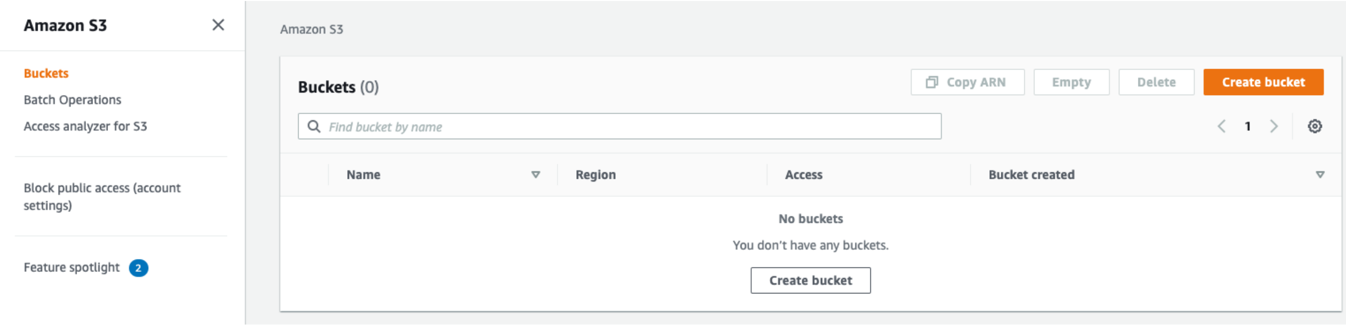
Part-1: Creating The Bucket

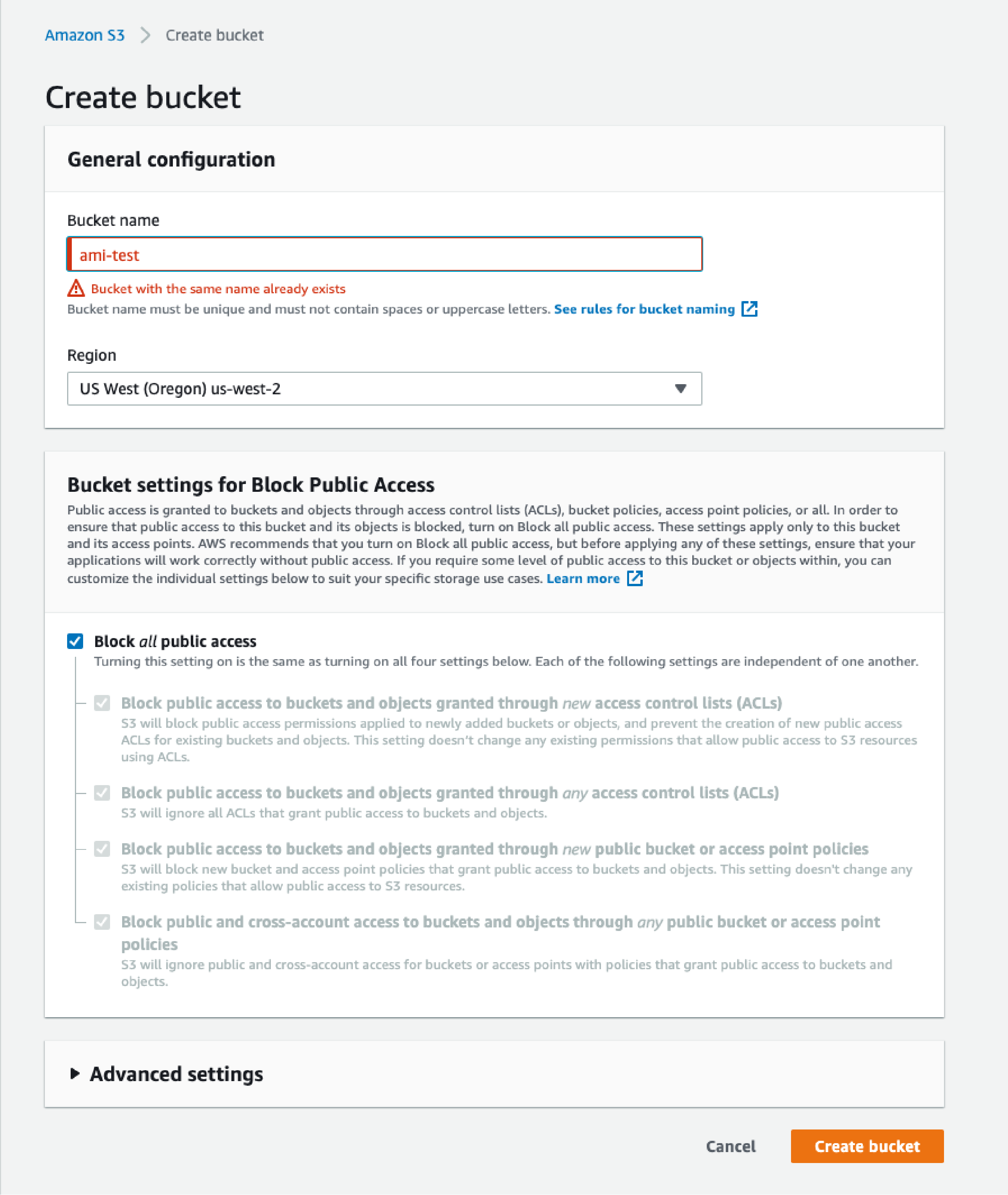
1. Log out of the root account user by clicking on the top right email next between the **Bell icon** and the **Global** dropdown menu
2. Log in to the console as the manager, using the information from you've got from the previous step
3. Navigate to the S3 console
4. Create a new bucket (remember that bucket names are globally unique across all AWS accounts)



