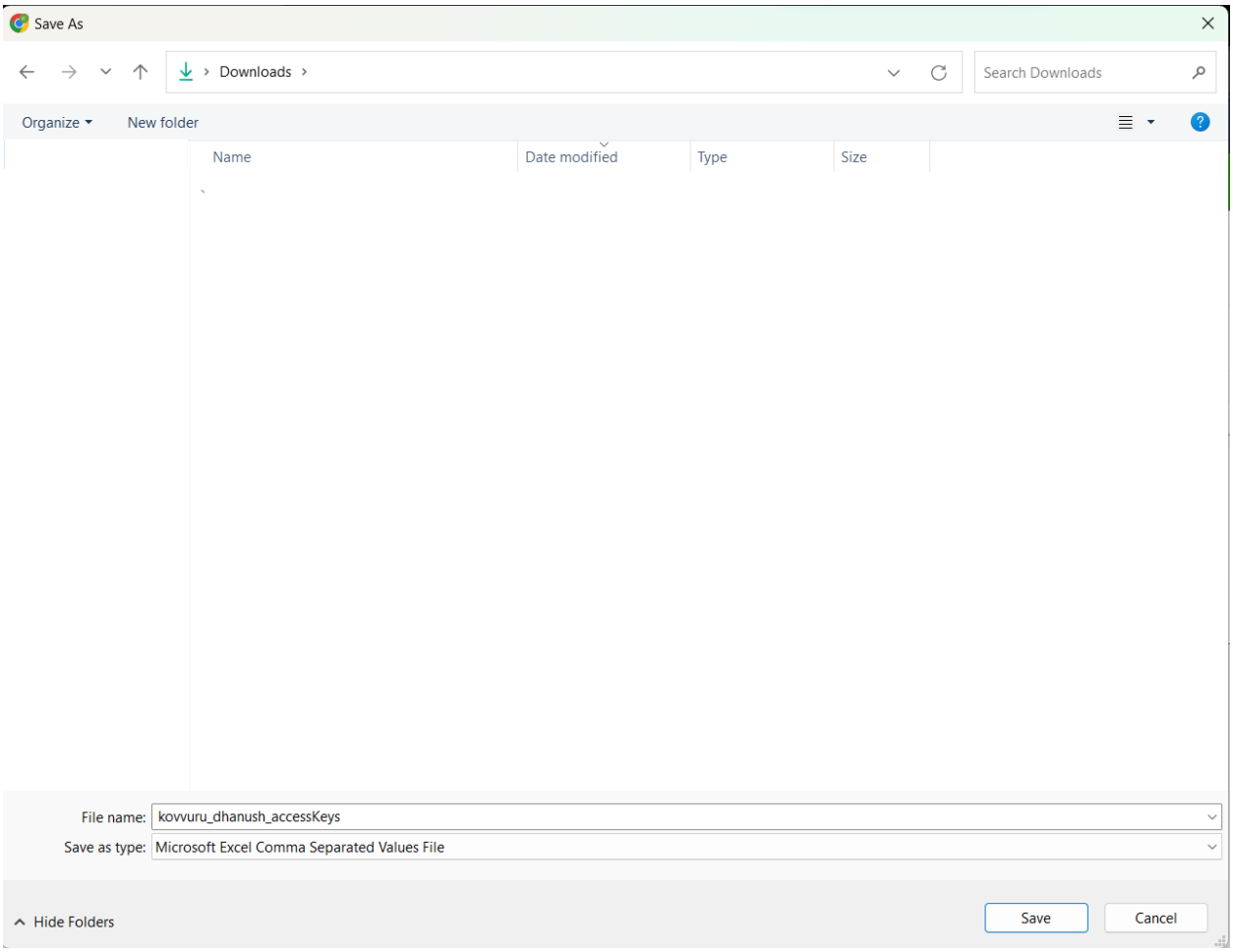
Now click on the create Access key.



