AWS KMS

What is AWS KMS?

AWS Key Management Service (KMS) is Amazon's managed service that lets you **create, store, and control encryption keys**.
These keys are used to protect your data stored on AWS services like S3, RDS, EBS, Lambda, Secrets Manager, etc.

Before KMS existed, companies had to manually create and manage encryption keys, store them securely, rotate them, set permissions, and ensure no one misused them.
This was risky and hard to audit.

KMS solves this by giving:

- secure key creation
- automatic key storage
- permissions and access control
- key rotation
- auditing via CloudTrail

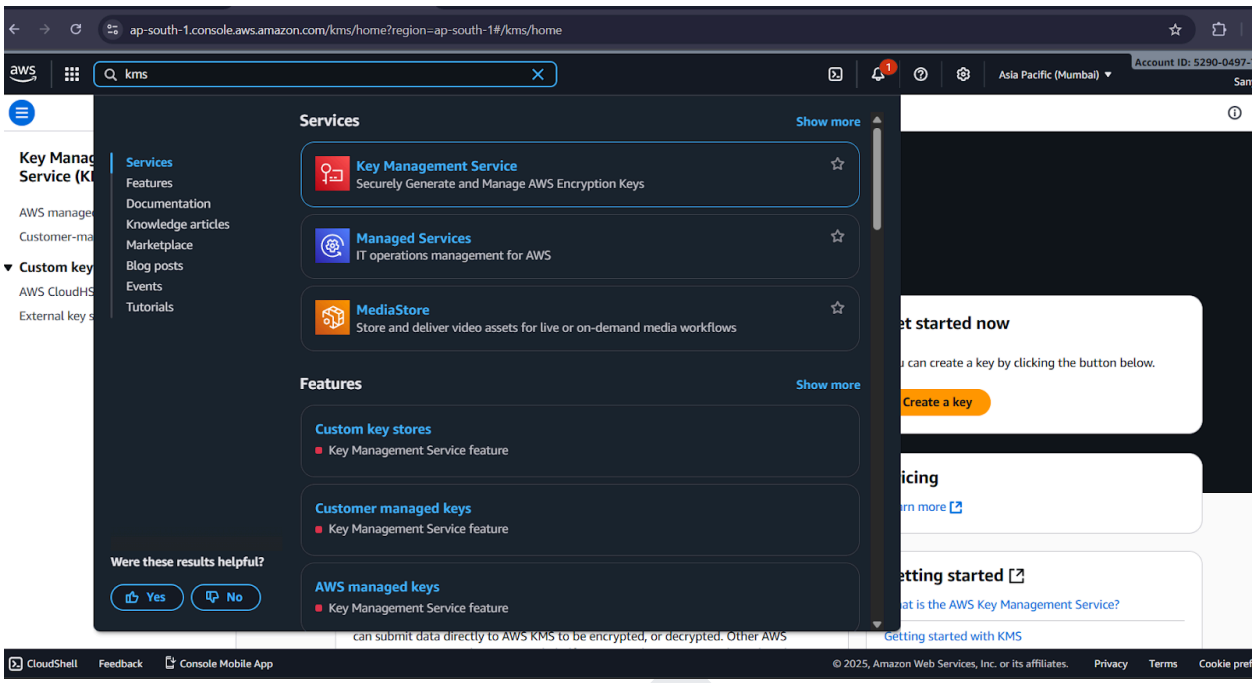
Steps-

1. Open AWS Console → Open KMS Service

You first opened the AWS Management Console and navigated to **Key Management Service (KMS)**.
This dashboard shows:

- your keys
- how they are being used
- the option to create new keys

This is where your key lifecycle starts.



2. Start “Create Key” Wizard

When you click **Create Key**, AWS asks you to choose the **type of key**.

