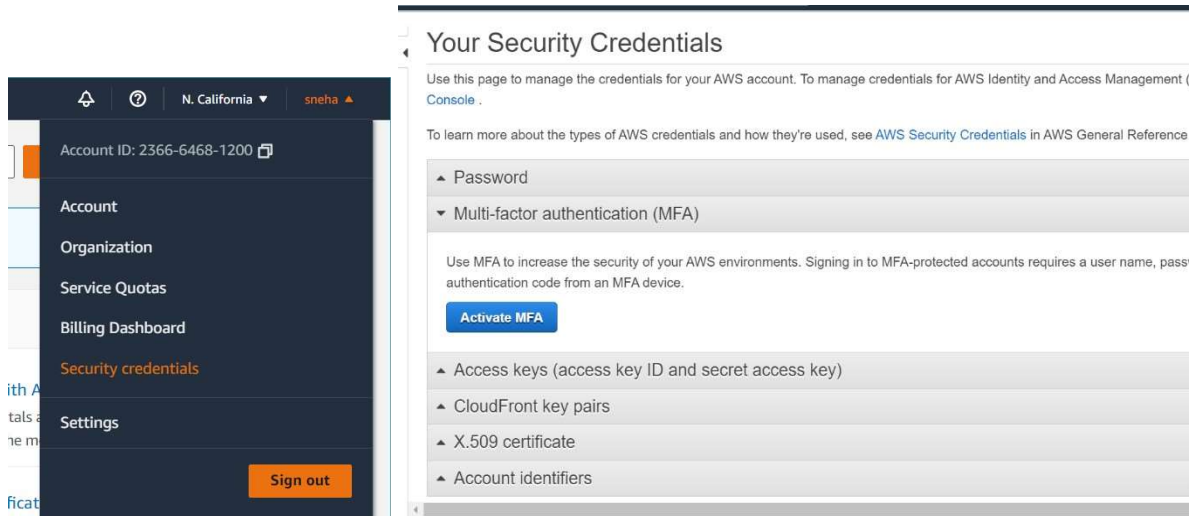


Name	Mohammad Faraz M Khan
Enrolment Number	A70405219039
Experiment Number	3b
Batch	1

AIM:

1. To Set MFA for Root AWS user




2. Setting up virtual MFA device using Authy application and go to Security Credential

3. Set up Virtual MFA Device

Set up virtual MFA device

1. Install a compatible app on your mobile device or computer
[See a list of compatible applications](#)

2. Use your virtual MFA app and your device's camera to scan the QR code



Alternatively, you can type the secret key. [Show secret key](#)