Note that if a bucket name already exists you will get a warning.

Note:

Deleting a bucket takes time, so creating the same bucket name after a deletion would not allow you to create the bucket and will result in a "Bucket already exists error"



Amazon S3 > Create bucket

Create bucket

General configuration

Bucket name

ami-test

Bucket with the same name already exists

Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming

Region

US West (Oregon) us-west-2

Bucket settings for Block Public Access

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

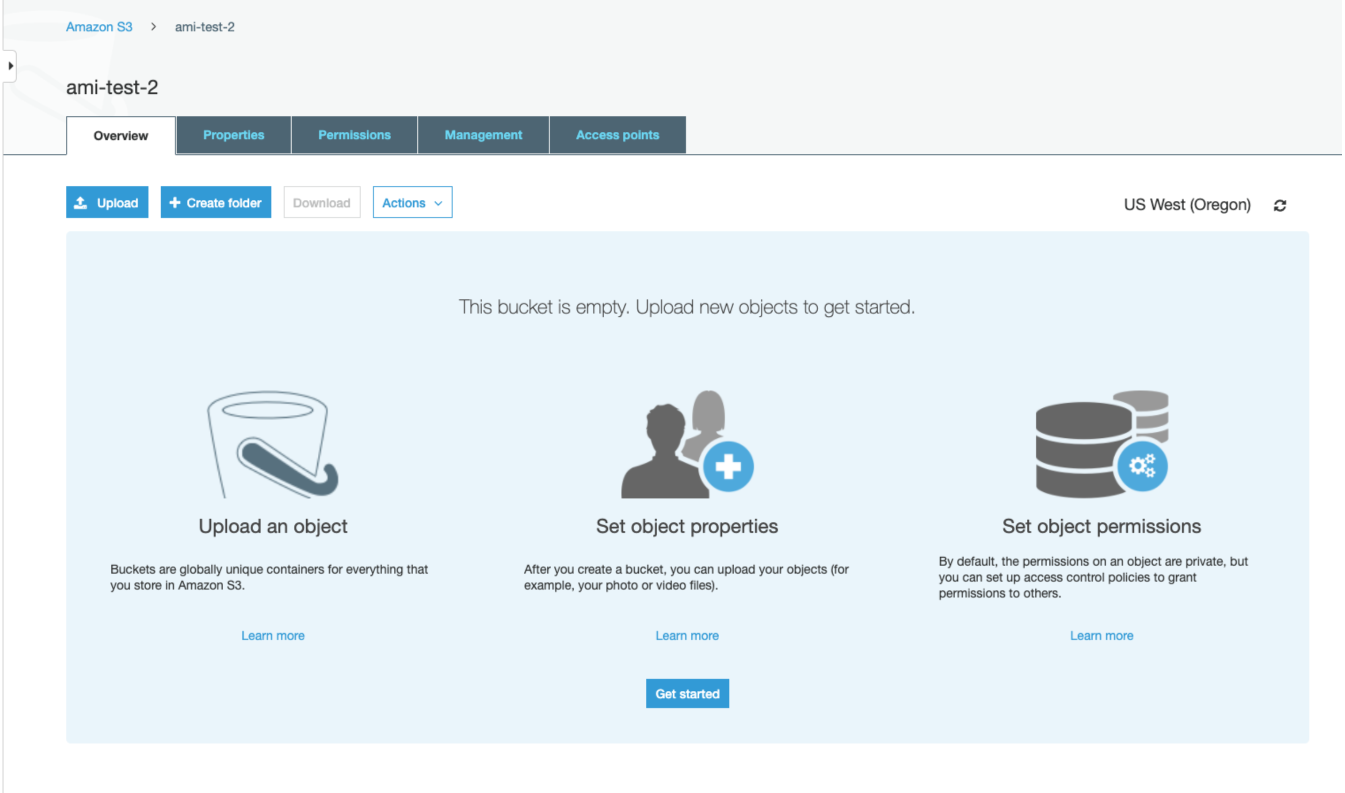
☑ Block *all* public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☑ Block public access to buckets and objects granted through *new* access control lists (ACLs)
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☑ Block public access to buckets and objects granted through *any* access control lists (ACLs)
  S3 will ignore all ACLs that grant public access to buckets and objects.
- ☑ Block public access to buckets and objects granted through *new* public bucket or access point policies
  S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☑ Block public and cross-account access to buckets and objects through *any* public bucket or access point policies
  S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

