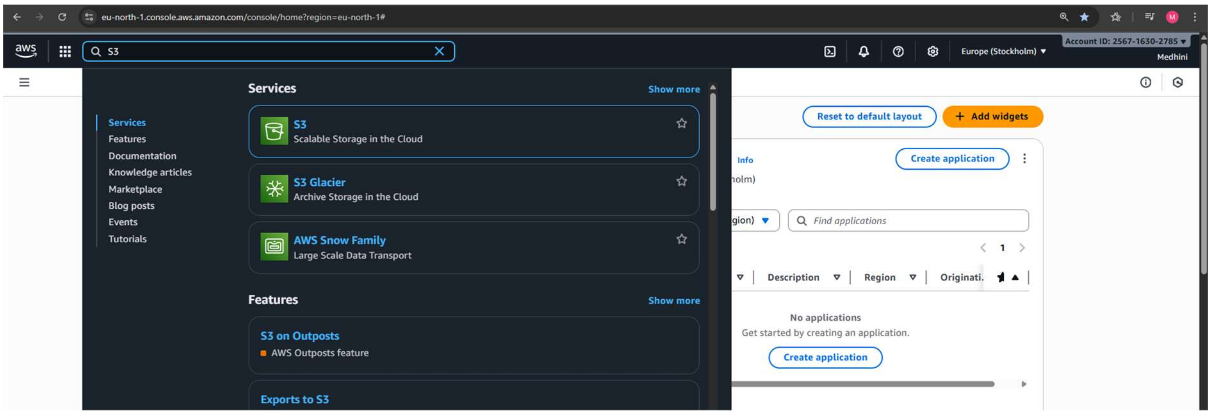
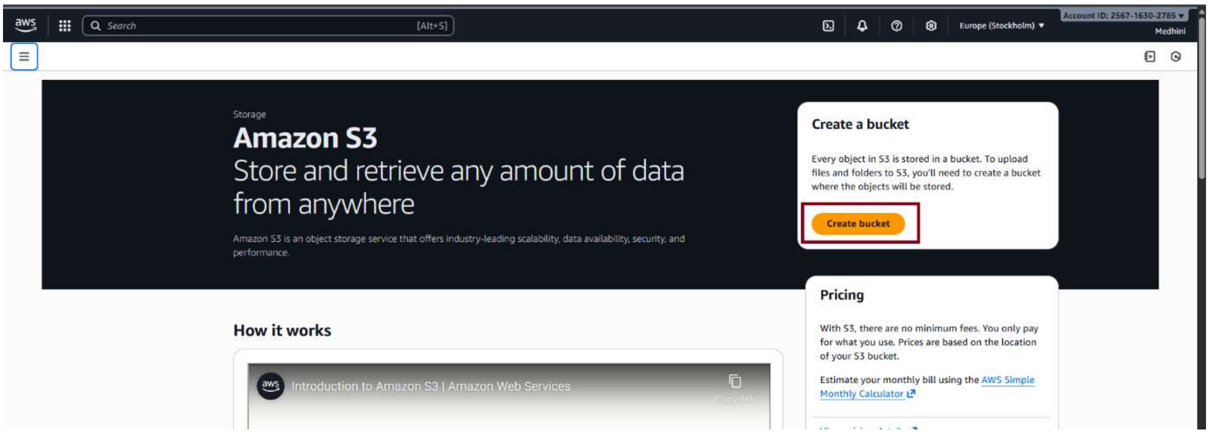
S3 Bucket Creation

Step 1: Login to account, Search for S3 as shown in below picture and click on **“S3”**



Step 2: Click on **“Create Bucket”**


Search
[Alt+S]
Europe (Stockholm)
Account ID: 2567-1630-2785
Medhini
Storage
Amazon S3
Store and retrieve any amount of data from anywhere
Create a bucket
Create bucket
Pricing
How it works
Introduction to Amazon S3 | Amazon Web Services
Copy link

