IAM- Identity Access Management

Aunthentication:

It means users entering their username and password.

Authorization:

It means what rights are given to the users to perform their operations.

IAM User:

An **IAM User** is an individual identity in AWS with specific **login credentials**.

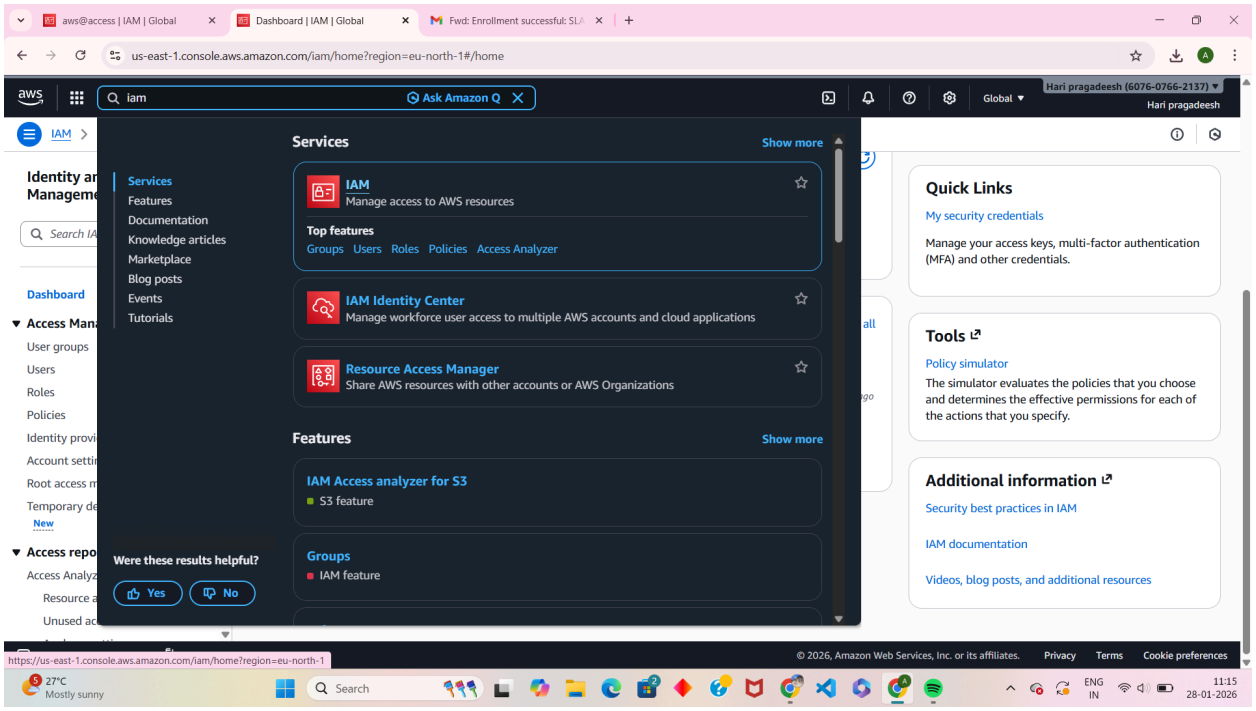
It represents a **person or application** and is given **permissions** to access AWS resources.

IAM Group:

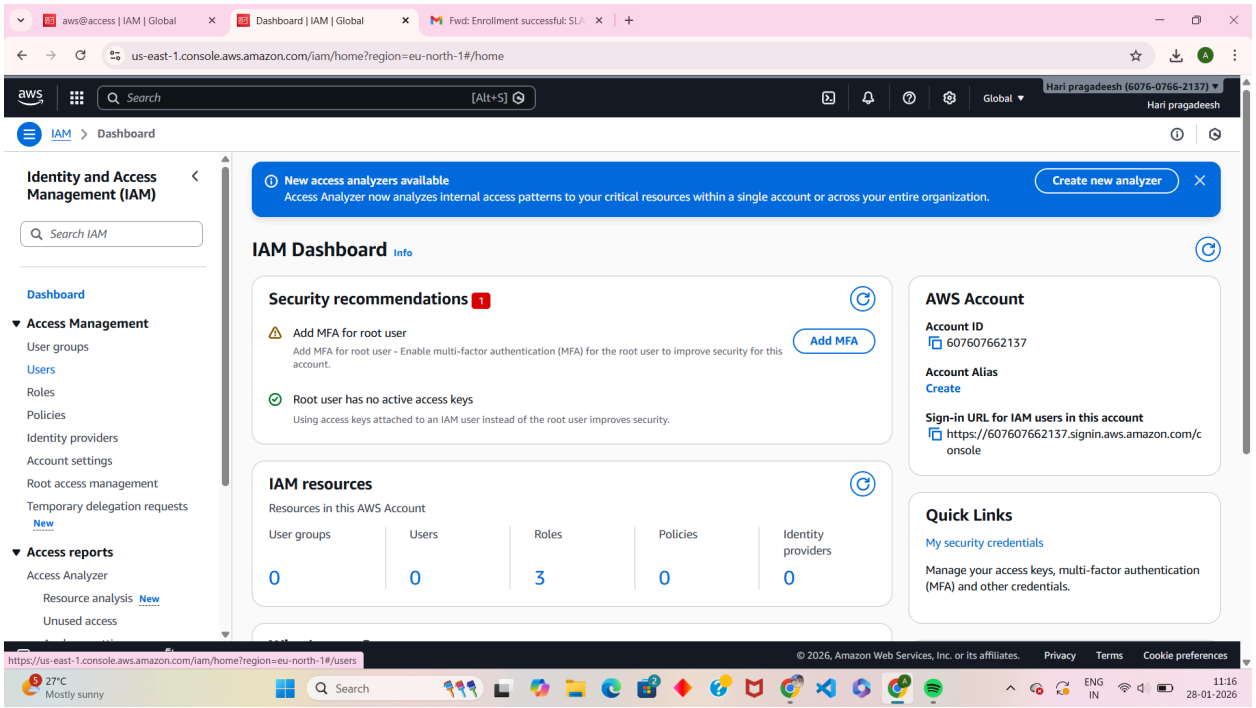
An **IAM Group** is a collection of IAM users.

Permissions are assigned to the **group**, and all users in the group automatically get those permissions.

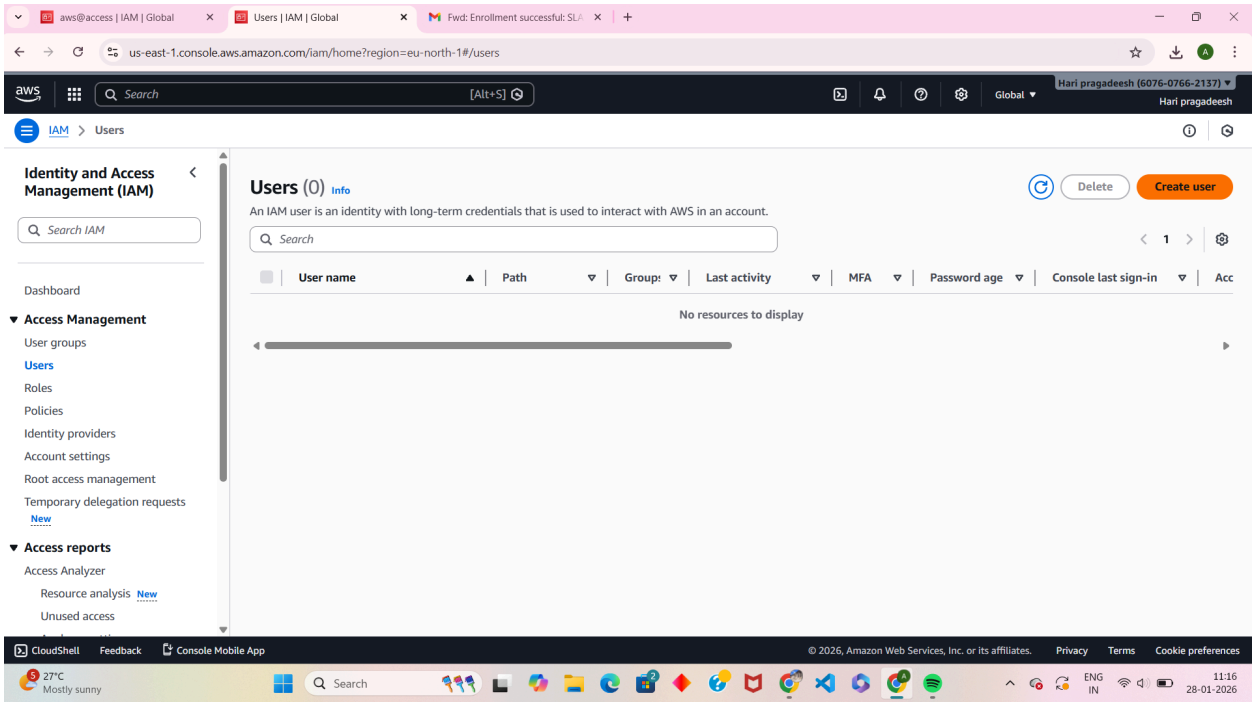
Now we can see how to create IAM user in AWS



