**What is AWS KMS-Managed Keys (SSE-KMS)..?**

**AWS KMS-Managed Keys (SSE-KMS).**

When you create an **object**, you can specify the use of **server-side encryption** with **AWS Key Management Service (AWS KMS)** keys to encrypt your data. This **encryption** is known as **SSE-KMS**. You can apply encryption when you are either uploading a new object or copying an existing object.

You can specify **SSE-KMS** using the **Amazon S3 console**, **REST API operations**, **AWS SDKs**, and **AWS Command Line Interface (AWS CLI)**. For more information, see the following topics.

To add or change encryption for an object

Sign in to the AWS Management Console and open the **Amazon S3 console** at https://console.aws.amazon.com/s3/.

In the **Buckets list**, choose the name of the **bucket** that contains the **object**.

In the **Objects list**, choose the name of the object that you want to add or change encryption for.

The Object overview opens, displaying the properties for your object.

Under **Server-side encryption** settings, choose Edit.

The Edit **server-side encryption** page opens

To enable **server-side encryption** for your object, under **Server-side encryption**, choose Enable.

Under **Encryption key type**, choose **AWS Key Management Service** **key (SSE-KMS)**.

Under **AWS KMS** key, choose one of the following:

**AWS managed key (aws/s3)**

**Choose from your AWS KMS keys, and choose your KMS key.**

Enter **KMS master key ARN**, and enter your **AWS KMS key Amazon Resource Name (ARN)**.

For more information about creating an **AWS KMS key**, see Creating Keys in the **AWS Key Management Service Developer** Guide. For more information about using **AWS KMS** with **Amazon S3**, see Protecting data using **server-side encryption** with **AWS Key Management Service (SSE-KMS)**.

Choose Save changes.