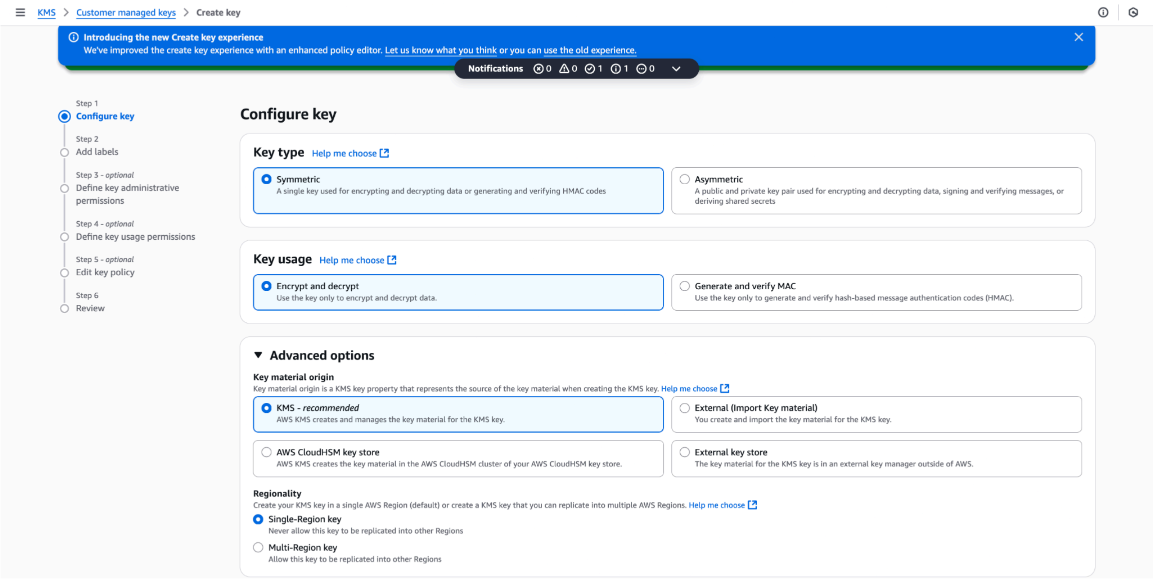
🛠 Steps to Create a Customer Managed KMS Key

1. Create a Symmetric Key

1. Go to **AWS KMS → Customer Managed Keys**.
2. Select **Create Key → Symmetric**.
3. Keep defaults → proceed.



KMS > Customer managed keys > Create key

Introducing the new Create key experience
We've improved the create key experience with an enhanced policy editor. Let us know what you think or you can use the old experience.

Notifications ⊗0 ⚠0 ✓1 ⓘ1 ⊖0

Step 1
● Configure key

Step 2
○ Add labels

Step 3 - *optional*
○ Define key administrative permissions

Step 4 - *optional*
○ Define key usage permissions

Step 5 - *optional*
○ Edit key policy

Step 6
○ Review

Configure key

Key type Help me choose

● Symmetric
A single key used for encrypting and decrypting data or generating and verifying HMAC codes

○ Asymmetric
A public and private key pair used for encrypting and decrypting data, signing and verifying messages, or deriving shared secrets

Key usage Help me choose

● Encrypt and decrypt
Use the key only to encrypt and decrypt data.

○ Generate and verify MAC
Use the key only to generate and verify hash-based message authentication codes (HMAC).

▼ **Advanced options**

Key material origin
Key material origin is a KMS key property that represents the source of the key material when creating the KMS key. Help me choose

● KMS - *recommended*
AWS KMS creates and manages the key material for the KMS key.

○ External (Import Key material)
You create and import the key material for the KMS key.

○ AWS CloudHSM key store
AWS KMS creates the key material in the AWS CloudHSM cluster of your AWS CloudHSM key store.

○ External key store
The key material for the KMS key is in an external key manager outside of AWS.