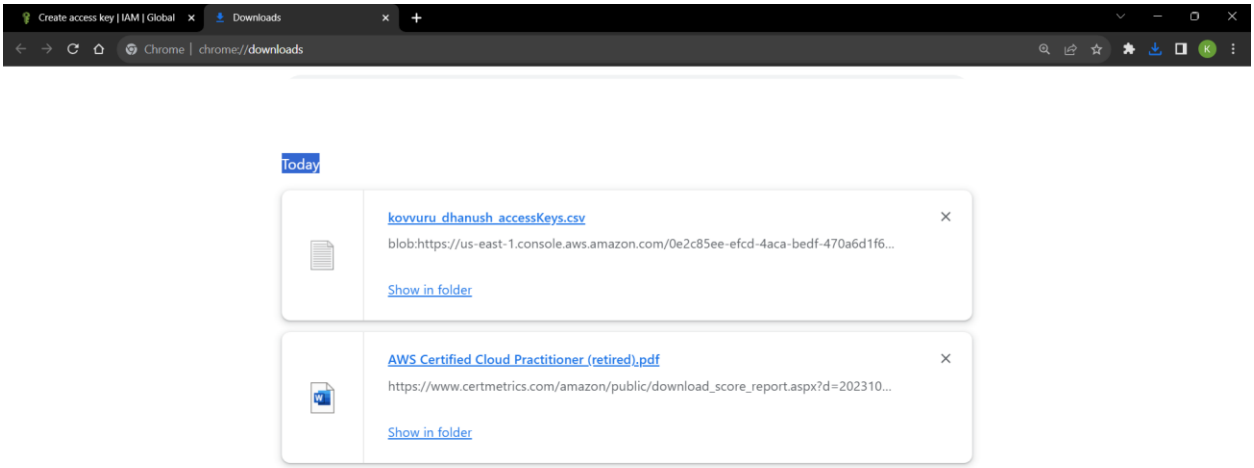
Now Access key and Secret Access key was generated Successfully.



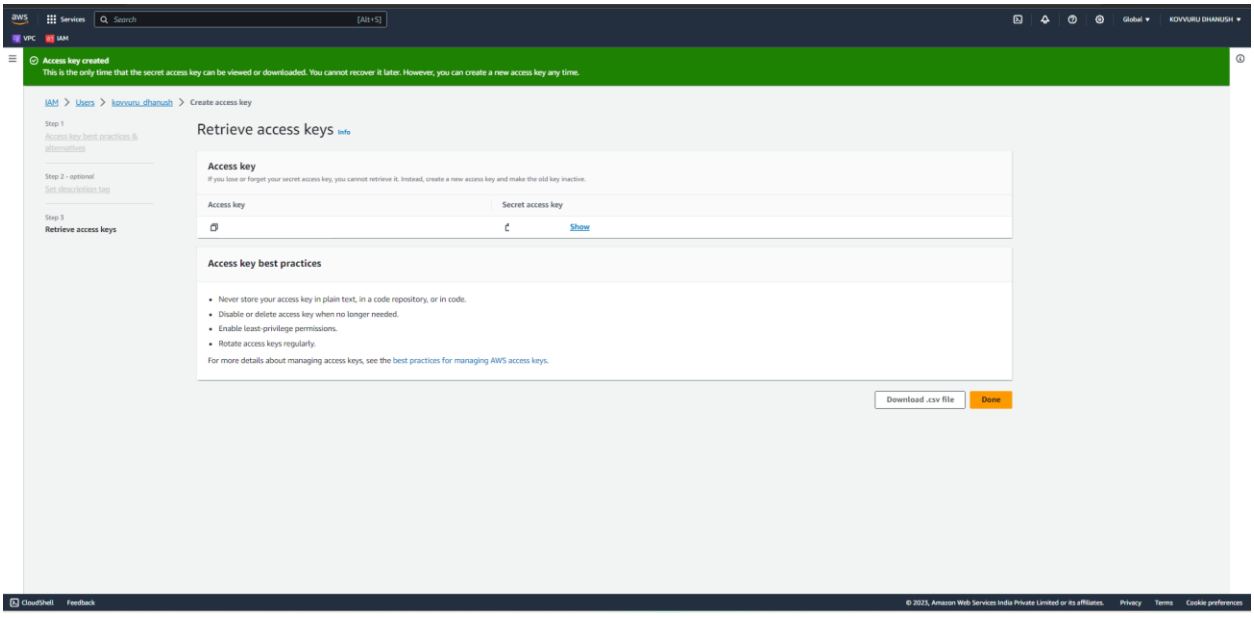
Click on Download .csv file.