- In search bar enter IAM and click IAM



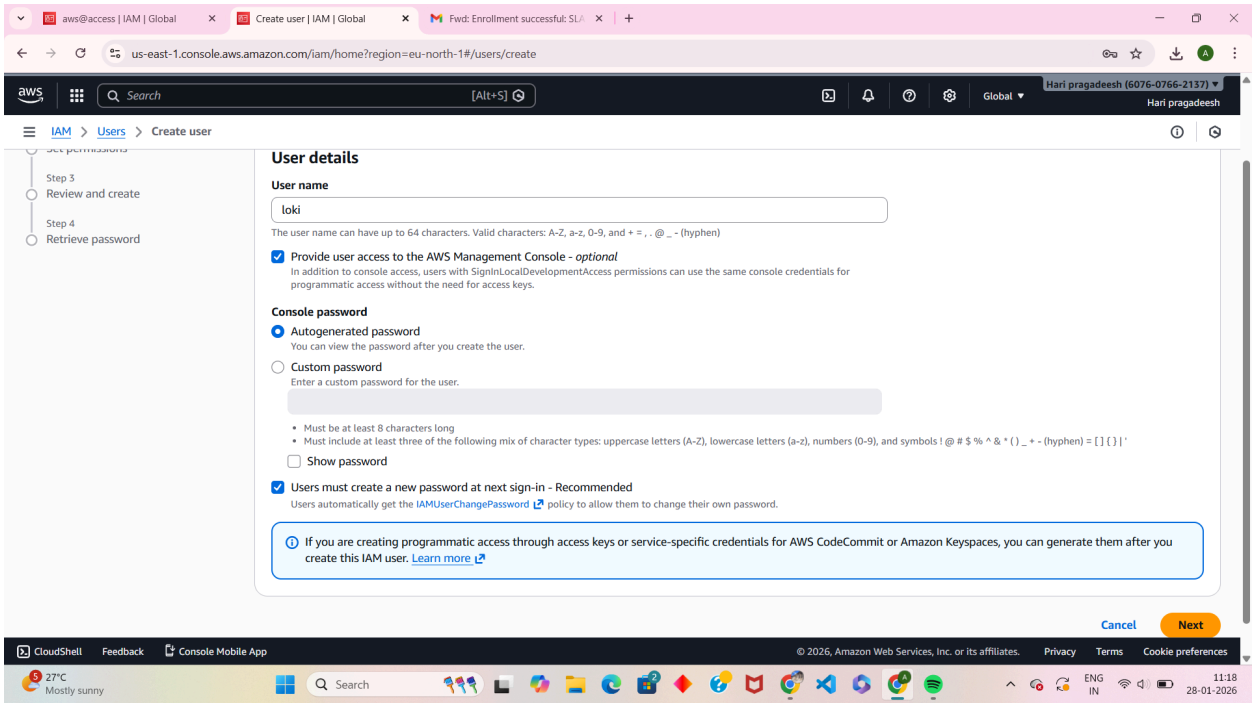
- Then the IAM dashboard will open.
- Then click users.



Opened **Users** section in IAM

No IAM users created yet

Option available to **Create user**



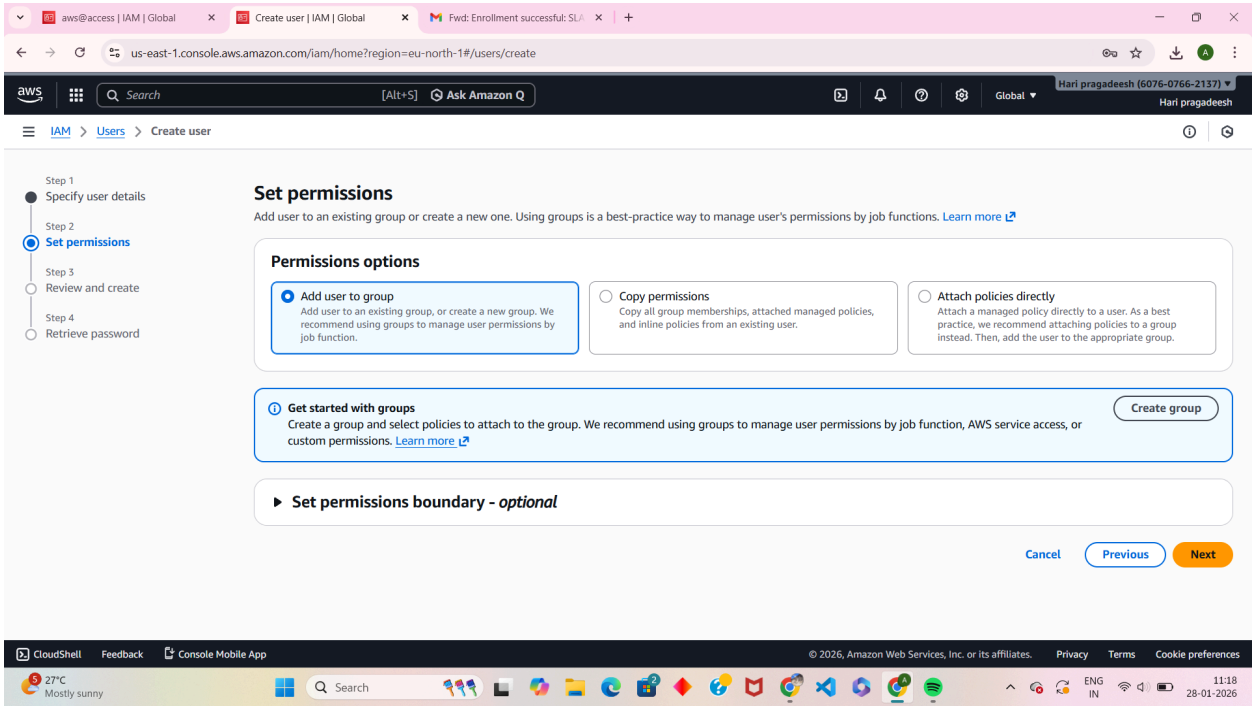
Started creating a new IAM user

Entered user name: loki

Enabled AWS Management Console access

Selected auto-generated password

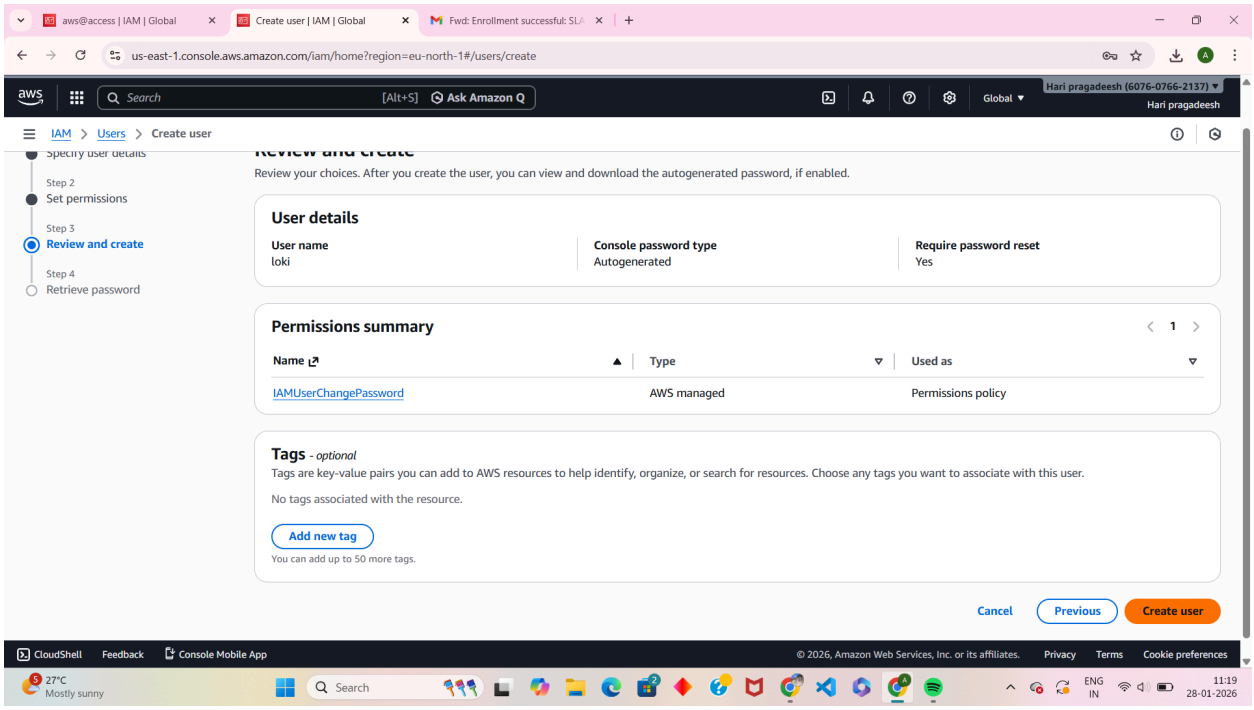
Enabled “User must change password at next sign-in”