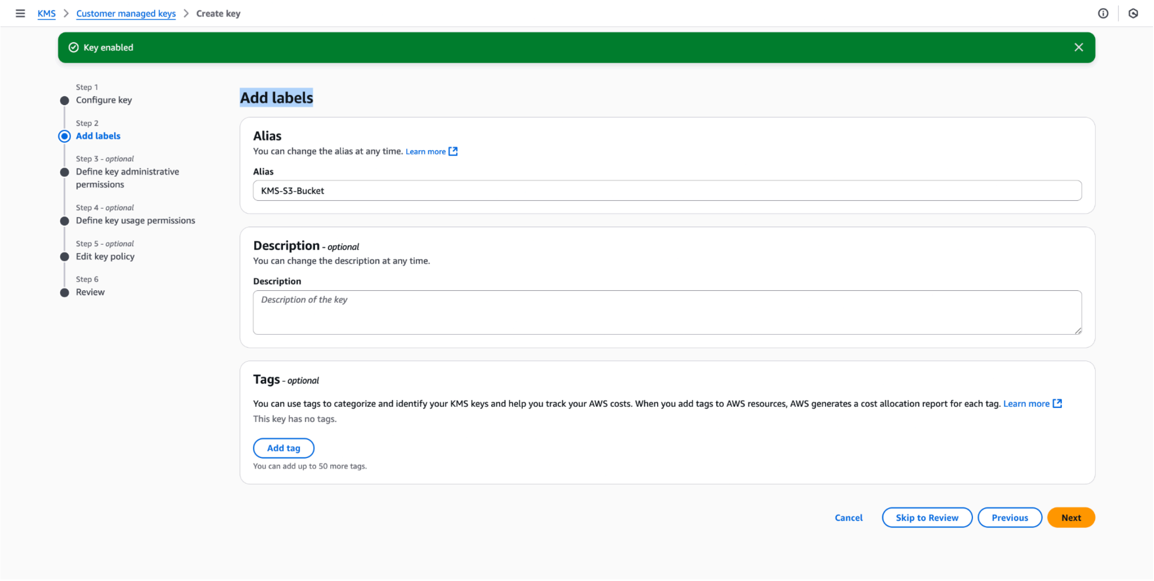
Regionality
Create your KMS key in a single AWS Region (default) or create a KMS key that you can replicate into multiple AWS Regions. Help me choose

● Single-Region key
Never allow this key to be replicated into other Regions

○ Multi-Region key
Allow this key to be replicated into other Regions

2. Add Labels

- Assign an **alias** (friendly name).
- Optionally add **tags**.
- Leave defaults and continue.



KMS > Customer managed keys > Create key

Key enabled

Step 1
● Configure key

Step 2
● Add labels

Step 3 - *optional*
● Define key administrative permissions

Step 4 - *optional*
● Define key usage permissions

Step 5 - *optional*
● Edit key policy

Step 6
● Review

Add labels

Alias
You can change the alias at any time. Learn more

Alias
KMS-S3-Bucket

Description - *optional*
You can change the description at any time.

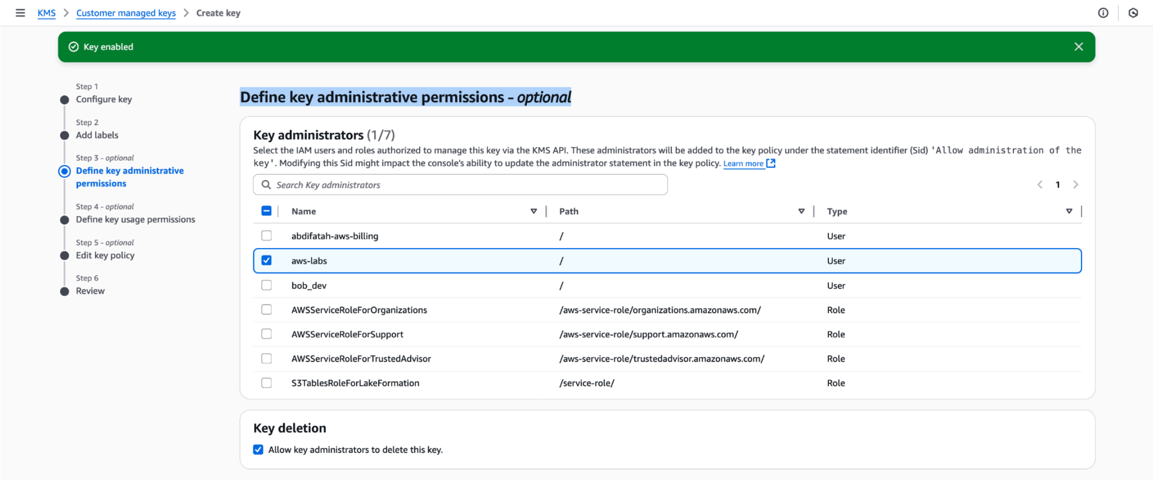
Description
Description of the key

Tags - *optional*
You can use tags to categorize and identify your KMS keys and help you track your AWS costs. When you add tags to AWS resources, AWS generates a cost allocation report for each tag. Learn more
This key has no tags.