✔ Key Type: Symmetric or Asymmetric

Symmetric Key:

- the same key is used for encryption & decryption
- used for S3, EBS, Secrets Manager, Lambda, etc.
- default option, recommended for most AWS use-cases

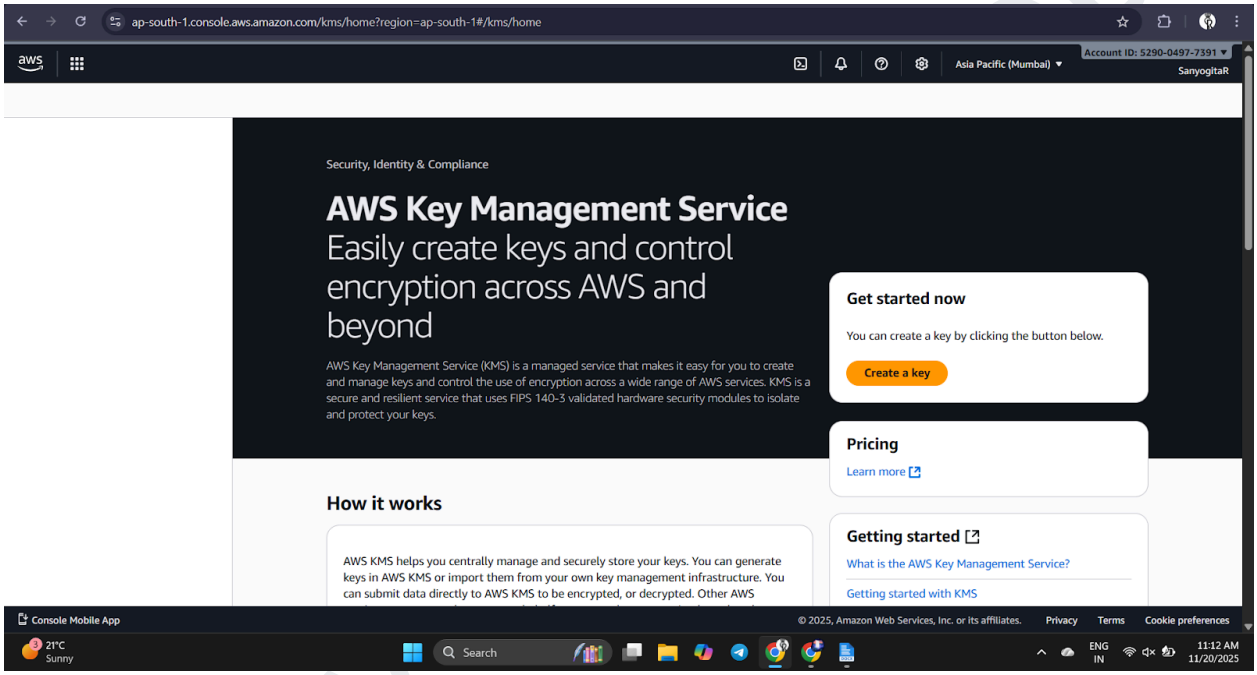
Asymmetric Key:

- has public + private key pair
- used for digital signatures, encryption between users, etc.

When to choose what?

- Choose **symmetric** when encrypting data inside AWS (most common).
- Choose **asymmetric** when building apps that need secure communication or signing documents.

You selected **Symmetric**, which is correct for beginners.