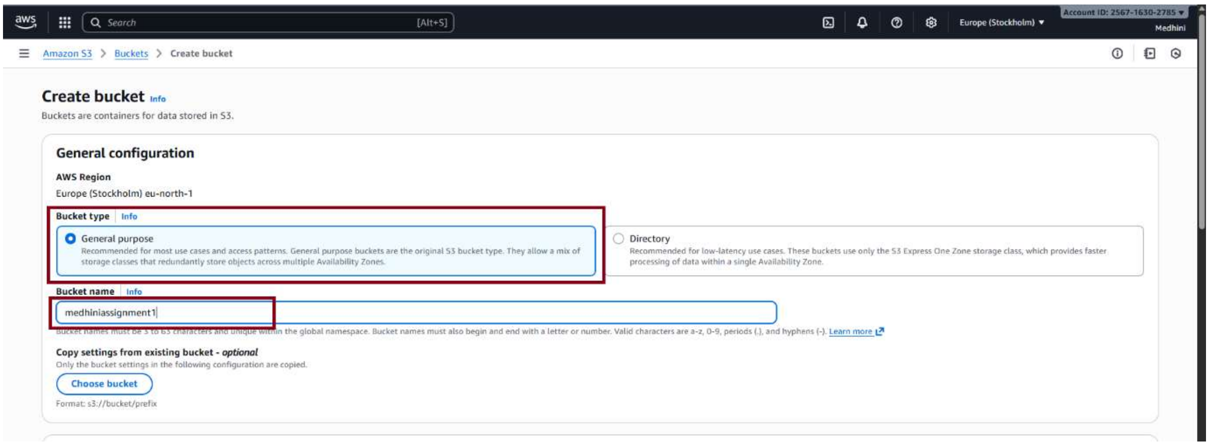
Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the AWS Simple Monthly Calculator

Step 3: Select **“General Purpose”** and give Unique name for S3 bucket. There will be no same name for S3 bucket across the whole world. Name should be Unique.


Search
[Alt+S]
Europe (Stockholm)
Account ID: 2567-1630-2785
Medhini
Amazon S3 > Buckets > Create bucket
Info
Choose bucket

Create bucket

Buckets are containers for data stored in S3.

General configuration

AWS Region: Europe (Stockholm) eu-north-1

Bucket type

● General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

○ Directory
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name: medhiniassignment1

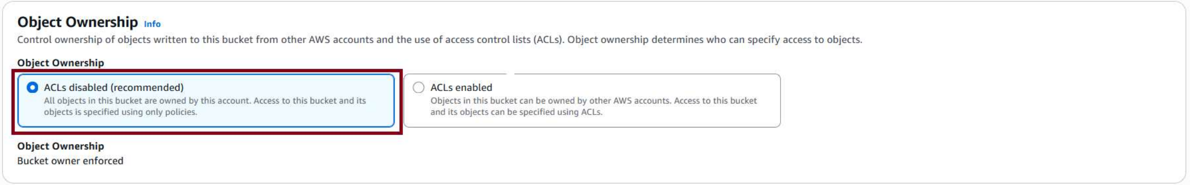
Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). Learn more

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

Step 4: Object ownership – This control who owns the uploaded file. (if ACL enabled it will allow object to have different owners to control files.)



Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

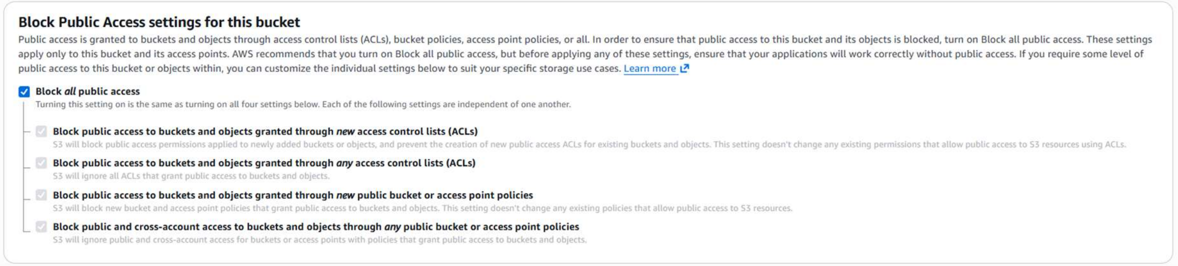
Object Ownership

● ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

○ ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership
Bucket owner enforced

Step 5: As per the assignment the object should have public access.