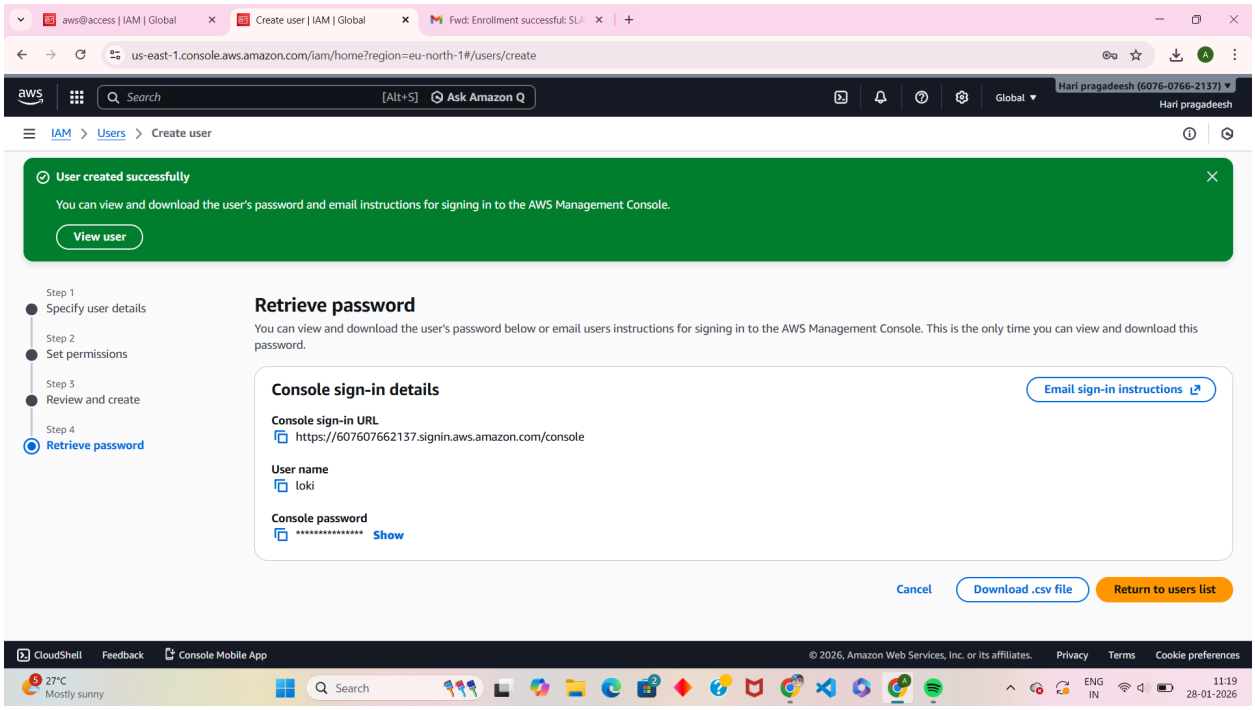
Selected Add user to group (best practice)

No group created yet

Permissions to be assigned using groups



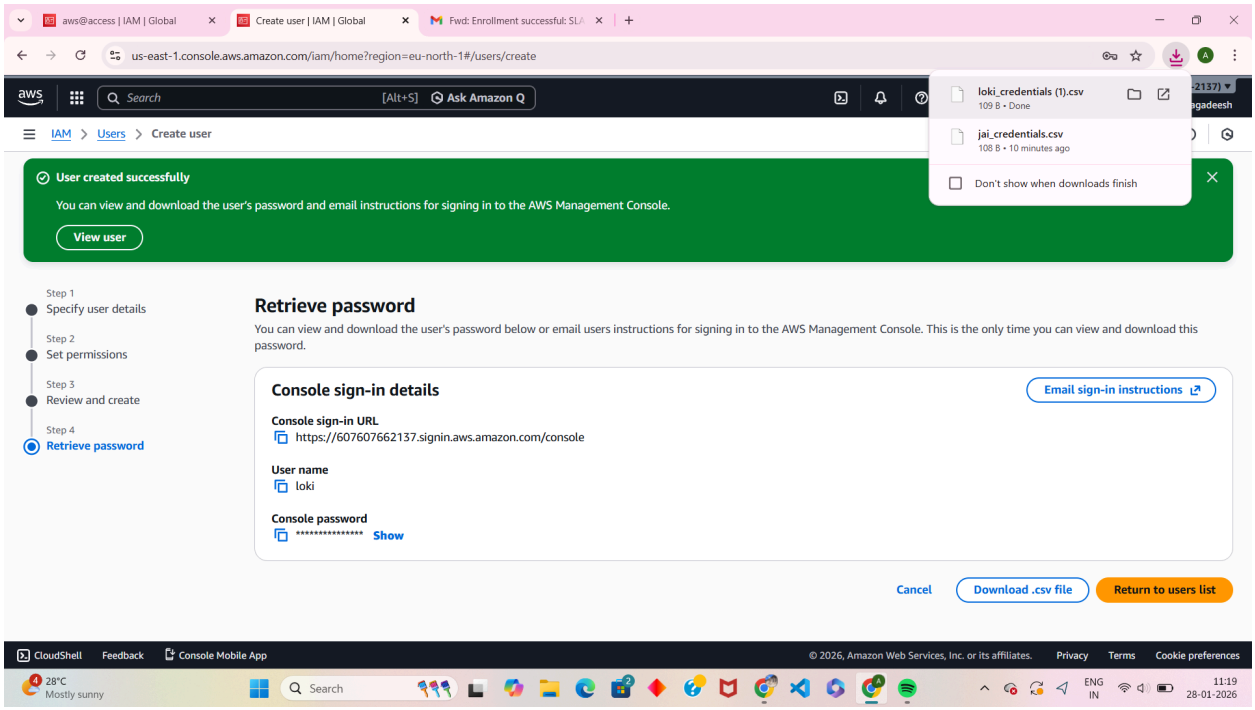
- Reviewed user details
- Console password type: Auto-generated
- Password reset required at first login
- Attached policy: **IAMUserChangePassword**



