

**AMITY SCHOOL OF ENGINEERING & TECHNOLOGY**



**(Academic Year 2022-23)**

**LAB-3(b)**

**Student Name: Vikas Rajbhar**

**Class: B.Tech(CSE) Semester: 7**

**Enrollment Number: A70405219037**

**Faculty In-charge**

{Department of CSE}

ASET, AUM

## AIM:

1. Set the MFA for Root AWS user.
2. Set the password policy.
3. Configure AWS CLI. (work with different user creation and deletion and group creation and deletion).
4. Create IAM Role.
5. AWS command.

### 1. Set the mfa for root aws user

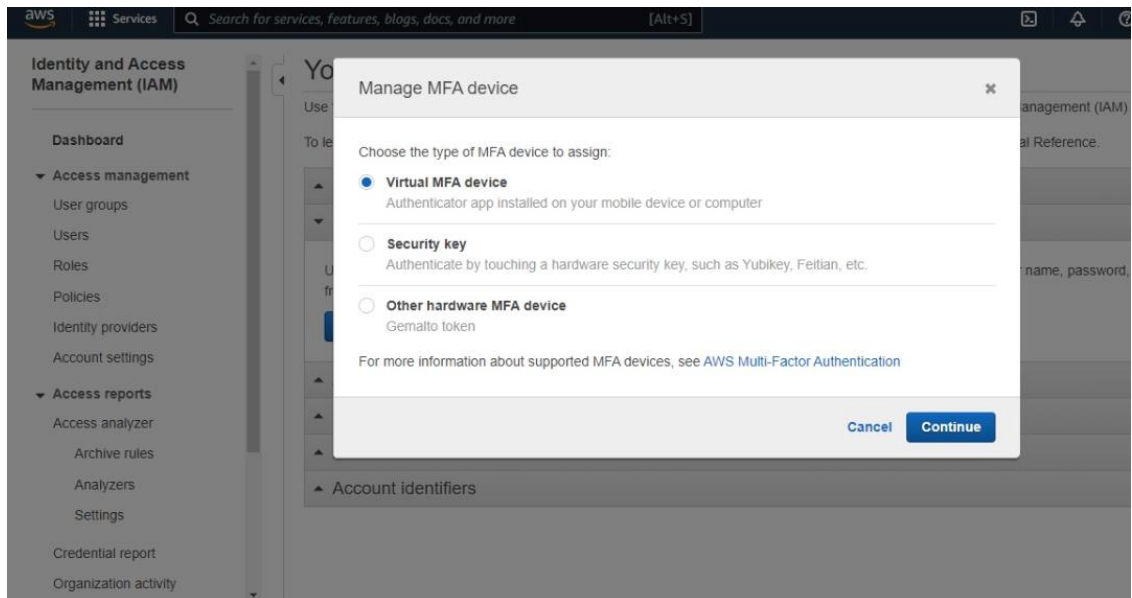
#### a) First, click on your username and select **Security credentials**.

The screenshot shows the AWS IAM Management Console interface. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like 'Dashboard', 'Access management', 'Access reports', and 'Account settings'. The main content area shows the 'Users' tab for the 'ADMIN1' group. A dropdown menu is open for the user 'user3', displaying various account management options. The 'Security credentials' option is highlighted in the dropdown menu.

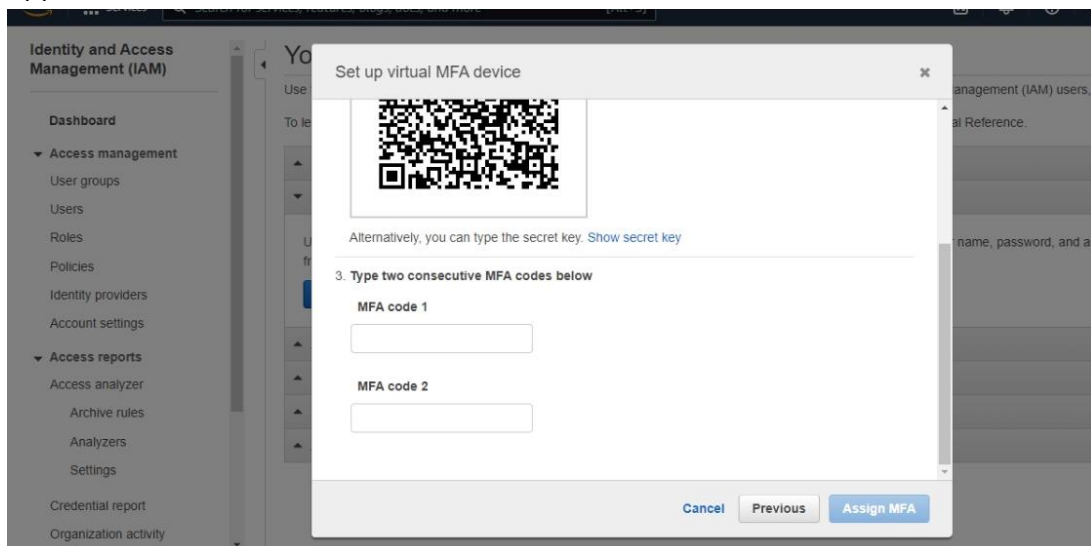
#### b) Now Click on **Multi-factor authentication** and click on **Activate MFA**.