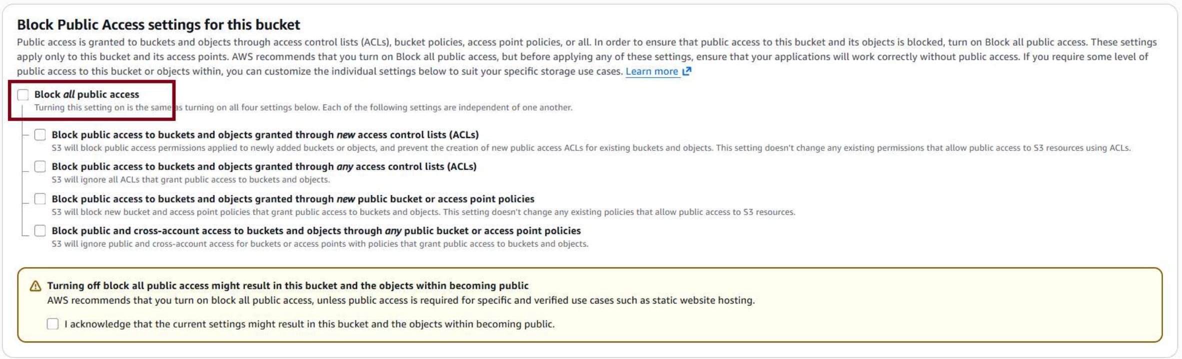
Block Public Access settings for this bucket

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.

So, uncheck the below marked **"Public access"** *it will allow object public later* still it is not accessible.



Block Public Access settings for this bucket

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

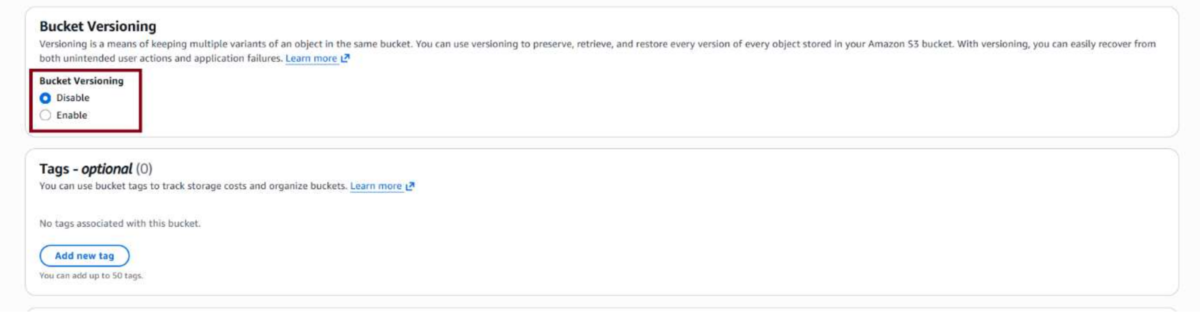
□ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- □ **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.

⚠ **Turning off block all public access might result in this bucket and the objects within becoming public**
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

□ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Step 6: Versioning will allow you to have multiple version of the object exist in the same bucket. For now, Click on **"Disable"**



Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning
● Disable
○ Enable

Tags - *optional* (0)

You can use bucket tags to track storage costs and organize buckets. Learn more

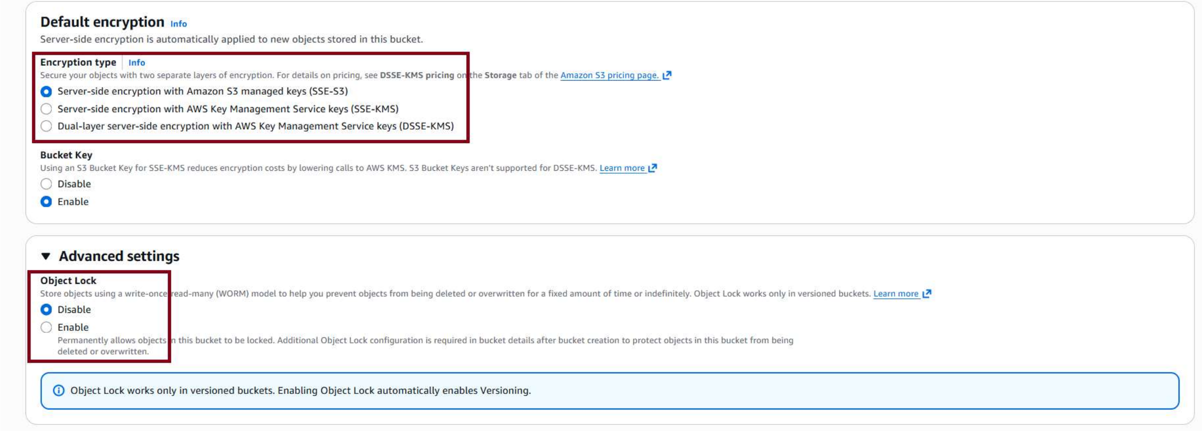
No tags associated with this bucket.