▶ Advanced settings

5. Once the bucket is created, click on the **Create folder** button to create a **manager** folder



This bucket is empty. Upload new objects to get started.

Upload an object

Buckets are globally unique containers for everything that you store in Amazon S3.

Learn more

Set object properties

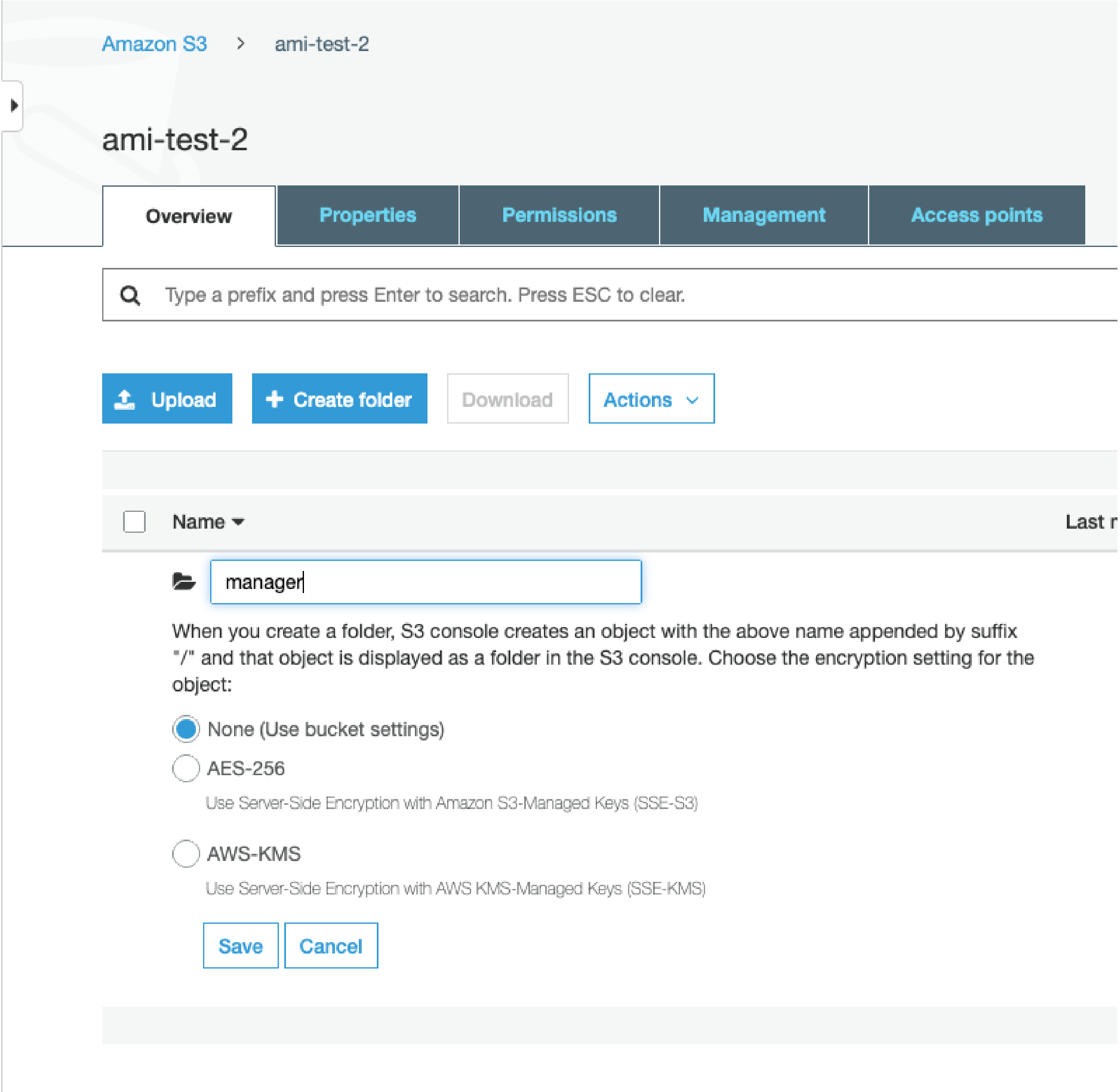
After you create a bucket, you can upload your objects (for example, your photo or video files).

