# Lesson 04 Demo 08

# Creating and Deleting Keys with Amazon KMS

**Objectives:** To create and delete customer-managed keys using Amazon KMS and control access to your encrypted data

**Tools required:** None

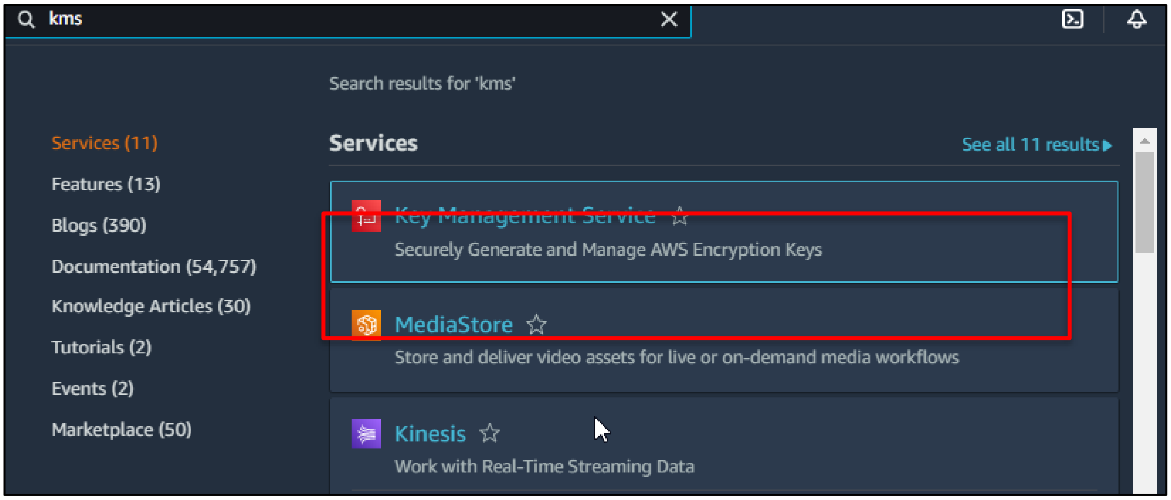
**Prerequisites:** AWS account with an S3 bucket created

Steps to be followed:

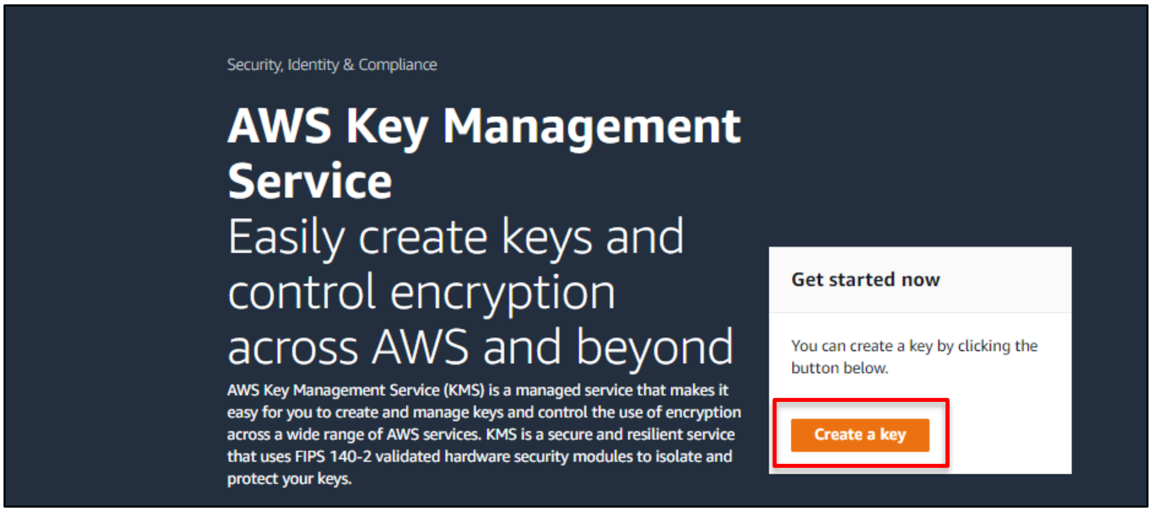
1. Create a customer-managed key
2. Delete a customer-managed key