Add tag
You can add up to 50 more tags.

3. Define Administrative Permissions *(Optional)*

- Choose IAM **users/roles** who can manage the key.
- Optionally allow administrators to **delete the key**.



KMS > Customer managed keys > Create key

Key enabled

Step 1
Configure key

Step 2
Add labels

Step 3 - *optional*
Define key administrative permissions

Step 4 - *optional*
Define key usage permissions

Step 5 - *optional*
Edit key policy

Step 6
Review

Define key administrative permissions - *optional*

Key administrators (1/7)

Select the IAM users and roles authorized to manage this key via the KMS API. These administrators will be added to the key policy under the statement identifier (Sid) `'Allow administration of the key'`. Modifying this Sid might impact the console's ability to update the administrator statement in the key policy. Learn more

Search Key administrators

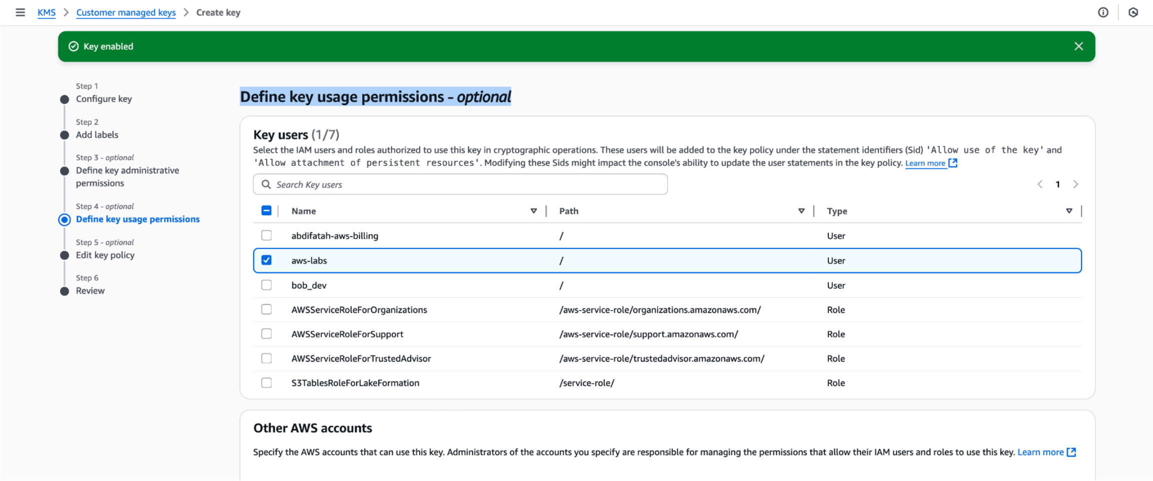
	Name	Path	Type
□	abdifatah-aws-billing	/	User
☑	aws-labs	/	User
□	bob_dev	/	User
□	AWSServiceRoleForOrganizations	/aws-service-role/organizations.amazonaws.com/	Role
□	AWSServiceRoleForSupport	/aws-service-role/support.amazonaws.com/	Role
□	AWSServiceRoleForTrustedAdvisor	/aws-service-role/trustedadvisor.amazonaws.com/	Role
□	S3TablesRoleForLakeFormation	/service-role/	Role

Key deletion

☑ Allow key administrators to delete this key.

4. Define Usage Permissions *(Optional)*

- Assign IAM **users/roles** who can use the key for encryption. Example 9 (was-labs)
- Continue with defaults → review → finish.



KMS > Customer managed keys > Create key

Key enabled

Step 1
Configure key

Step 2
Add labels

Step 3 - *optional*
Define key administrative permissions

Step 4 - *optional*
Define key usage permissions

Step 5 - *optional*
Edit key policy

Step 6
Review

Define key usage permissions - *optional*

Key users (1/7)

Select the IAM users and roles authorized to use this key in cryptographic operations. These users will be added to the key policy under the statement identifiers (Sid) `'Allow use of the key'` and `'Allow attachment of persistent resources'`. Modifying these Sids might impact the console's ability to update the user statements in the key policy. Learn more