Learn more

Set object permissions

By default, the permissions on an object are private, but you can set up access control policies to grant permissions to others.

Learn more



manager

When you create a folder, S3 console creates an object with the above name appended by suffix "/" and that object is displayed as a folder in the S3 console. Choose the encryption setting for the object:

● None (Use bucket settings)

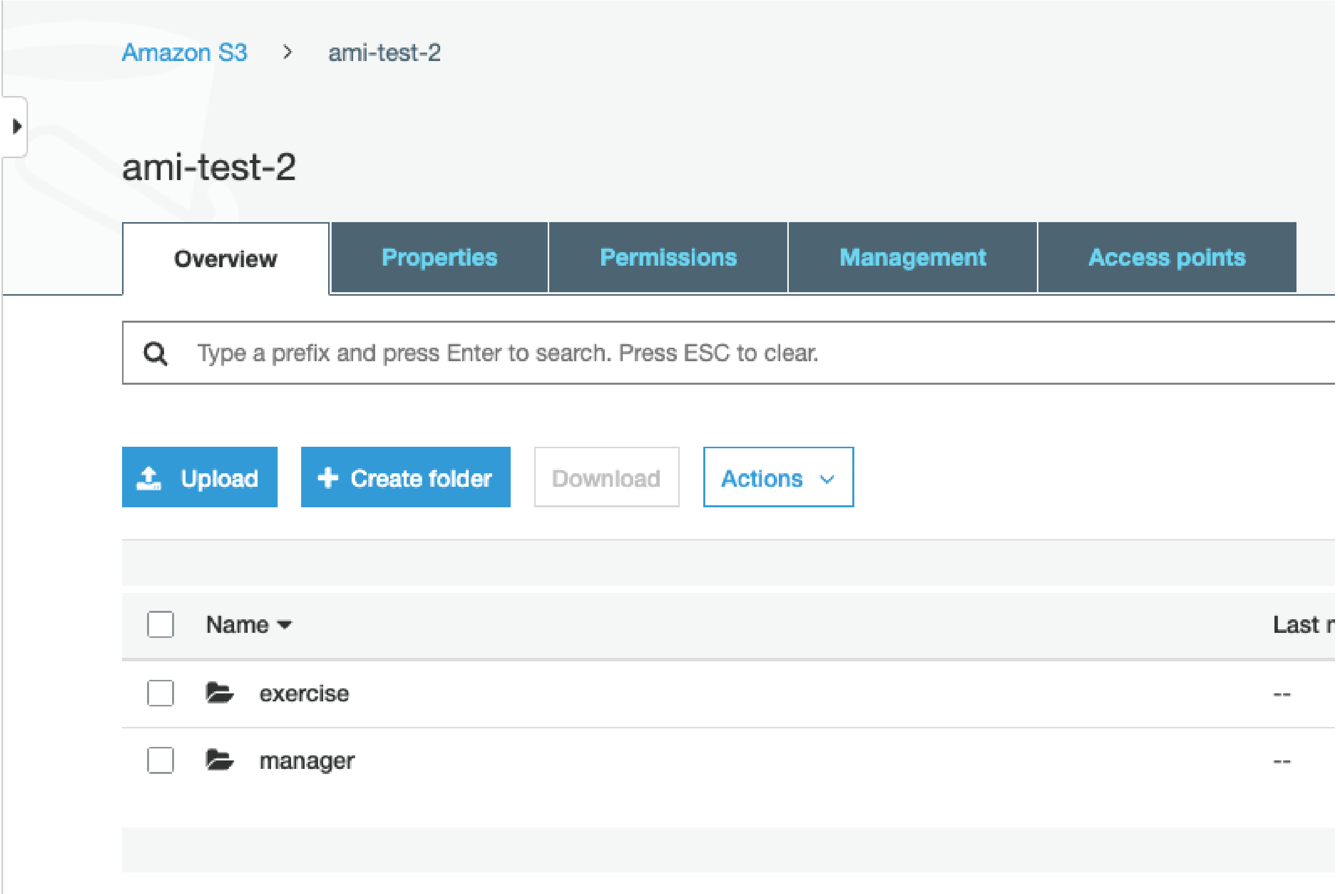
○ AES-256

Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

○ AWS-KMS

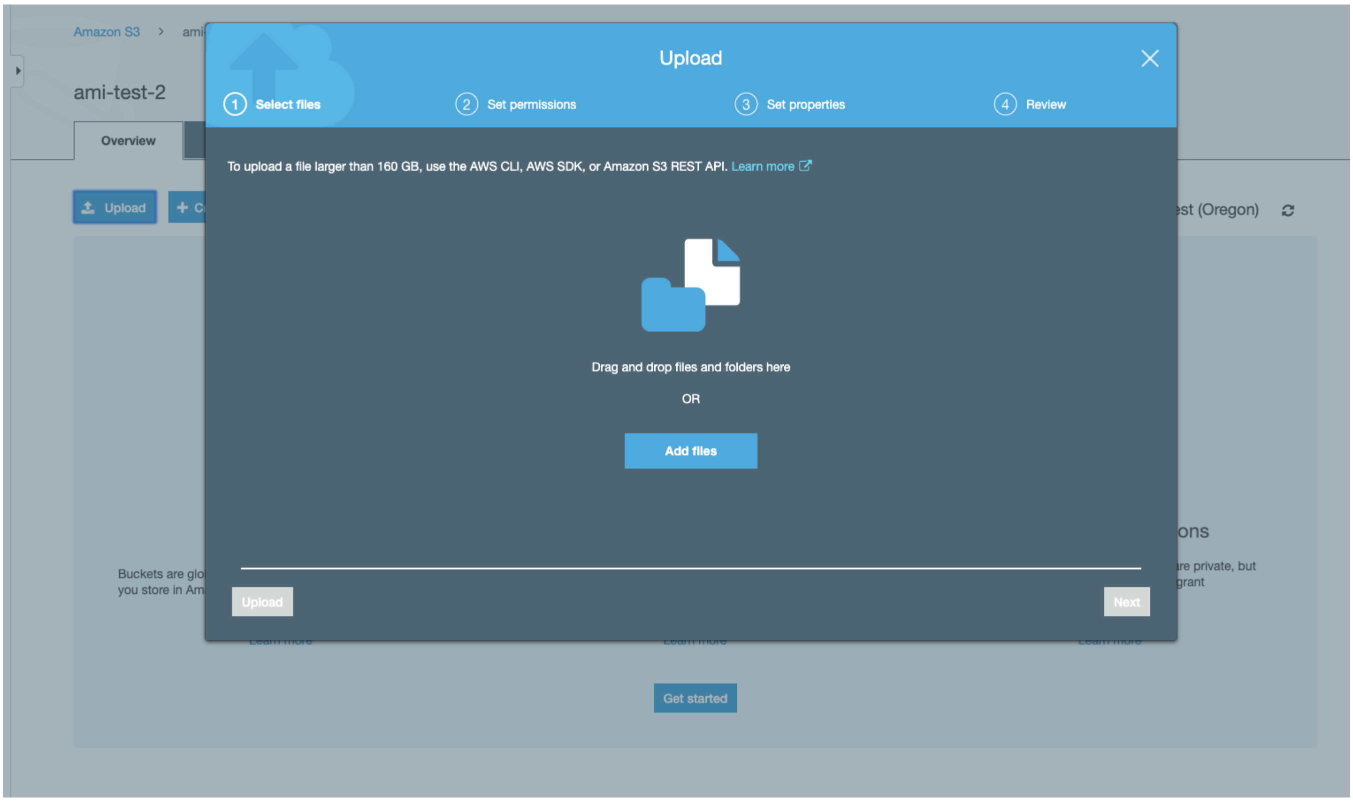
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

6. Create another folder called **exercise**



Type a prefix and press Enter to search. Press ESC to clear.

7. Click on the **exercise** folder to get into that folder
8. Click on the **Upload** button to upload a file (any file) into that folder