## Step 1: Create a customer-managed key

1.1 Access the AWS Management Console homepage, search for **Key Management Service**, and select it



1.2 Click on **Create a key**



Security, Identity & Compliance

**AWS Key Management Service**

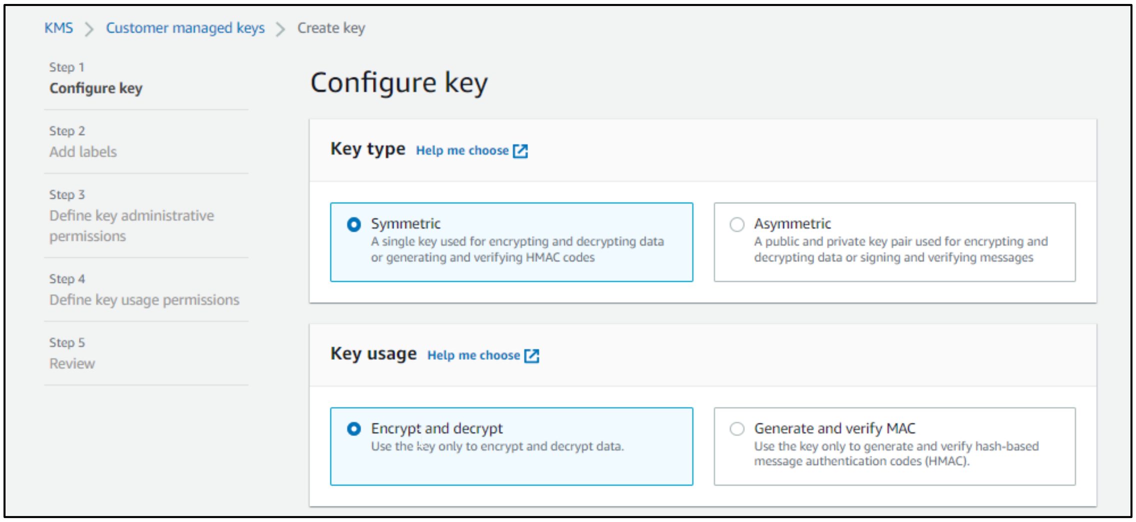
Easily create keys and control encryption across AWS and beyond

AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and manage keys and control the use of encryption across a wide range of AWS services. KMS is a secure and resilient service that uses FIPS 140-2 validated hardware security modules to isolate and protect your keys.

**Get started now**

You can create a key by clicking the button below.

1.3 Configure the key using default settings and proceed to the next step



KMS > Customer managed keys > Create key
Step 1
Configure key
Step 2
Add labels
Step 3
Define key administrative permissions
Step 4
Define key usage permissions
Step 5
Review

Configure key

**Key type** Help me choose

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

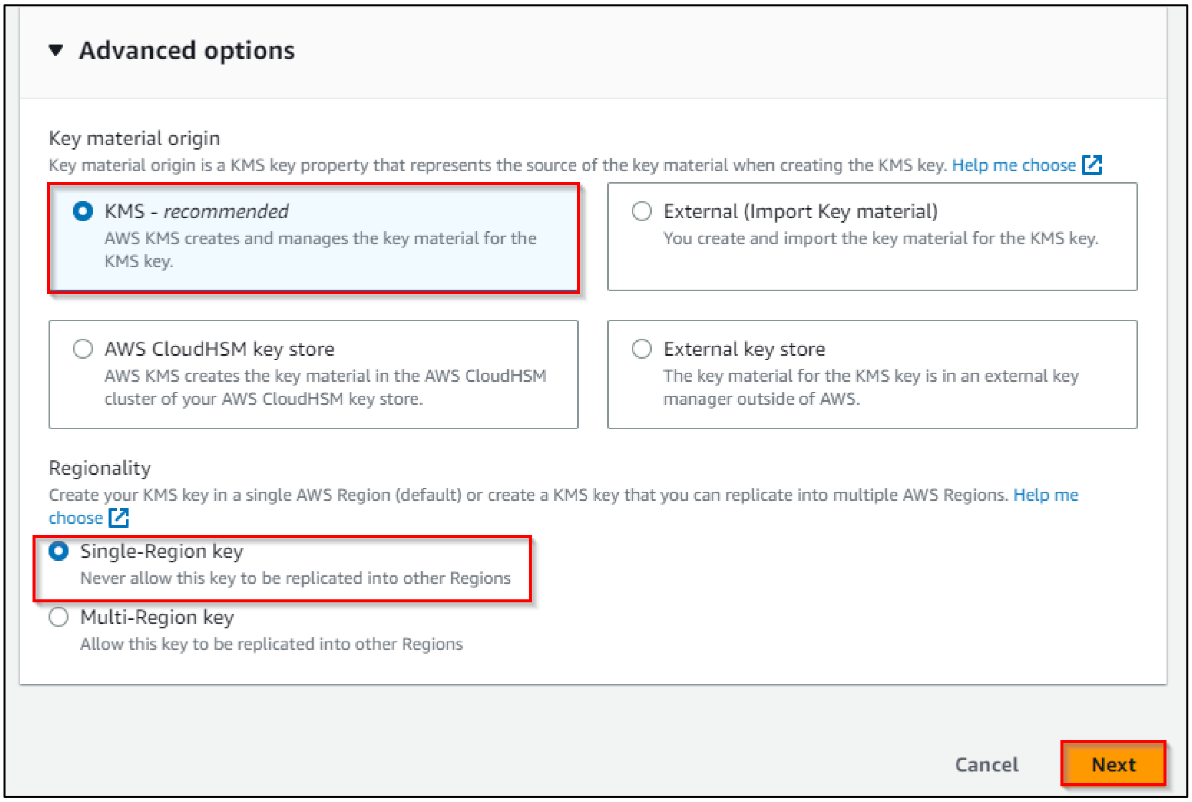
○ Asymmetric
A public and private key pair used for encrypting and decrypting data or signing and verifying messages

**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).

1.4 Click on Advanced options, select **KMS - recommended** for Key material origin, choose **Single-Region key** for Regionality, and then click **Next**



▼ 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.