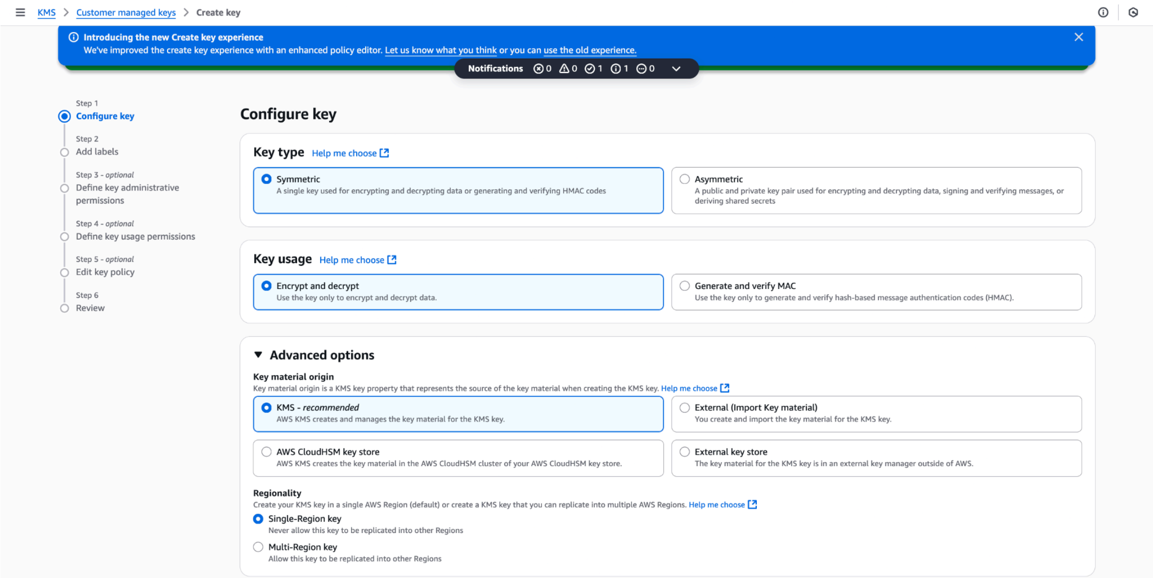
Search Key users

	Name	Path	Type
□	abdifatah-aws-billing	/	User
☑	aws-labs	/	User
□	bob_dev	/	User
□	AWSServiceRoleForOrganizations	/aws-service-role/organizations.amazonaws.com/	Role
□	AWSServiceRoleForSupport	/aws-service-role/support.amazonaws.com/	Role
□	AWSServiceRoleForTrustedAdvisor	/aws-service-role/trustedadvisor.amazonaws.com/	Role
□	S3TablesRoleForLakeFormation	/service-role/	Role

Other AWS accounts

Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. Learn more

“Next, we will create a second KMS key, which will be different from the first Symmetric key. Below are the step-by-step instructions to create it.”



KMS > Customer managed keys > Create key

Introducing the new Create key experience
We've improved the create key experience with an enhanced policy editor. Let us know what you think or you can use the old experience.

Notifications ⊗0 ⚠0 ✓1 ⓘ1 ⊖0

Step 1
● Configure key

Step 2
○ Add labels

Step 3 - *optional*
○ Define key administrative permissions

Step 4 - *optional*
○ Define key usage permissions

Step 5 - *optional*
○ Edit key policy

Step 6
○ Review

Configure key

Key type Help me choose

● Symmetric
A single key used for encrypting and decrypting data or generating and verifying HMAC codes

○ Asymmetric
A public and private key pair used for encrypting and decrypting data, signing and verifying messages, or deriving shared secrets

Key usage Help me choose

● Encrypt and decrypt
Use the key only to encrypt and decrypt data.

○ Generate and verify MAC
Use the key only to generate and verify hash-based message authentication codes (HMAC).

▼ Advanced options

Key material origin
Key material origin is a KMS key property that represents the source of the key material when creating the KMS key. Help me choose

● KMS - *recommended*
AWS KMS creates and manages the key material for the KMS key.

○ External (Import Key material)
You create and import the key material for the KMS key.

○ AWS CloudHSM key store
AWS KMS creates the key material in the AWS CloudHSM cluster of your AWS CloudHSM key store.

○ External key store
The key material for the KMS key is in an external key manager outside of AWS.

