

Encrypt S3 data using Encryption Key

edureka!

edureka!

© Brain4ce Education Solutions Pvt. Ltd.

Overview

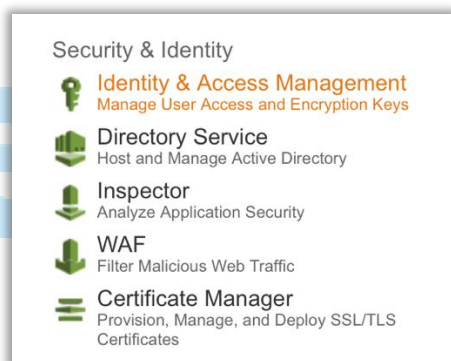
This guide introduces you to the Introduction to AWS Key Management Service (KMS) self-paced lab.

The lab will give you the basic understanding of KMS. It will demonstrate the basic steps required to get started with this service, creating keys, assigning management and usage permissions for the keys and encrypting data.

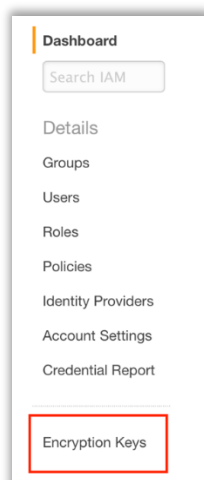
Creating Keys

You can use the IAM section of the AWS Management Console to create a customer master key (CMK).

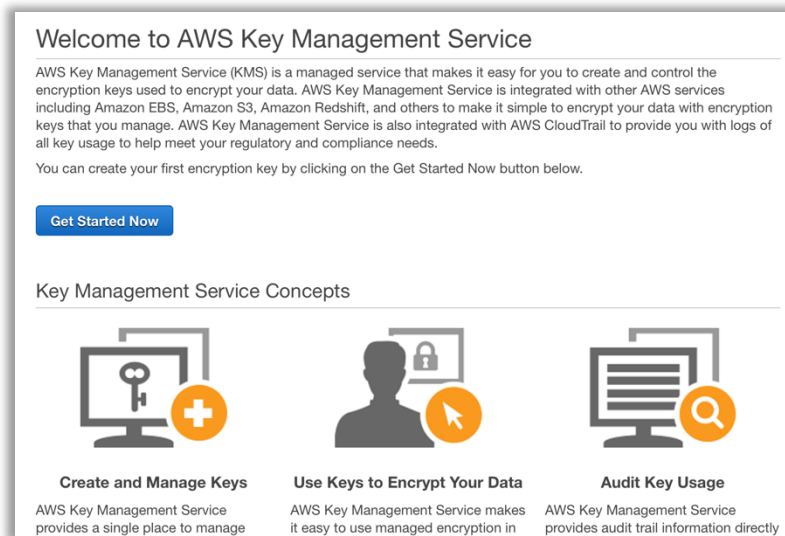
1. Login to AWS Management Console and click [Identity and Access Management](#) within [Security & Identity](#) section.



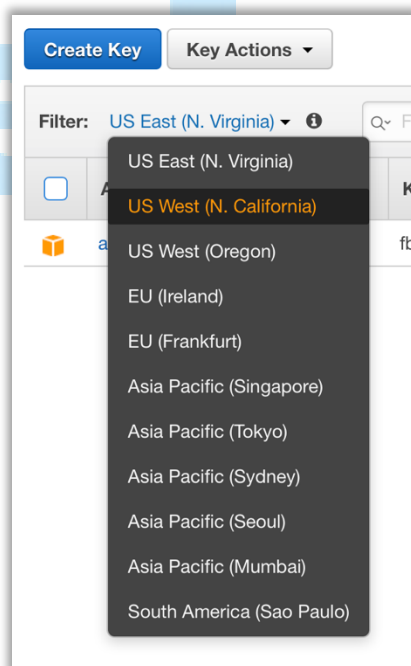
2. Click [Encryption Keys](#) on the IAM Dashboard.



- This will take you to AWS Key Management Service dashboard. Click [Get Started Now](#).



- For [Filter](#), choose the appropriate AWS region. Do not use the region selector in the menu bar (top right corner).



- Choose [Create Key](#).
- Type an alias and a description for the CMK. Click [Next Step](#).

Create Alias and Description

Provide an alias and a description for this key. These properties of the key can be changed later. [Learn more](#).

Alias (required)

Description

7. Select which IAM users and roles can administer the CMK. Choose [Next Step](#).

Define Key Administrative Permissions

▼ Key Administrators

Choose the IAM users and roles that 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](#).

Q Filter Showing 12 results

<input type="checkbox"/>	Name ↕	Path ↕	Type ↕
<input checked="" type="checkbox"/>	chris	/	User
<input checked="" type="checkbox"/>	john	/	User
<input checked="" type="checkbox"/>	michael	/	User

8. Select which IAM users and roles can use the CMK to encrypt and decrypt data with the AWS KMS API. Choose [Next Step](#).

