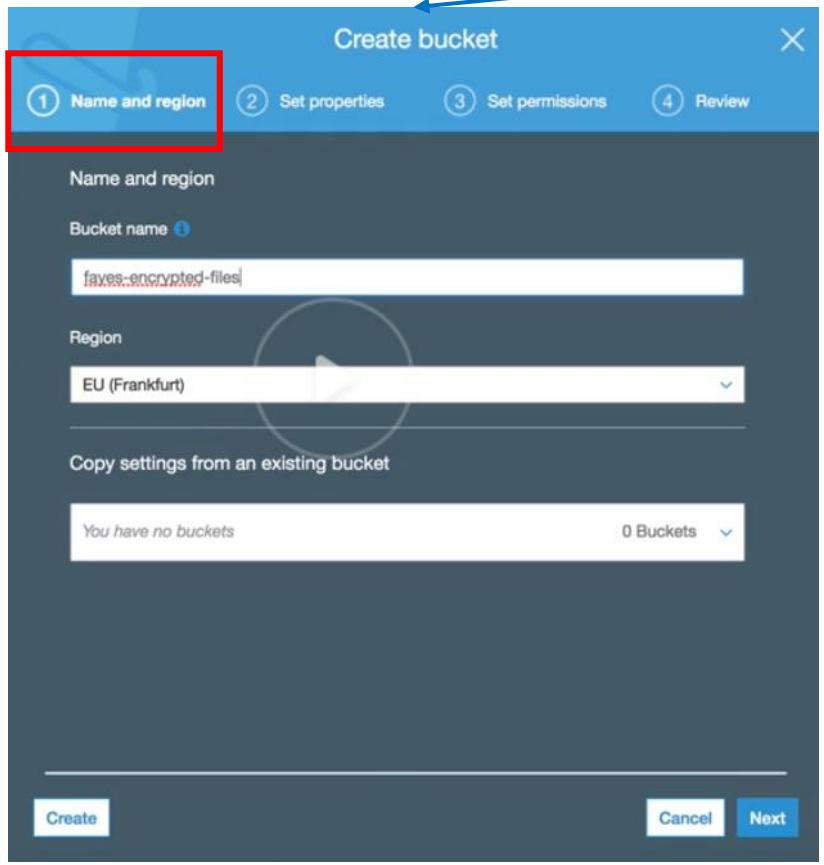
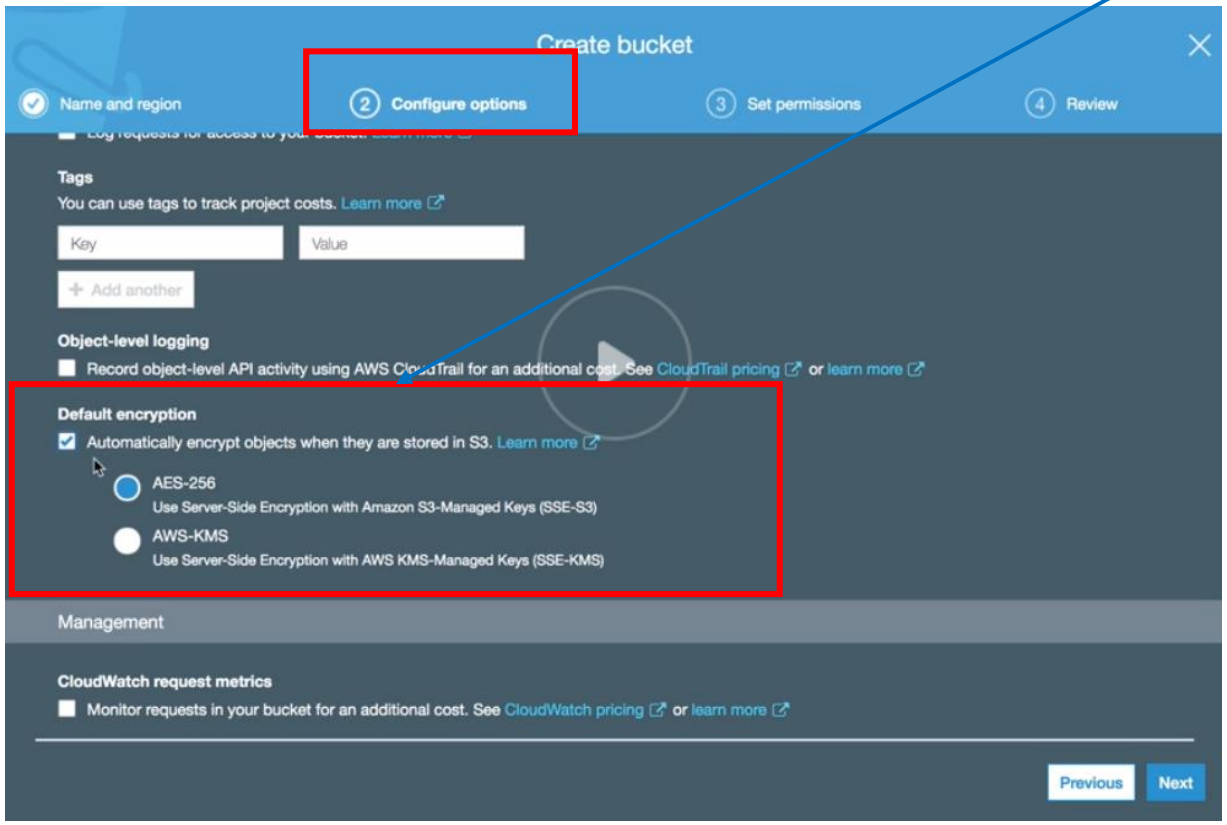
services → s3 → Create bucket