The screenshot shows the 'Your Security Credentials' page in the AWS IAM Management Console. The page title is 'Your Security Credentials'. Below the title, there is a section for 'Multi-factor authentication (MFA)' which is expanded. It contains a description of MFA and a blue button labeled 'Activate MFA'. Other sections visible include 'Password', 'Access keys (access key ID and secret access key)', 'CloudFront key pairs', 'X.509 certificate', and 'Account identifiers'.

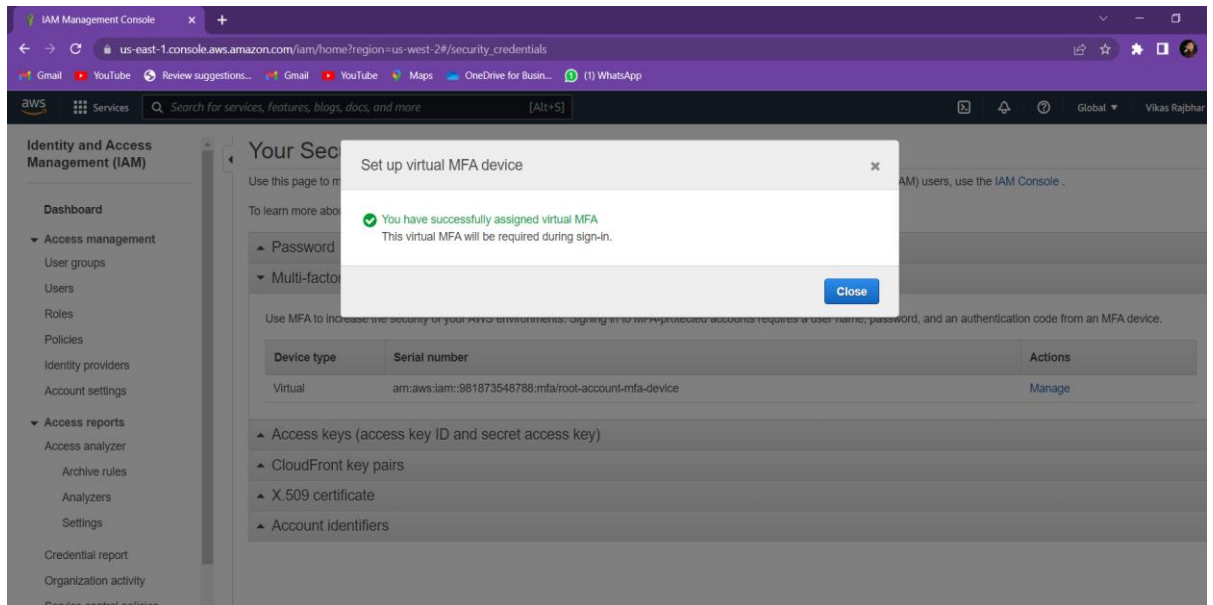
c) Now select **virtual MFA device** and click continue



d) Now, scan the QR code and then type the two consecutive MFA codes from the 2FA app.

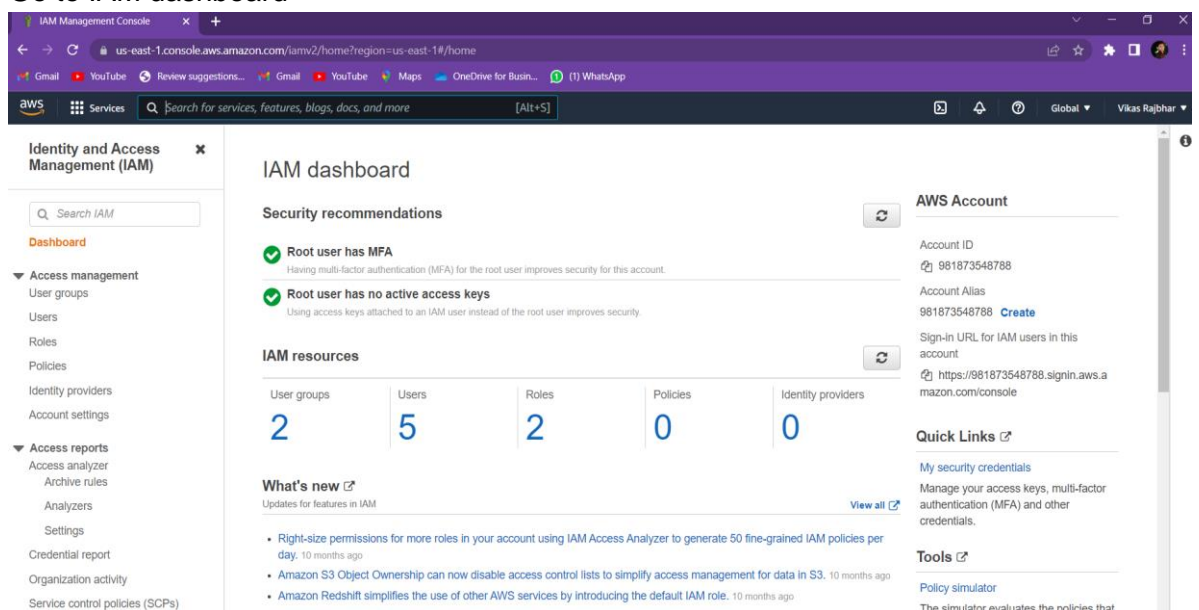


e) You have successfully assigned virtual MFA



## 2. Set the password policy

### a) Go to IAM dashboard



### b) Go to **Account setting** and click on **Change password policy**

**Identity and Access Management (IAM)**

- Dashboard
- Access management
  - User groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
- Access reports
  - Access analyzer
  - Archive rules
  - Analyzers
  - Settings
- Credential report
- Organization activity