3. Type two consecutive MFA codes below

MFA code 1

Cancel

Previous

Assign MFA

4. Add MFA Code from authy app

3. Type two consecutive MFA codes below

MFA code 1

982779

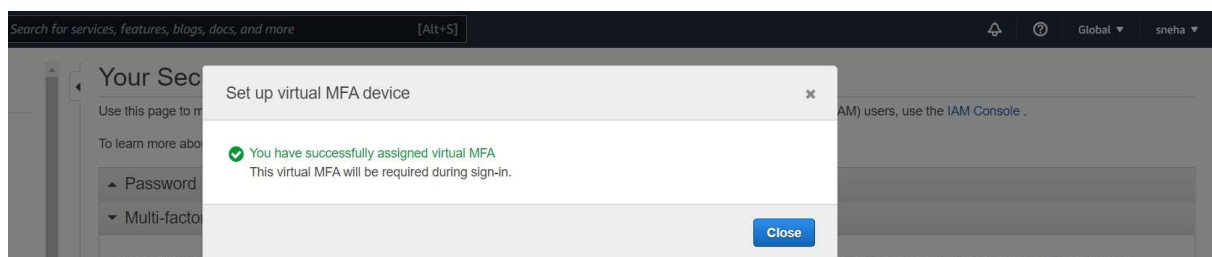
MFA code 2

852282

Cancel

Previous

Assign MFA



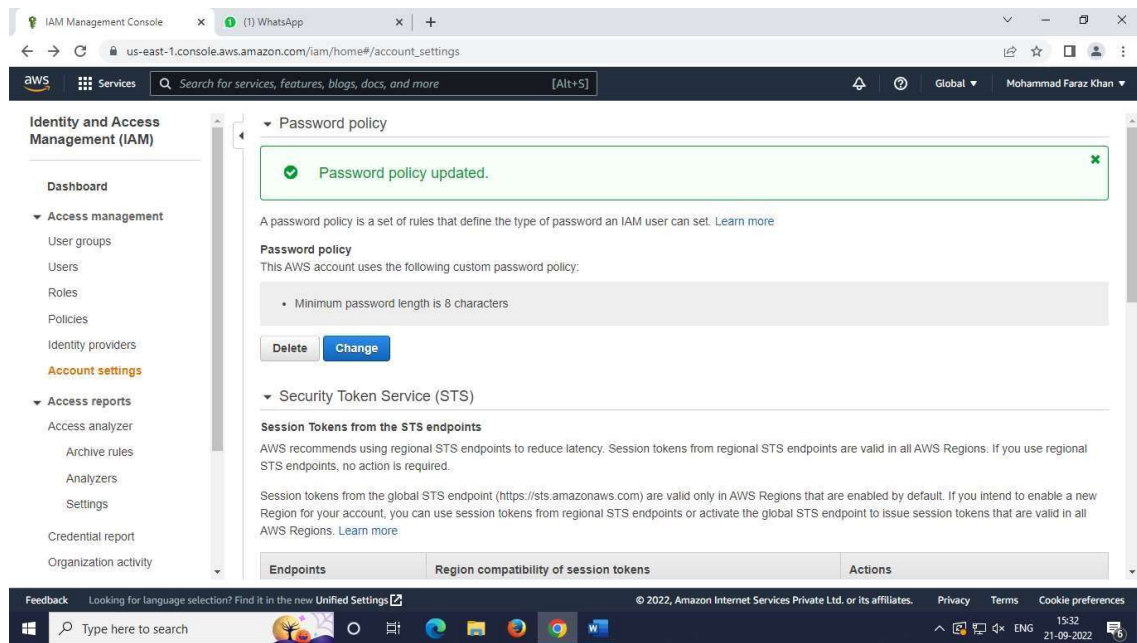
2. Set the password policy

Got to account setting-> Password Policy-> Set password

The screenshot shows the AWS IAM dashboard. On the left is a navigation menu with options like Dashboard, Access management, Access reports, and Settings. The main area displays 'IAM dashboard' with 'Security recommendations' showing two green checkmarks: 'Root user has MFA' and 'Root user has no active access keys'. Below this is a table of 'IAM resources' with counts for User groups (3), Users (6), Roles (2), Policies (0), and Identity providers (0). On the right, the 'AWS Account' section shows account details like ID and Alias. At the bottom, there's a 'What's new' section with updates for IAM features.

The screenshot shows the 'Set password policy' page in the AWS IAM console. It includes a description of password policies and a section titled 'Select your account password policy requirements:'. This section contains several checkboxes for configuring password rules, such as 'Enforce minimum password length' (set to 8 characters), 'Require at least one uppercase letter', 'Require at least one lowercase letter', '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', and 'Prevent password reuse'. At the bottom right, there are 'Cancel' and 'Save changes' buttons. The page footer shows the AWS logo, a search bar, and various utility links.