3. Choose Key Usage

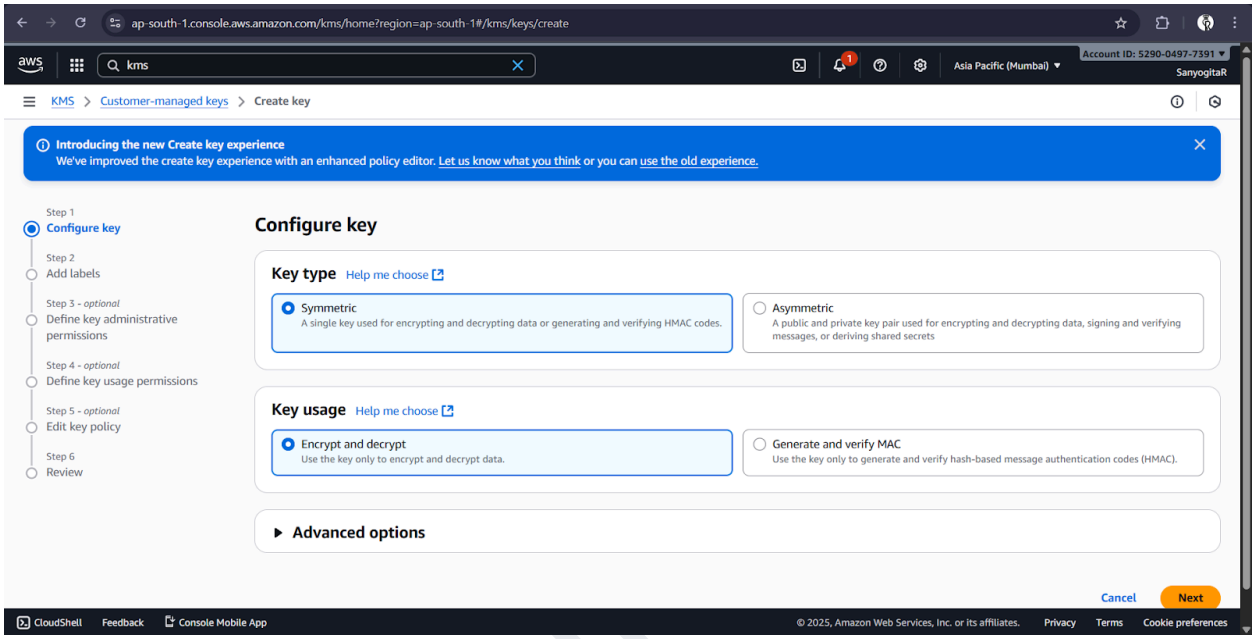
This defines what the key will be used for.

Common options:

- **Encrypt/Decrypt** → for general data protection
- **Generate Data Key** → when services need temporary keys
- **Sign/Verify** (Only for asymmetric keys)

When to choose?

- Choose **Encrypt/Decrypt** if your goal is simple encryption for AWS services.
- Choose **Generate Data Key** if designing your own encryption workflow.



4. Configure Key Details Page

Here you gave basic identification to your key.

✔ Key Alias

An easy-to-remember name like `my-project-key`
Used so you don't need to remember complicated Key IDs.