Regionality
Create your KMS key in a single AWS Region (default) or create a KMS key that you can replicate into multiple AWS Regions. Help me choose

● Single-Region key
Never allow this key to be replicated into other Regions

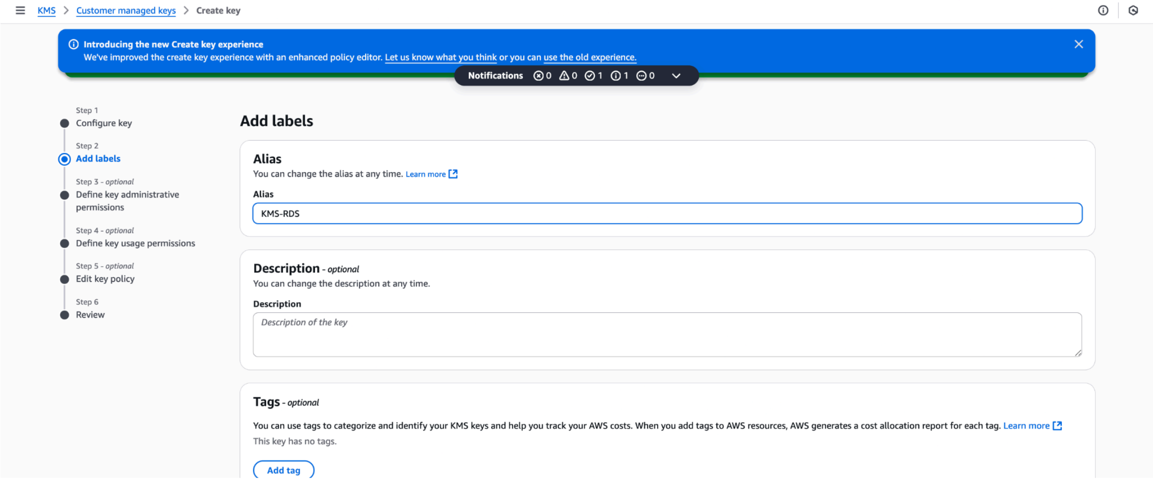
○ Multi-Region key
Allow this key to be replicated into other Regions

Add Labels:

- Assign an **alias** (e.g., KMS-RDS) to identify the key.
- Leave the remaining options at their default values.
- Optionally, add **tags** for better organization before moving on to the *Define Key* step.

Define Key Administrative Permissions (Optional):

- Keep the default settings (do not select any users or roles).
- Continue to the next step until you reach the **Key Policy Editor**.
- Once there, click **Edit** and add the custom policy provided.



KMS > Customer managed keys > Create key

Introducing the new Create key experience
We've improved the create key experience with an enhanced policy editor. Let us know what you think or you can use the old experience.

Notifications ⊗0 ⚠0 ✓1 ⓘ1 ⊖0

Step 1
● Configure key

Step 2
● Add labels

Step 3 - *optional*
● Define key administrative permissions

Step 4 - *optional*
● Define key usage permissions

Step 5 - *optional*
● Edit key policy

Step 6
● Review

Add labels

Alias
You can change the alias at any time. Learn more

Alias
KMS-RDS

Description - *optional*
You can change the description at any time.