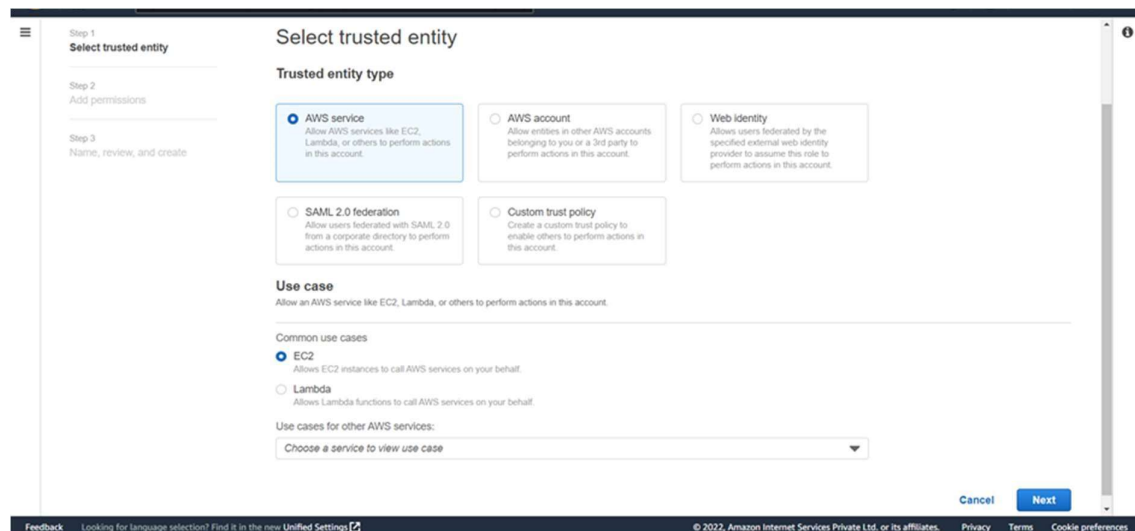
Save changes and its Done



3. Create the IAM Role

Now to create role go to -> IAM -> roles-> Create roles

Select EC2 and click on next



Add permission "Iamreadonlyaccess" and select and do next.

IAM Management Console | (1) WhatsApp | us-east-1.console.aws.amazon.com/iamv2/home#/roles/create?commonUseCase=EC2&step=addPermission&trustedEntityType=AWS_SERVICE

Search for services, features, blogs, docs, and more [Alt+S]

Global | Mohammad Faraz Khan

Step 1: Select trusted entity

Step 2: **Add permissions**

Step 3: Name, review, and create

Add permissions

Permissions policies (767)
Choose one or more policies to attach to your new role.

Filter policies by property or policy name and press enter. 1 match < 1 > ⚙

iamreadonly ✕ Clear filters

<input type="checkbox"/>	Policy name	Type	Description
<input type="checkbox"/>	iamreadonly	IAMReadOnlyAccess	Provides read only access to IAM via the AWS Management Console.

Set permissions boundary - optional
Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

Cancel Previous Next

Feedback | Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Type here to search

Name as something and next to create Role.

IAM Management Console | (1) WhatsApp | us-east-1.console.aws.amazon.com/iamv2/home#/roles/create?commonUseCase=EC2&step=review&trustedEntityType=AWS_SERVICE

Search for services, features, blogs, docs, and more [Alt+S]

Global | Mohammad Faraz Khan

Step 2: Add permissions

Step 3: **Name, review, and create**

Role details

Role name
Enter a meaningful name to identify this role.

Admin

Maximum 64 characters. Use alphanumeric and '+', '=', '@', '_' characters.

Description
Add a short explanation for this role.

Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+', '=', '@', '_' characters.