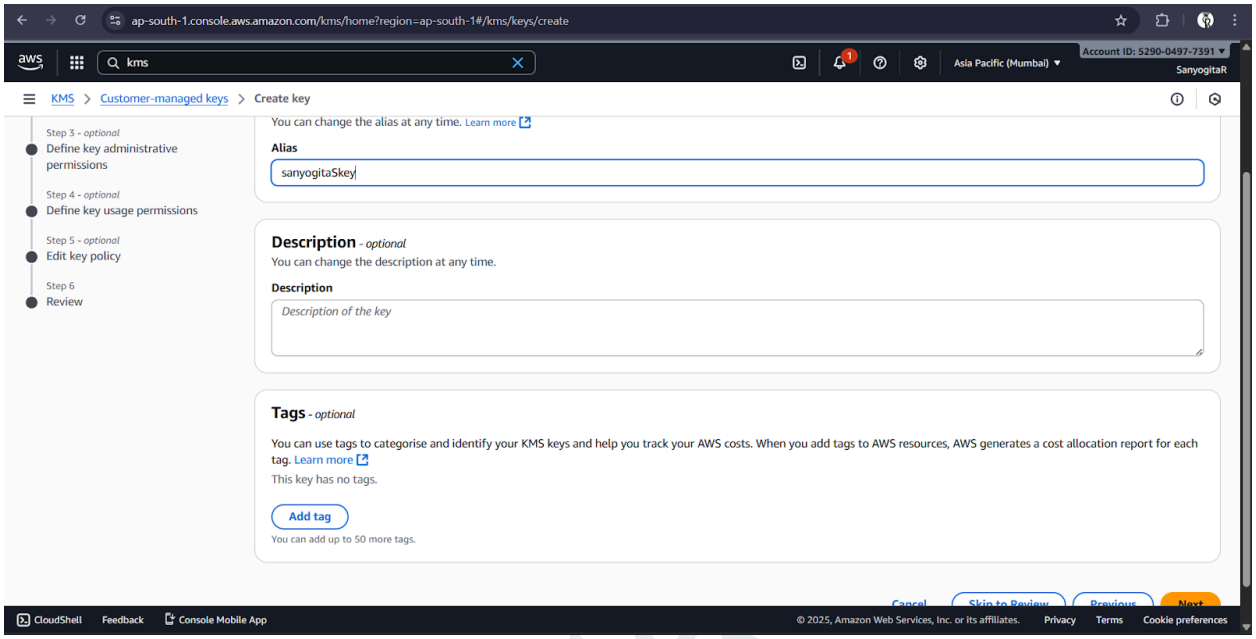
✔ Description

Explains what the key is for, example:
"Key for encrypting S3 files for experiment."

✔ Tags (Optional)

Tags help identify billing or project usage.
Use them when you want cost tracking, e.g.,

```
Project = AWS-Learning
```



5. Define Key Administrative Permissions

This is where you decide **who can manage the key**.

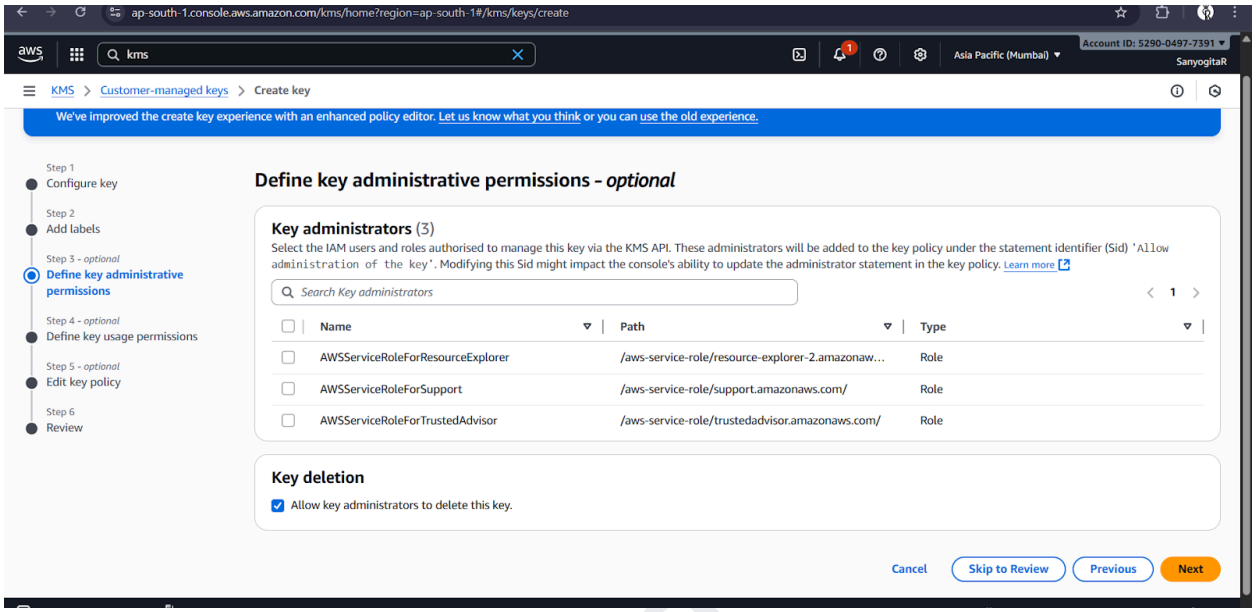
Admins can:

- enable/disable the key
- rotate it
- change permissions
- delete the key

This does NOT give them permission to encrypt data.
It only gives administrative control.

When to choose?

- Give yourself (your IAM user) admin privileges.
- In real companies, separate “admin users” from “data users” for higher security.