Add new tag

You can add up to 50 tags.

Step 7: Choose "**Default encryption"** and **"Object lock"** a shown in below picture

Assignment S3 - Bucket Creation and Upload 5 different extension files



Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type | Info

Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

- ● Server-side encryption with Amazon S3 managed keys (SSE-S3)
- ○ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- ○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more

- ○ Disable
- ● Enable

Advanced settings

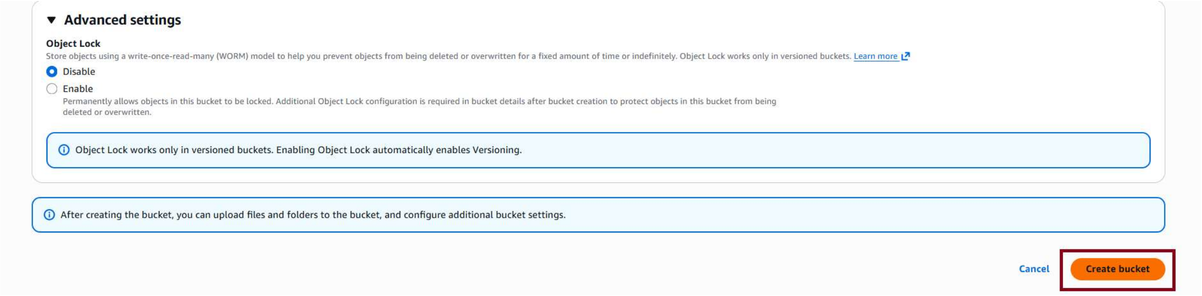
Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. Learn more

- ● Disable
- ○ Enable
  Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Versioning.

Step 8: Click on **"Create Bucket"**



Advanced settings

Object Lock

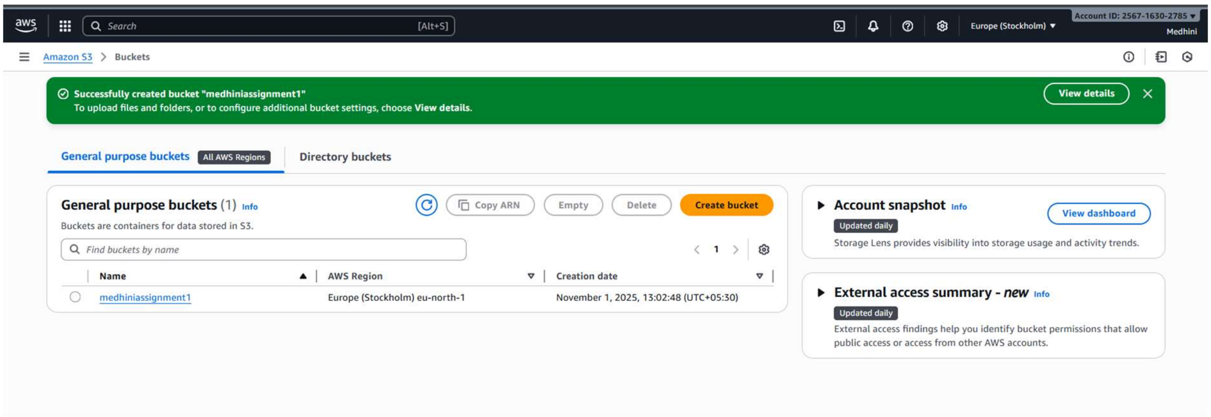
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. Learn more

- ● Disable
- ○ Enable
  Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Versioning.

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Step 9: The bucket is created as shown in below picture



Successfully created bucket "medhiniassignment1"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

General purpose buckets (1) Info

Buckets are containers for data stored in S3.

Name	AWS Region	Creation date
medhiniassignment1	Europe (Stockholm) eu-north-1	November 1, 2025, 13:02:48 (UTC+05:30)

Account snapshot Info

Updated daily

Storage Lens provides visibility into storage usage and activity trends.