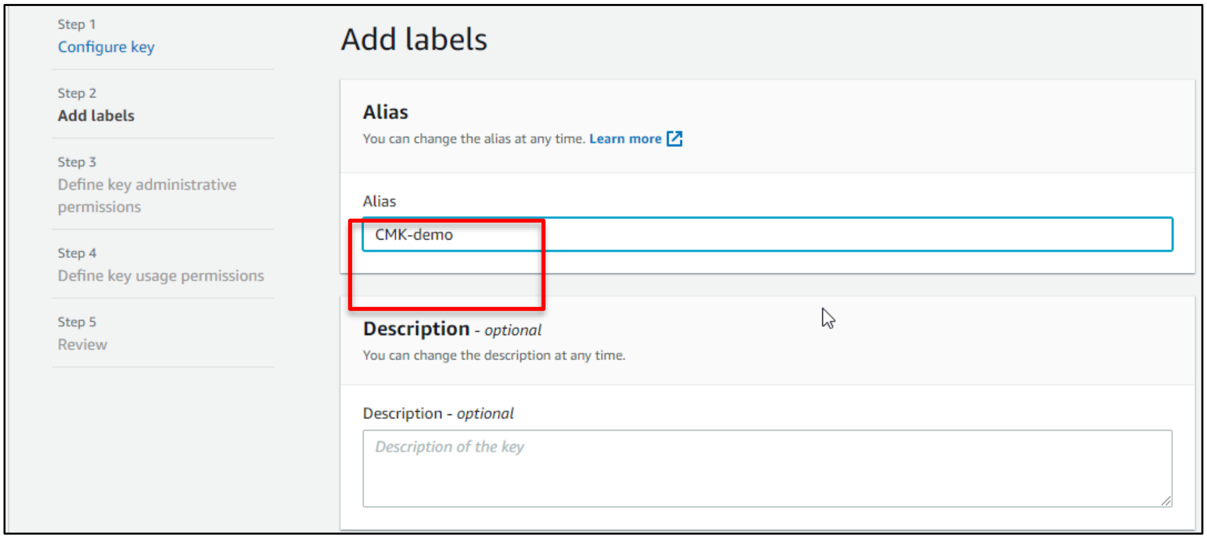
Regionality

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

1.5 Enter **CMK-demo** as the **Alias** name and click on **Next**



Step 1
Configure key
Step 2
Add labels
Step 3
Define key administrative permissions
Step 4
Define key usage permissions
Step 5
Review

Add labels

Alias

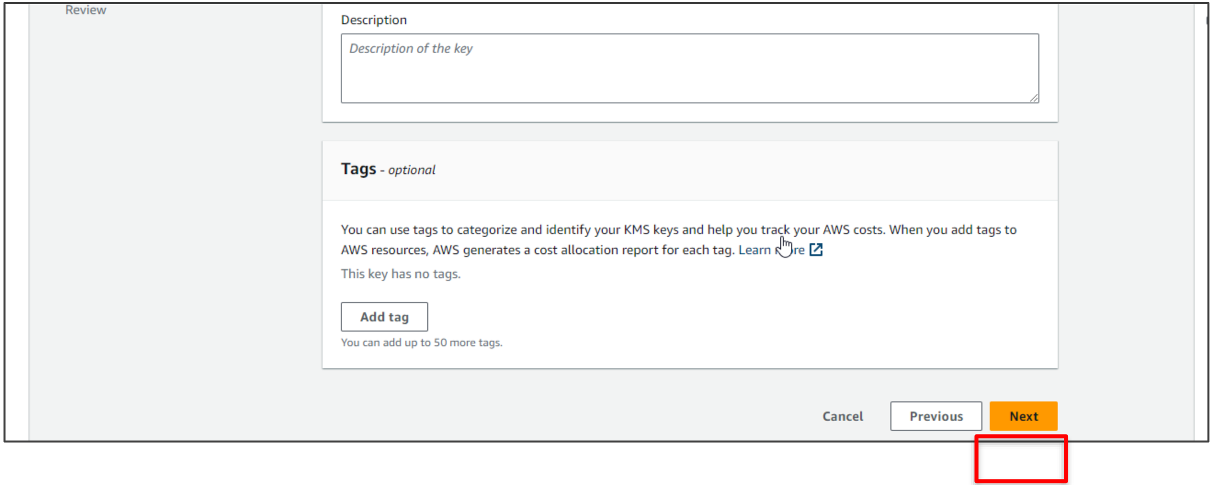
You can change the alias at any time. Learn more

Alias: CMK-demo

Description - *optional*

You can change the description at any time.

