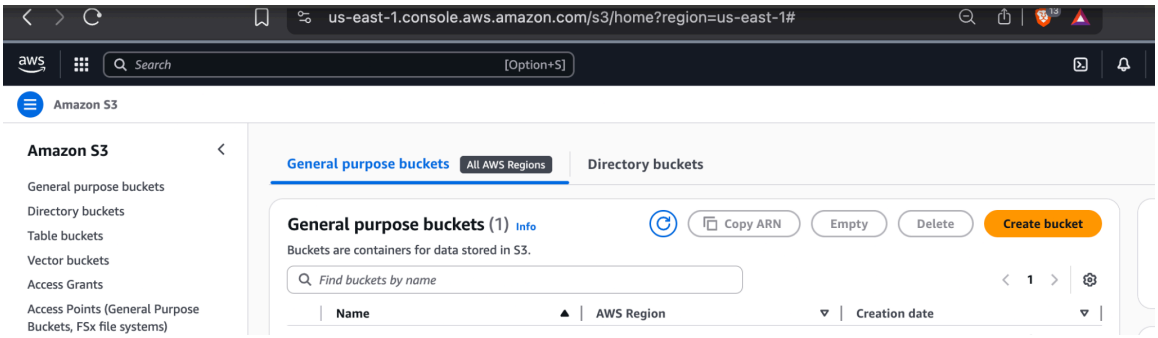
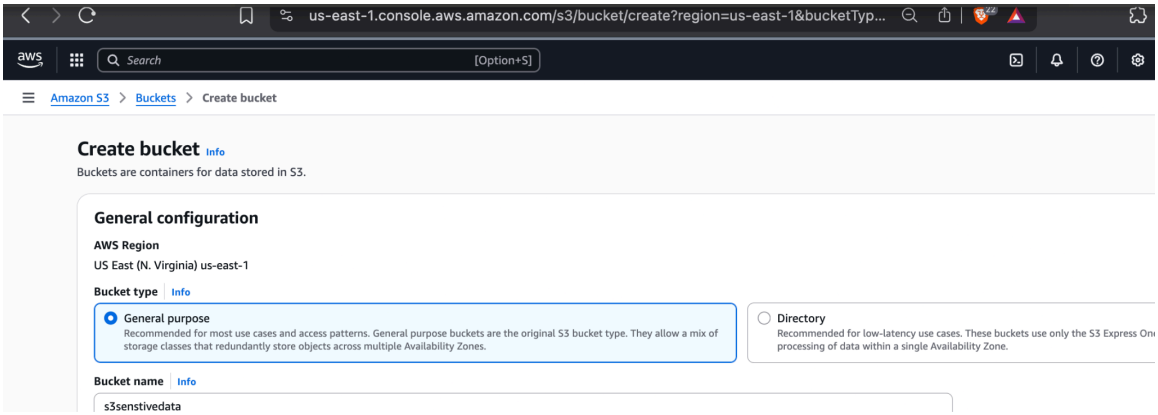
How to create S3 bucket

- In the AWS Management Console, search for **S3** in the search bar and select **S3**.

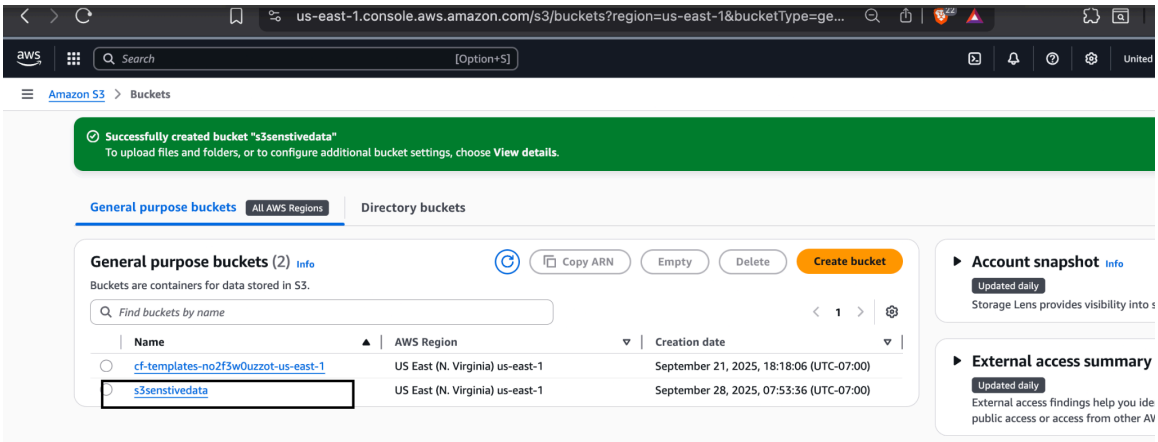


Create the Bucket

1. Click **Create bucket**.
2. Enter a **Bucket name** (for example: s3sensitivedata).
3. Leave all other settings at their default values and click **Create bucket**.

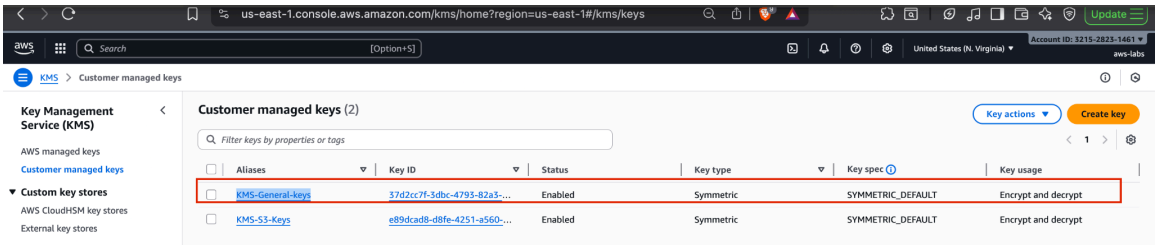


You should now see your new bucket listed.