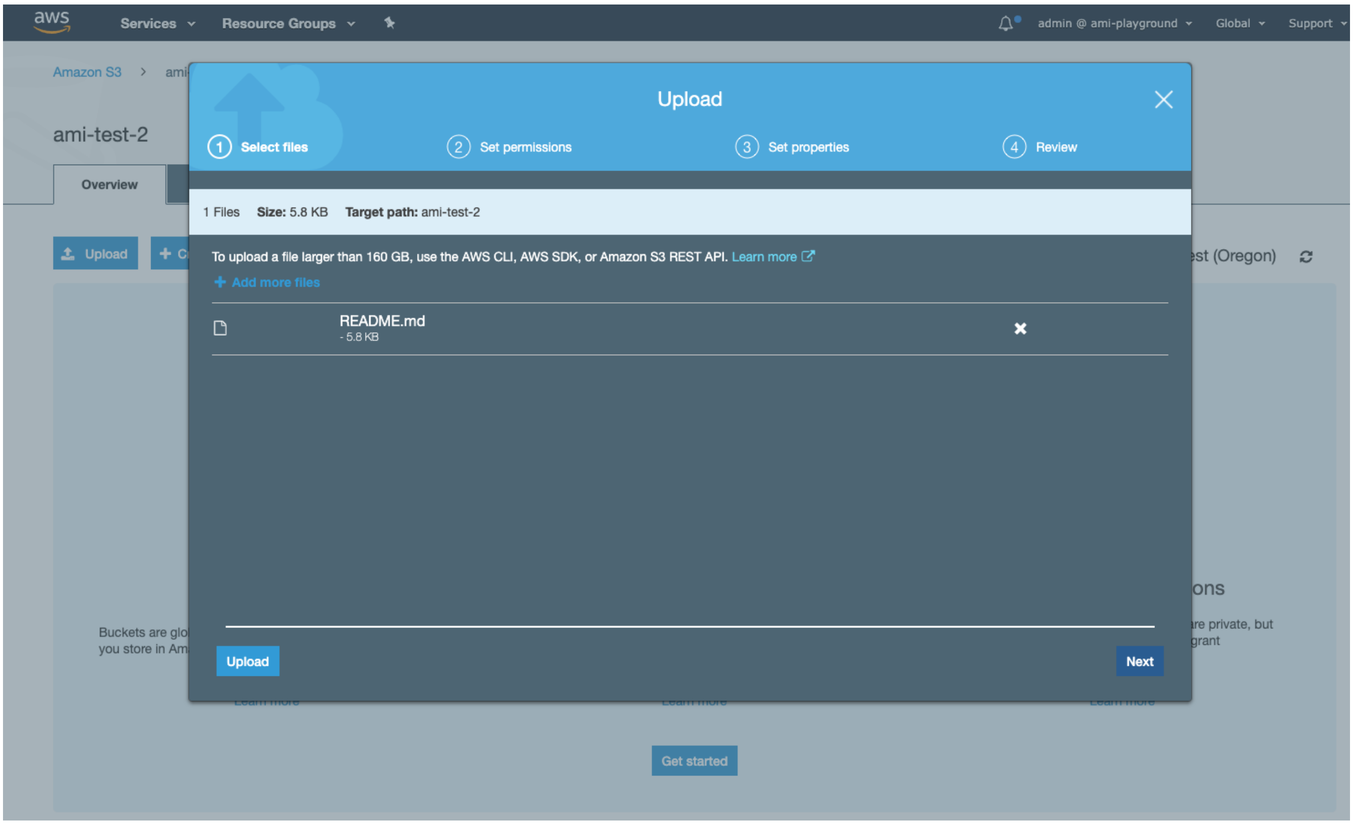


To upload a file larger than 160 GB, use the AWS CLI, AWS SDK, or Amazon S3 REST API. Learn more