Description - *optional*: *Description of the key*



Review

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

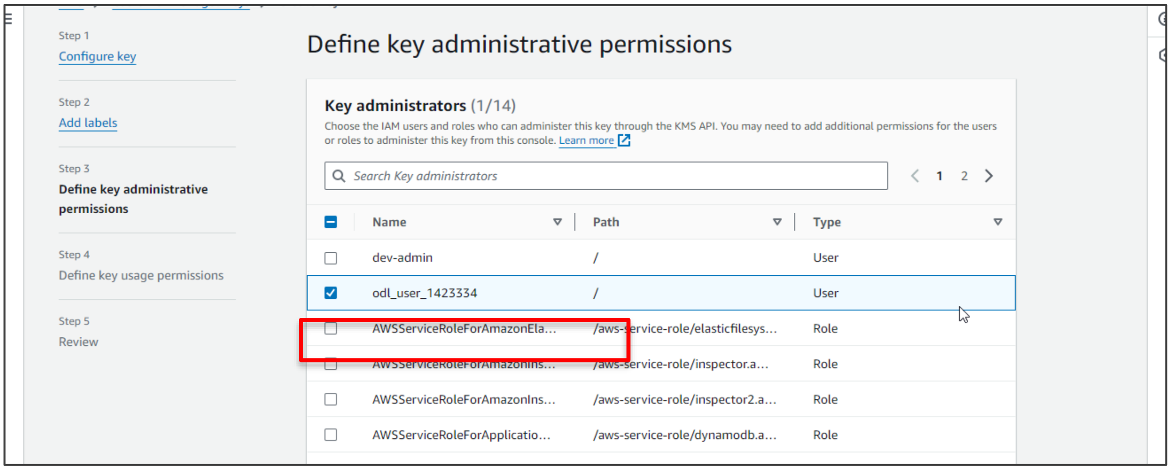
This key has no tags.

Add tag

You can add up to 50 more tags.

Cancel | Previous | Next

1.6 Select the username associated with your AWS Lab as **Key administrators**



Step 1
Configure key

Step 2
Add labels

Step 3
**Define key administrative permissions**

Step 4
Define key usage permissions

Step 5
Review

## Define key administrative permissions

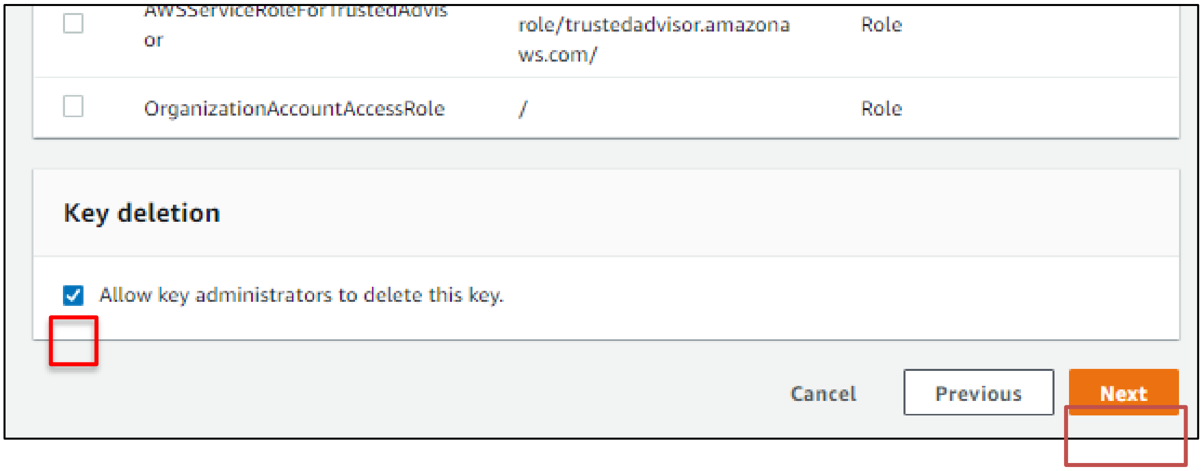
**Key administrators** (1/14)

Choose the IAM users and roles who can administer this key through the KMS API. You may need to add additional permissions for the users or roles to administer this key from this console. Learn more

*Search Key administrators*   < 1 2 >

| ☐ | Name | Path | Type |
|---|---|---|---|
| ☐ | dev-admin | / | User |
| ☑ | odl_user_1423334 | / | User |
| ☐ | AWSServiceRoleForAmazonEla… | /aws-service-role/elasticfilesys… | Role |
| ☐ | AWSServiceRoleForAmazonIns… | /aws-service-role/inspector.a… | Role |
| ☐ | AWSServiceRoleForAmazonIns… | /aws-service-role/inspector2.a… | Role |
| ☐ | AWSServiceRoleForApplicatio… | /aws-service-role/dynamodb.a… | Role |

