

Shaikh Ateeb Ahmed

11-08-2025

Image Hosting and Website Setup with AWS S3

Create the bucket

Console: **S3** → **Buckets** → **Create bucket**.

Bucket type: General purpose

Bucket name: type a globally unique name (e.g. my-Ateeb02).

Under Object Ownership: Keep ACLs disabled (recommended).

Block all public access → **ON** (it's default).

Leave versioning Disabled.

No tags.

Default encryption: SSE-S3 (default).

Leave all other options at their **default** values (do not enable any special options).

Click **Create bucket**.

Shaikh Ateeb Ahmed

11-08-2025

Create bucket [info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region
Asia Pacific (Mumbai) ap-south-1

Bucket type [info](#)

☒ **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 [info](#)

my-Ateeb02

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.

[Choose bucket](#)

Format: s3://bucket/prefix

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.

☒ **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

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 revoke public access permissions assigned 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 bucket or object permissions to 18 reserved using ACLs.

☒ **Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will revoke 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 grant public and cross-account access to buckets or objects only when policies that grant public access to buckets and objects.

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.

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 [DISE-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

[After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.](#)

[Cancel](#) [Create bucket](#)

Upload an image

Click your newly created bucket in the bucket list.

Click **Upload** → **Add files** → select the image file from your machine → **Upload**.

After upload, click the uploaded object in the bucket list to view its **Overview**.

Account ID: 6180-9181-6802

Shahin Ateeb Ahmed

you_are_being_monitored-wallpaper-1920x1080.jpg

Copy S3 URI

Download

Open

Object actions

Properties

Permissions

Versions

Object overview

Owner

625694907cd535681dfc4652309e2e1b85c91e4c8497ed9264893f806a7bf22

AWS Region

Asia Pacific (Mumbai) ap-south-1

Last modified

September 6, 2025, 12:45:52 (UTC+05:30)

Size

832.5 KB

Type

JPG

Key

you_are_being_monitored-wallpaper-1920x1080.jpg

S3 URI

s3://my-ateeb02/you_are_being_monitored-wallpaper-1920x1080.jpg

Amazon Resource Name (ARN)

arn:aws:s3::my-ateeb02/you_are_being_monitored-wallpaper-1920x1080.jpg

Entity tag (ETag)

9370d6c3a1477840ff505e675875ce58

Object URL

https://my-ateeb02.s3.ap-south-1.amazonaws.com/you_are_being_monitored-wallpaper-1920x1080.jpg

Object management overview

The following bucket properties and object management configurations impact the behavior of this object.

Bucket properties

Bucket Versioning

When enabled, multiple variants of an object can be stored in the bucket to easily recover from unintended user actions and application failures.

Disabled

Enable Bucket Versioning

Management configurations

Replication status

When a replication rule is applied to an object the replication status indicates the progress of the operation.

View replication rules

Expiration date

The object will be permanently deleted on this date.

Storage class

Amazon S3 offers a range of storage classes designed for different use cases. [Learn more](#) or see [Amazon S3 pricing](#)

Standard

Edit

Server-side encryption settings

Server-side encryption protects data at rest.

Encryption type: Server-side encryption with Amazon S3 managed keys (SSE-S3)

Edit

Checksums

Checksums are used for data integrity verification of new objects. [Learn more](#)

Checksum function

CRC32C

Checksum type

Full object

Checksum value

LF3JUM7M46M+

Tags (0)

Track storage cost of other criteria by tagging your objects. [Learn more](#)

Key

Value

No tags associated with this resource.

Edit

Metadata (1)

Metadata is optional information provided as a name-value (key-value) pair. [Learn more](#)

Type

Key

Value

System defined

Content-Type

image/png

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](#)

Object Lock

Disabled

This bucket doesn't have Object Lock enabled. You can enable Object Lock for a versioned bucket under the bucket's [properties](#) tab. [Learn more](#)