Drag and drop files and folders here

OR

9. Either drag and drop a file onto the window or click the **Add files** button to start the upload process

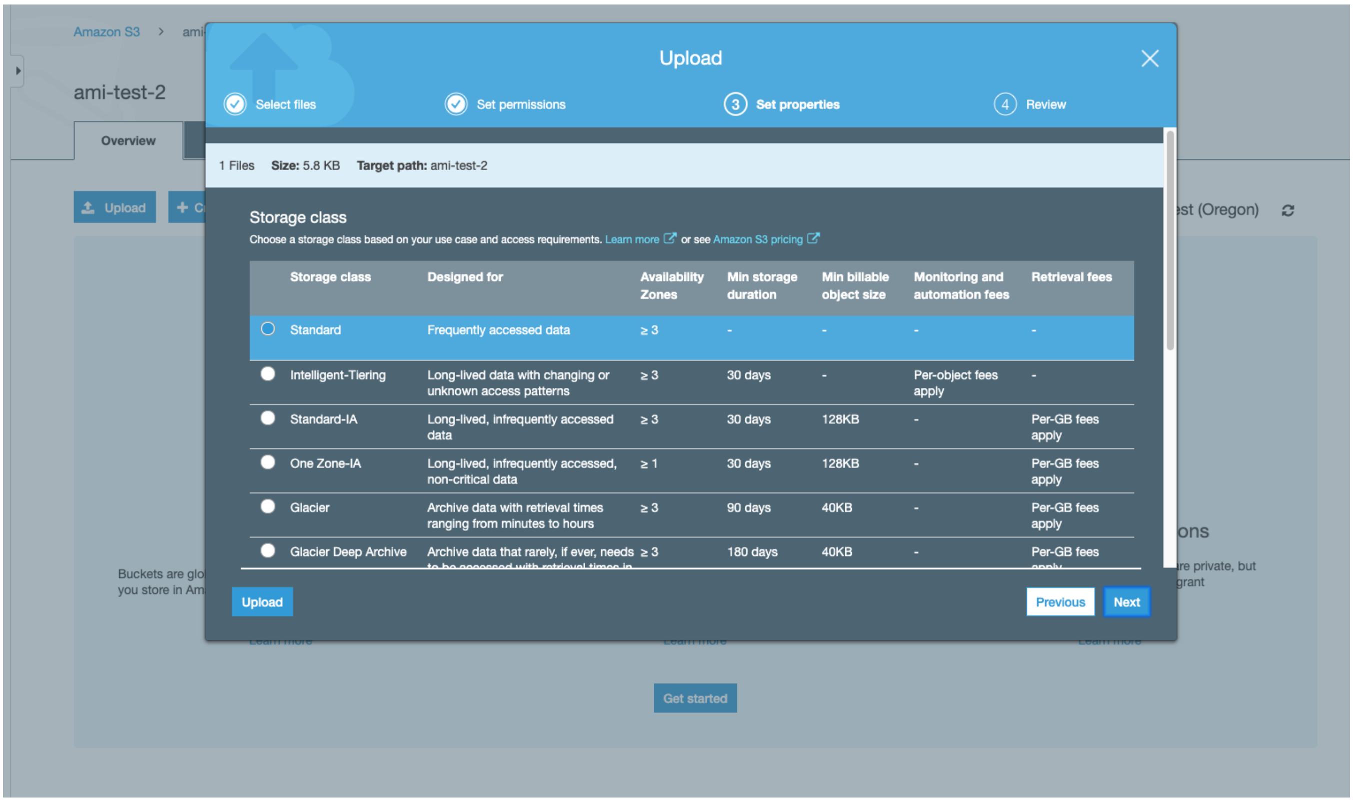


1 Files **Size:** 5.8 KB **Target path:** ami-test-2

To upload a file larger than 160 GB, use the AWS CLI, AWS SDK, or Amazon S3 REST API. Learn more

README.md