6. Define Key Usage Permissions

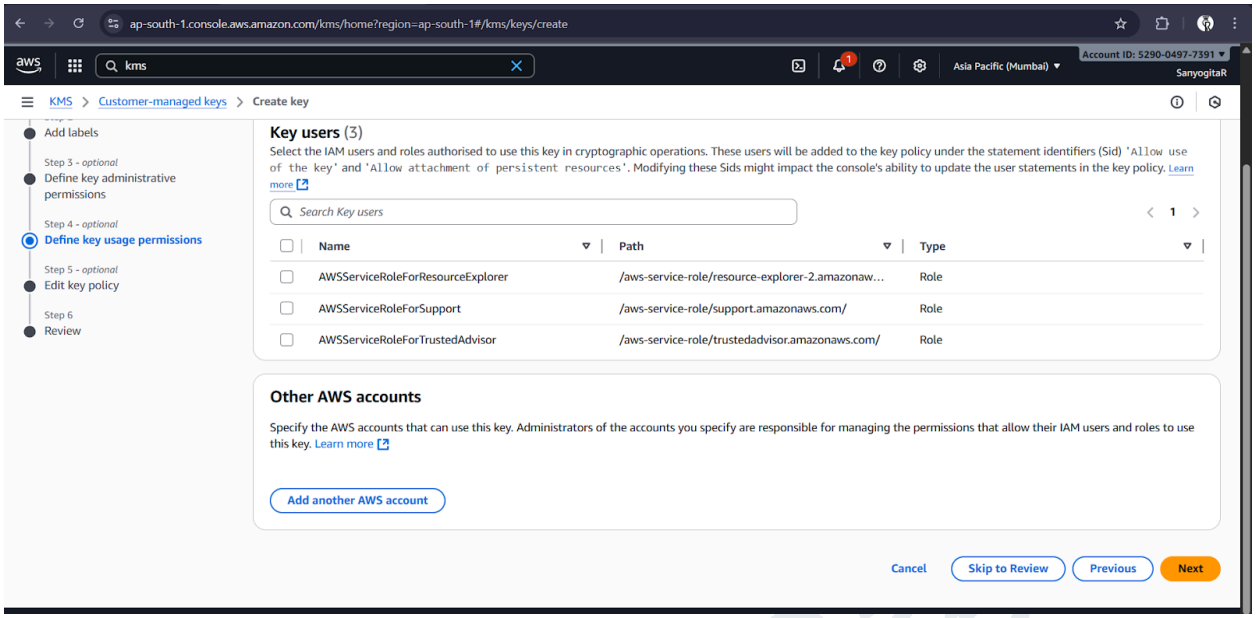
Now AWS asks:
Who is allowed to use this key to encrypt/decrypt data?

This is important because the wrong user can misuse the key and view encrypted information.

When to enable?

- Give your own IAM user access if you want to test encrypt/decrypt.
- Give a service role access if the key will be used by S3, Lambda, RDS, etc.

For your experiment, you probably selected **your IAM user or role**.



7. Edit Key Policy (Advanced Option)

The **Key Policy** is the real power of KMS.
Even if IAM users have permission, the key policy decides if they are actually allowed.