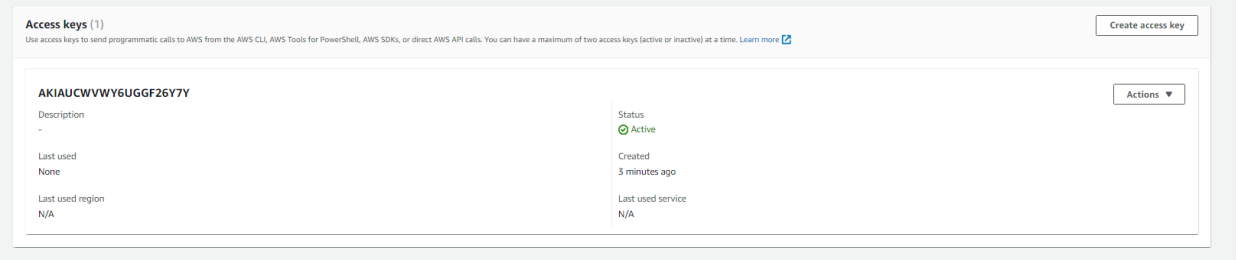
Download it to your system.



See Downloaded Successfully.



Now click on done.



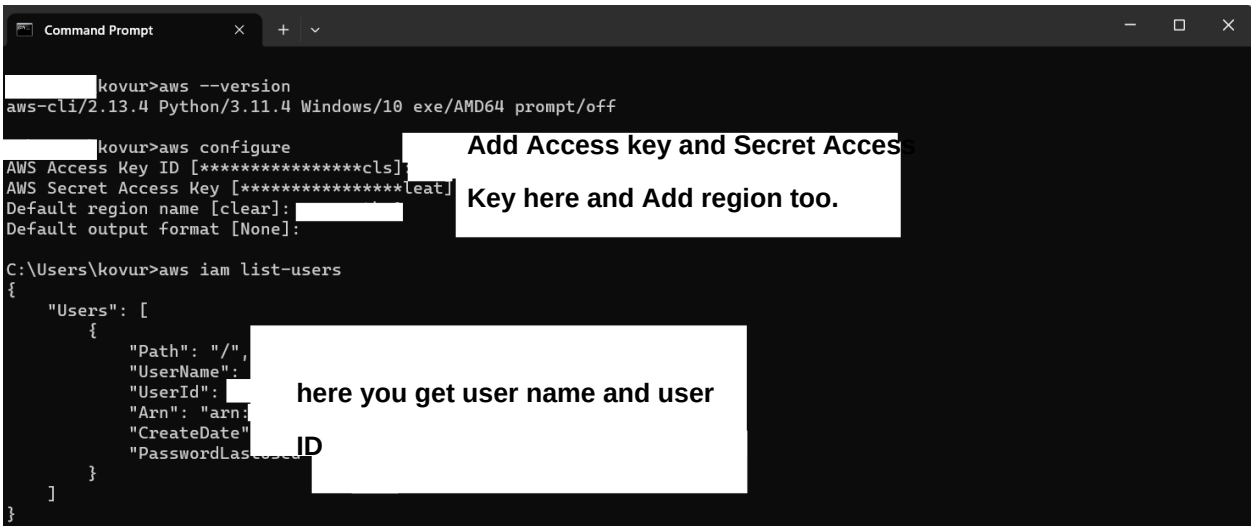
check the status it is active now.

Now open your CLI.

The aws configure command is used to set up the AWS Command Line Interface (CLI) with your AWS account credentials. It allows you to provide your AWS Access Key ID, Secret Access Key, default region, and default output format. This information is necessary for the CLI to communicate with your AWS account.