---

**▼ Password policy**

A password policy is a set of rules that define the type of password an IAM user can set. [Learn more](#)

**Password policy**

This AWS account uses the following default password policy:

- Minimum password length is 8 characters
- Include a minimum of three of the following mix of character types: uppercase, lowercase, numbers, and !@#\$%^&\*()\_+-=[]{}|'`
- Must not be identical to your AWS account name or email address

[Change password policy](#)

---

**▼ Security Token Service (STS)**

**Session Tokens from the STS endpoints**

AWS recommends using regional STS endpoints to reduce latency. Session tokens from regional STS endpoints are valid in all AWS Regions. If you use STS endpoints, no action is required.

Session tokens from the global STS endpoint (<https://sts.amazonaws.com>) are valid only in AWS Regions that are enabled by default. If you intend to use session tokens from the global STS endpoint, you can use session tokens from regional STS endpoints or activate the global STS endpoint to issue session tokens that are valid in all AWS Regions. [Learn more](#)

Endpoints	Region compatibility of session tokens	Actions
Global endpoint	Valid only in AWS Regions enabled by default	<a href="#">Edit</a>

c) Set the password policy and click on **Save changes**

**Set password policy**

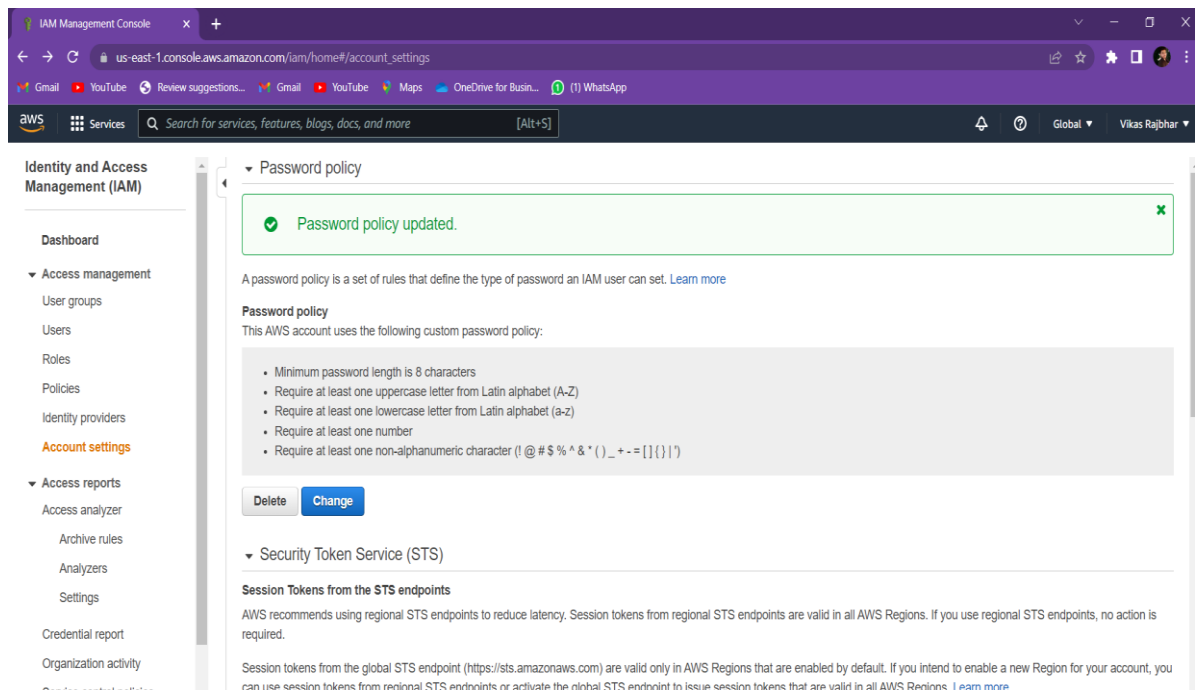
A password policy is a set of rules that define complexity requirements and mandatory rotation periods for your IAM users' passwords. [Learn more](#)

