**IAM**

It’s related to administration.

* AWS Identity and Access Management (IAM) helps securely control access to AWS resources.
* Every company has only one AWS root account which can create user accounts and assign limited privileges.

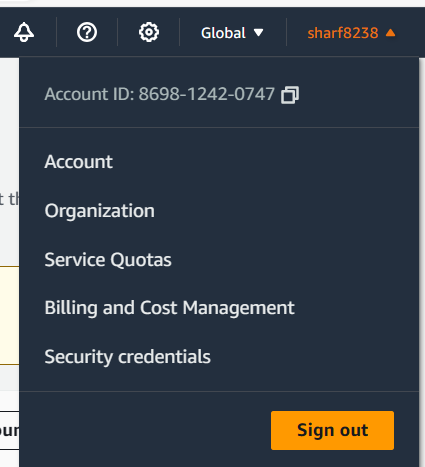
**Key Concepts:**

* **Users:** Individual users with specific access permissions.
* **Groups:** Collections of users who share the same access permissions.
* **Policies:** Define the permissions granted to users or groups.
* **Access keys:** Used to access AWS resources through the CLI or programmatic access.
* **MFA:** Multi-factor authentication for added security.

**Practical Implementation:**

Login to AWS

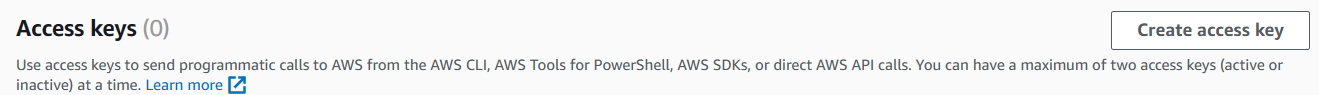
Go to IAM Services > security credentials



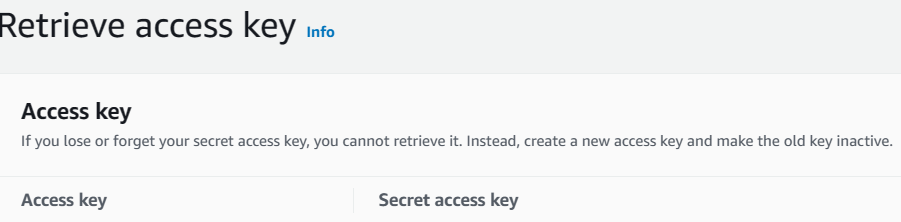
Access AWS via Graphical User Interface (GUI) or Command Line Interface (CLI).

To login to AWS using GUI, we need email address and password

To login to AWS using CLI, we need access keys.



Create access key > Continue to create access key > access key will be created.



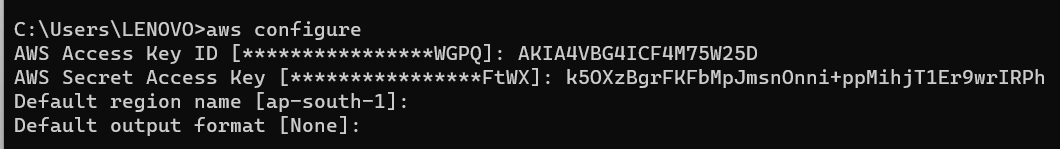
Keep it downloaded for future use.

To login to aws cli you must have installed aws cli on your laptop.

[Command Line Interface - AWS CLI - AWS (amazon.com)](https://aws.amazon.com/cli/)

