

Setup Website:

Mission

- 1) Create S3 bucket
- 2) Attach policy to S3 bucket (Granting read-only permission to an anonymous user)
- 3) Enable Static Web Hosting

1) Create S3 bucket

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

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

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

Allow Public Access (uncheck default marked boxes) ----->>>

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.

Click Create bucket

Name	AWS Region	Access
serverless-web-application-anup	Asia Pacific (Mumbai) ap-south-1	Objects can be public


2) Attach Policy (Allow public read-only access)

- Select all files from V1/Site and Drag & Drop to bucket (do not upload folder V1/Site folder directly)
- Go to permissions → Bucket Policy → Edit
- Copy [granting read only permission to anonymous user](#) policy and add it with change in bucket name as ours.

Amazon S3 > Buckets > serverless-web-application-anup > Edit bucket policy



Edit bucket policy [Info](#)

Bucket policy
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies

Bucket ARN
 arn:aws:s3:::serverless-web-application-anup

Policy

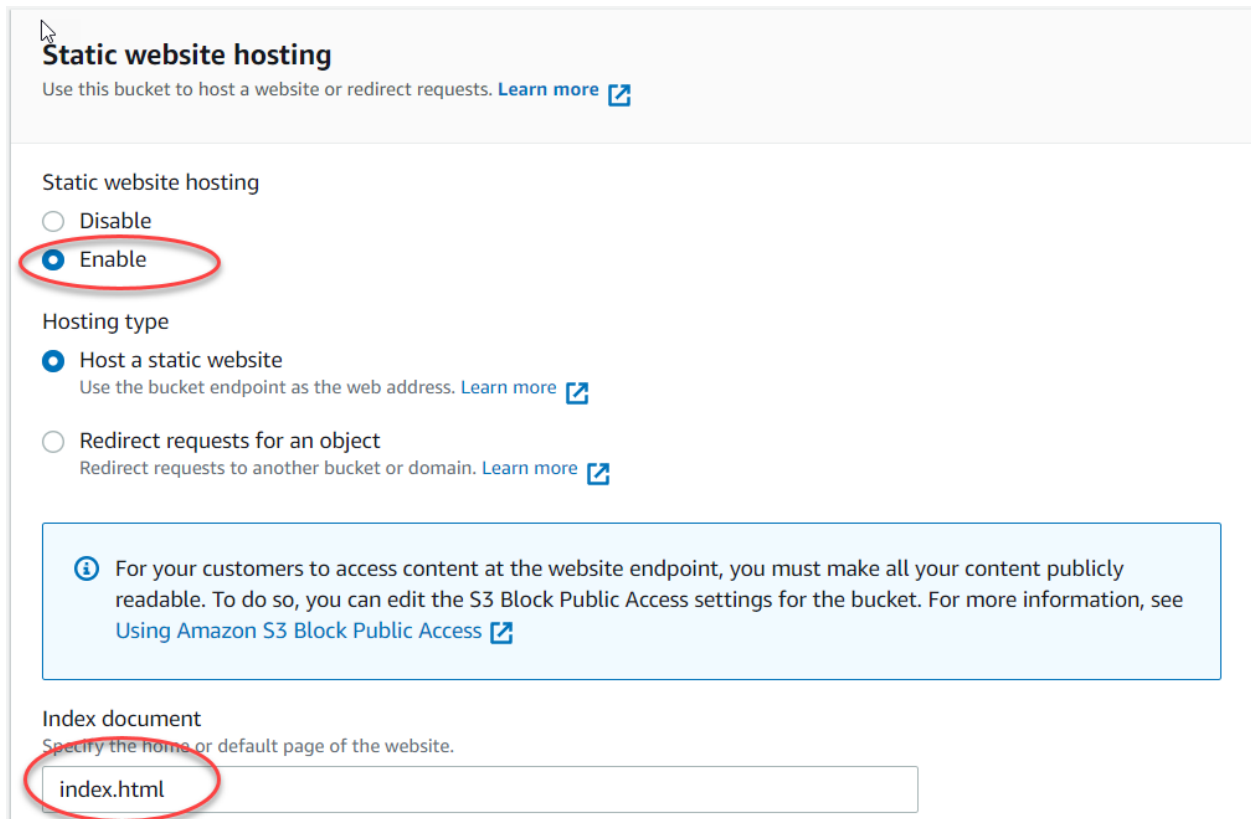
```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "PublicRead",  
6       "Effect": "Allow",  
7       "Principal": "*",  
8       "Action": [  
9         "s3:GetObject",  
10        "s3:GetObjectVersion"  
11      ],  
12      "Resource": [  
13        "arn:aws:s3:::serverless-web-application-anup/*"  
14      ]  
15    }  
16  ]  
17 }
```

	Name	AWS Region	Access
	serverless-web-application-anup	Asia Pacific (Mumbai) ap-south-1	 Public

Click Save Changes

3) Enable Static Web Hosting

Buckets→Select your bucket→ Properties→(scroll bottom) Static web hosting→Edit→Enable→Add **index.html** text in index document field → Save Changes



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](#)

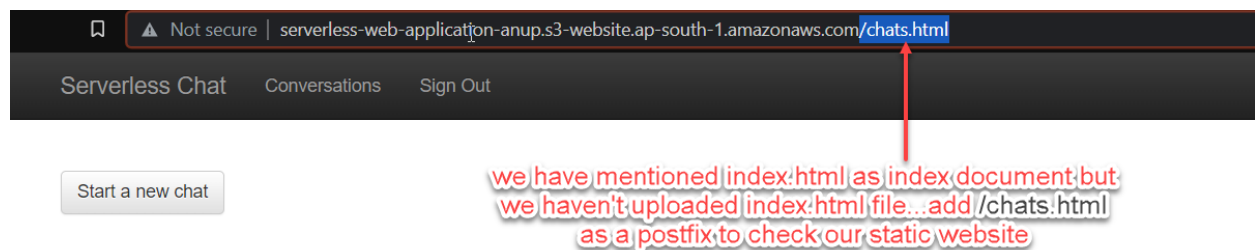
☐ Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#)

Info 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.

index.html

Again go to properties→ Static web hosting→ Copy the url generated & paste into URL bar of browser



Mission Accomplished