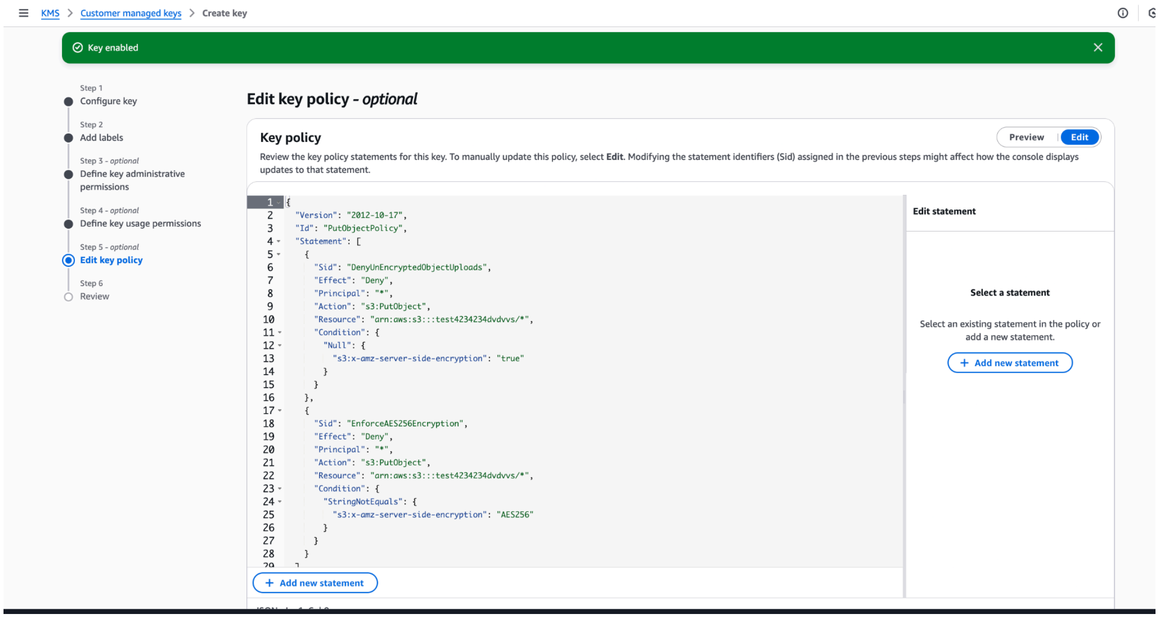
Description
Description of the key

Tags - *optional*
You can use tags to categorize and identify your KMS keys and help you track your AWS costs. When you add tags to AWS resources, AWS generates a cost allocation report for each tag. Learn more
This key has no tags.

Add tag

Edit Key Policy (Optional):

- In this step, you can customize the key policy.
- Click **Edit** to modify the default policy and add your required statements.



KMS > Customer managed keys > Create key

Key enabled

Step 1
Configure key

Step 2
Add labels

Step 3 - *optional*
Define key administrative permissions

Step 4 - *optional*
Define key usage permissions

Step 5 - *optional*
Edit key policy

Step 6
Review

Edit key policy - *optional*

Key policy

Preview | Edit

Review the key policy statements for this key. To manually update this policy, select **Edit**. Modifying the statement identifiers (Sid) assigned in the previous steps might affect how the console displays updates to that statement.

```
{
  "Version": "2012-10-17",
  "Id": "PutObjectPolicy",
  "Statement": [
    {
      "Sid": "DenyUnEncryptedObjectUploads",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::test4234234dvdvvs/*",
      "Condition": {
        "Null": {
          "s3:x-amz-server-side-encryption": "true"
        }
      }
    },
    {
      "Sid": "EnforceAES256Encryption",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::test4234234dvdvvs/*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption": "AES256"
        }
      }
    }
```

+ Add new statement

Edit statement

Select a statement

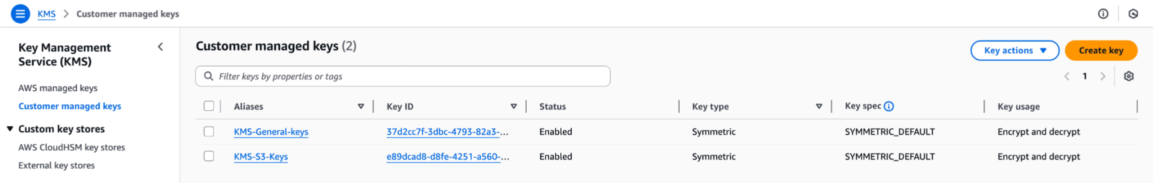
Select an existing statement in the policy or add a new statement.

+ Add new statement

"Edit Policy:"

```
{
 "Version": "2012-10-17",
 "Id": "PutObjectPolicy",
 "Statement": [
  {
   "Sid": "DenyUnEncryptedObjectUploads",
   "Effect": "Deny",
   "Principal": "*",
   "Action": "s3:PutObject",
   "Resource": "arn:aws:s3:::test4234234dvdvvs/*",
   "Condition": {
    "Null": {
     "s3:x-amz-server-side-encryption": "true"
    }
   }
  },
  {
   "Sid": "EnforceAES256Encryption",
   "Effect": "Deny",
   "Principal": "*",
   "Action": "s3:PutObject",
   "Resource": "arn:aws:s3:::test4234234dvdvvs/*",
   "Condition": {
    "StringNotEquals": {
     "s3:x-amz-server-side-encryption": "AES256"
    }
   }
  }
 ]
}
```

Customer managed keys for both Encrypt and Decrypt



Customer managed keys (2)

□	Aliases	Key ID	Status	Key type	Key spec	Key usage
□	KMS-General-keys	37d2cc7f-3dbc-4793-82a3-…	Enabled	Symmetric	SYMMETRIC_DEFAULT	Encrypt and decrypt
□	KMS-S3-Keys	e89dcad8-d8fe-4251-a560-…	Enabled	Symmetric	SYMMETRIC_DEFAULT	Encrypt and decrypt