If you have installed, open command prompt and enter commands

aws configure



To confirm it. You can check with aws commands

aws ec2 describe-instances

aws s3 ls

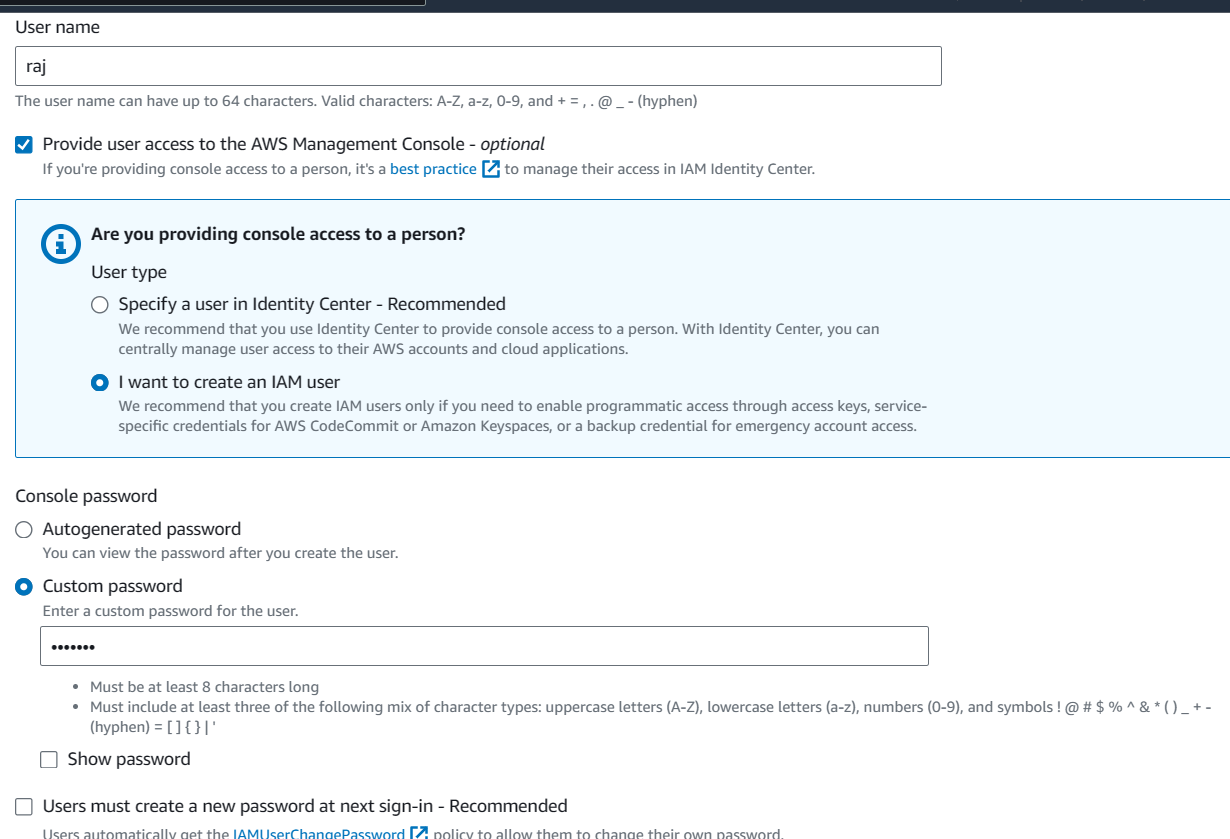
Activating MFA on the root account adds an extra layer of security.

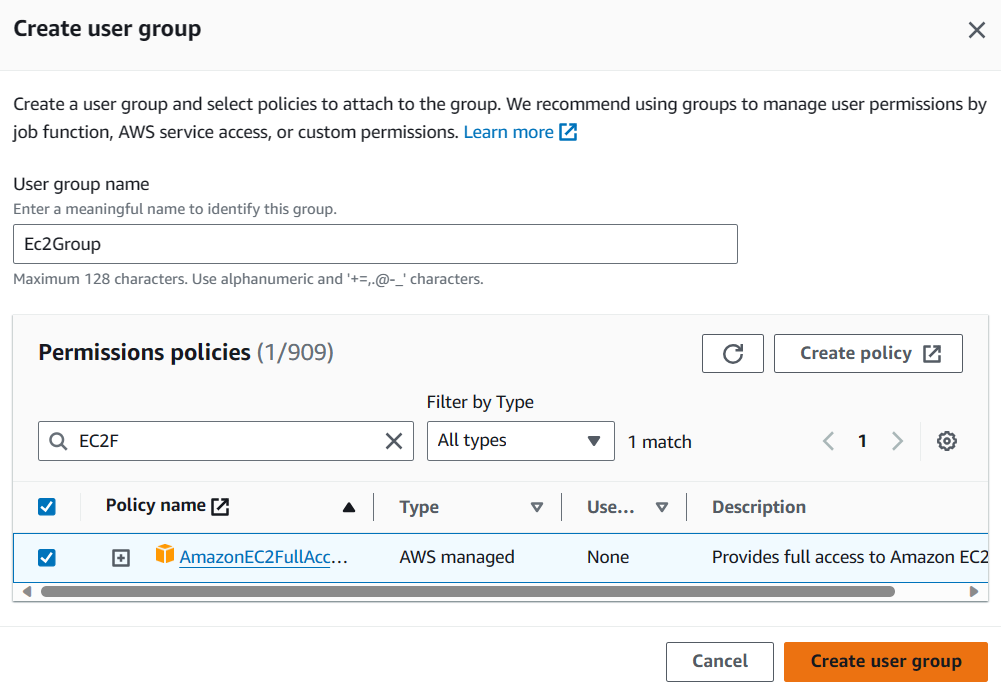
Select activate MFA on your root account > Assign MFA Device > Virtual MFA device > Show QR code.