Define Key Usage Permissions

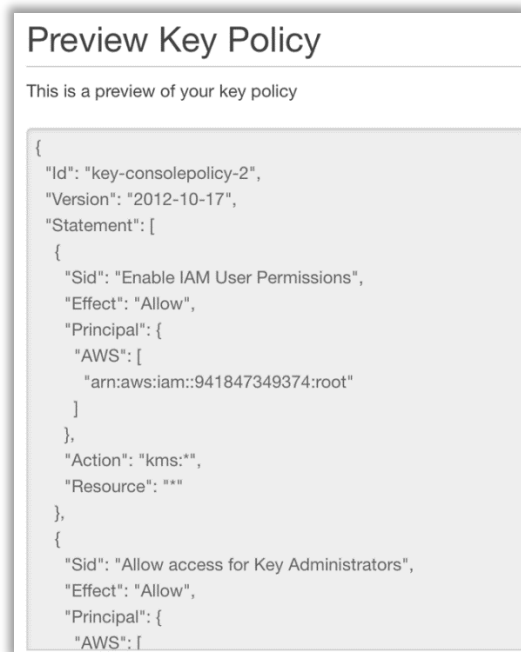
▼ This Account

Choose the IAM users and roles that can use this key to encrypt and decrypt data from within applications and when using AWS services integrated with KMS. [Learn more](#).

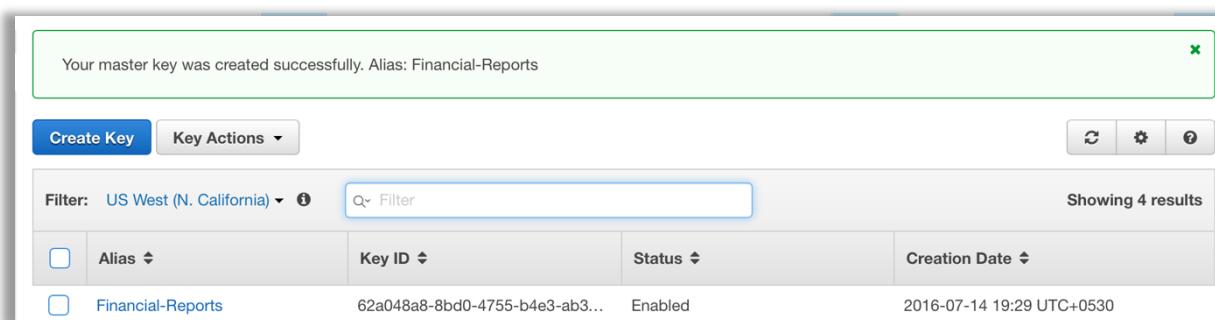
Q Filter Showing 12 results

<input type="checkbox"/>	Name ↕	Path ↕	Type ↕
<input checked="" type="checkbox"/>	chris	/	User
<input checked="" type="checkbox"/>	john	/	User

9. You will get a preview of your key policy. Choose [Finish](#) to create the CMK.



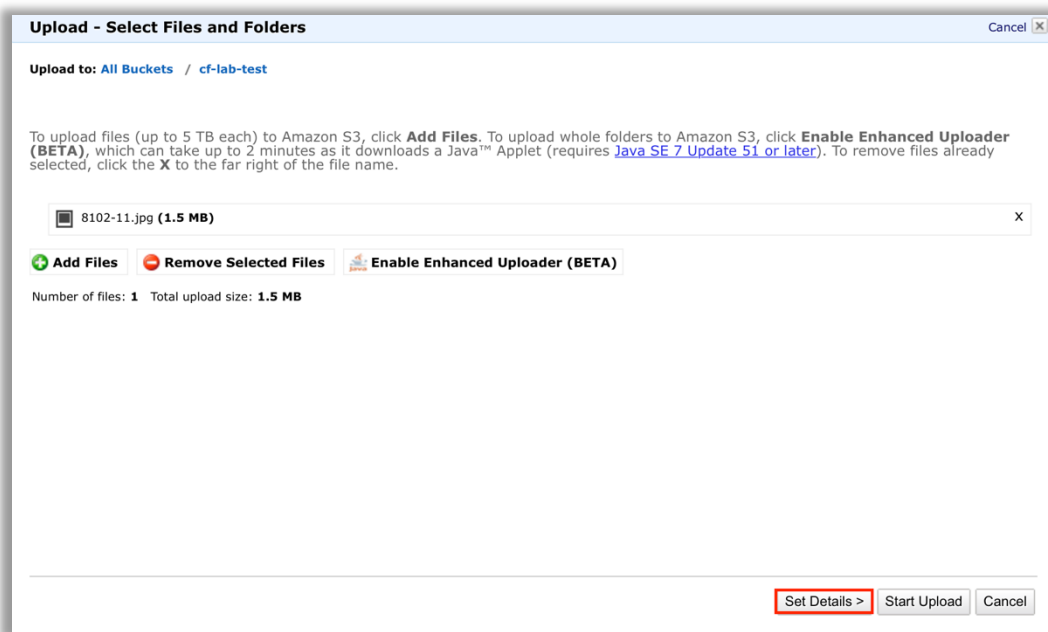
This creates your master key successfully.