**Select your account password policy requirements:**

- ☒ Enforce minimum password length
 

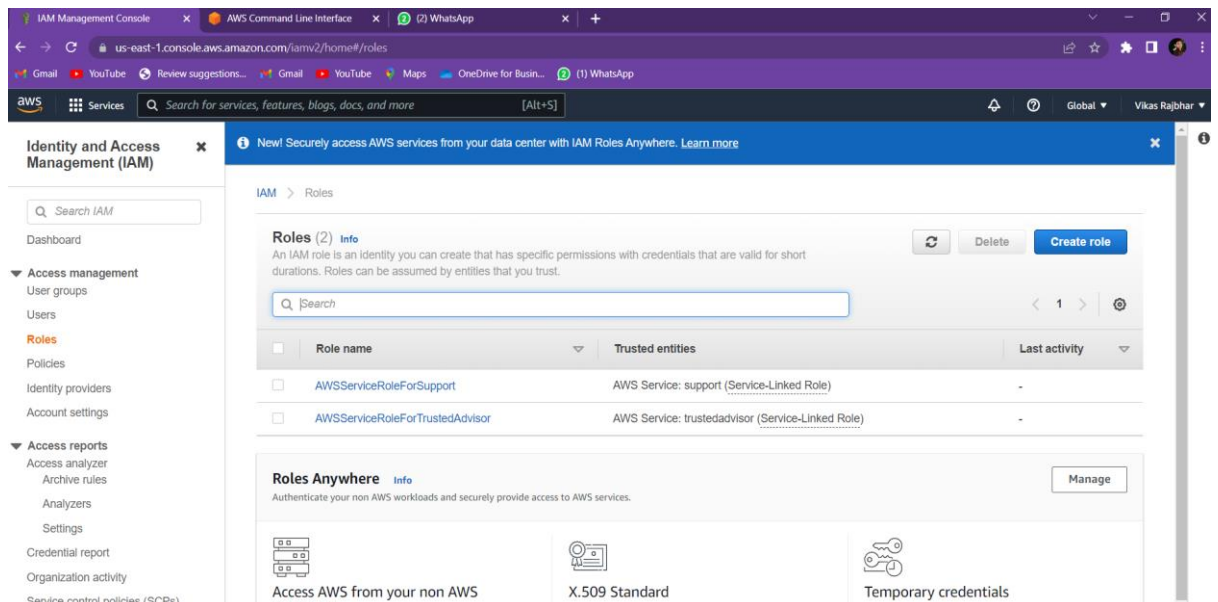
characters
- ☐ Require at least one uppercase letter from Latin alphabet (A-Z)
- ☐ Require at least one lowercase letter from Latin alphabet (a-z)
- ☐ Require at least one number
- ☐ Require at least one non-alphanumeric character (!@#\$%^&\*()\_+-=[]{}|'`)
- ☐ Enable password expiration
- ☐ Password expiration requires administrator reset
- ☐ [Allow users to change their own password](#)
- ☐ Prevent password reuse

d) The password policy has been updated successfully.