IAM user **loki** created successfully

Confirmation message displayed

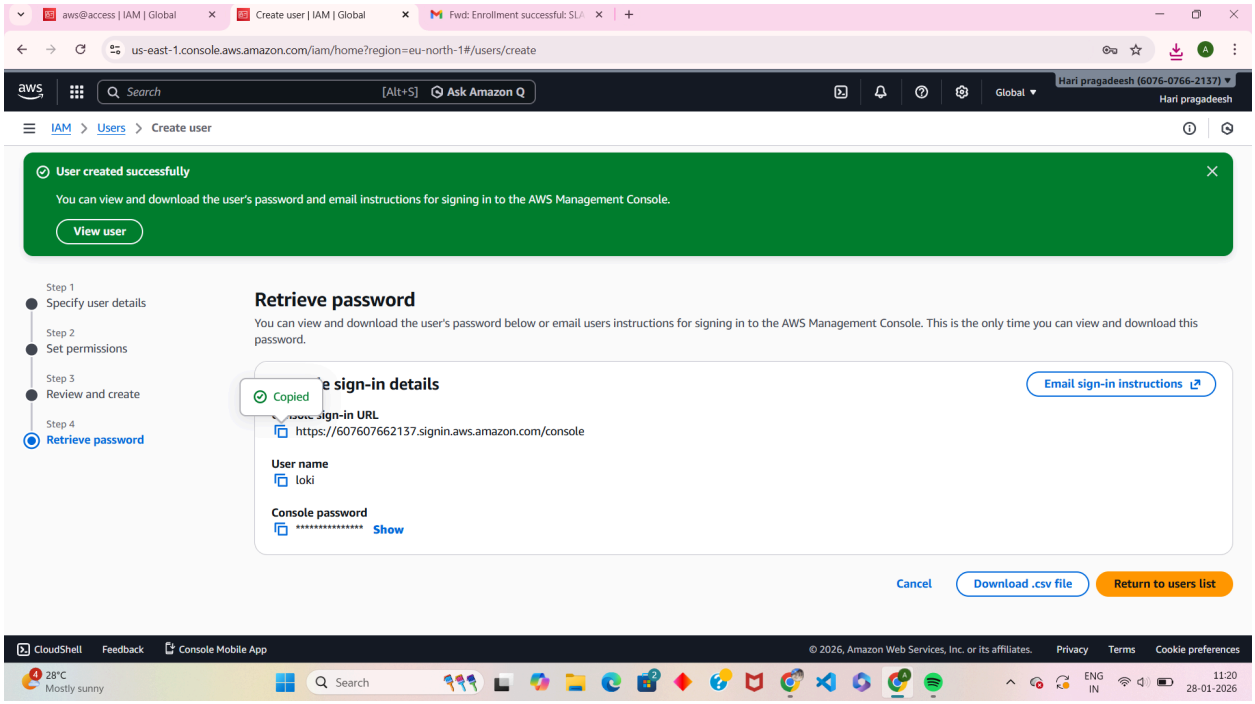
Option to view user details



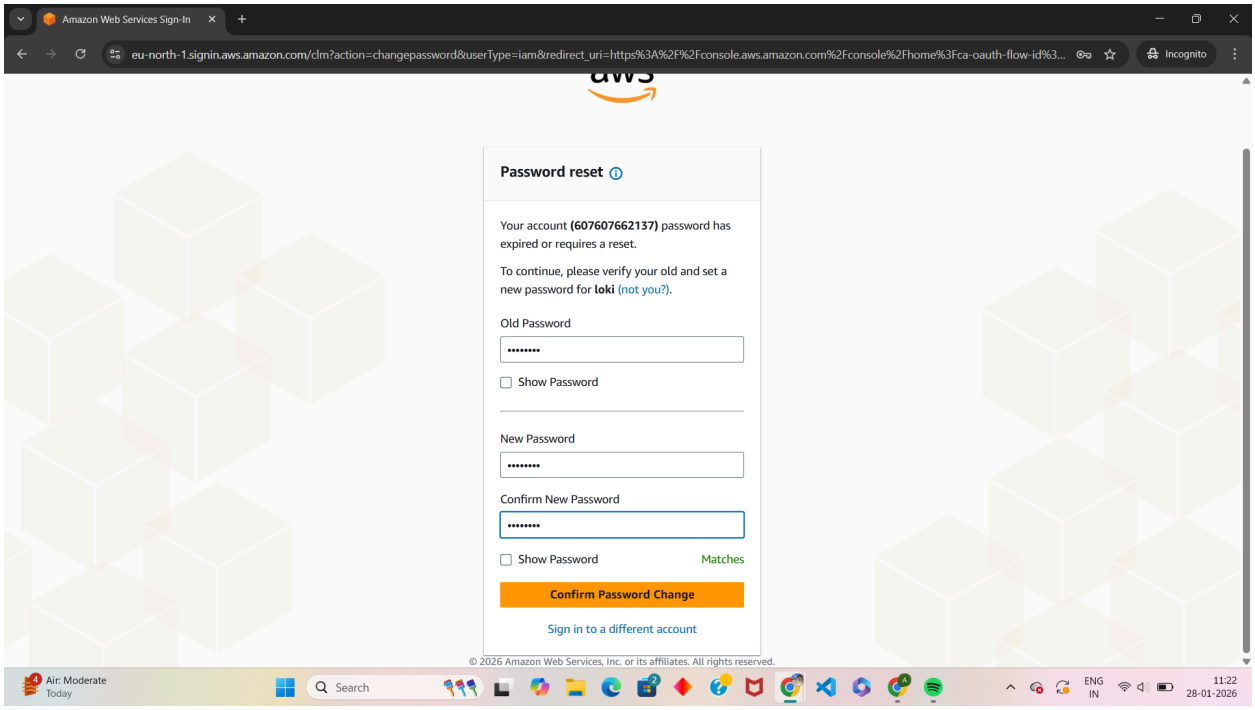
Credentials downloaded as **CSV file**

File contains username and password

Used for first-time login



- Console sign-in URL copied
- User can log in using provided credentials
- Password must be changed after first login

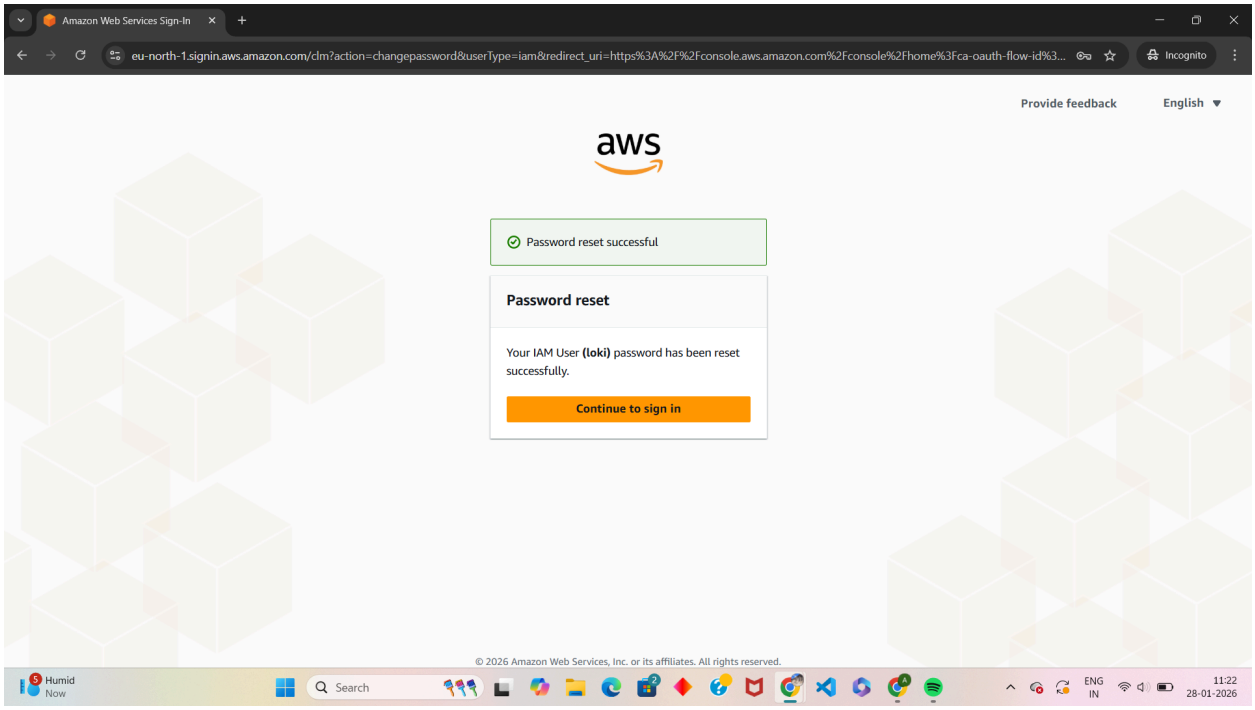


IAM user **loki** is signing in for the first time

AWS forces password reset (temporary password expired)

Old password entered

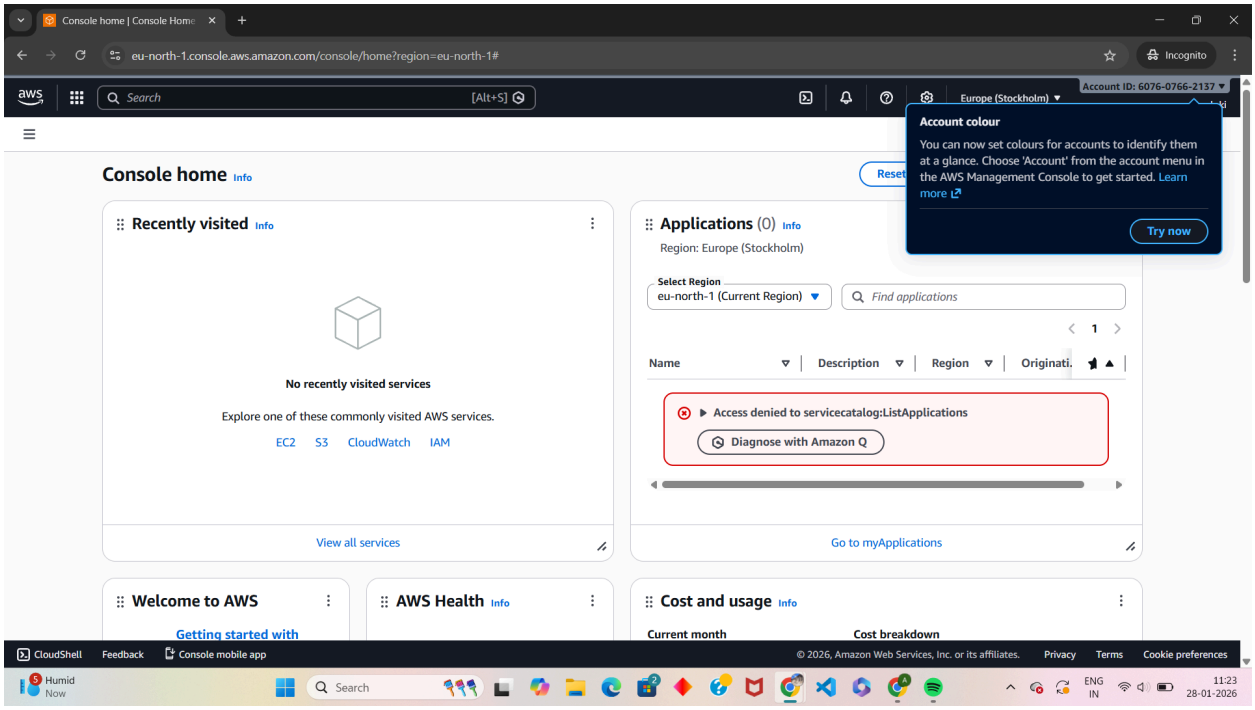
New password and confirm password entered