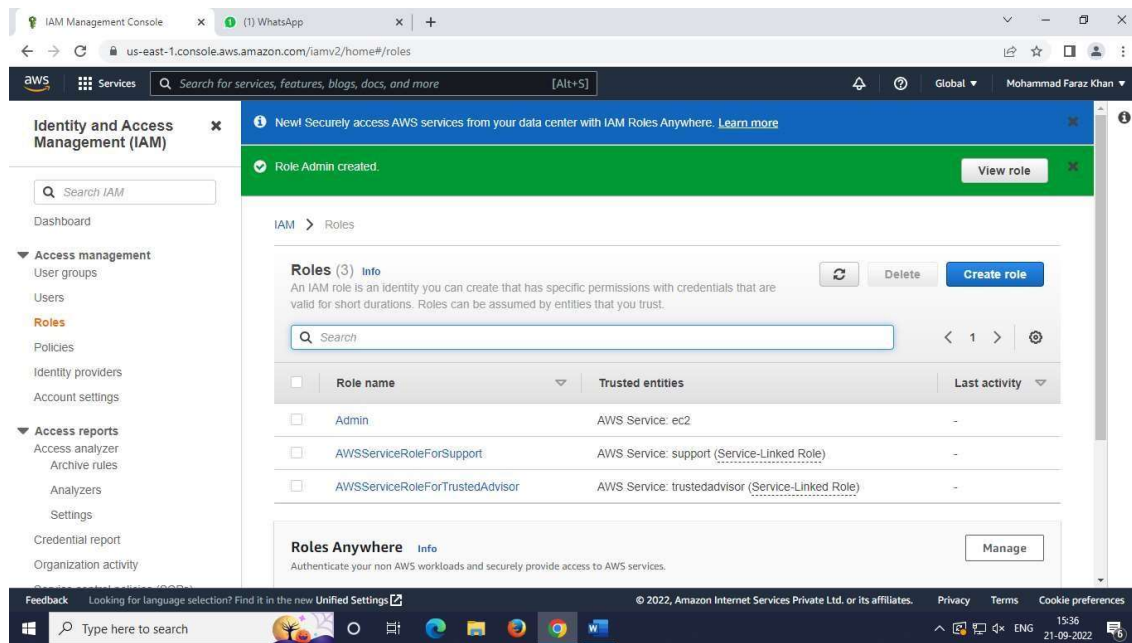
Step 1: Select trusted entities Edit

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "sts:AssumeRole"
8       ],
9       "Principal": {
```

Feedback | Looking for language selection? Find it in the new Unified Settings

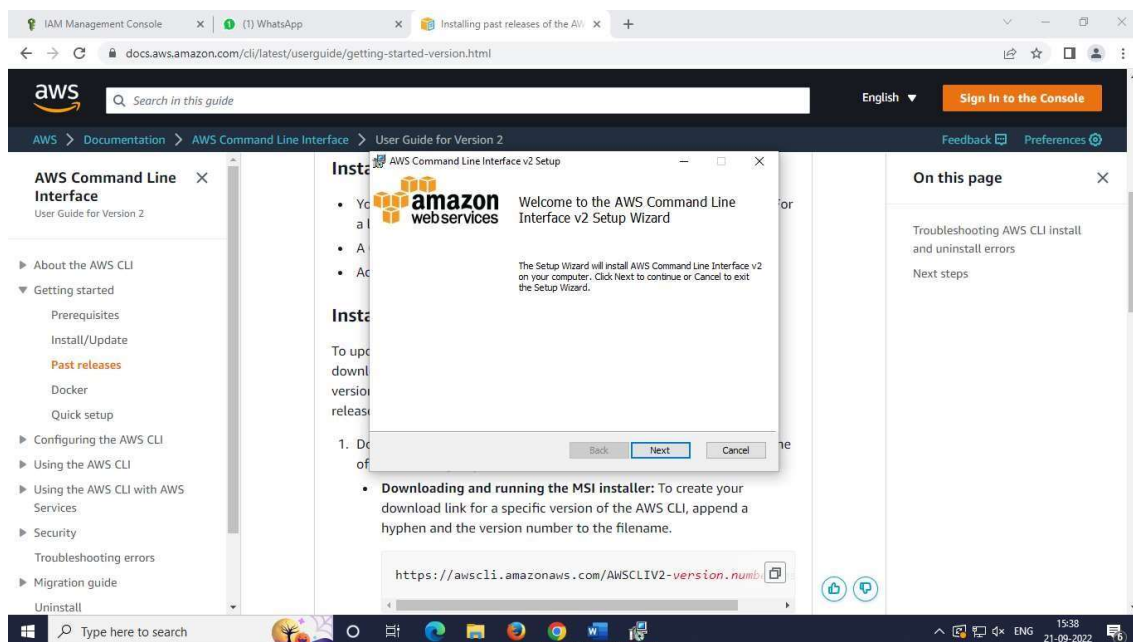
© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