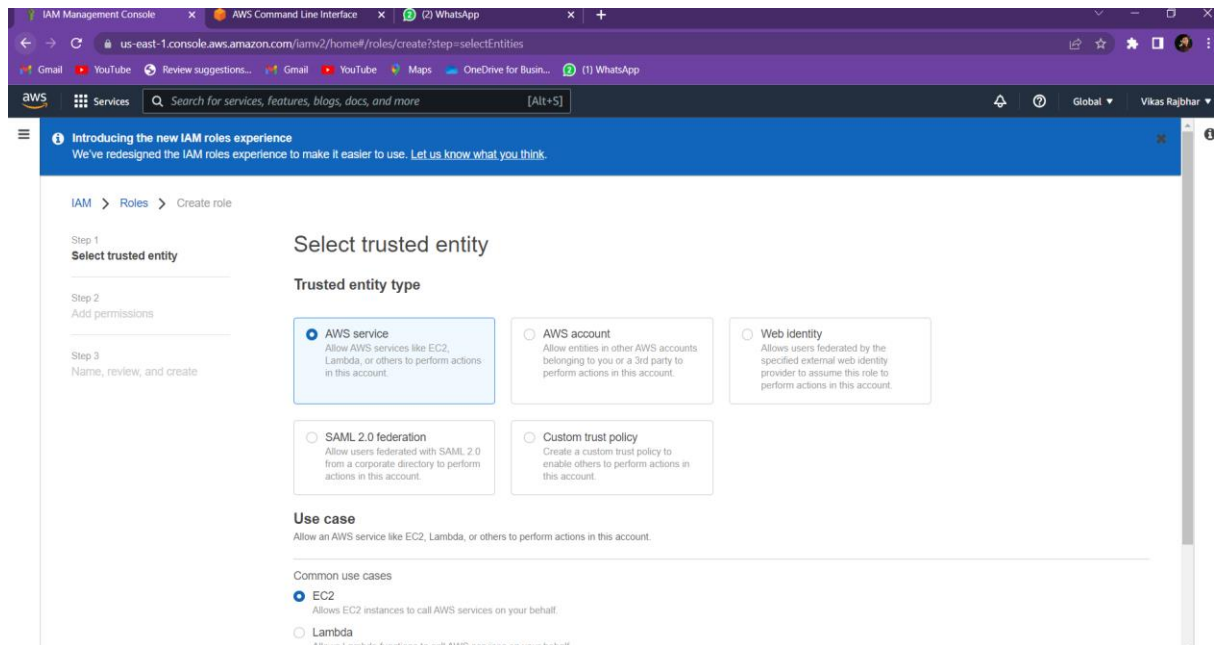


### 3. Create iam role

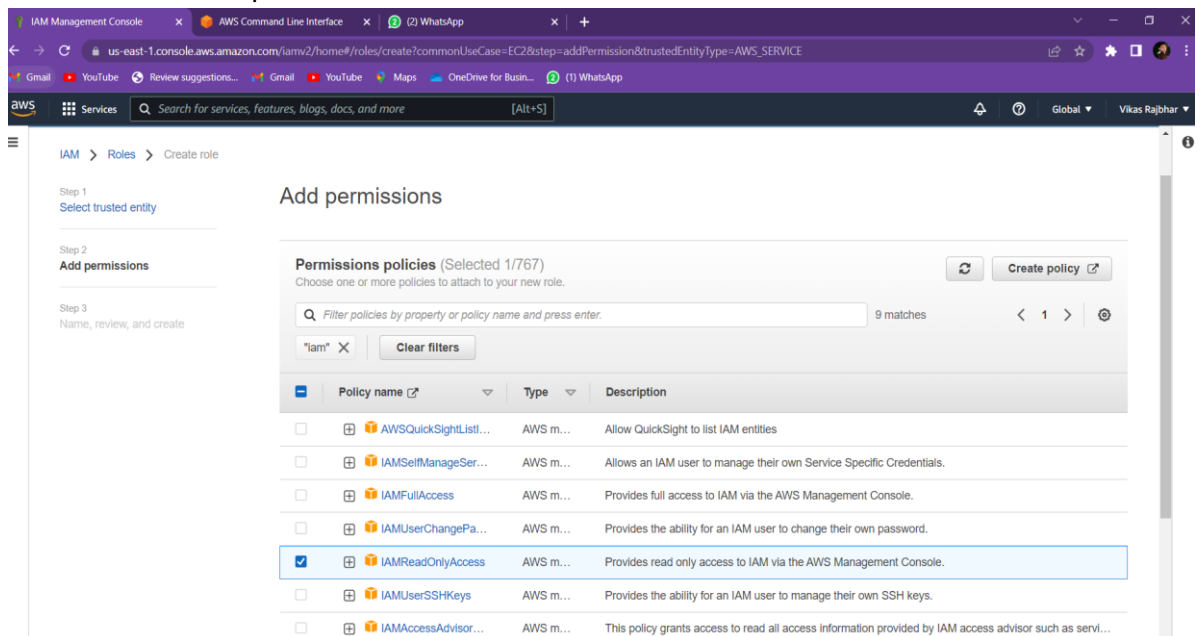
a) Go to IAM dashboard and click on **Roles** then click on create role.



b) Select trusted entity type as **AWS service** and for the Use case select **EC2**. Click **Next**.