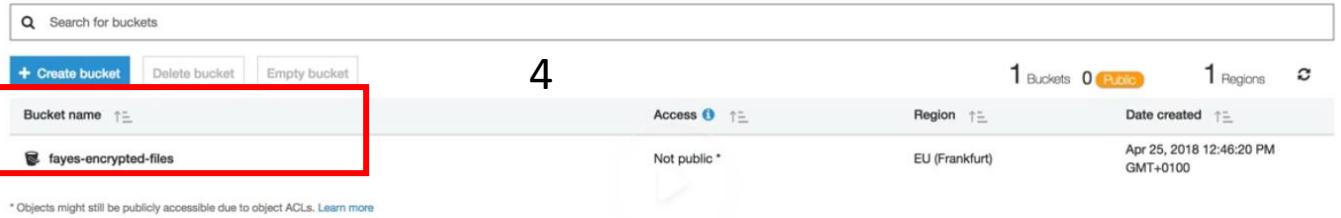
2 ways to enable encryption:
1. Via console
2. S3 bucket policy

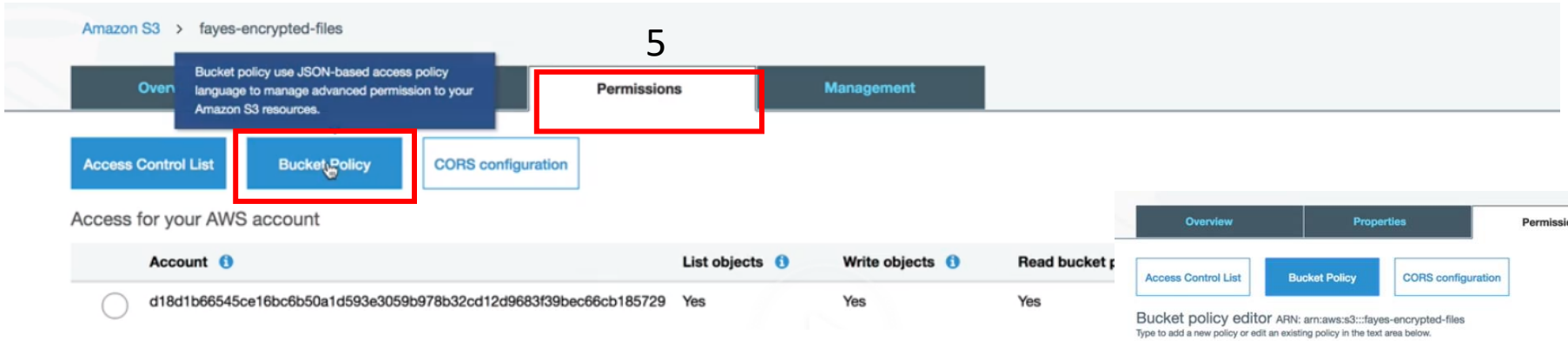


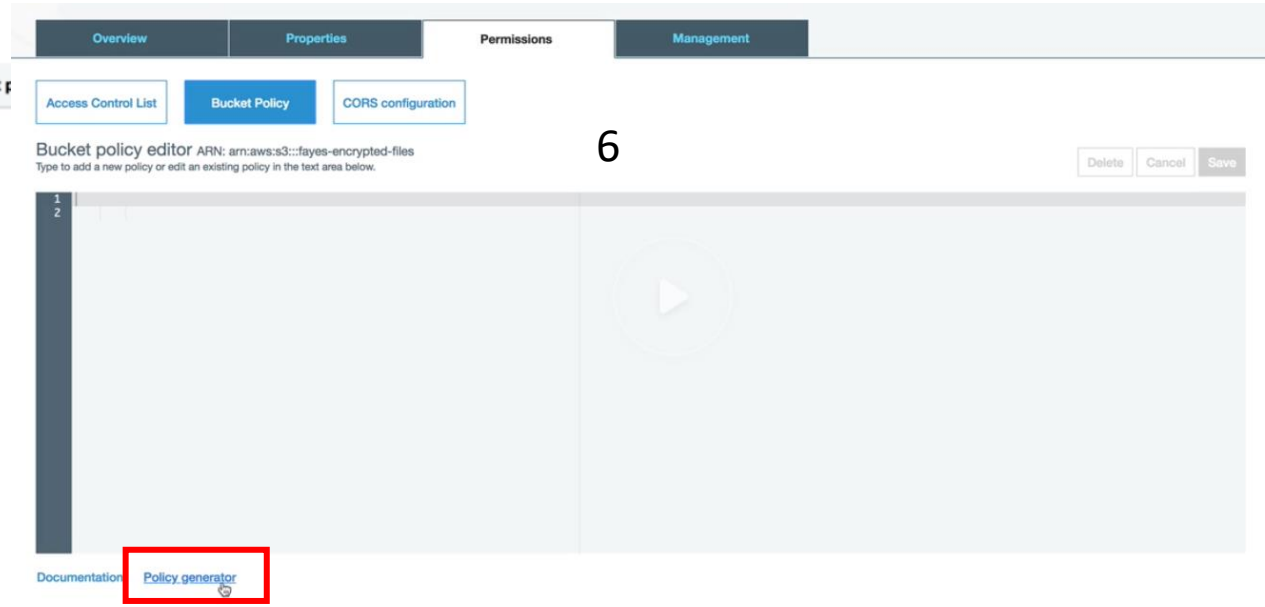


Encryption using s3 bucket policy

1 services → 2 s3 → 3 Create bucket by checking default encryption







7

AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect Allow Deny

Principal *

Use a comma to separate multiple values.

AWS Service Amazon S3 All Services ('*')

Use multiple statements to add permissions for more than one service.

Actions 1 Action(s) Selected All Actions ('*')

Amazon Resource Name (ARN) fayes-encrypted-files

ARN should follow the following format: arn:aws:s3:::<bucket_name>/<key_name>.
Use a comma to separate multiple values.

Add Conditions (Optional)

Add Statement

PutObject

* → User who uses this bucket to upload files without server-side encryption is going to be denied

```
"Resource": "arn:aws:s3:::fayes-encrypted-files/*",
```

some services do not let you specify specific actions for individual resources.
/* action will apply to all resources within that service and not just the bucket

8

Add Conditions (Optional)

Conditions are any restrictions or details about the statement.(More Details).

