

AWS Cloud Practical

Name: Pooja Prakash Belgaumkar

1. SSE-KMS encryption for object in S3

- **SSE-S3** → AWS encrypts, no extra control
- **SSE-KMS** → AWS encrypts and IAM/KMS decides who can decrypt

The screenshot shows the AWS S3 console's 'Upload' page for the bucket 's3-dmos-bucket'. The breadcrumb navigation at the top reads 'Amazon S3 > Buckets > s3-dmos-bucket > Upload'. The main heading is 'Upload' with an 'Info' link. Below this, a message states: 'Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)'. A dashed box contains the instruction: 'Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.' Below this is a section titled 'Files and folders (1 total, 259.2 KB)' with 'Remove', 'Add files', and 'Add folder' buttons. A note says 'All files and folders in this table will be uploaded.' There is a search bar with the placeholder 'Find by name'. A table lists the upload items:

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	3.jpg	-	image/jpeg	259.2 KB

Below the table is a 'Destination' section with an 'Info' link. It shows the destination as 's3://s3-dmos-bucket' with a link icon. A section titled 'Destination details' explains: 'Bucket settings that impact new objects stored in the specified destination.'

- While uploading the object into S3 bucket enable the SSE-KMS option in the Server-side encryption as shown below.
- Choose AWS managed key (aws/s3)

Server-side encryption [Info](#)

Server-side encryption protects data at rest.

Server-side encryption

- ☐ Don't specify an encryption key
The bucket settings for default encryption are used to encrypt objects when storing them in Amazon S3.
- ☒ Specify an encryption key
The specified encryption key is used to encrypt objects before storing them in Amazon S3.

Encryption settings [Info](#)

- ☐ Use bucket settings for default encryption
- ☒ Override bucket settings for default encryption

Encryption type [Info](#)

Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the [Storage](#) tab of the [Amazon S3 pricing page](#).

- ☐ Server-side encryption with Amazon S3 managed keys (SSE-S3)
- ☒ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- ☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

AWS KMS key [Info](#)

- ☒ Choose from your AWS KMS keys
- ☐ Enter AWS KMS key ARN

Available AWS KMS keys

arn:aws:kms:eu-north-1:787169320097:key/d64cb4f4-383a-4c9d-94...



[Create a KMS key](#)

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

- ☐ Disable
- ☒ Enable

Server-side encryption settings [Info](#)

[Edit](#)

Server-side encryption protects data at rest.

Encryption type [Info](#)

Server-side encryption with AWS Key Management Service keys (SSE-KMS)

Encryption key ARN

[arn:aws:kms:eu-north-1:787169320097:key/d64cb4f4-383a-4c9d-943b-b334b14757a0](#)

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)
Enabled

- In SSE-KMS, objects are encrypted using AWS Key Management Service. Access to the encrypted object depends on IAM permissions to use the KMS key, providing finer access control.