1.7 Check **Allow key administrators to delete this key** and click **Next**



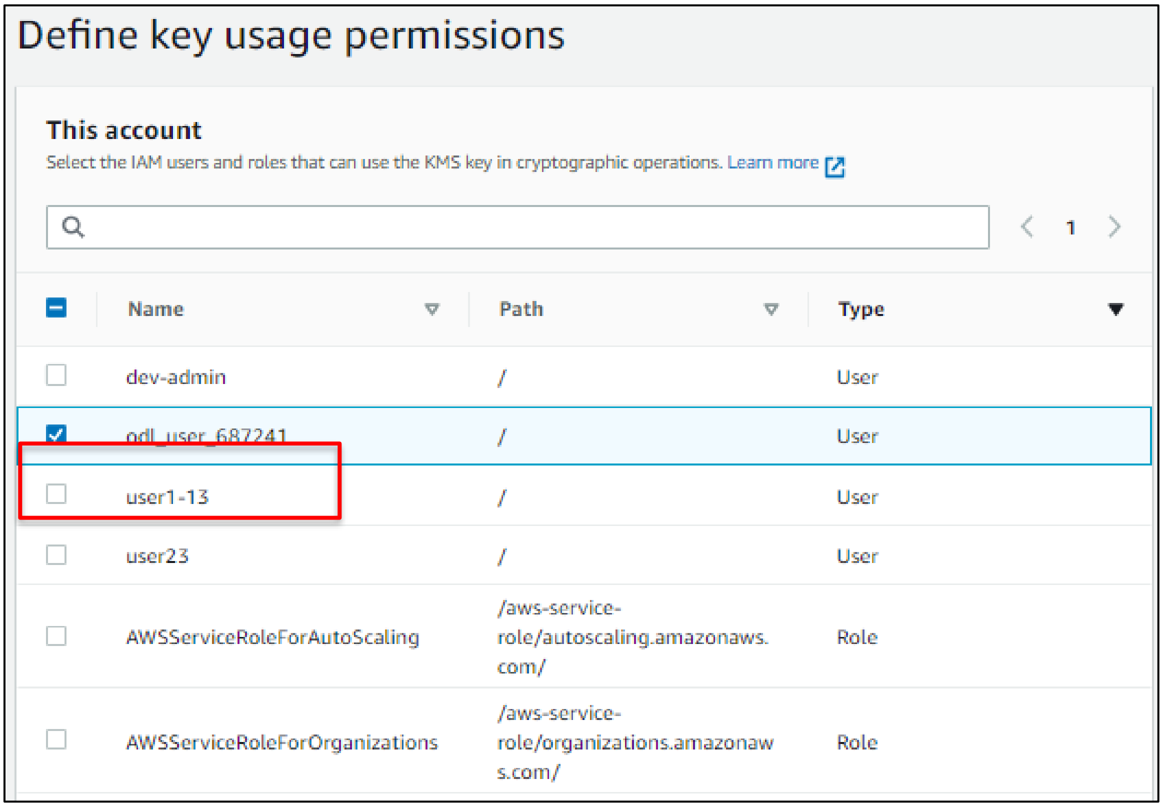
| | | | |
|---|---|---|---|
| ☐ | AWSServiceRoleForTrustedAdvisor | role/trustedadvisor.amazonaws.com/ | Role |
| ☐ | OrganizationAccountAccessRole | / | Role |

**Key deletion**

☑ Allow key administrators to delete this key.

Cancel | Previous | Next

1.8 Under **Define key usage permissions**, select the username of your AWS Lab and click **Next**

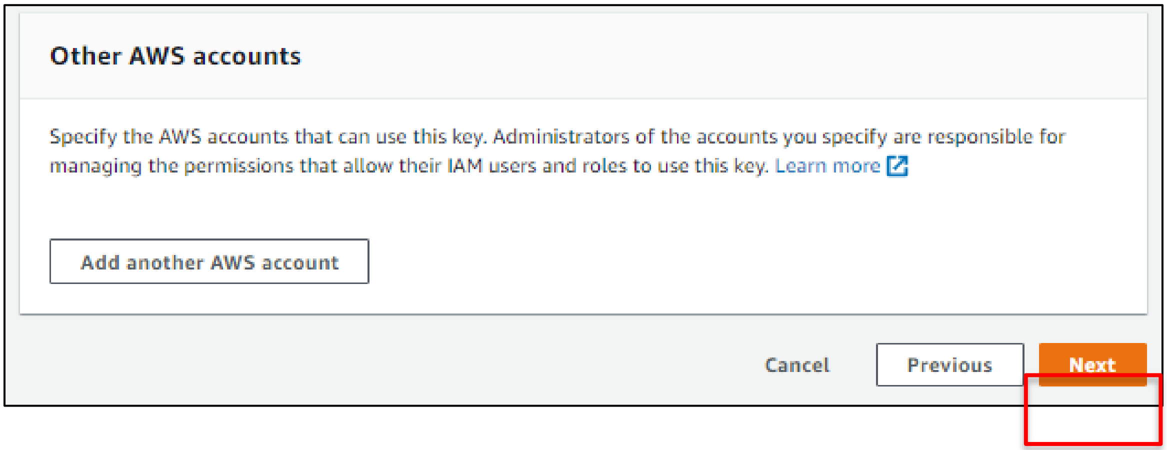


Define key usage permissions

**This account**

Select the IAM users and roles that can use the KMS key in cryptographic operations. Learn more