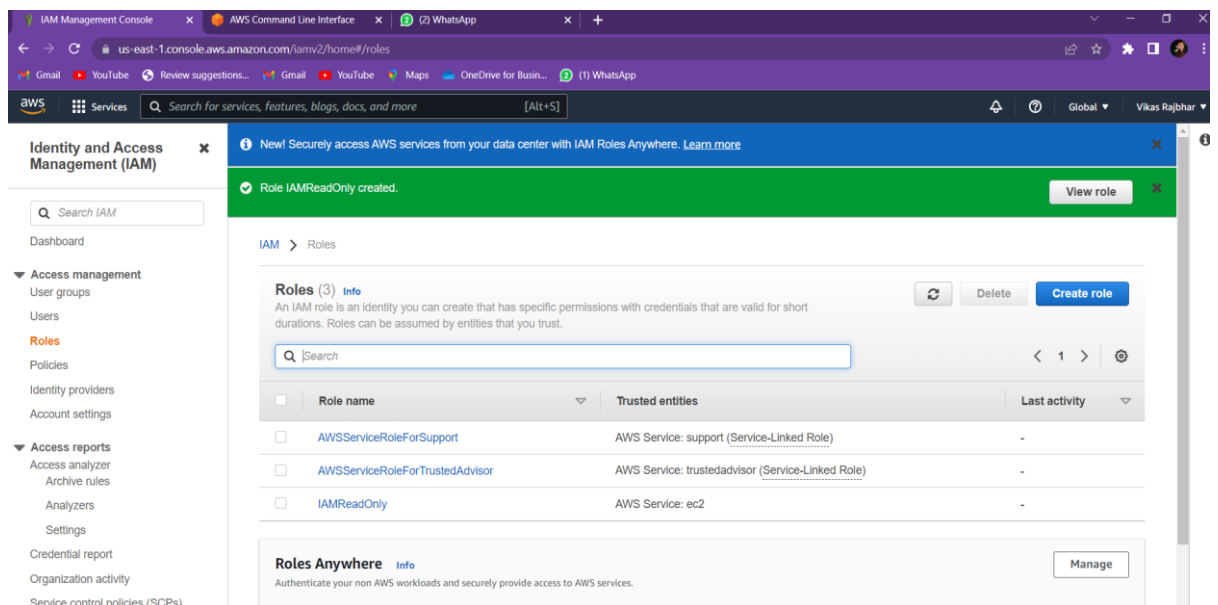
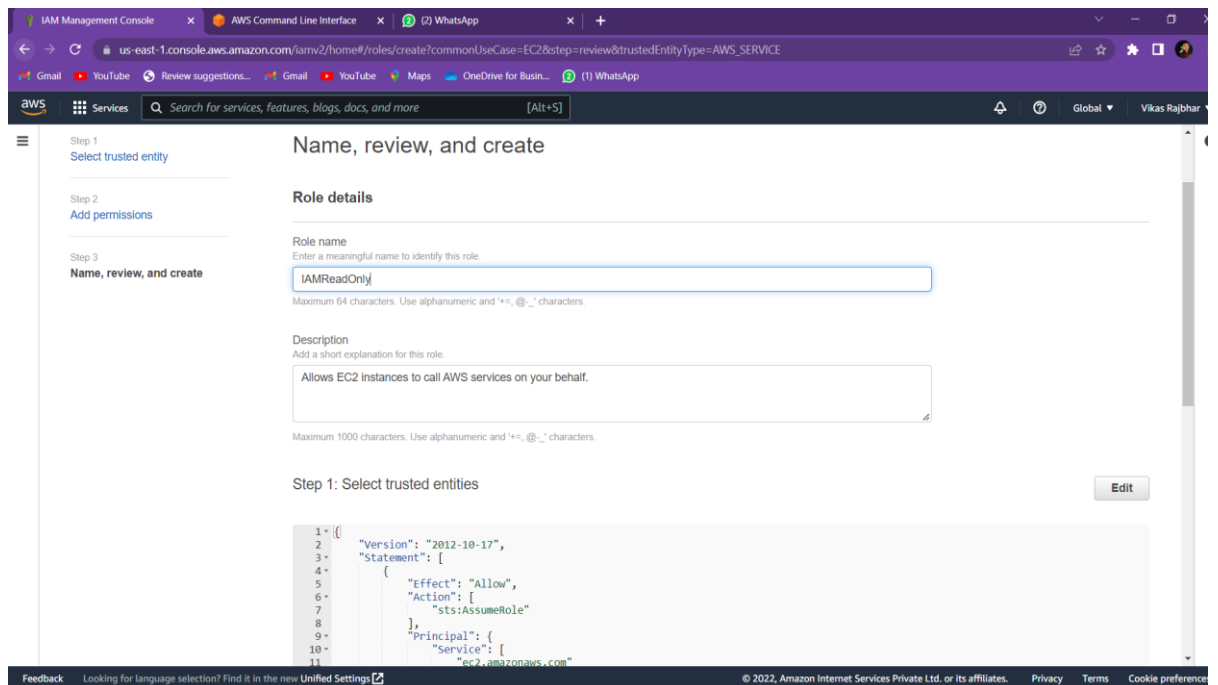


c) Select the desired permissions and then click **Next**.



d) Enter a name for the role then click on **Create role**.  
New role is created