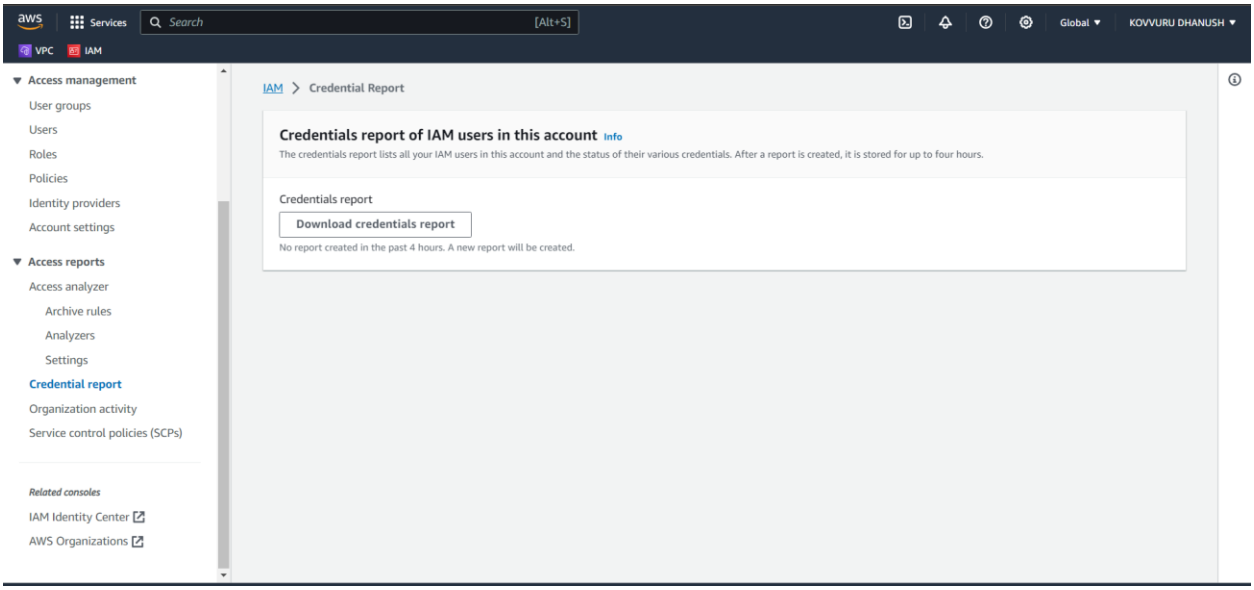
Now you have downloaded .csv file right open that and copy Access key and paste it on the console.

Now you have downloaded the .csv file, open it right and copy the Secret Access key and paste it on the console.