Condition StringNotEquals

Key s3:x-amz-server-side-encryption

Value aws:kms

Add Condition

Add Statement

9

Policy JSON Document

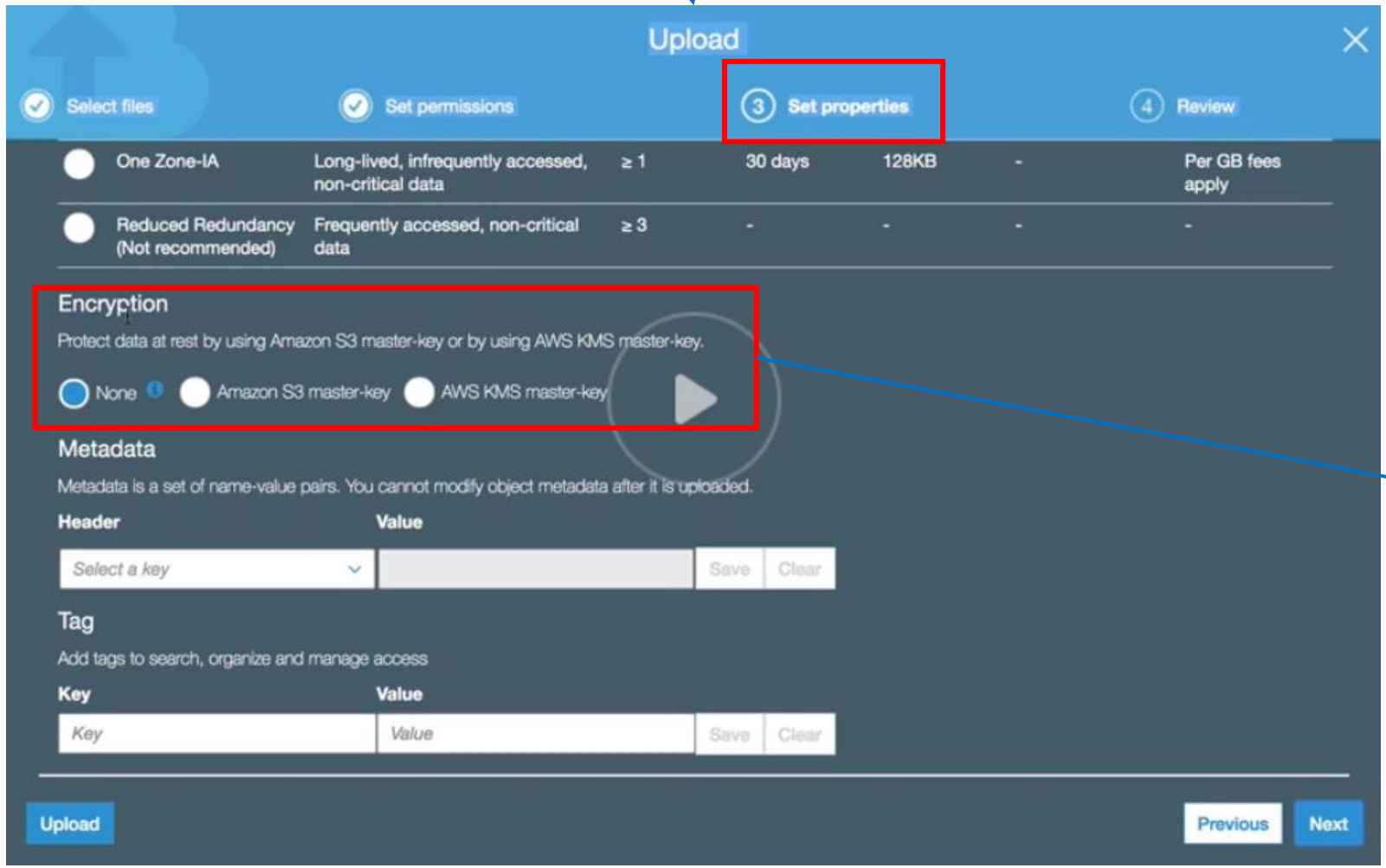
Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will **not be reflected in the policy generator tool.**

```
{
  "Id": "Policy1524656917361",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1524656913941",
      "Action": [
        "s3:PutObject"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::fayes-encrypted-files",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption": "aws:kms"
        }
      },
      "Principal": "*"
    }
  ]
}
```

Close

Testing the bucket policy added

bucket → Upload object / files



None – Forbidden error
Amazon s3 master-key – forbidden error
AWS KMS master key – file gets uploaded to s3

It works only for the specified encryption.
When we try to upload to the S3 bucket without specified encryption – we get forbidden error.