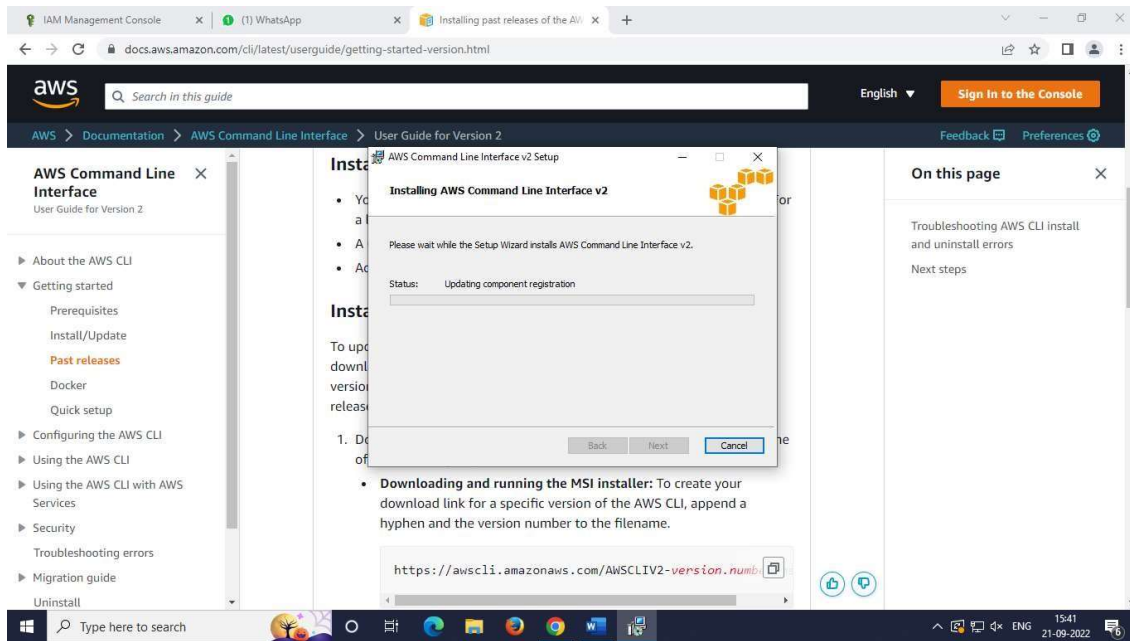
Type here to search



4. Configure AWS CLI

Now we need to install Aws Version 2 from website and then open command line to work on it.

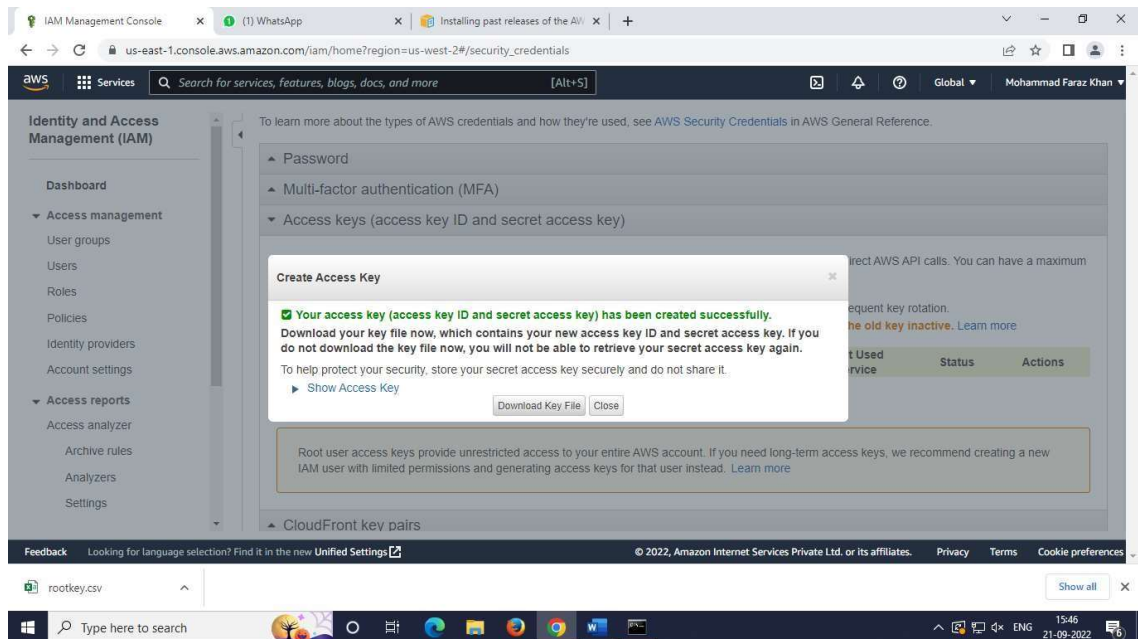




Now check the version of aws.



Once it's done we need access key to run it so for that go again to IAM and download the key.