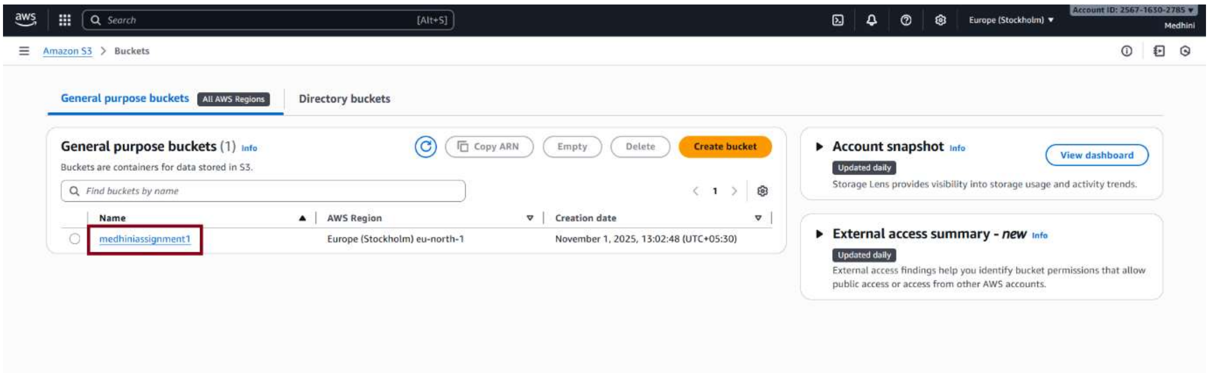
External access summary - *new* Info

Updated daily

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

Upload 5 different types of different file extensions

Step 1: Click on **"Created Bucket"**



General purpose buckets (1) Info

Buckets are containers for data stored in S3.

Name	AWS Region	Creation date
medhiniassignment1	Europe (Stockholm) eu-north-1	November 1, 2025, 13:02:48 (UTC+05:30)

Account snapshot Info

Updated daily

Storage Lens provides visibility into storage usage and activity trends.

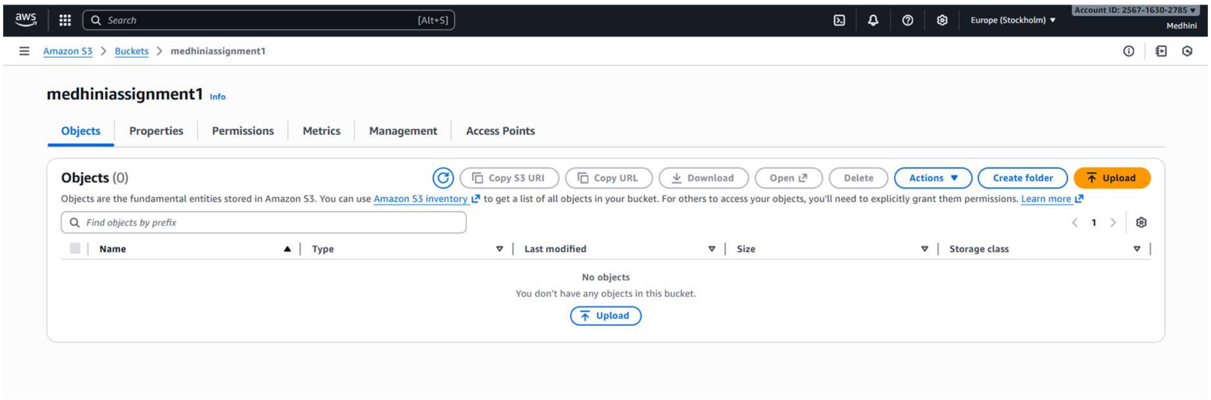
External access summary - *new* Info

Updated daily

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

Assignment S3 - Bucket Creation and Upload 5 different extension files

Step 2: Upload 5 different files here



medhiniassignment1 Info

Objects (0)