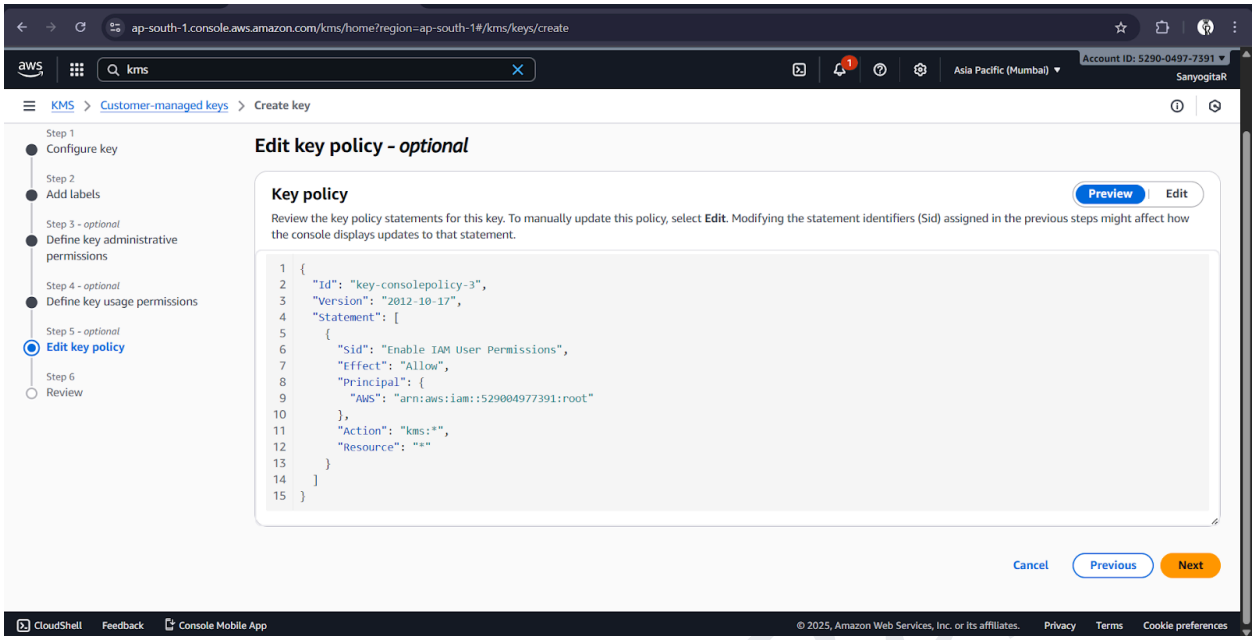
You reviewed the JSON policy that includes:

- key administrators
- key users
- AWS service access

Most beginners keep the “default policy,” which is safe.

When to edit manually?

- When integrating with external applications
- When giving access to other AWS accounts
- When limiting permissions with zero-trust approach