Password reset completed successfully

IAM user **loki** password updated

User can continue to AWS Console

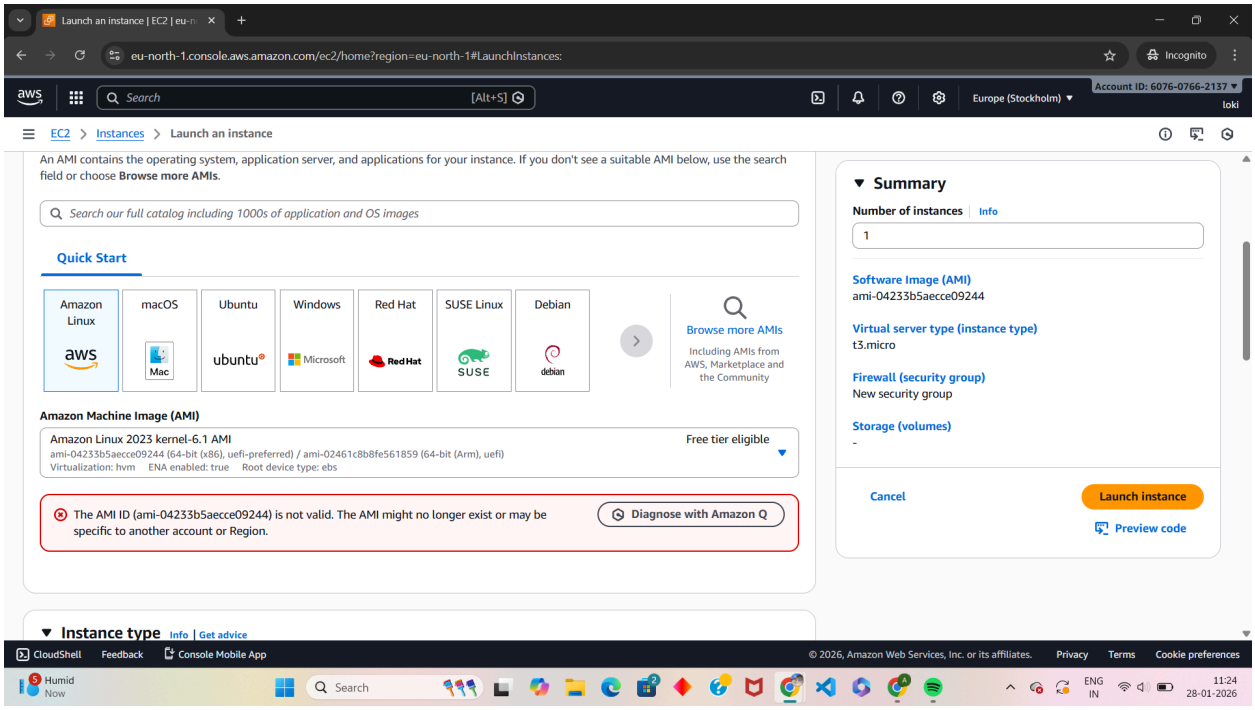


User logged into AWS Console

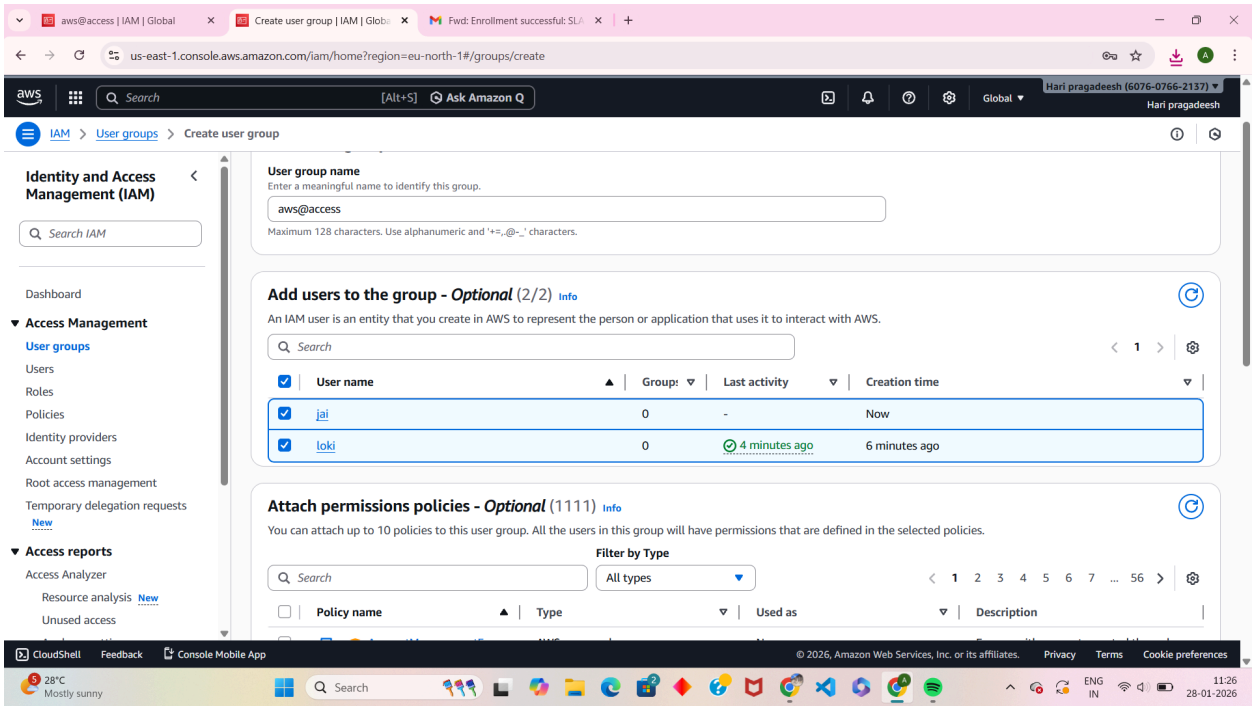
Region selected: **Europe (Stockholm)**

Access denied error shown for some services

Indicates **insufficient IAM permissions**



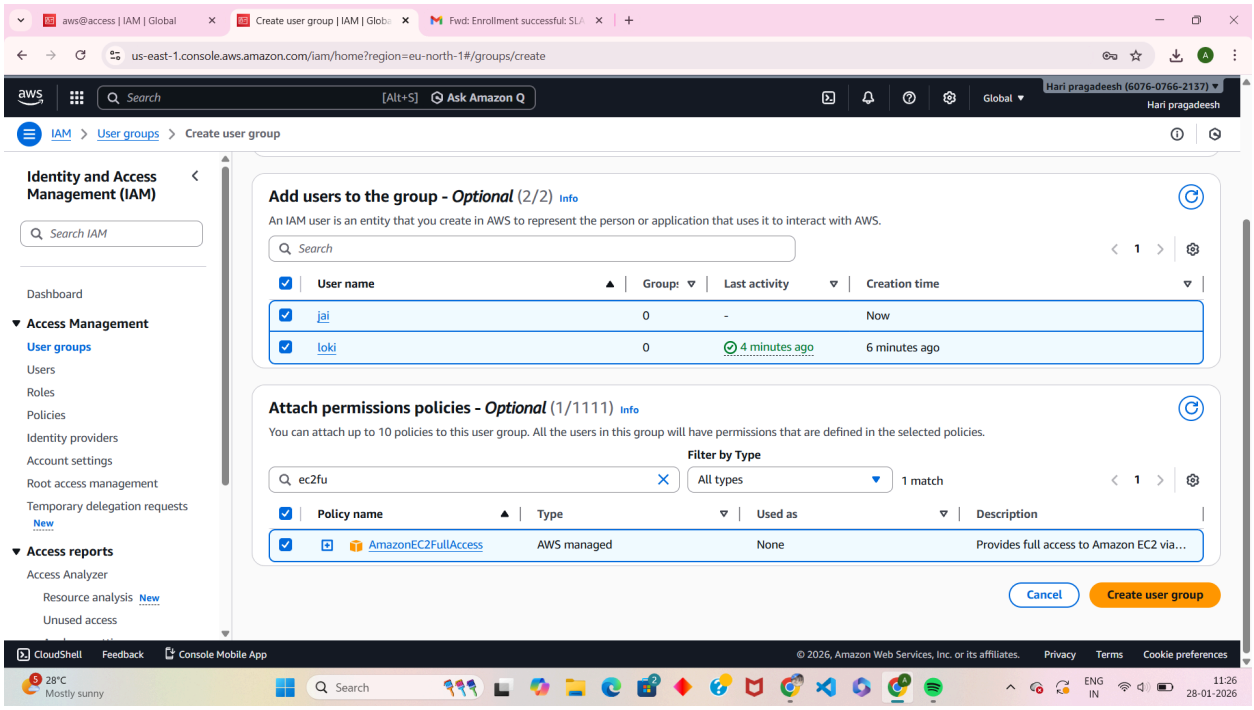
- User tried to launch an EC2 instance
- AMI ID error displayed
- Access issue due to **missing EC2 permissions**
- Shows need for EC2 policy assignment