```
Command Prompt - aws iam list-users
help
C:\Users\student1>aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": "User1",
      "UserId": "AIDAT5JHZ6W5IAU3K2BG1",
      "Arn": "arn:aws:iam::269055817146:user/User1",
      "CreateDate": "2022-09-14T09:57:58+00:00",
      "PasswordLastUsed": "2022-09-14T10:00:30+00:00"
    },
    {
      "Path": "/",
      "UserName": "User2",
      "UserId": "AIDAT5JHZ6W5GZLF73UA2",
      "Arn": "arn:aws:iam::269055817146:user/User2",
      "CreateDate": "2022-09-14T10:24:07+00:00"
    },
    {
      "Path": "/",
      "UserName": "User3",
      "UserId": "AIDAT5JHZ6W5GZLF73UA2",
      "Arn": "arn:aws:iam::269055817146:user/User3",
      "CreateDate": "2022-09-14T10:28:24+00:00"
    },
    {
      "Path": "/",
      "UserName": "User4",
      "UserId": "AIDAT5JHZ6W5PNPDHAFK1",
      "Arn": "arn:aws:iam::269055817146:user/User4",
      "CreateDate": "2022-09-14T10:28:24+00:00"
    }
  ]
}
-- More --
```

After Configure root user

1. Configure admin user
2. Create user through admin user in CLI

```
C:\Users\student1>aws iam create-user --user-name User7
{
  "User": {
    "Path": "/",
    "UserName": "User7",
    "UserId": "AIDAT5JHZ6W5KKZSVS26B",
    "Arn": "arn:aws:iam::269055817146:user/User7",
    "CreateDate": "2022-09-21T10:36:11+00:00"
  }
}
C:\Users\student1>
```

3. Remove user from admin group from console

```
C:\Users\student1>aws iam create-user --user-name User7
{
  "User": {
    "Path": "/",
    "UserName": "User7",
    "UserId": "AIDAT5JHZ6W5KKZSVS26B",
    "Arn": "arn:aws:iam::269055817146:user/User7",
    "CreateDate": "2022-09-21T10:36:11+00:00"
  }
}
C:\Users\student1>aws iam delete-user --user-name User7
C:\Users\student1>
```

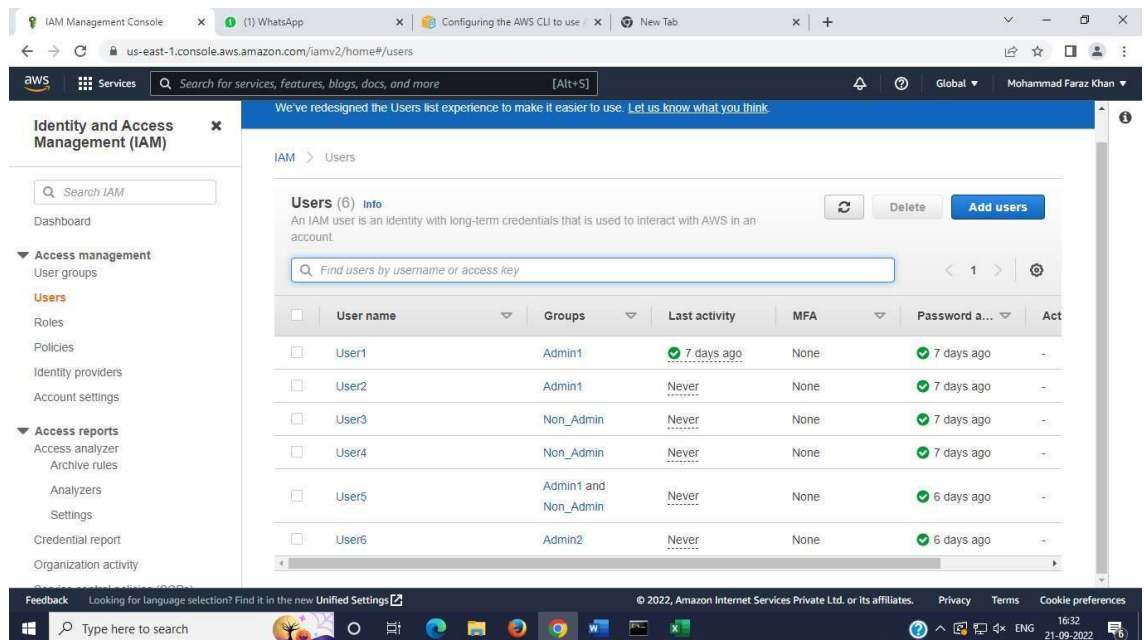
4. Check again through CLI to create users