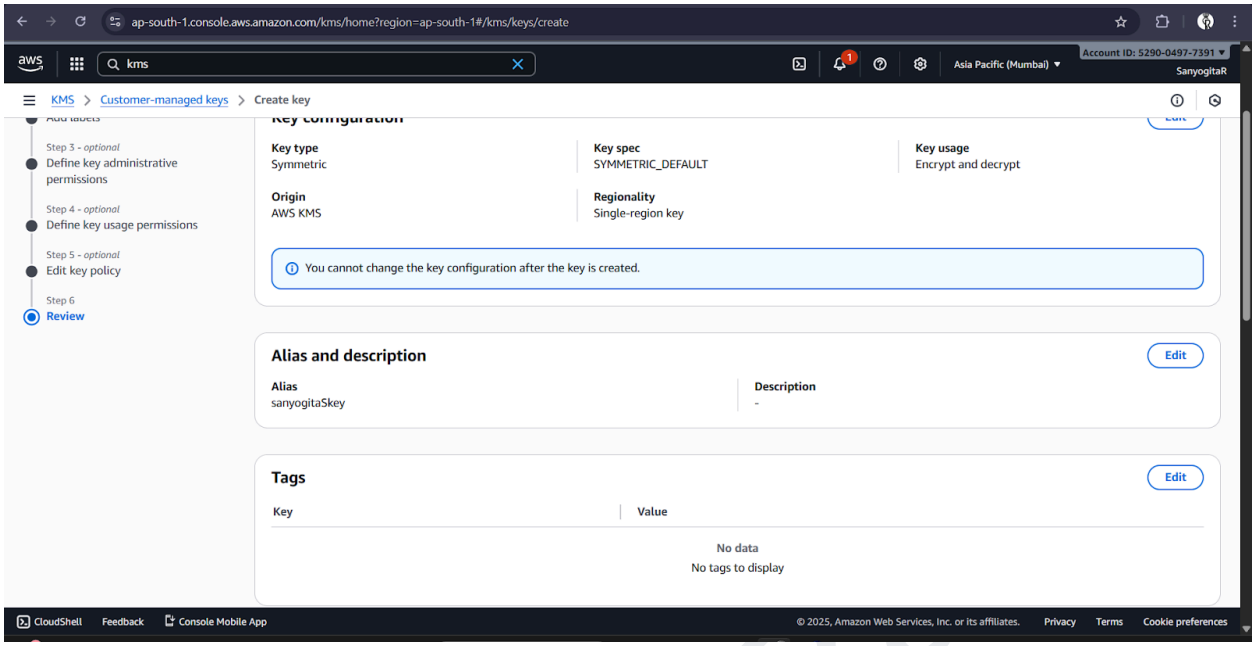
8. Review and Create

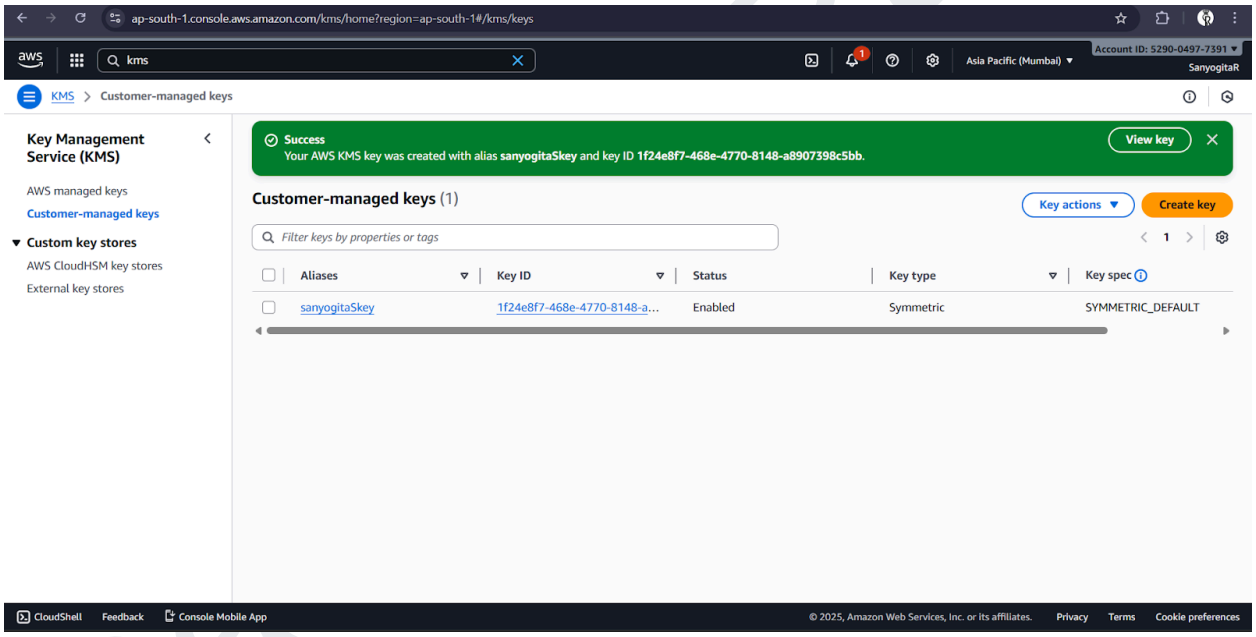
The final review page shows all:

- key type
- key permissions
- policy
- admin users
- usage users

If everything looks correct, click **Create Key**.

And your **Customer Managed Key (CMK)** is ready.





Important: How to Delete the Key Without Costing Anything

KMS keys **are free to create**, but **AWS charges for every request** made using the key.

To delete a key properly:

✔ Step 1: Disable the Key

Open your key → choose **Disable Key**
This stops any cost-producing usage by accident.

✔ Step 2: Schedule Key Deletion

KMS does not allow instant deletion for safety.
You must schedule deletion for **7–30 days**.
Choose **7 days** (minimum).

✔ Step 3: Confirm

Make sure:

- no S3 bucket or service is using the key
- otherwise the service might fail to decrypt files

Once the waiting period ends → the key is permanently deleted → *no more charges*.