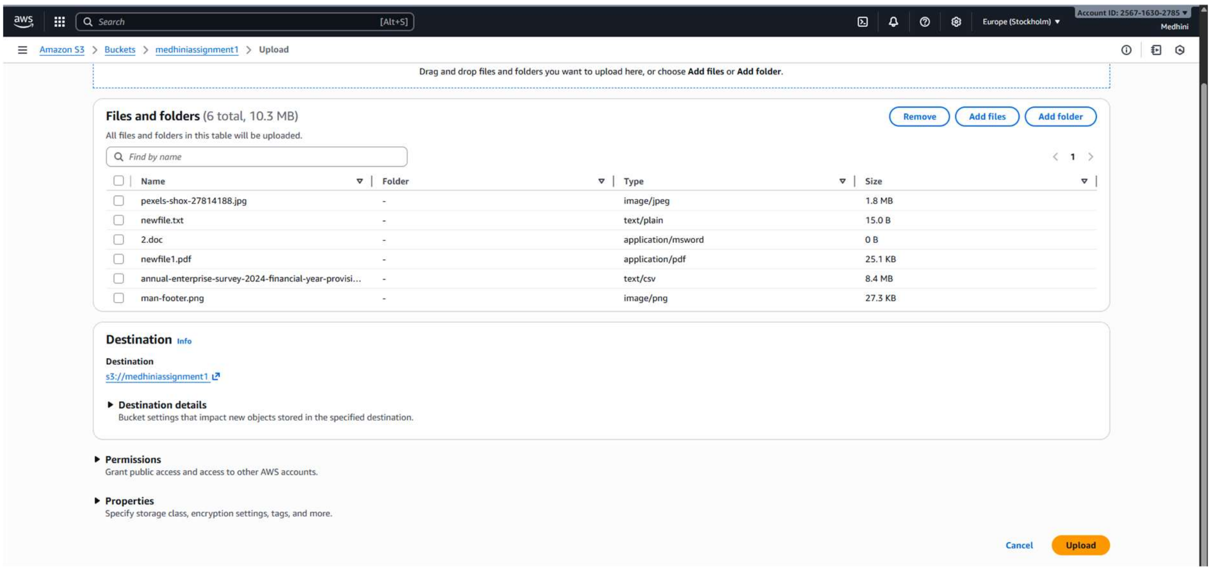
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Name	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.

Uploaded different files and click on **"Upload"** at the bottom right



Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (6 total, 10.3 MB)

All files and folders in this table will be uploaded.

	Name	Folder	Type	Size
□	pexels-shox-27814188.jpg	-	image/jpeg	1.8 MB
□	newfile.txt	-	text/plain	15.0 B
□	2.doc	-	application/msword	0 B
□	newfile1.pdf	-	application/pdf	25.1 KB
□	annual-enterprise-survey-2024-financial-year-provisi...	-	text/csv	8.4 MB
□	man-footer.png	-	image/png	27.3 KB

Destination Info

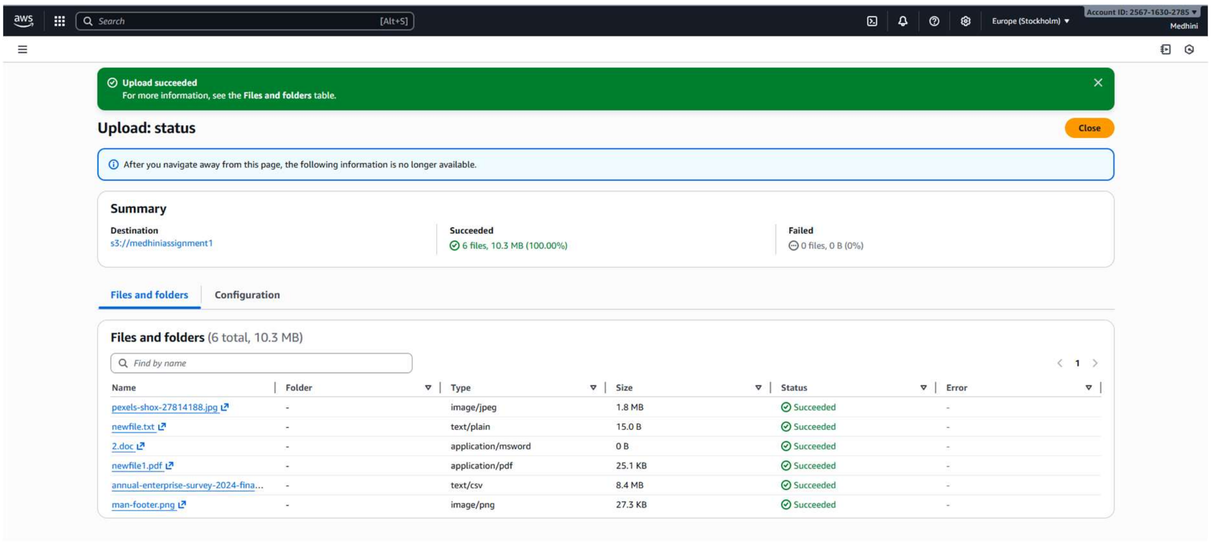
Destination
s3://medhiniassignment1

▸ **Destination details**
Bucket settings that impact new objects stored in the specified destination.