```
Command Prompt - aws iam list-users

{
  "Users": [
    {
      "Path": "/",
      "UserName": "User1",
      "UserId": "AIDATS3HZ6W5IAU3K2BG1",
      "Arn": "arn:aws:iam::269855817146:user/User1",
      "CreateDate": "2022-09-14T09:57:58+00:00",
      "PasswordLastUsed": "2022-09-14T10:30+00:00"
    },
    {
      "Path": "/",
      "UserName": "User2",
      "UserId": "AIDATS3HZ6W5EAAOG0BPQ",
      "Arn": "arn:aws:iam::269855817146:user/User2",
      "CreateDate": "2022-09-14T10:24:07+00:00"
    },
    {
      "Path": "/",
      "UserName": "User3",
      "UserId": "AIDATS3HZ6W5GZLF7JUA2",
      "Arn": "arn:aws:iam::269855817146:user/User3",
      "CreateDate": "2022-09-14T10:28:24+00:00"
    },
    {
      "Path": "/",
      "UserName": "User4",
      "UserId": "AIDATS3HZ6W5PNPDHAFKT",
      "Arn": "arn:aws:iam::269855817146:user/User4",
      "CreateDate": "2022-09-14T10:30:20+00:00"
    },
    {
      "Path": "/",
      "UserName": "User5",
      "UserId": "AIDATS3HZ6W5KH7TSFXJB",
      "Arn": "arn:aws:iam::269855817146:user/User5",
      "CreateDate": "2022-09-14T11:15:07+00:00"
    },
    {
      "Path": "/",
      "UserName": "User6",
      "UserId": "AIDATS3HZ6W5PSZKWTUFE",
      "Arn": "arn:aws:iam::269855817146:user/User6",
      "CreateDate": "2022-09-14T11:15:07+00:00"
    }
  ]
}
```

User7 is not there

5. Add user back through AWS Console



The screenshot shows the AWS IAM console with the 'Users' page selected. The 'Users (6) Info' section indicates that there are 6 users listed. The table below shows the details for each user:

	User name	Groups	Last activity	MFA	Password a...	Act
<input type="checkbox"/>	User1	Admin1	7 days ago	None	7 days ago	-
<input type="checkbox"/>	User2	Admin1	Never	None	7 days ago	-
<input type="checkbox"/>	User3	Non_Admin	Never	None	7 days ago	-
<input type="checkbox"/>	User4	Non_Admin	Never	None	7 days ago	-
<input type="checkbox"/>	User5	Admin1 and Non_Admin	Never	None	6 days ago	-
<input type="checkbox"/>	User6	Admin2	Never	None	6 days ago	-

6. Create a new group and add user in CLI

```
C:\Users\student1>aws iam create-group --group-name Group1
{
  "Group": {
    "Path": "/",
    "GroupName": "Group1",
    "GroupId": "AGPAT5JHZ6W5EFT6WGP65",
    "Arn": "arn:aws:iam::269055817146:group/Group1",
    "CreateDate": "2022-09-21T10:59:17+00:00"
  }
}

C:\Users\student1>aws iam add-user-to-group --user-name User6 --group-name Group1

C:\Users\student1>
```

So we have added User6 to group named as “Group1”.