Edit Object Lock

Shaikh Ateeb Ahmed

11-08-2025

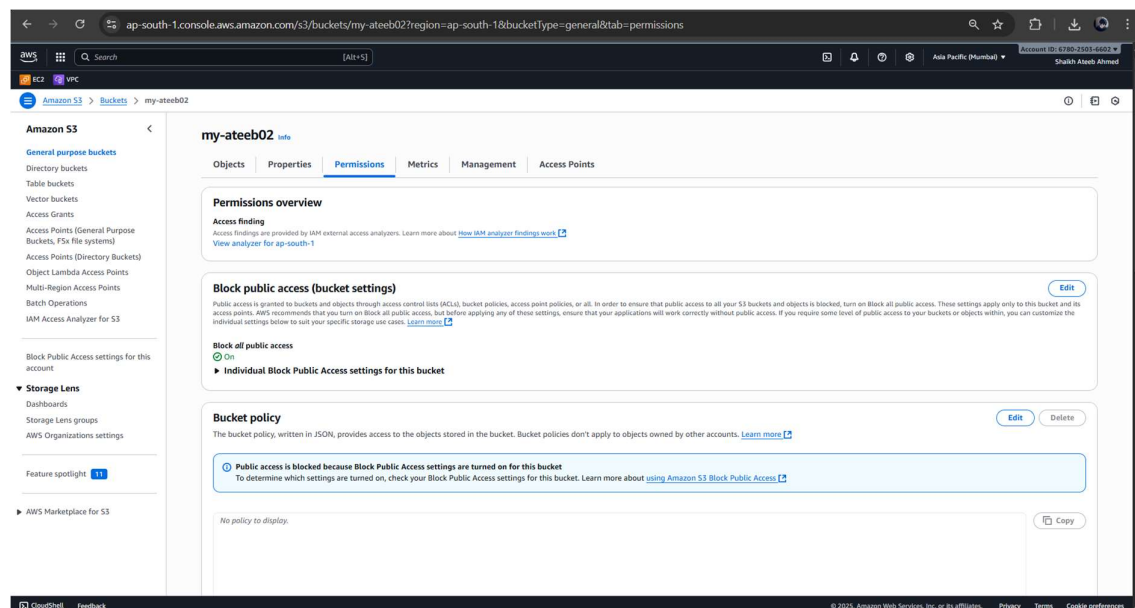
Copy or click **Object URL** (this is the S3 object link shown in the object overview). If the bucket is private (default), opening this URL in a browser will show **Access Denied**. (This is expected).



Turn off bucket Block Public Access (bucket-level)

AWS sets Block Public Access to prevent accidental public exposure. It can override bucket policies and object ACLs.

In the bucket page, open **Permissions** → **Block public access (bucket settings)**.

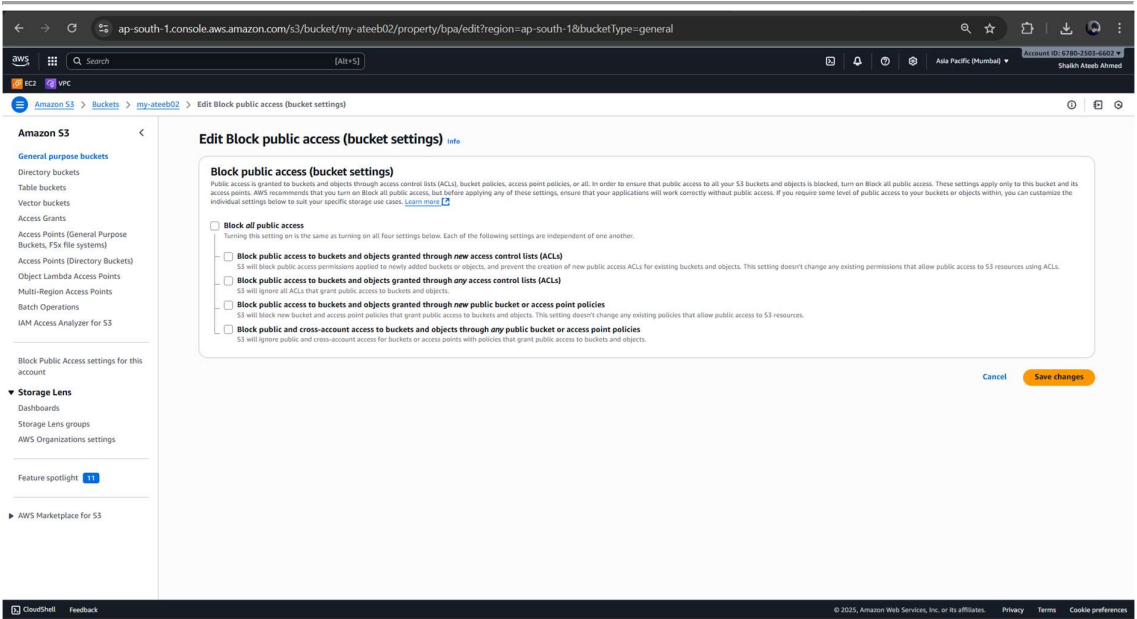


Click **Edit**.