▸ **Permissions**
Grant public access and access to other AWS accounts.

▸ **Properties**
Specify storage class, encryption settings, tags, and more.

Upload is successful



Upload succeeded
For more information, see the **Files and folders** table.

Upload: status

After you navigate away from this page, the following information is no longer available.

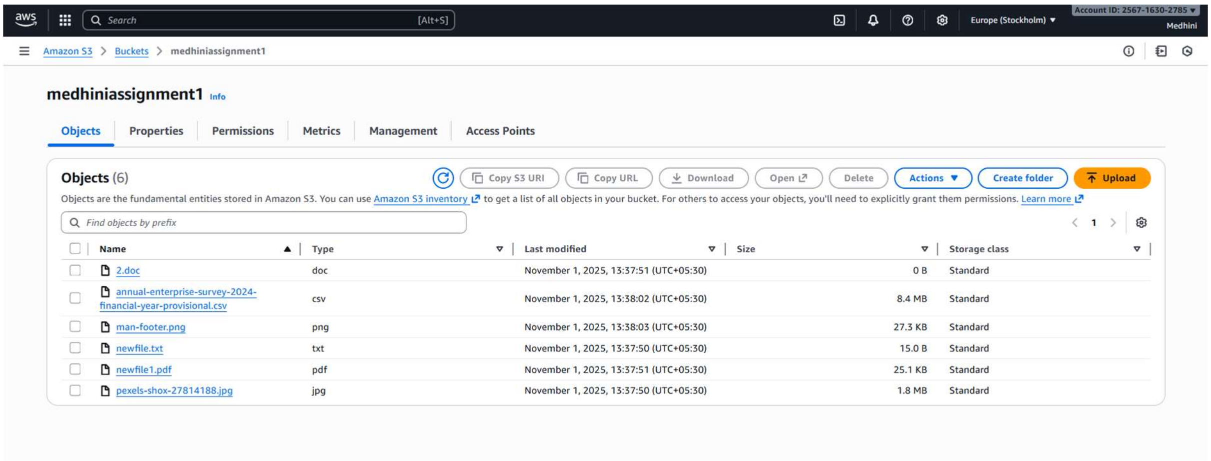
Summary

Destination	Succeeded	Failed
s3://medhiniassignment1	6 files, 10.3 MB (100.00%)	0 files, 0 B (0%)

Files and folders (6 total, 10.3 MB)

Name	Folder	Type	Size	Status	Error
pexels-shox-27814188.jpg	-	image/jpeg	1.8 MB	✓ Succeeded	-
newfile.txt	-	text/plain	15.0 B	✓ Succeeded	-
2.doc	-	application/msword	0 B	✓ Succeeded	-
newfile1.pdf	-	application/pdf	25.1 KB	✓ Succeeded	-
annual-enterprise-survey-2024-fina...	-	text/csv	8.4 MB	✓ Succeeded	-
man-footer.png	-	image/png	27.3 KB	✓ Succeeded	-

Assignment S3 - Bucket Creation and Upload 5 different extension files



aws
Search [Alt+S]
Europe (Stockholm)
Account ID: 2567-1630-2785
Medhini
Amazon S3 > Buckets > medhiniassignment1

medhiniassignment1 Info

Objects | Properties | Permissions | Metrics | Management | Access Points

Objects (6)

Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name	Type	Last modified	Size	Storage class
□	2.doc	doc	November 1, 2025, 13:37:51 (UTC+05:30)	0 B	Standard
□	annual-enterprise-survey-2024-financial-year-provisional.csv	csv	November 1, 2025, 13:38:02 (UTC+05:30)	8.4 MB	Standard
□	man-footer.png	png	November 1, 2025, 13:38:03 (UTC+05:30)	27.3 KB	Standard
□	newfile.txt	txt	November 1, 2025, 13:37:50 (UTC+05:30)	15.0 B	Standard
□	newfile1.pdf	pdf	November 1, 2025, 13:37:51 (UTC+05:30)	25.1 KB	Standard
□	pexels-shox-27814188.jpg	jpg	November 1, 2025, 13:37:50 (UTC+05:30)	1.8 MB	Standard