

Go to AWS console and search as kms

The screenshot shows the AWS KMS landing page. On the left, there's a sidebar with navigation links: 'Key Management Service (KMS)', 'AWS managed keys', 'Customer managed keys', and 'Custom key stores' (which is expanded, showing 'AWS CloudHSM key stores' and 'External key stores'). The main content area has a dark header 'Security, Identity & Compliance'. Below it, the title 'AWS Key Management Service' is displayed in large bold letters, followed by the subtitle 'Easily create keys and control encryption across AWS and beyond'. A paragraph explains that KMS is a managed service for creating and managing encryption keys. To the right, there's a 'Get started now' button and a 'Pricing' section with a 'Learn more' link. At the bottom, there are three buttons: 'How it works', 'Getting started', and 'Create a key'.

Click on create key and select key type as symmetric and key usage as encrypt and decrypt.

The screenshot shows the 'Configure key' step of the 'Create key' wizard. On the left, a sidebar lists steps: Step 1 (Configure key, selected), Step 2 (Add labels), Step 3 - optional (Define key administrative permissions), Step 4 - optional (Define key usage permissions), Step 5 - optional (Edit key policy), and Step 6 (Review). The main area is titled 'Configure key'. It has two sections: 'Key type' and 'Key usage'. Under 'Key type', 'Symmetric' is selected. Under 'Key usage', 'Encrypt and decrypt' is selected. At the bottom, there are 'Advanced options' and 'Cancel' and 'Next' buttons.

Select name for 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.

- 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

my-key

Description - optional

You can change the description at any time.

Description

Description of the key

Select your user or IAM role .

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.

- 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 (1/4)
Select the IAM users and roles authorized to manage this 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](#)

Name	Type
user-1	User
AWSServiceRoleForResourceExplorer	/aws-service-role/resource-explorer-2.amazonaws.com/
AWSServiceRoleForSupport	/aws-service-role/support.amazonaws.com/
AWSServiceRoleForTrustedAdvisor	/aws-service-role/trustedadvisor.amazonaws.com/

Key deletion
 Allow key administrators to delete this key.

Then click on create key.

Success
Your AWS KMS key was created with alias my-key and key ID 1532056f-98eb-49e7-b3e2-819d38cfec5d.

Customer managed keys (1/3)

Aliases	Key ID	Status	Key type	Key spec
MyNewProjectKey (+1 more)	28f48ff3-f0e0-4b10-936d-8f...	Pending deletion	Symmetric	SYMMETRIC_DEFAULT
-	ce4d8d52-23b4-4666-8026...	Pending deletion	Symmetric	SYMMETRIC_DEFAULT
my-key	1532056f-98eb-49e7-b3e2...	Enabled	Symmetric	SYMMETRIC_DEFAULT

Go to the s3 bucket and add a text file and go to the properties and edit the default encryption.

The screenshot shows the AWS S3 Bucket Properties page for 'nv-bucket456'. In the 'Default encryption' section, it is set to 'Server-side encryption with Amazon S3 managed keys (SSE-S3)'. There is an 'Edit' button next to the encryption type. The 'Bucket Key' section shows 'Enabled' with an 'Edit' button.

Select server side encryption(SSE-KMS) and click on save.

The screenshot shows the 'Edit default encryption' page for 'nv-bucket456'. Under 'Encryption type', the 'Server-side encryption with AWS Key Management Service keys (SSE-KMS)' option is selected. Under 'AWS KMS key', the 'Enter AWS KMS key ARN' option is selected. A yellow warning box at the bottom states: '⚠️ Changing the default encryption settings might cause in-progress replication and Batch Replication jobs to fail. These jobs might fail because of missing AWS KMS permissions on the IAM role that's specified in replication configuration. If you change the default encryption settings, make sure that this IAM role has the necessary AWS KMS permissions.' There is a 'Create a KMS key' button in the top right of the ARN input field.

Now your file is encrypted using your KMS key.