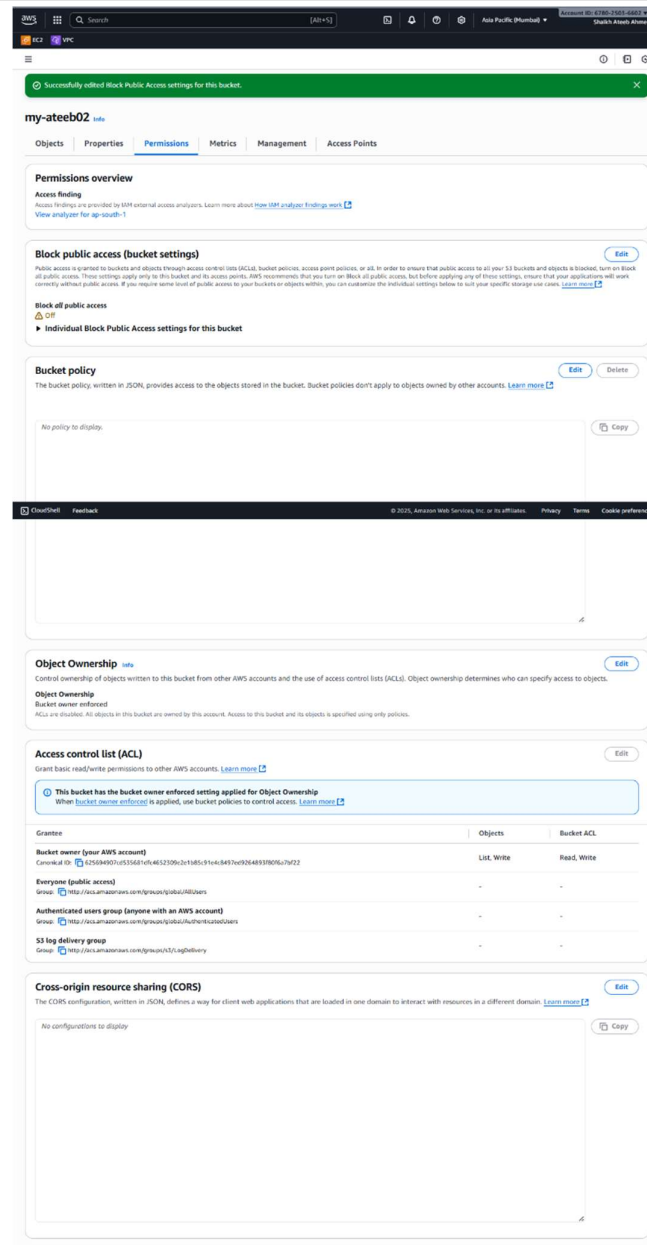
Uncheck all the checkboxes (i.e., disable the block settings for this bucket).

Shaikh Ateeb Ahmed

11-08-2025



Click **Save changes**, then **Confirm** in the popup.



If the console refuses or you see a message that account-level Block Public Access is preventing changes, you must also edit **Block Public Access settings for this account** (S3 console → left menu → *Block Public Access settings for this account* → Edit → adjust as needed).