Created a new IAM group named **aws@access**

Selected users **jai** and **loki**

Users added to the group

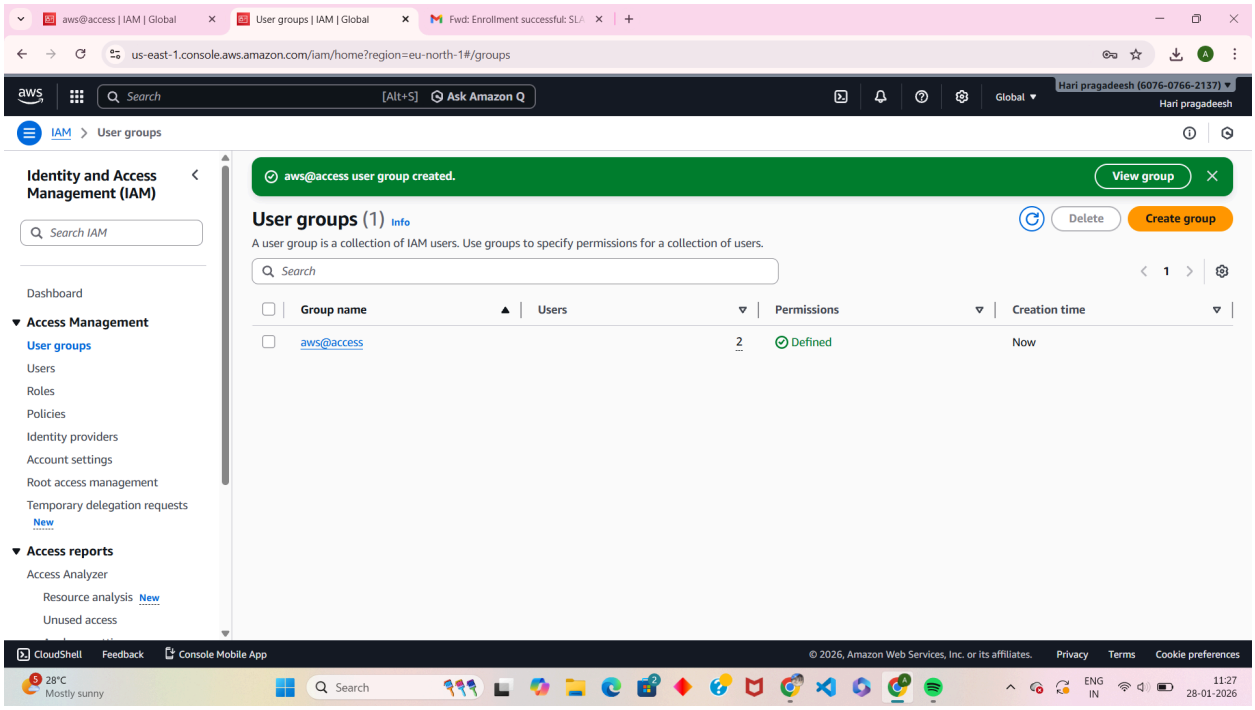


Searched for EC2 policy

Selected **AmazonEC2FullAccess**

Policy attached to the user group

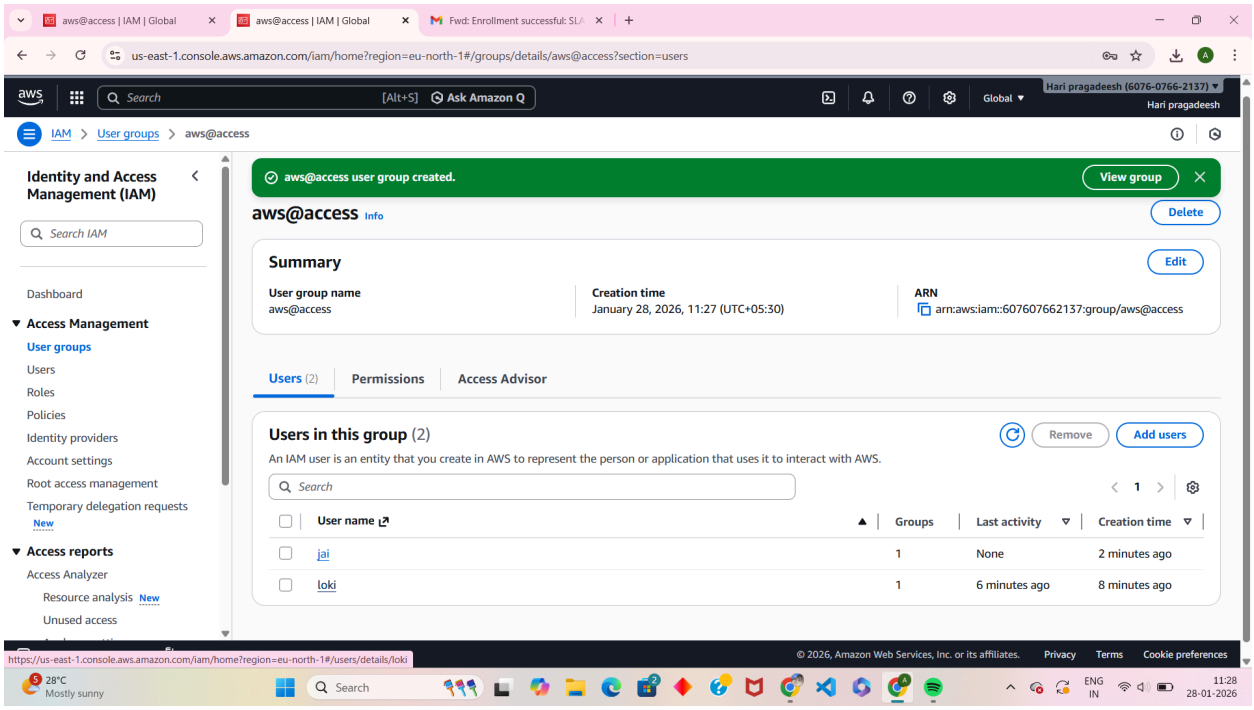
Group provides full EC2 access



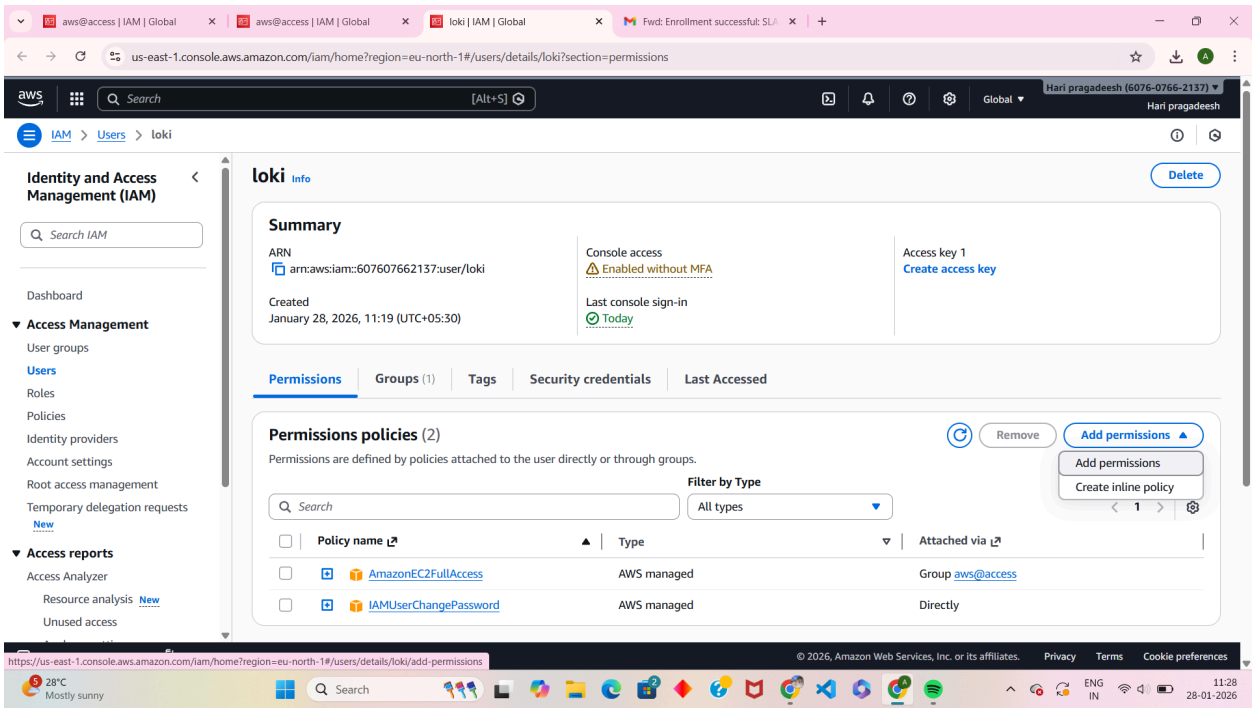
IAM user group **aws@access** created

Group contains **2 users**

Permissions status shown as **Defined**



- Opened **aws@access** group details
- Shows group ARN and creation time
- Lists users **jai** and **loki**



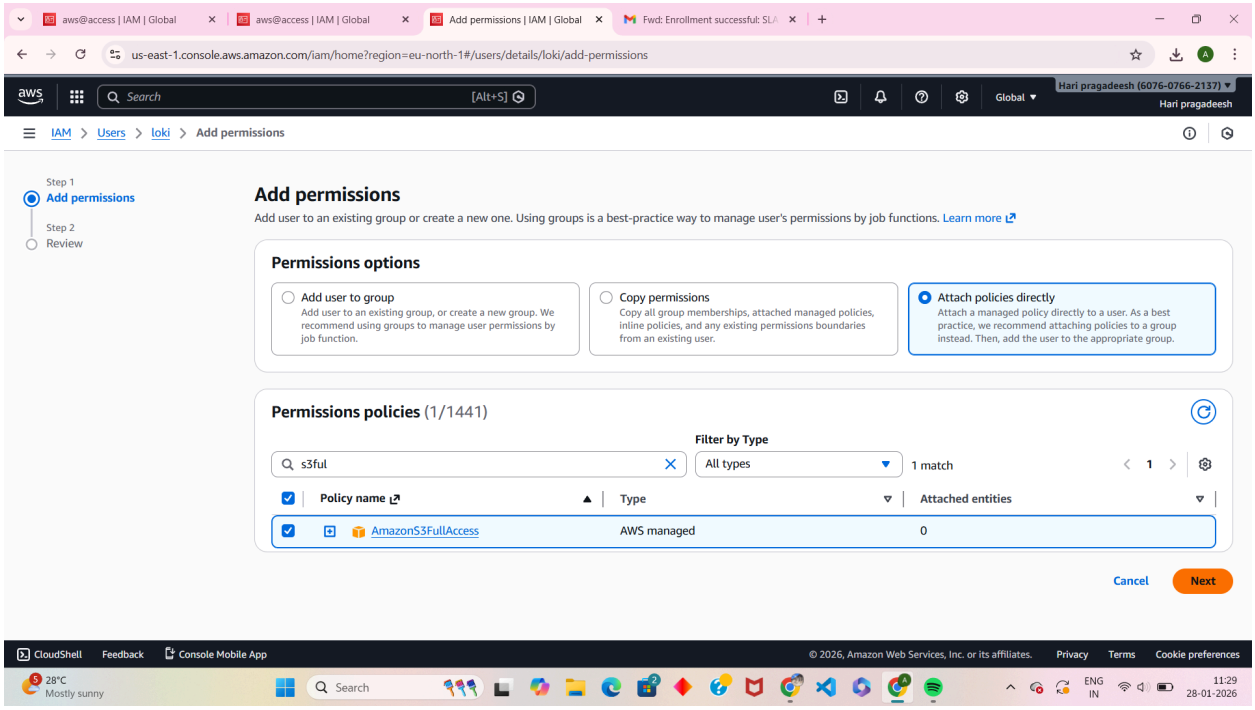
IAM user **loki** summary page

Console access enabled (without MFA)