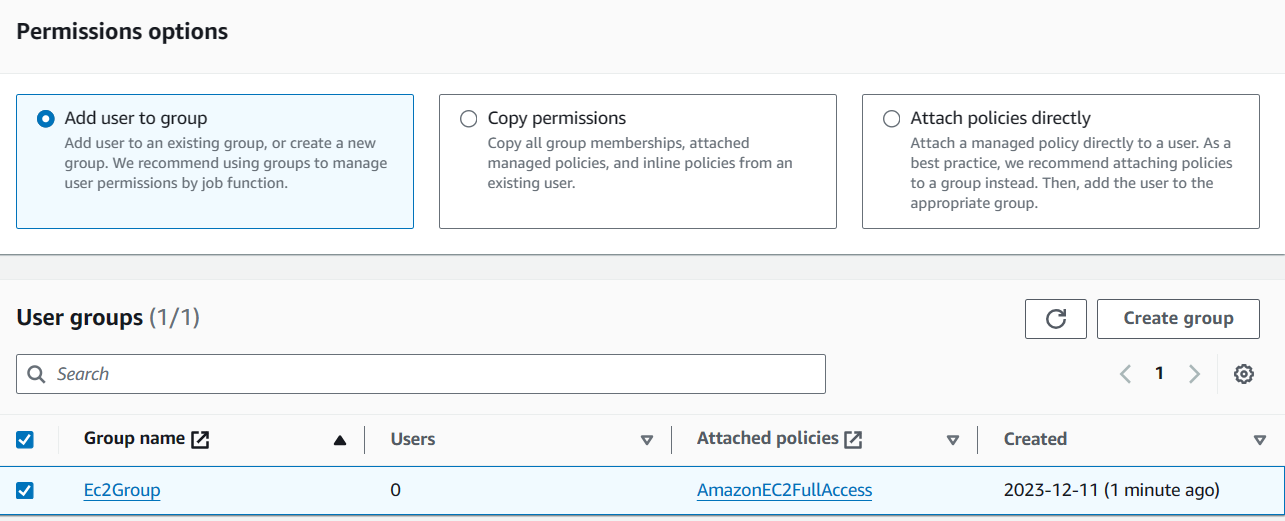
Now, scan QR code by using "Google Authenticator Mobile APP"