Encrypting Data in an S3 bucket

You will now upload a file to S3 and encrypt it using the encryption key you created earlier.

10. Open the S3 bucket and click [Upload](#).
11. Click [Add Files](#), then navigate to the file that you want to upload from your system and select it.
12. Click [Set Details](#) which is in the bottom right of the file upload dialog.

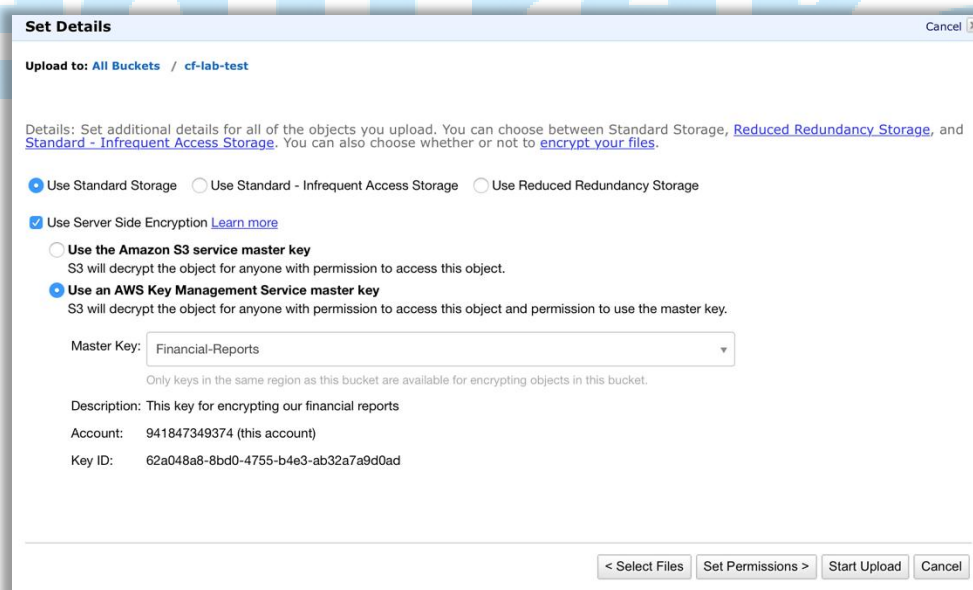


13. Select [Use Server Side Encryption](#).

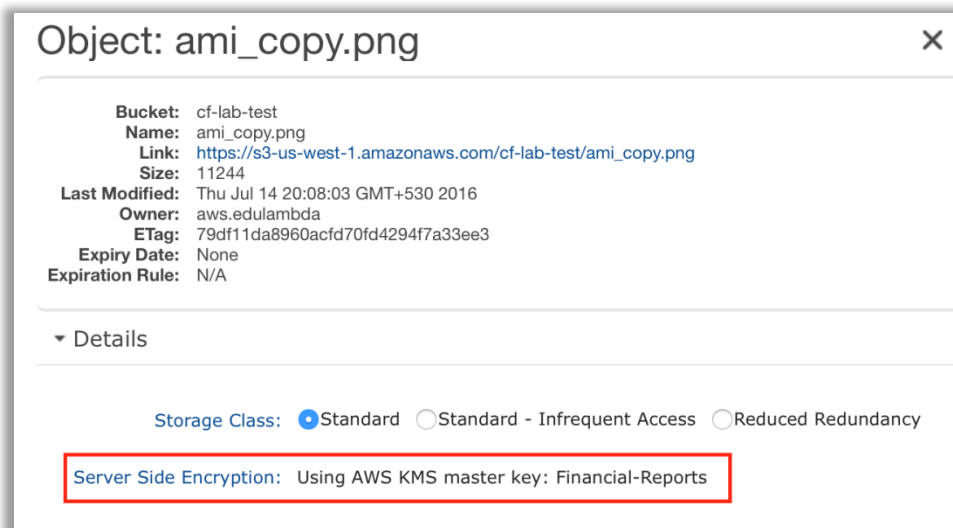
14. Select [Use an AWS Key Management Service Master Key](#).

15. In the [Master Key](#) drop down box select the [financial-reports](#) key you created.

16. Click [Start Upload](#).



17. Once the file has been uploaded right click and click [Properties](#). Click [Details](#) to expand the details section and note that the [Server Side Encryption](#): setting for this file is set to your encryption key.



Conclusion

Congratulations! You have now successfully:

- Created an Encryption Key.
- Encrypted data stored in a S3 bucket using an encryption key.