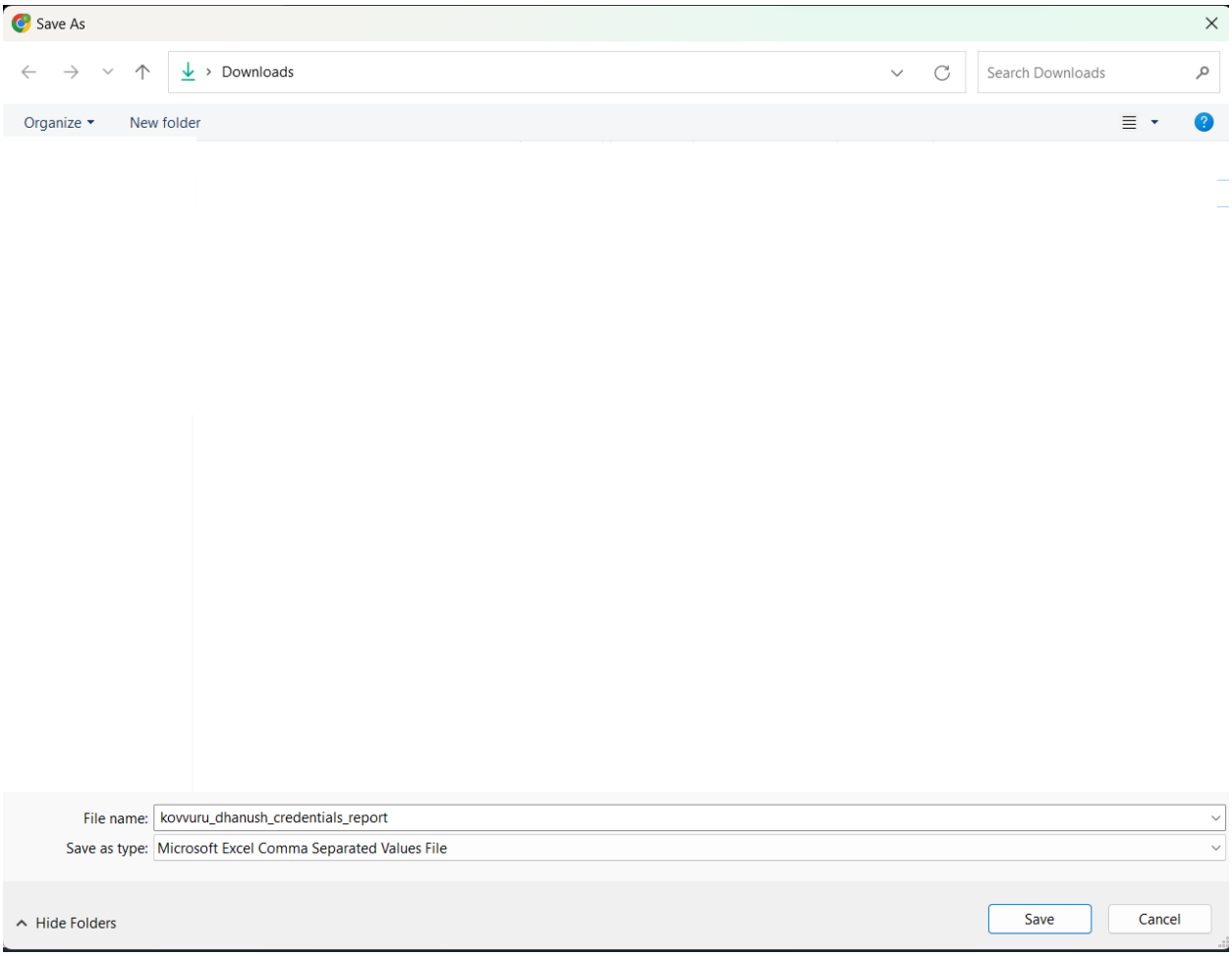


See we have listed out IAM Users in my account

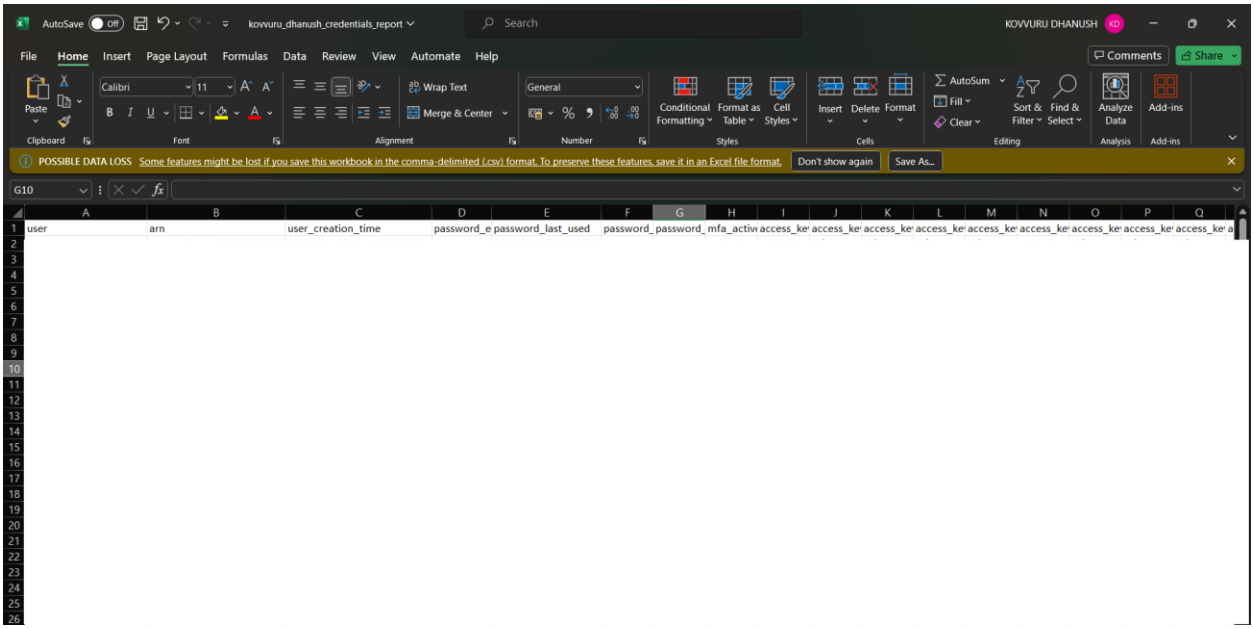
Credentials Report



Download credentials report.



Download the credentials Report



Download the credentials report

Thank You