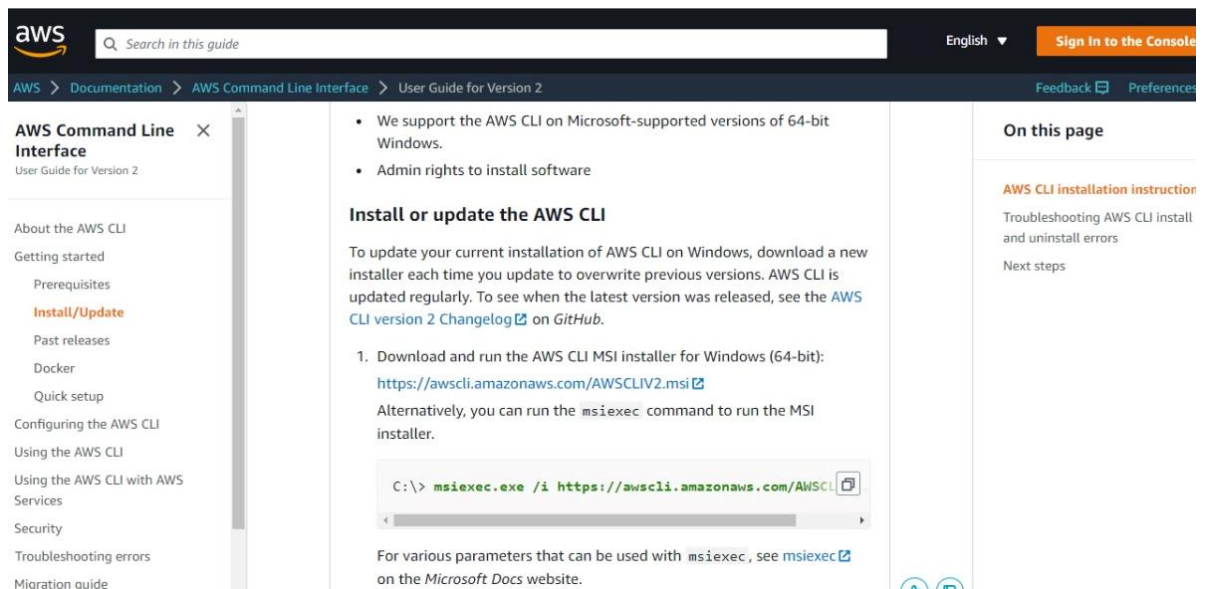




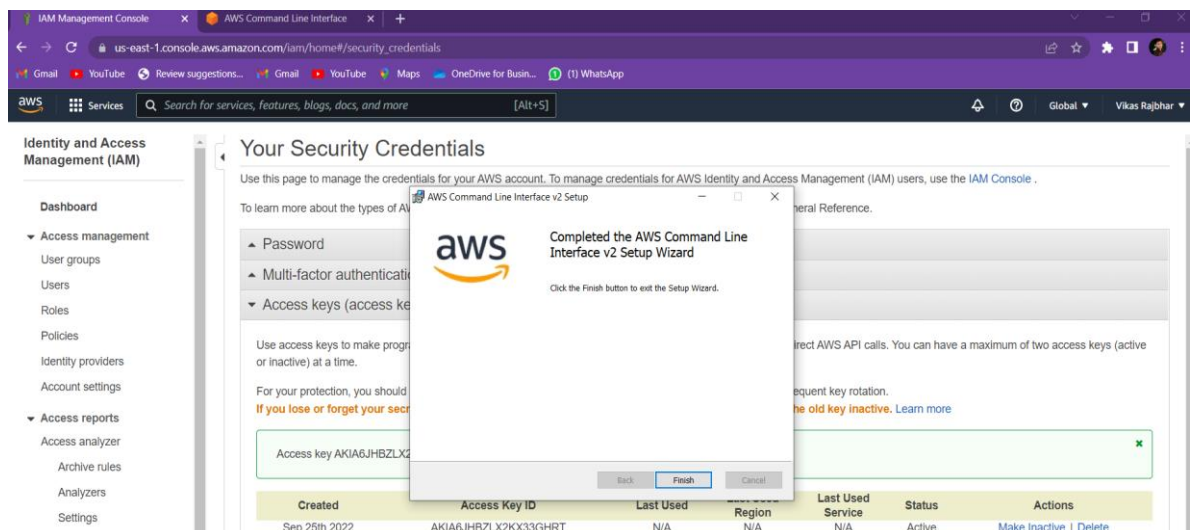
#### 4. Installing and using aws cli.

a) Search for aws cli installation wizard and download it.

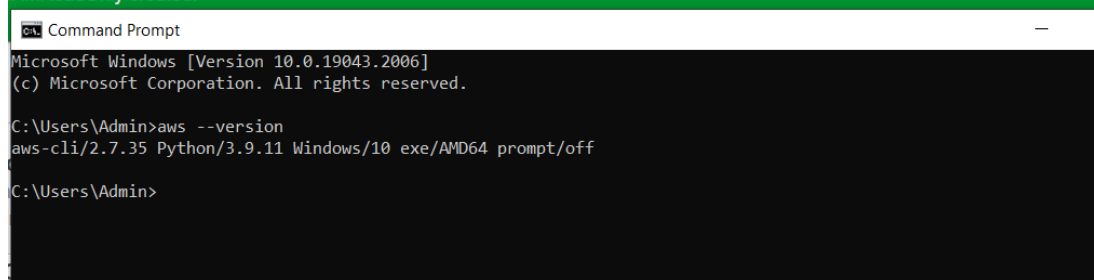




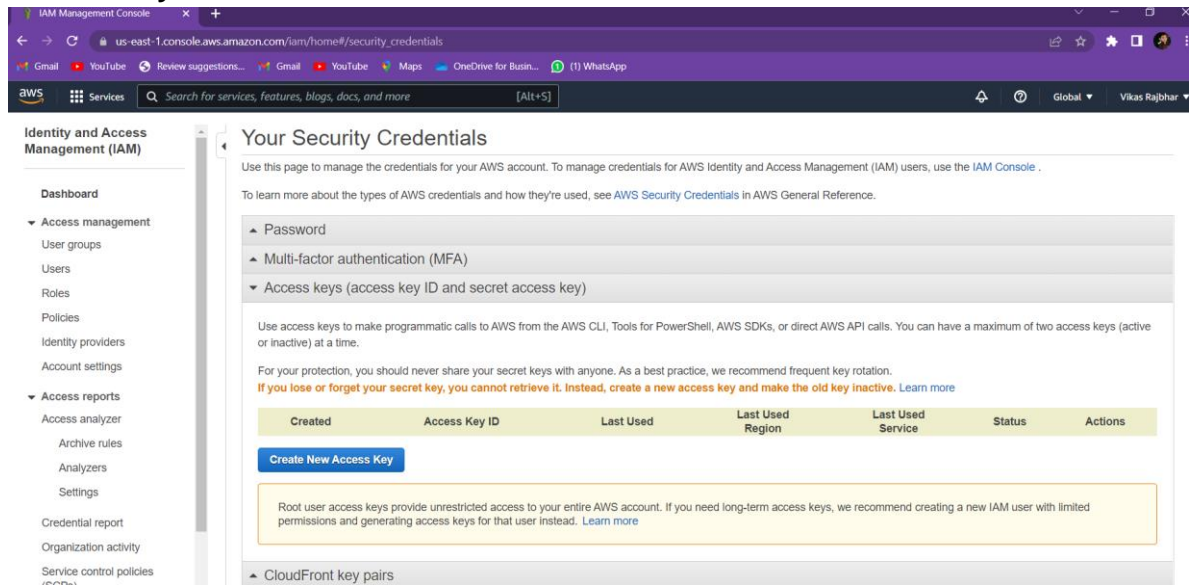
- b) Run the wizard.  
Complete the installation



- c) Confirm the installation using the **aws --version** command in the command prompt.