- 5.8 KB

10. Click the **Next** button to see the list of default permissions for this file (we will use IAM permission to access it rather than resource permissions)
11. Click Next to see the S3 storage classes, and leave the default **Standard** class selected



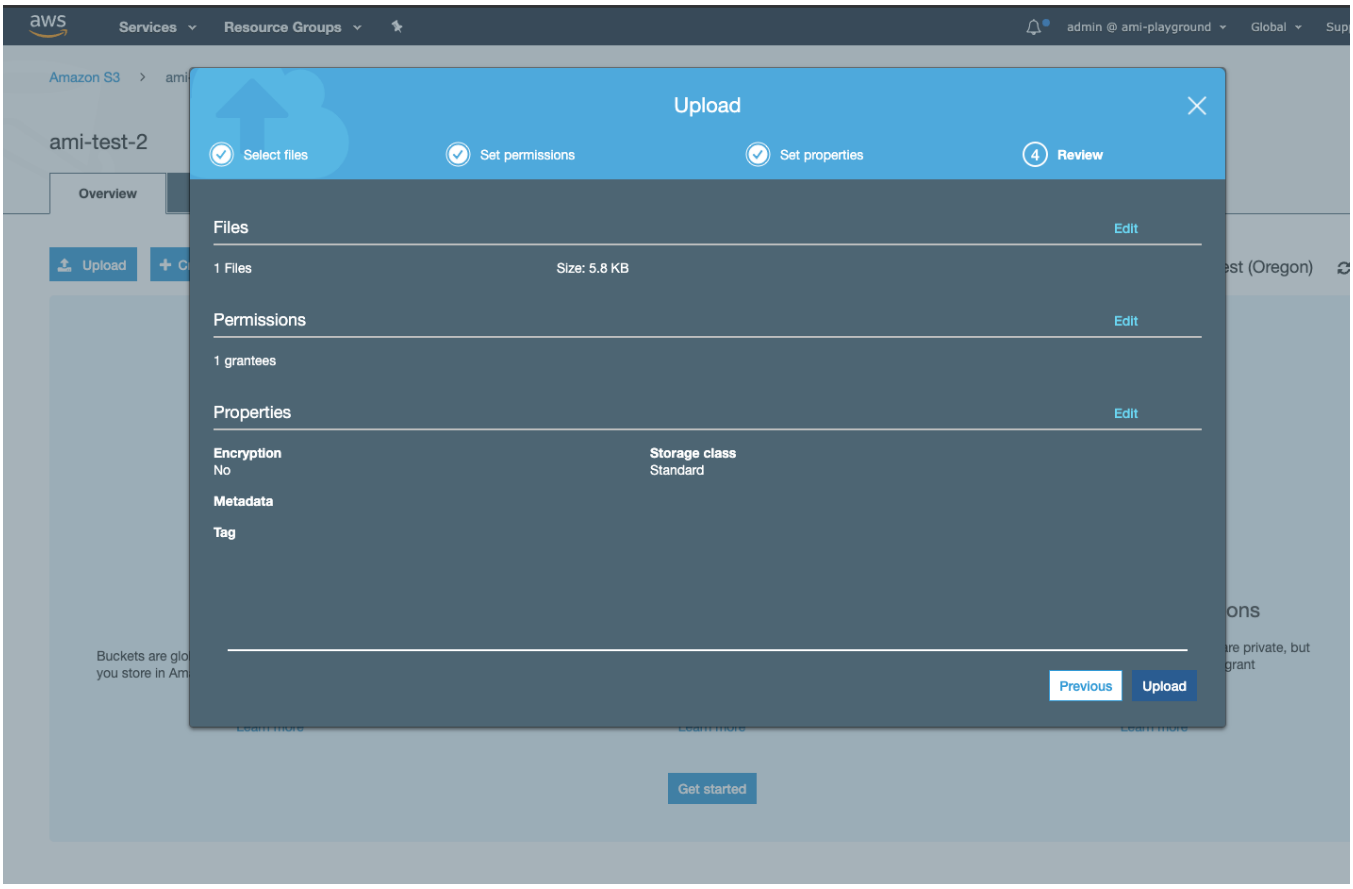
1 Files **Size:** 5.8 KB **Target path:** ami-test-2