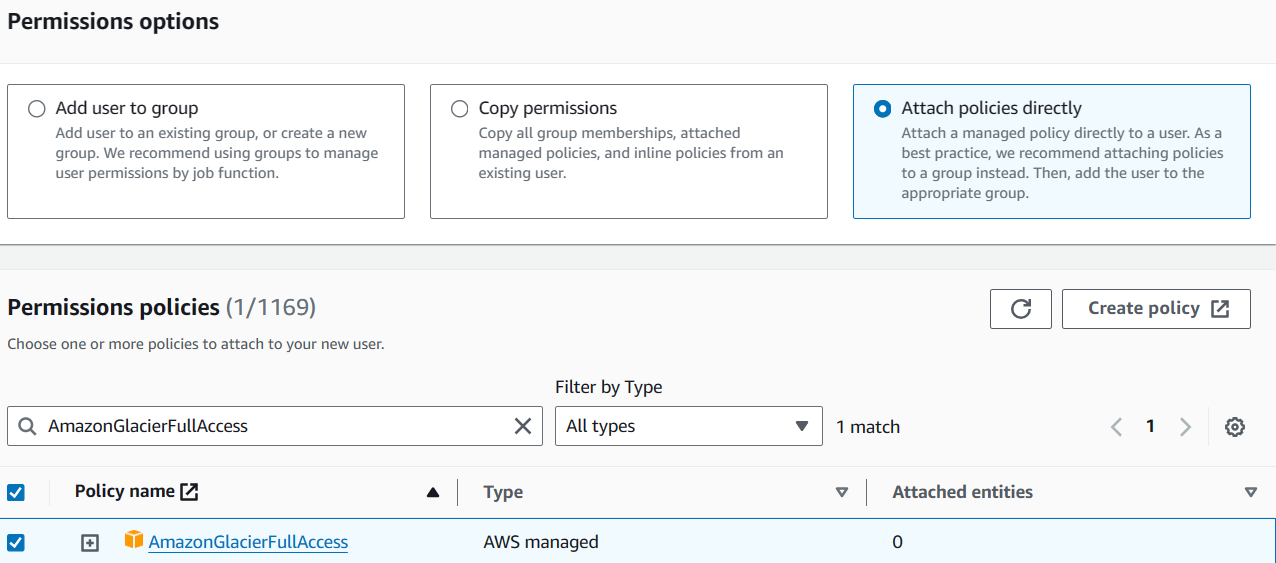
We will get MFA codes, Enter MFA codes

* **Created two users:** Raj and Hari.
* **Created two groups:** Ec2Group (full access to EC2) and S3Group (full access to S3).
* Assigned Raj to Ec2Group and Hari to S3Group.
* Attach "AmazonGlacierFullAccess" policy directly to both users.
* So, Now Hari will have two permissions (S3 full access and Glacier full access)
* If Hari is removed from the group, He will have only Glacier full access)









**Testing:**

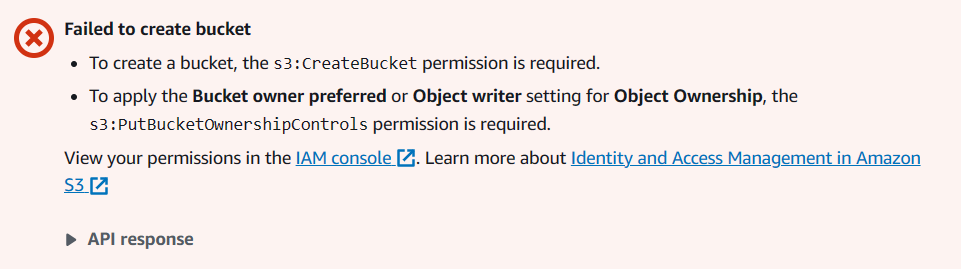
Logout and sign in with IAM user (raj)

Services > EC2

Test, can he launch instances?

Yes, we can.

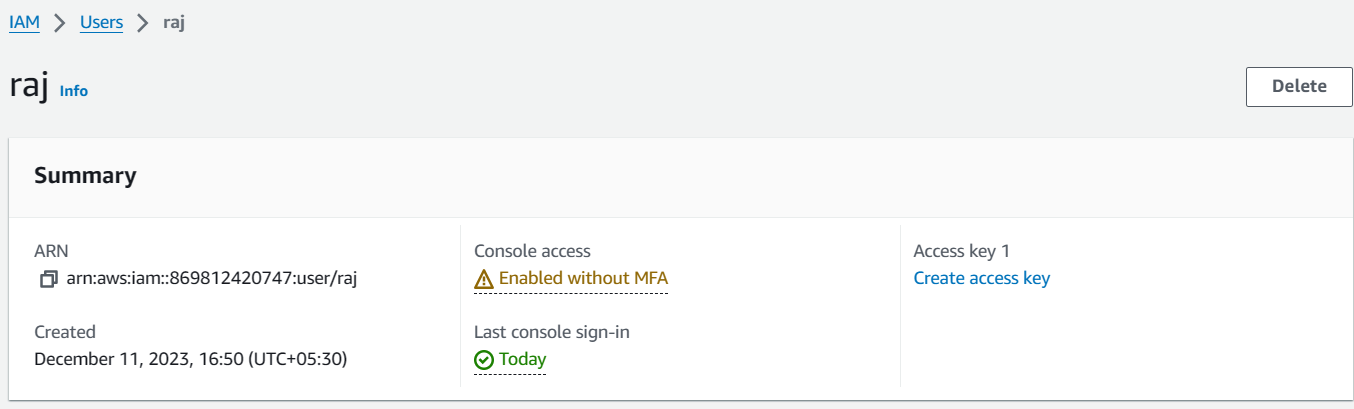
Service > S3



Error Access Denied!!!

Raj have only permission to access EC2 not S3.

To enable MFA or Create access key. Go to IAM > Users > username



Users -- Delete Users

Groups -- Delete Groups

Apply an IAM password policy ---> Manage password policy --> Delete password policy

Delete access keys