Policies attached:

- **AmazonEC2FullAccess** (via group)
- **IAMUserChangePassword** (direct)

User now has EC2 permissions



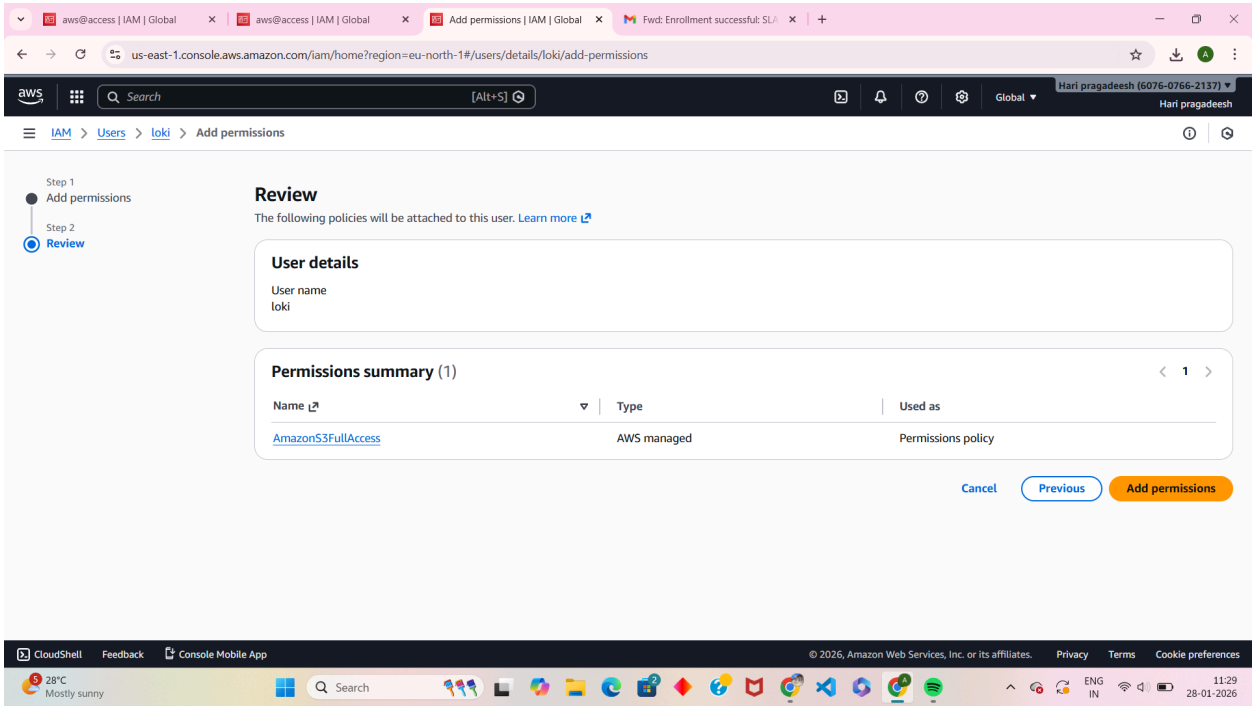
Opened IAM user **loki**

Selected **Attach policies directly**

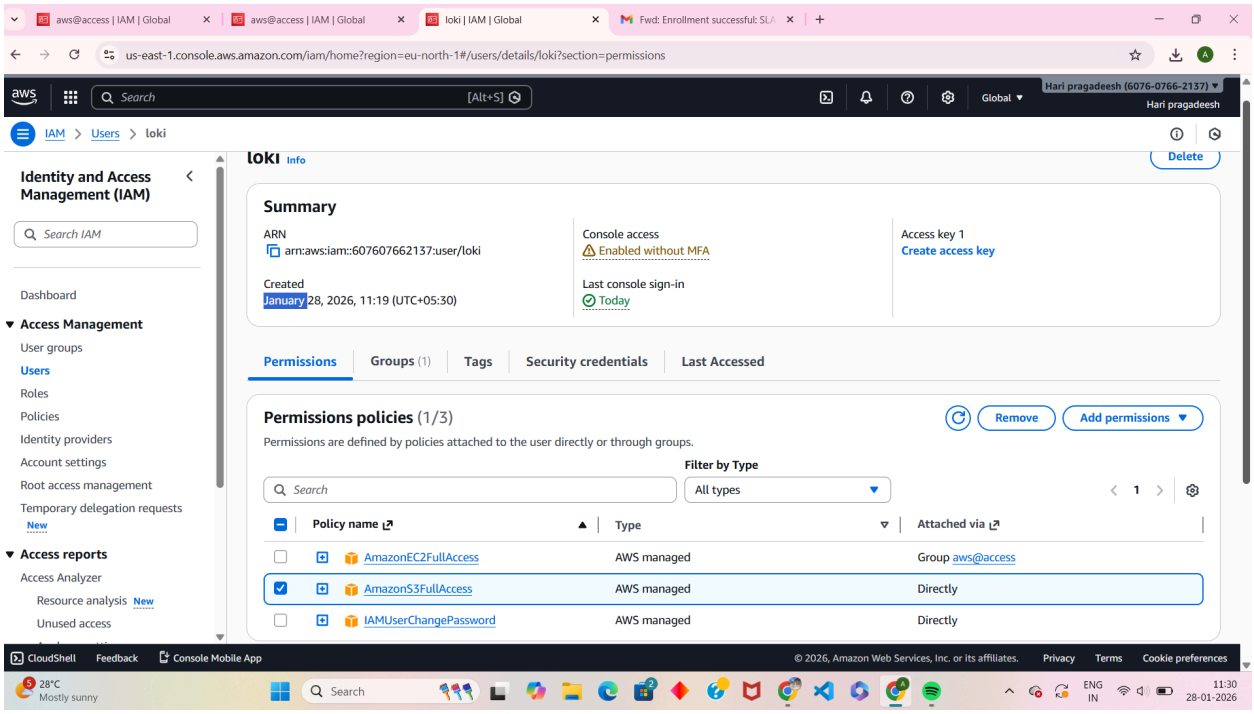
Searched for S3 policy

Selected **AmazonS3FullAccess**

Proceeded to next step



- Review page before attaching policy
- User name: **loki**
- Policy to be attached: **AmazonS3FullAccess**
- Clicked **Add permissions**