Storage class

Choose a storage class based on your use case and access requirements. Learn more or see Amazon S3 pricing

	Storage class	Designed for	Availability Zones	Min storage duration	Min billable object size	Monitoring and automation fees	Retrieval fees
●	Standard	Frequently accessed data	≥ 3	-	-	-	-
○	Intelligent-Tiering	Long-lived data with changing or unknown access patterns	≥ 3	30 days	-	Per-object fees apply	-
○	Standard-IA	Long-lived, infrequently accessed data	≥ 3	30 days	128KB	-	Per-GB fees apply
○	One Zone-IA	Long-lived, infrequently accessed, non-critical data	≥ 1	30 days	128KB	-	Per-GB fees apply
○	Glacier	Archive data with retrieval times ranging from minutes to hours	≥ 3	90 days	40KB	-	Per-GB fees apply
○	Glacier Deep Archive	Archive data that rarely, if ever, needs	≥ 3	180 days	40KB	-	Per-GB fees

12. Click the **Upload** button to start the upload.



Files Edit

1 Files Size: 5.8 KB

Permissions Edit

1 grantees

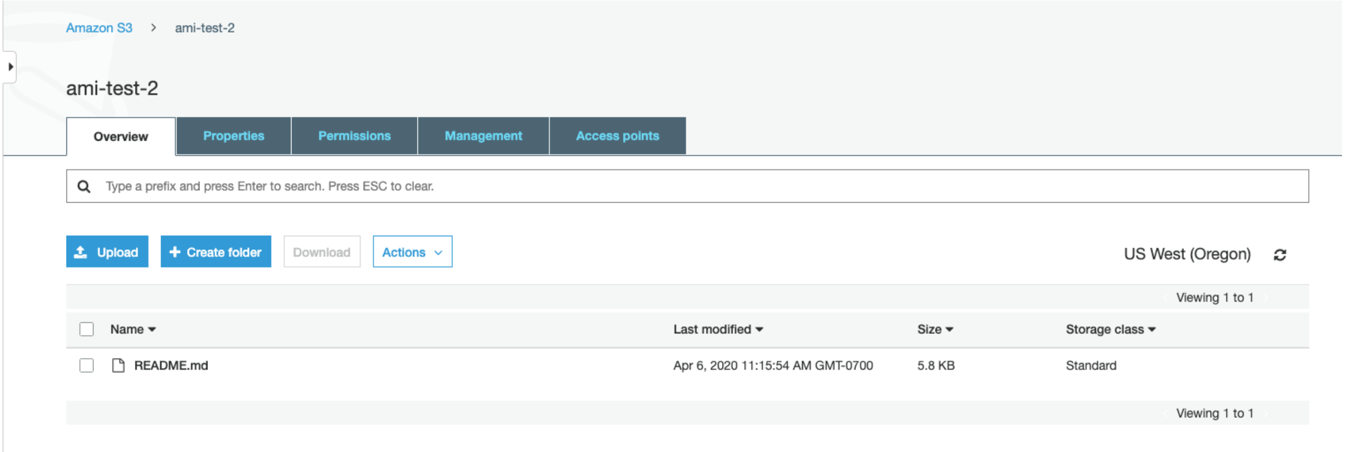
Properties Edit

Encryption: No

Storage class: Standard

Metadata

Tag



Viewing 1 to 1

Name	Last modified	Size	Storage class
README.md	Apr 6, 2020 11:15:54 AM GMT-0700	5.8 KB	Standard

Viewing 1 to 1