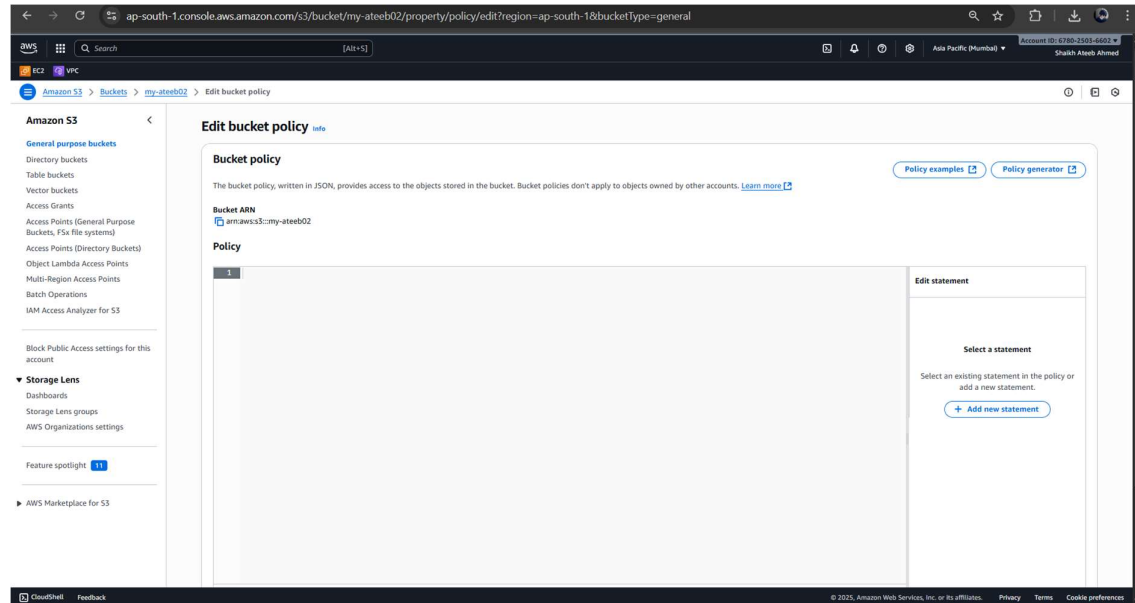
Shaikh Ateeb Ahmed

11-08-2025

Create a public bucket policy using the Policy Generator

Still in the bucket: go to **Permissions** → **Bucket policy** → **Edit**.

Click **Policy generator** (link/button in the console opens the AWS Policy Generator).



In the Policy Generator:

Type of policy: S3 Bucket Policy (or S3 depending on the generator UI).

Add Statement:

Effect: Allow

Principal: * (makes objects readable by anyone)

Action: pick **GetObject**

Amazon Resource Name (ARN): arn:aws:s3:::YOUR_BUCKET_NAME/* (replace YOUR_BUCKET_NAME with your actual bucket name and **include /*** at the end to allow access to *objects* inside the bucket (not the bucket itself)).

aws

Browser Default

AWS

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, [key concepts in Using AWS Identity and Access Management](#).

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](#).

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.

Actions

All Actions ("*")

--Select Actions--

Amazon Resource Name (ARN)

All Resources ("*")

ARN should follow the following format: arn:aws:s3:::{BucketName}/{KeyName}. Use a comma to separate multiple values.

► Add conditions (optional)

Add Statement

Statements added (1)

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource(s)	Condition(s)	Remove
*	Allow	s3:GetObject	arn:aws:s3:::my-ateeb02/*	None	Remove

Step 3: Generate policy

A policy is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

Generate Policy

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

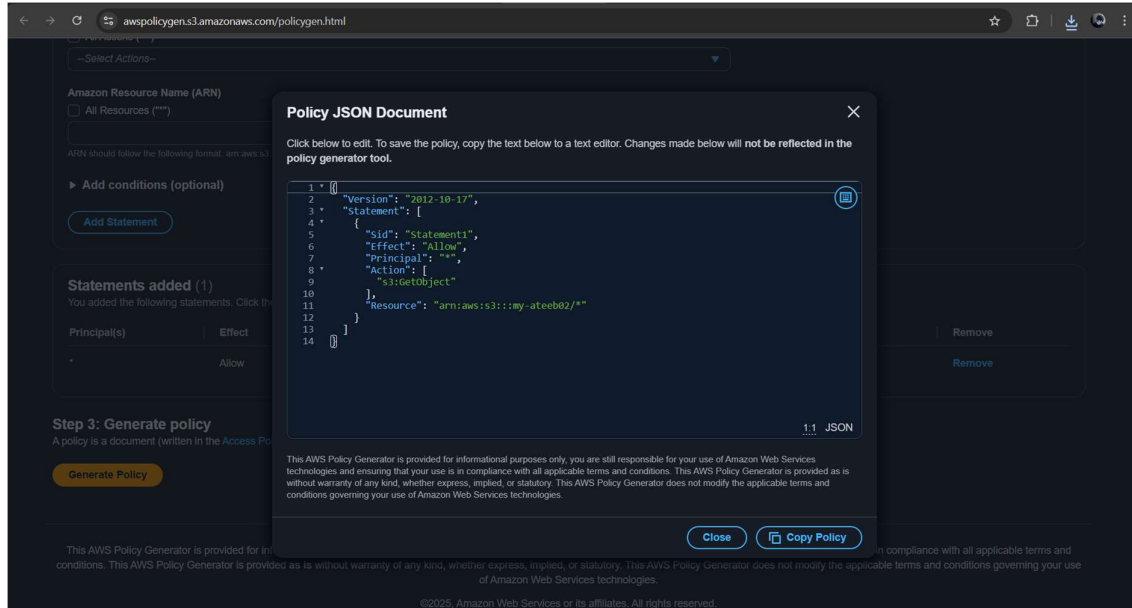
©2025, Amazon Web Services or its affiliates. All rights reserved.

