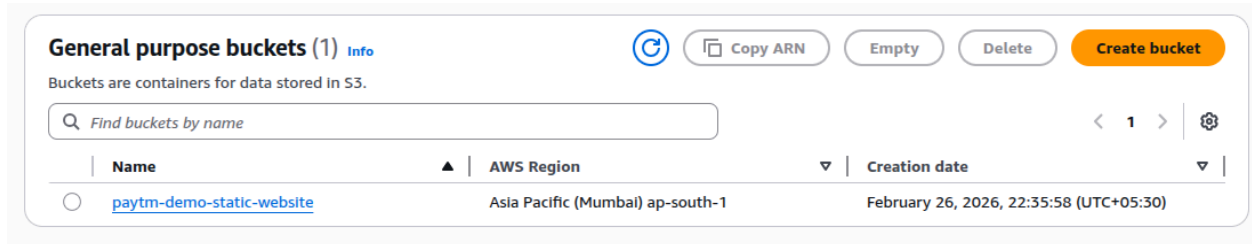


How to host a static website in S3

CREATE A BUCKET:

- Search S3 in search bar and select bucket
- Now, click on create bucket



Give a unique bucket name

Bucket name [Info](#)

paytm-demo-s3

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 (-).

- Unselect the block public access setting for this bucket and click **Create bucket**

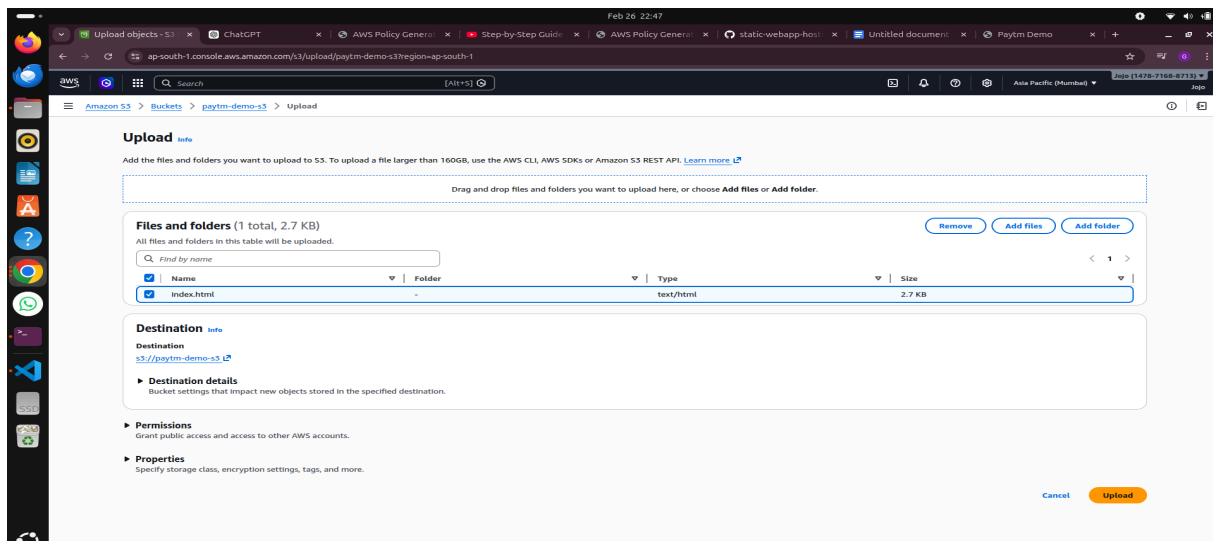
Block Public Access settings for this bucket

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.

- Then upload your file in the bucket you have created



Hosting a website:

- Go to the **Properties** in the bucket you have created and enable the static website hosting

Edit static website hosting [Info](#)

Static website hosting
Use this bucket to host a website or redirect requests. [Learn more](#) [↗](#)

Static website hosting
☐ Disable
☒ Enable

Hosting type
☒ Host a static website
Use the bucket endpoint as the web address. [Learn more](#) [↗](#)
☐ Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#) [↗](#)

ⓘ For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#) [↗](#)

Index document
Specify the home or default page of the website.

Error document - optional
This is returned when an error occurs.

Redirection rules - optional
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#) [↗](#)

1		

- Open a new tab and search for policy generator for S3 bucket
- Select the policy type → **S3 Bucket Policy**

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](#) [↗](#)

Type of 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 ("*")

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)

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.

- Select allow in effects
- In principal type → *
- In actions select → getObject
- In ARN → copy the Bucket Arn from **Bucket policy** in **Permissions**
- Select **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:::paytm-demo-s3	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](#)

- Click on **Generate Policy** and copy the **copy policy**

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**.

```

1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Sid": "Statement1",
6        "Effect": "Allow",
7        "Principal": "*",
8        "Action": [
9          "s3:GetObject"
10       ],
11       "Resource": "arn:aws:s3:::paytm-demo-s3"
12     }
13   ]
14 }

```

1:1 JSON

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.

[Close](#) [Copy Policy](#)


- Now go to **PERMISSION** and paste the code in **Bucket policy** and copy paste the **copy policy** and add /* at the end of resource name ("Resource": "arn:aws:s3:::paytm-demo-s3/*")

Edit bucket policy [Info](#)

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Bucket ARN

 arn:aws:s3:::paytm-demo-s3

Policy

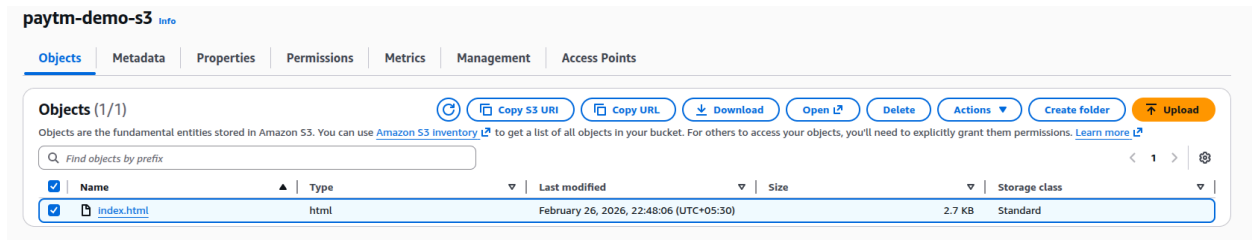
```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "Statement1",  
6       "Effect": "Allow",  
7       "Principal": "*",  
8       "Action": [  
9         "s3:GetObject"  
10      ],  
11      "Resource": "arn:aws:s3:::paytm-demo-s3/*"  
12    }  
13  ]  
14 }
```

THIS is sample from the policy generator

```
1. {  
2.   "Version": "2012-10-17",  
3.   "Statement": [  
4.     {  
5.       "Sid": "Statement1",  
6.       "Effect": "Allow",  
7.       "Principal": "*",  
8.       "Action": [  
9.         "s3:GetObject"  
10.      ],  
11.      "Resource": "arn:aws:s3:::paytm-demo-s3/*"  
12.    }  
13.  ]  
14. }
```

Result:

- To see the output go OBJECTS, select the file and copy the copy url



Once the copy Url is copied pasted it in the incognito mode of your browser