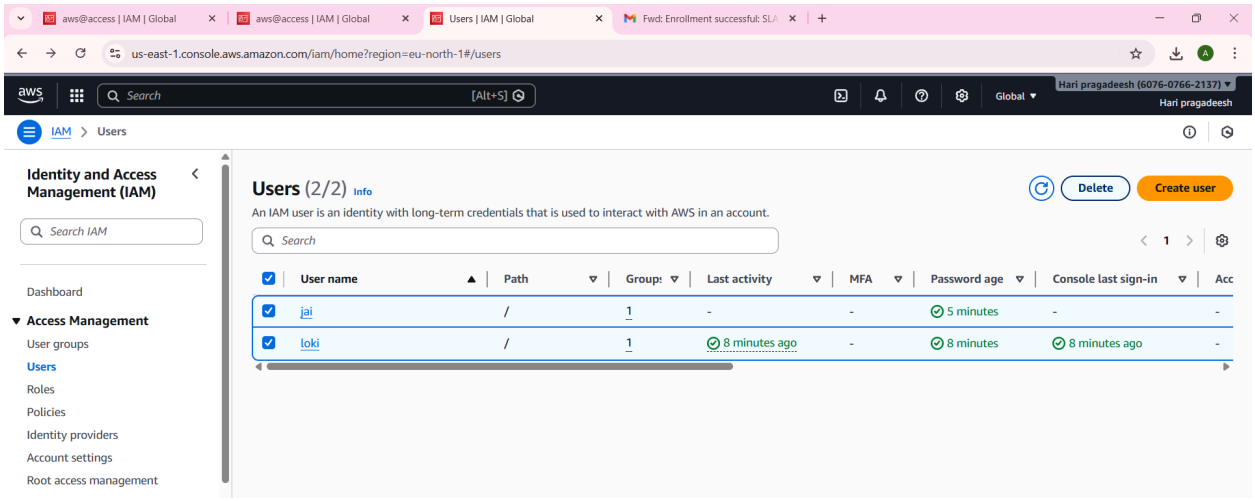


IAM user **loki** permissions page

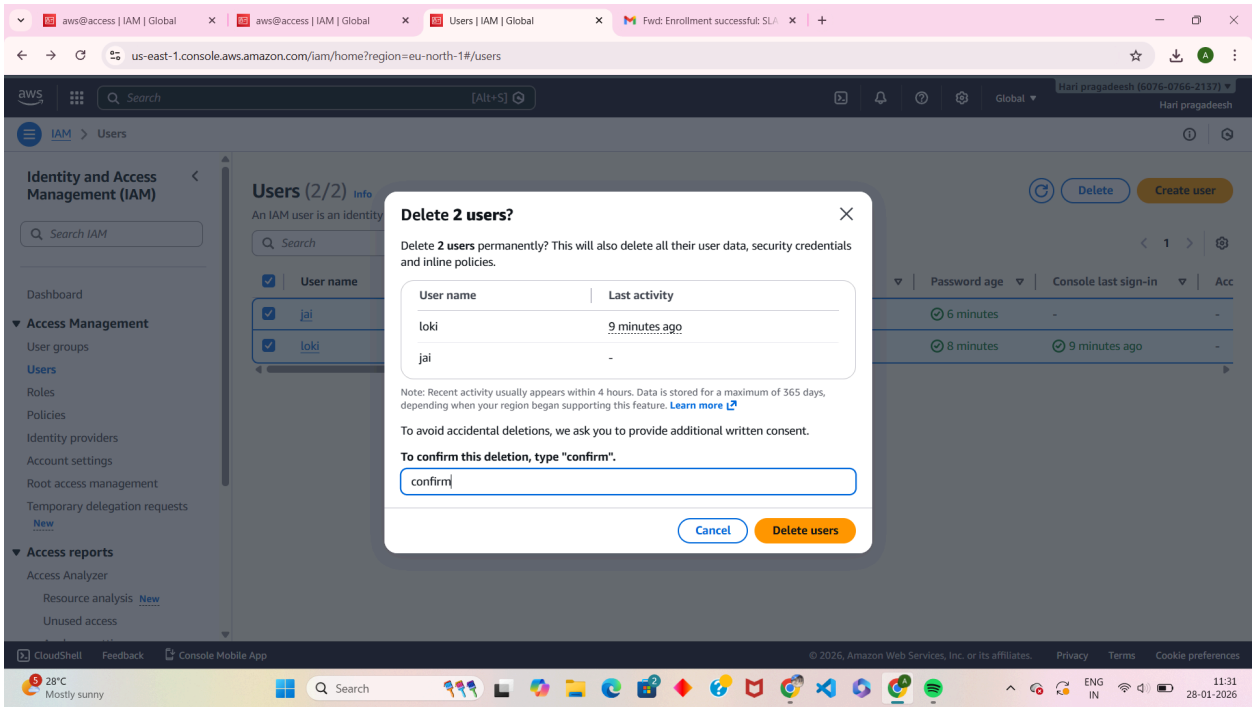
Policies attached:

- AmazonEC2FullAccess (via group)
- AmazonS3FullAccess (direct)
- IAMUserChangePassword (direct)

User now has EC2 and S3 access



- Displayed list of IAM users
- Users shown: **jai** and **loki**
- Both users belong to one group
- Shows last activity and password age

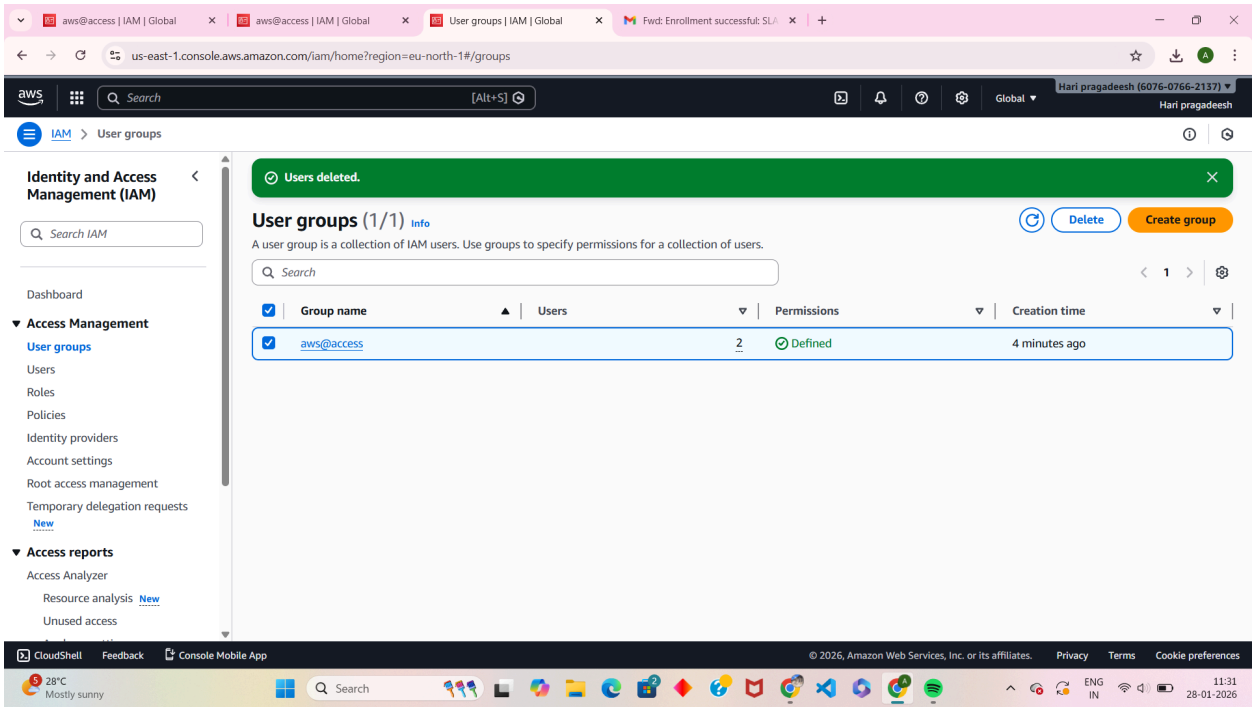


Selected users **jai** and **loki**

Delete users confirmation popup opened

Shows last activity details

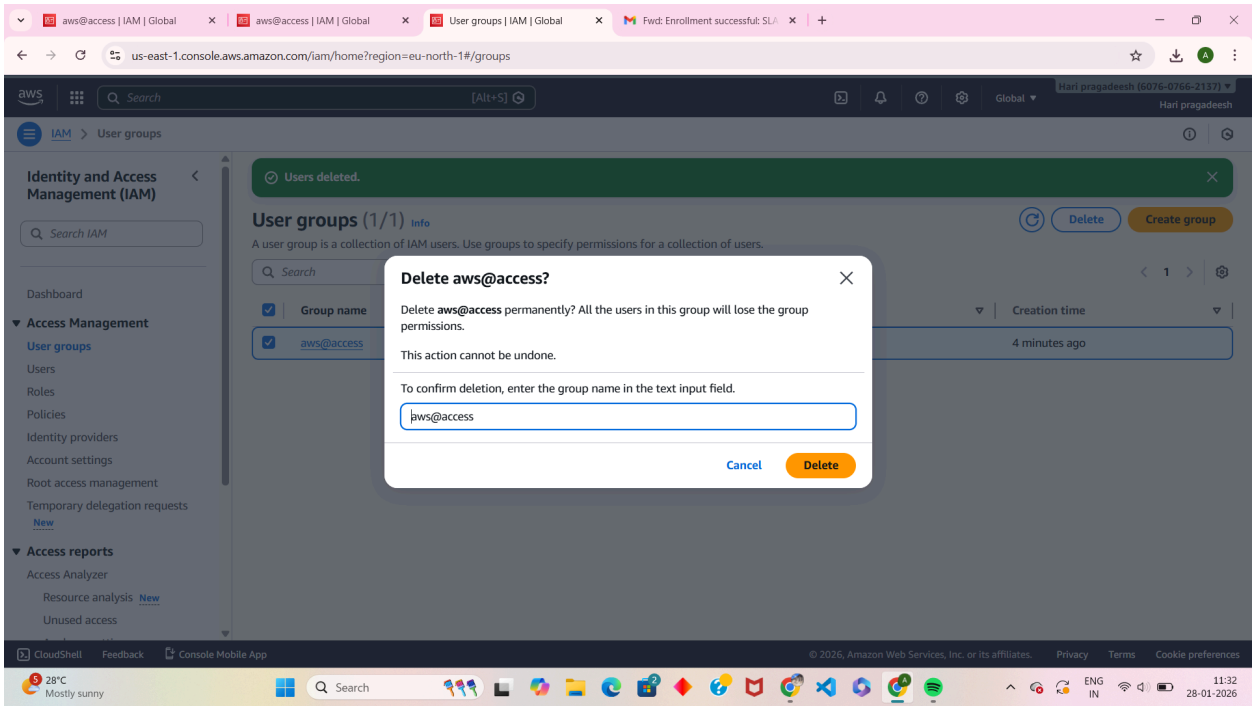
Typed **confirm** to proceed



Confirmation message: **Users deleted**

IAM Users list is now empty

Users removed permanently from account



Group name entered correctly

Ready to delete **aws@access** group

This removes all group permissions