Shaikh Ateeb Ahmed

11-08-2025

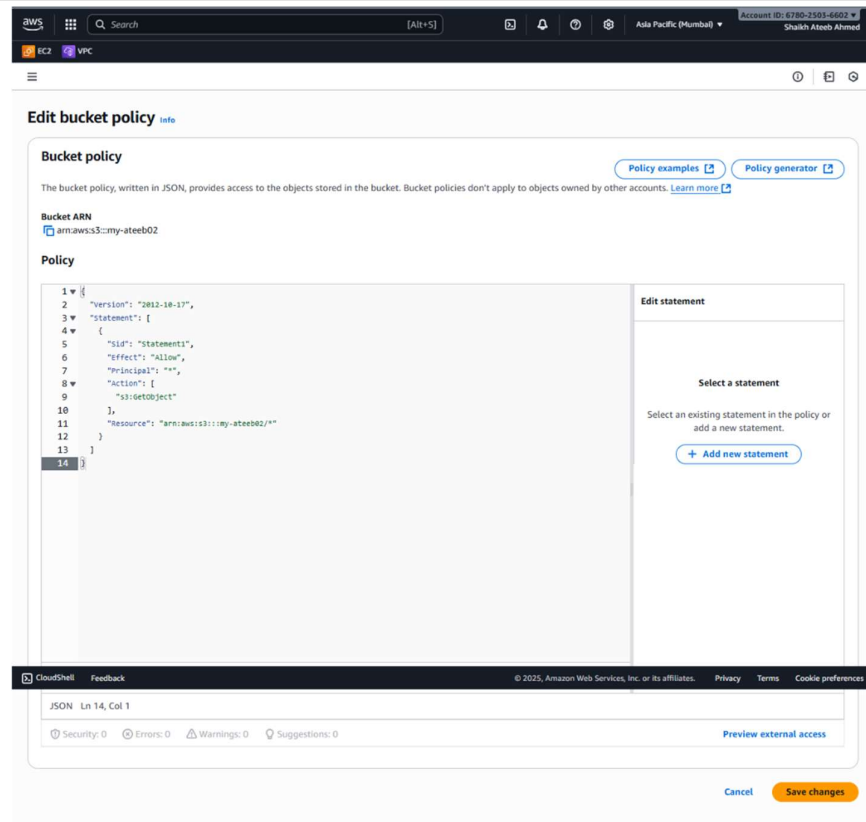
Click add statement then **Generate Policy**.

Copy the generated JSON from the Policy Generator.



Paste and save the bucket policy

Back in **S3** → **Bucket** → **Permissions** → **Bucket policy** → **Edit**, paste the JSON policy you copied.



Click **Save changes**.

AWS may warn you about making the bucket public; confirm if you intend to proceed.

Example policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::YOUR_BUCKET_NAME/*"
    }
  ]
}
```

Shaikh Ateeb Ahmed

11-08-2025