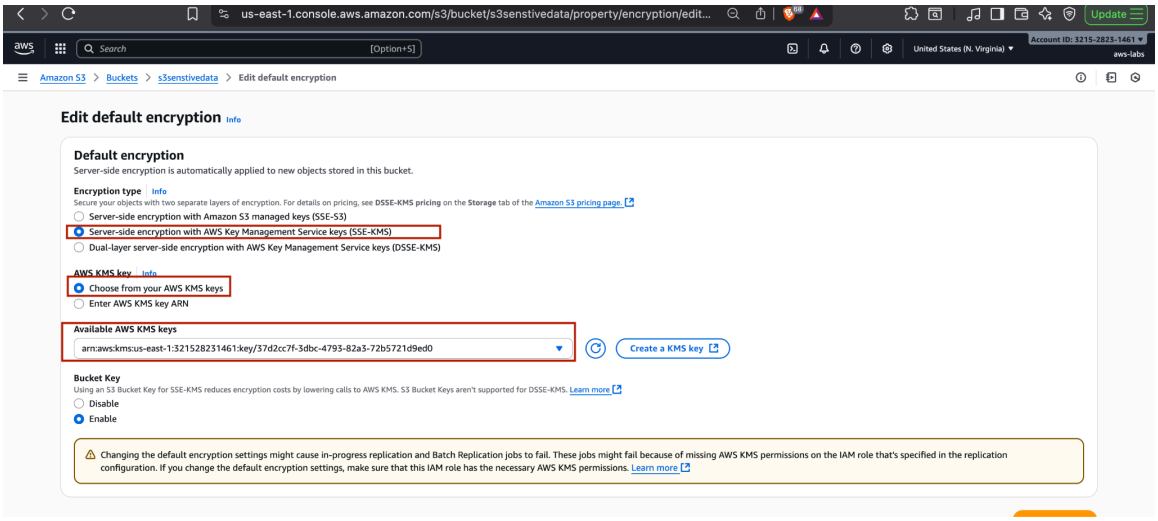


Enforce KMS Encryption for the S3 Bucket

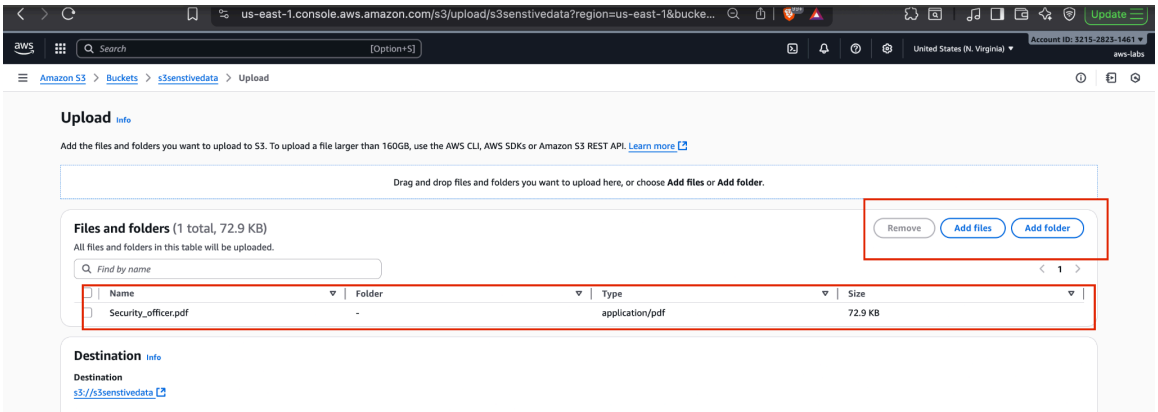
In this step, we'll enable default encryption for the S3 bucket using the **KMS-General-keys** key. To begin, open the bucket's **Properties** tab and click **Default encryption** to configure the settings



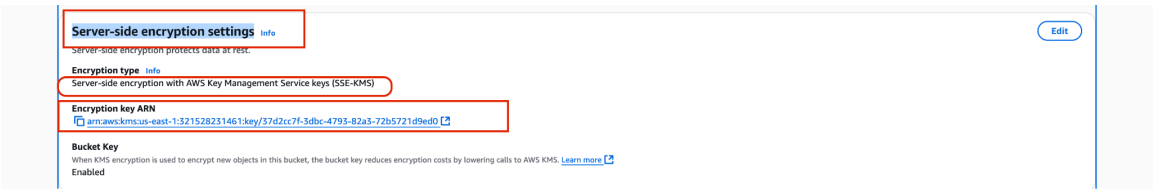
Next, open the S3 bucket, navigate to the **Properties** tab, and click **Edit** under **Default encryption**. In the highlighted section, select **KMS-General-keys** as the encryption key, then click **Save** to apply the setting.



Now upload the data you want to encrypt. Click **Upload**, add your files, and **do not** specify a separate encryption key—use the bucket's default encryption settings. Finally, click **Upload** at the bottom, and you should see a confirmation message that the upload was successful.



If you select an object in the S3 bucket, you can view its **Server-side encryption** settings to confirm that encryption has been applied.


Server-side encryption settings Info
Edit
Encryption type Info
Server-side encryption with AWS Key Management Service keys (SSE-KMS)
Encryption key ARN
arn:aws:kms:us-east-1:321528231461:key/37d2cc7f-3dbc-4793-82a3-72b5721d9ed0
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