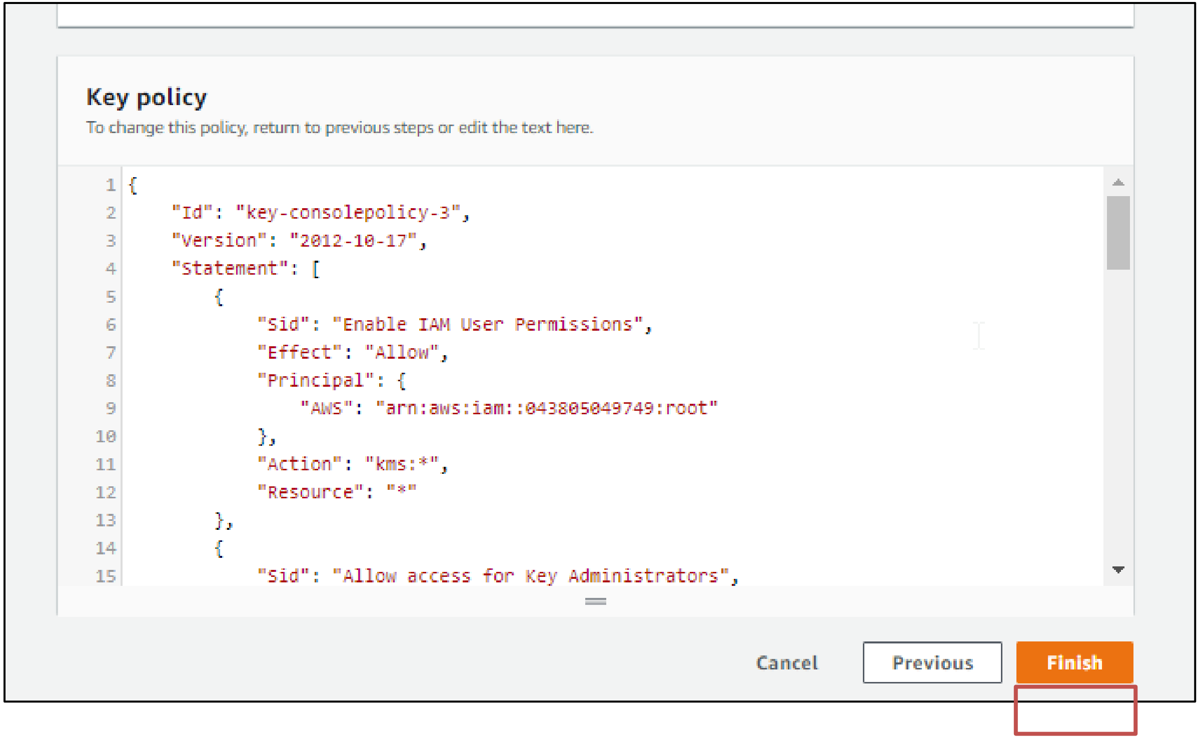
| | Name | Path | Type |
|---|---|---|---|
| ☐ | dev-admin | / | User |
| ☑ | odl_user_687241 | / | User |
| ☐ | user1-13 | / | User |
| ☐ | user23 | / | User |
| ☐ | AWSServiceRoleForAutoScaling | /aws-service-role/autoscaling.amazonaws.com/ | Role |
| ☐ | AWSServiceRoleForOrganizations | /aws-service-role/organizations.amazonaws.com/ | 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

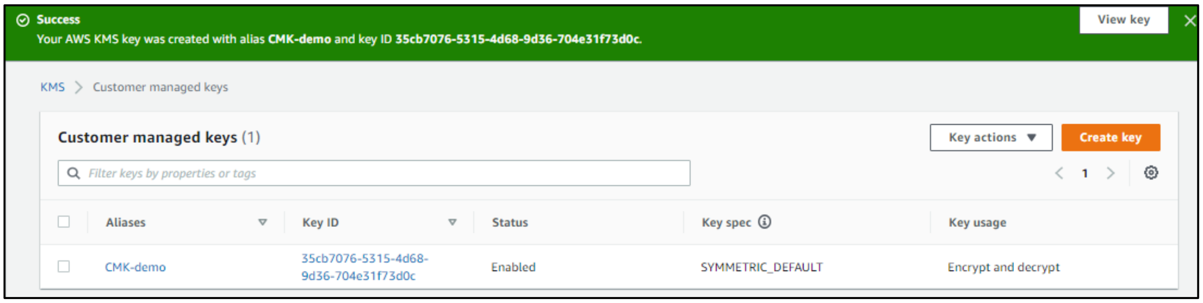
1.9 Scroll down to the Key policy tab and click **Finish**



**Key policy**

To change this policy, return to previous steps or edit the text here.

```
{
    "Id": "key-consolepolicy-3",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::043805049749:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow access for Key Administrators",
```



**Success**
Your AWS KMS key was created with alias **CMK-demo** and key ID **35cb7076-5315-4d68-9d36-704e31f73d0c.**

View key
KMS > Customer managed keys
Key actions ▼
Create key
Filter keys by properties or tags
< 1 >

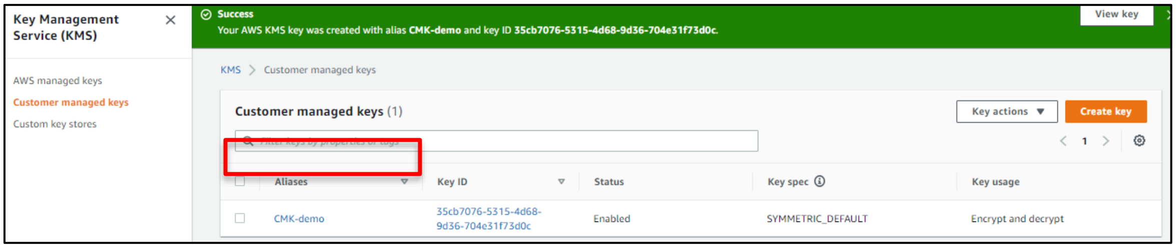
**Customer managed keys** (1)

| □ | Aliases | Key ID | Status | Key spec | Key usage |
|---|---|---|---|---|---|
| □ | CMK-demo | 35cb7076-5315-4d68-9d36-704e31f73d0c | Enabled | SYMMETRIC_DEFAULT | Encrypt and decrypt |

The KMS key has been successfully created.