```
}
```

```
]
```

```
}
```

Confirm the image is now public

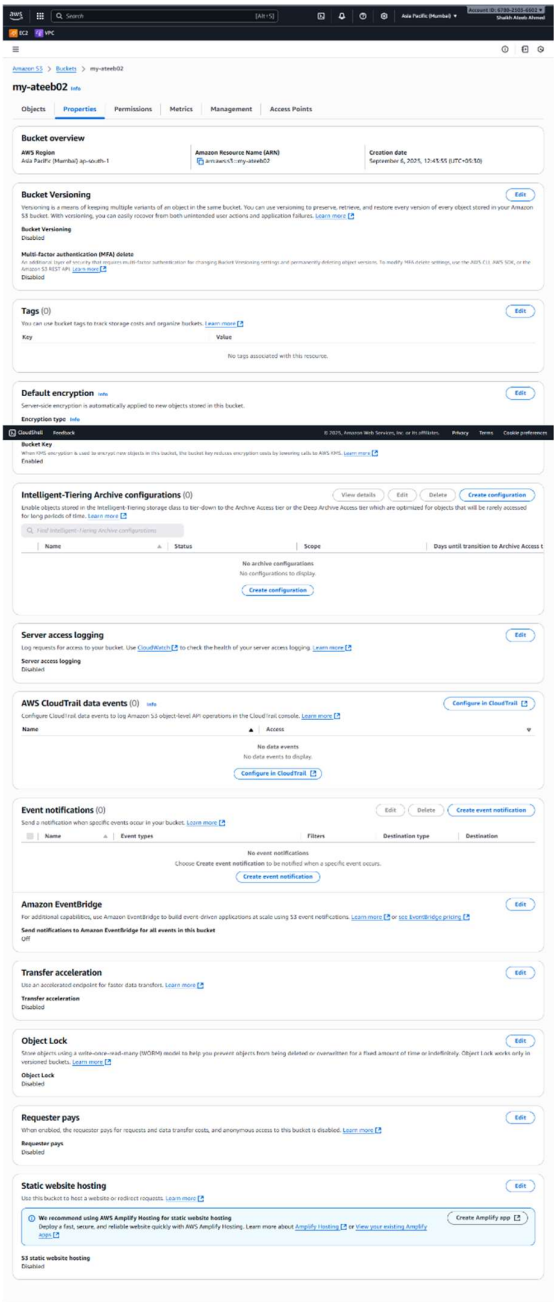
Return to the **Objects** list in your bucket, click the image object, and click the **Object URL**.

The image should now load in the browser (instead of Access Denied).



Enable static website hosting (so S3 exposes a website endpoint)

In the bucket, open **Properties** → **Static website hosting**

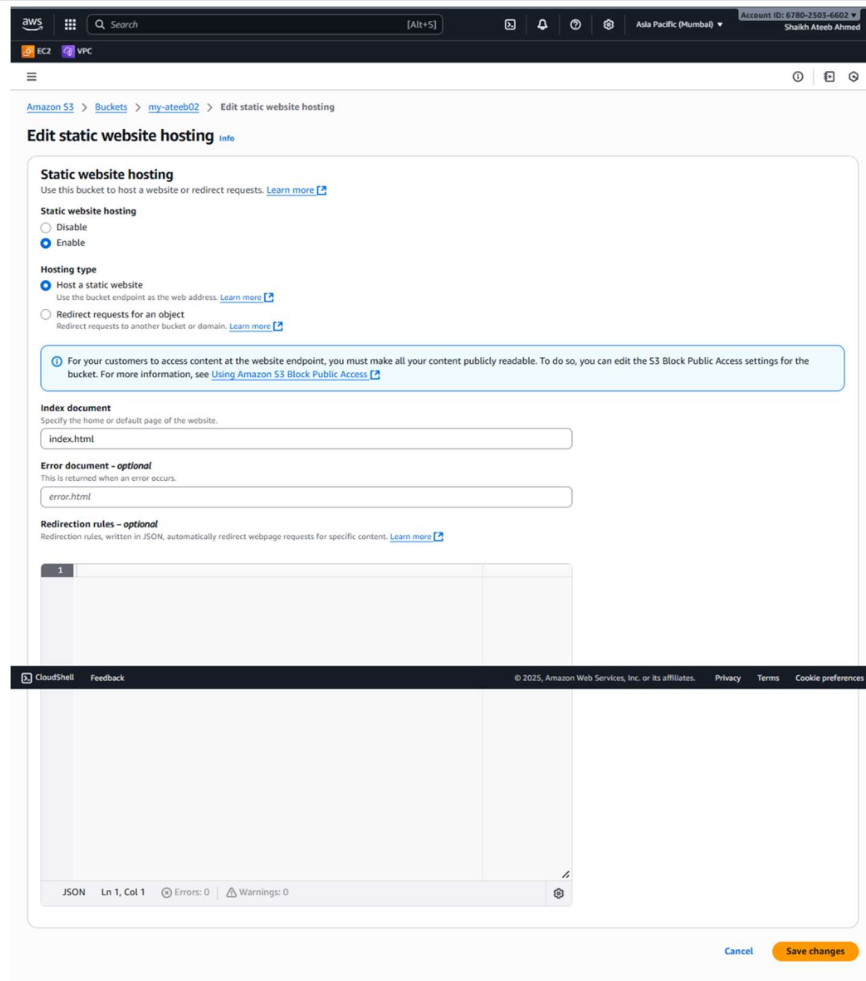


Edit (or Static website hosting pane).

Enable static website hosting.

Index document: type index.html.

Save changes.



Open the Bucket website endpoint

In **Properties** (bottom of page) you'll see **Bucket website endpoint** (a URL like `http://YOUR_BUCKET_NAME.s3-website-<region>.amazonaws.com`).

Click/open that endpoint. Because you have not uploaded `index.html`, the website will show **404 Not Found** (or the S3 error page) that's expected. If you upload an `index.html` at the bucket root, the site will show that page instead.