- d) Now go to **Security credential** in your profile and click on **Access key** to **Create New Access Key**.



- e) Use the Access key and secret key to Configure admin user.

E14							
	A	B	C	D	E	F	G
1	AWSAccessKeyId=AKIA6JHBZLX2OM7M5ECG						
2	AWSSecretKey=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						
3							
4							

Command Prompt

```
C:\Users\Admin>aws configure
AWS Access Key ID [*****G7N5]: AKIA6JHBZLX2OM7M5ECG
AWS Secret Access Key [*****nj0H]: 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
Default region name [ap-south1]: ap-south1
Default output format [None]:
```

## 5. AWS cli commands

- a) Showing Number of iam users

#### Command Prompt

```
C:\Users\Admin>aws configure
AWS Access Key ID [*****G7N5]: AKIA6JHBZLX20M7M5ECG
AWS Secret Access Key [*****nj0H]: f5cQ7D+DdKDEpOKQ9QtEMK8zC54iP34RT1iOQXwd
Default region name [ap-south1]: ap-south1
Default output format [None]:

C:\Users\Admin>aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": "user1",
      "UserId": "AIDA6JHBZLX2JBKCM4JE4",
      "Arn": "arn:aws:iam::981873548788:user/user1",
      "CreateDate": "2022-09-14T10:11:53+00:00",
      "PasswordLastUsed": "2022-09-14T10:14:36+00:00"
    },
    {
      "Path": "/",
      "UserName": "user2",
      "UserId": "AIDA6JHBZLX2LK44UDSWU",
      "Arn": "arn:aws:iam::981873548788:user/user2",
      "CreateDate": "2022-09-14T10:38:59+00:00"
    },
    {
      "Path": "/",
      "UserName": "user3",
      "UserId": "AIDA6JHBZLX2C0G34G62S",
      "Arn": "arn:aws:iam::981873548788:user/user3",
      "CreateDate": "2022-09-14T11:12:19+00:00"
    },
    {
      "Path": "/",
      "UserName": "user4",
      "UserId": "AIDA6JHBZLX2M70IIP5BN",
      "Arn": "arn:aws:iam::981873548788:user/user4",
      "CreateDate": "2022-09-14T11:15:10+00:00"
    },
    {
      "Path": "/",
      "UserName": "user5",
      "UserId": "AIDA6JHBZLX2DEEC73CKJ",
      "Arn": "arn:aws:iam::981873548788:user/user5",
      "CreateDate": "2022-09-14T11:17:48+00:00"
    }
  ]
}
```

C:\Users\Admin>

b) Creating user with username Vikas

```
C:\Users\Admin>aws iam create-user --user-name Vikas
{
  "User": {
    "Path": "/",
    "UserName": "Vikas",
    "UserId": "AIDA6JHBZLX2DPAHT53YF",
    "Arn": "arn:aws:iam::981873548788:user/Vikas",
    "CreateDate": "2022-09-25T13:06:56+00:00"
  }
}

C:\Users\Admin>
```

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with sections like 'Identity and Access Management (IAM)', 'Access management', and 'Access reports'. The main content area displays the 'Summary' for the 'ADMIN1' group. It includes fields for 'User group name' (ADMIN1), 'Creation time' (September 14, 2022, 15:37 (UTC+05:30)), and 'ARN' (arn:aws:iam::981873548788:group/ADMIN1). Below this, there are tabs for 'Users', 'Permissions', and 'Access Advisor'. The 'Users' tab is active, showing a list of 'Users in this group (4)'. The list includes users 'user3', 'user5', 'Vikas', and 'user1' with their respective group counts, last activity, and creation times.

<input type="checkbox"/>	User name <a href="#">↗</a>	Groups	Last activity	Creation time
<input type="checkbox"/>	user3	1	None	11 days ago
<input type="checkbox"/>	user5	2	None	11 days ago
<input type="checkbox"/>	Vikas	1	None	1 minute ago
<input type="checkbox"/>	user1	1	11 days ago	11 days ago

### c) Adding the user Vikas to a group Admin1

```
C:\> Command Prompt

Microsoft Windows [Version 10.0.19043.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>aws iam add-user-to-group --group-name ADMIN1 --user-name Vikas
```

aws Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report

IAM > Users

Users (6) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Find users by username or access key

	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	user1	ADMIN1	11 days ago	None	11 days ago	-
<input type="checkbox"/>	user2	NonAdmin	Never	None	11 days ago	-
<input type="checkbox"/>	user3	ADMIN1	Never	None	11 days ago	-
<input type="checkbox"/>	user4	NonAdmin	Never	None	11 days ago	-
<input type="checkbox"/>	user5	NonAdmin and ADMIN1	Never	None	11 days ago	-
<input type="checkbox"/>	Vikas	ADMIN1	Never	None	None	-

d)remove user from admin group from console

```
C:\Users\Admin>aws iam delete-user --user-name Vikas
```