## Step 2: Delete a customer-managed key

2.1 Navigate to **Customer managed keys** and click on the created key

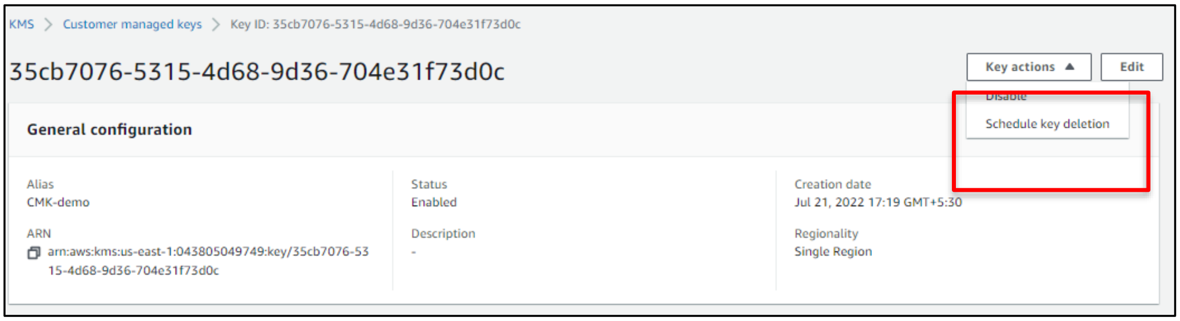


Success
Your AWS KMS key was created with alias **CMK-demo** and key ID **35cb7076-5315-4d68-9d36-704e31f73d0c.**

Customer managed keys (1)

| | Aliases | Key ID | Status | Key spec | Key usage |
|---|---|---|---|---|---|
| □ | CMK-demo | 35cb7076-5315-4d68-9d36-704e31f73d0c | Enabled | SYMMETRIC_DEFAULT | Encrypt and decrypt |

2.2 Under **Key actions**, select **Schedule key deletion**


KMS > Customer managed keys > Key ID: 35cb7076-5315-4d68-9d36-704e31f73d0c
Key actions ▲
Edit
Disable
Schedule key deletion

35cb7076-5315-4d68-9d36-704e31f73d0c

General configuration

Alias
CMK-demo

ARN
arn:aws:kms:us-east-1:043805049749:key/35cb7076-5315-4d68-9d36-704e31f73d0c

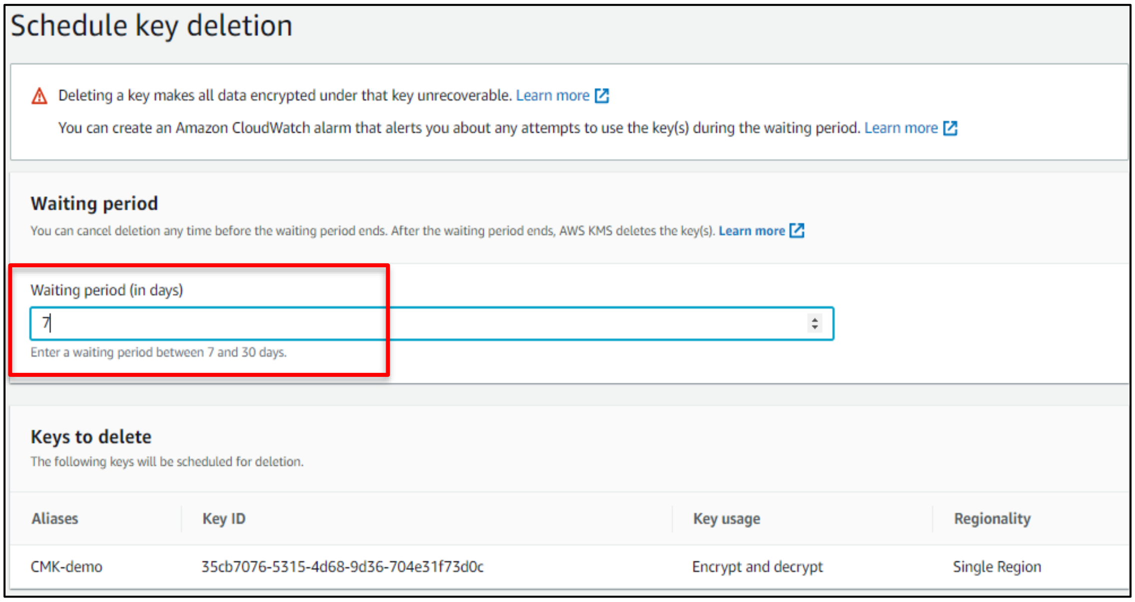
Status
Enabled

Description
-

Creation date
Jul 21, 2022 17:19 GMT+5:30

Regionality
Single Region

2.3 Under **Schedule key deletion**, add a number between **7** and **30** for the **Waiting period**



Schedule key deletion

Deleting a key makes all data encrypted under that key unrecoverable. Learn more

You can create an Amazon CloudWatch alarm that alerts you about any attempts to use the key(s) during the waiting period. Learn more

Waiting period

You can cancel deletion any time before the waiting period ends. After the waiting period ends, AWS KMS deletes the key(s). Learn more

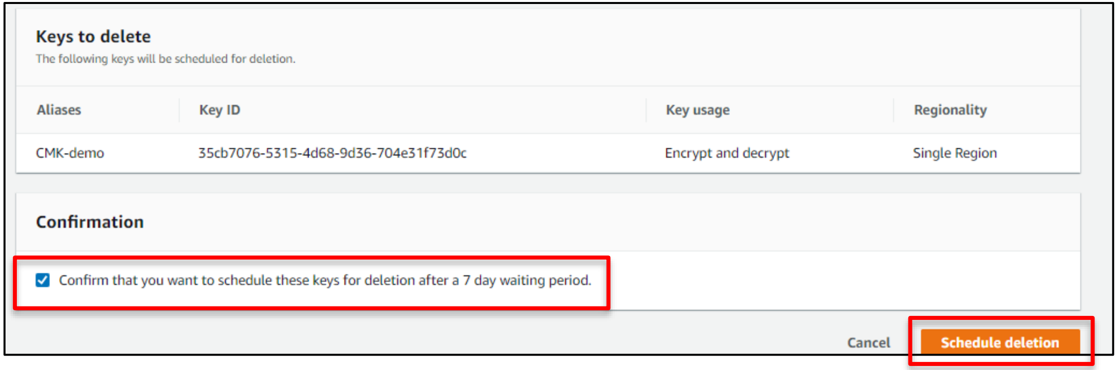
Waiting period (in days)
7
Enter a waiting period between 7 and 30 days.

Keys to delete

The following keys will be scheduled for deletion.

| Aliases | Key ID | Key usage | Regionality |
|---|---|---|---|
| CMK-demo | 35cb7076-5315-4d68-9d36-704e31f73d0c | Encrypt and decrypt | Single Region |

2.4 Confirm the deletion and click **Schedule deletion**



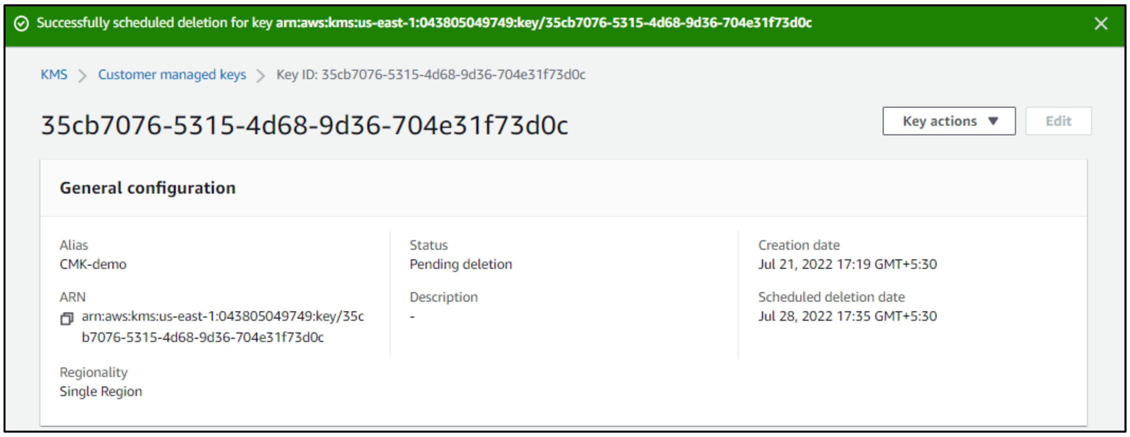
**Keys to delete**

The following keys will be scheduled for deletion.

| Aliases | Key ID | Key usage | Regionality |
|---|---|---|---|
| CMK-demo | 35cb7076-5315-4d68-9d36-704e31f73d0c | Encrypt and decrypt | Single Region |

**Confirmation**

☑ Confirm that you want to schedule these keys for deletion after a 7 day waiting period.



Successfully scheduled deletion for key arn:aws:kms:us-east-1:043805049749:key/35cb7076-5315-4d68-9d36-704e31f73d0c

KMS > Customer managed keys > Key ID: 35cb7076-5315-4d68-9d36-704e31f73d0c

35cb7076-5315-4d68-9d36-704e31f73d0c

**General configuration**

Alias: CMK-demo

ARN: arn:aws:kms:us-east-1:043805049749:key/35cb7076-5315-4d68-9d36-704e31f73d0c

Regionality: Single Region

Status: Pending deletion

Description: -

Creation date: Jul 21, 2022 17:19 GMT+5:30

Scheduled deletion date: Jul 28, 2022 17:35 GMT+5:30

The key has been successfully scheduled for deletion.

**Note:** The key will be deleted after seven days.

By following these steps, you have gained the ability to confidently manage cryptographic keys, ensuring robust security practices in your AWS environment.