

Deploy Static website on AWS S3

Step 1: - Create an S3 Bucket

- Go to AWS Management Console → S3.
- Click Create Bucket.
- Enter a unique bucket name
- Choose a **Region** close to your users.

Create bucket [info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region
US East (N. Virginia) us-east-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](#)

text-to-speech-demo

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 configurations are copied:

[Choose bucket](#)

Format: s3://bucket/prefix

Object Ownership [info](#)

Central 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 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](#)

- Uncheck Block all public access (since a website needs public access).
- Acknowledge the warning 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.

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](#)

Step 2. Upload Website Files

- Open the newly created bucket.
- Click Upload → Add your HTML, CSS, JS, images (your static website files).
- Upload all files and folders.
- After upload, ensure files are inside the bucket.

The first screenshot shows the 'Buckets' page in the AWS Management Console. It displays a table of general purpose buckets. The bucket 'my-text-to-speech-demo' is highlighted. The table has columns for Name, AWS Region, and Creation date.

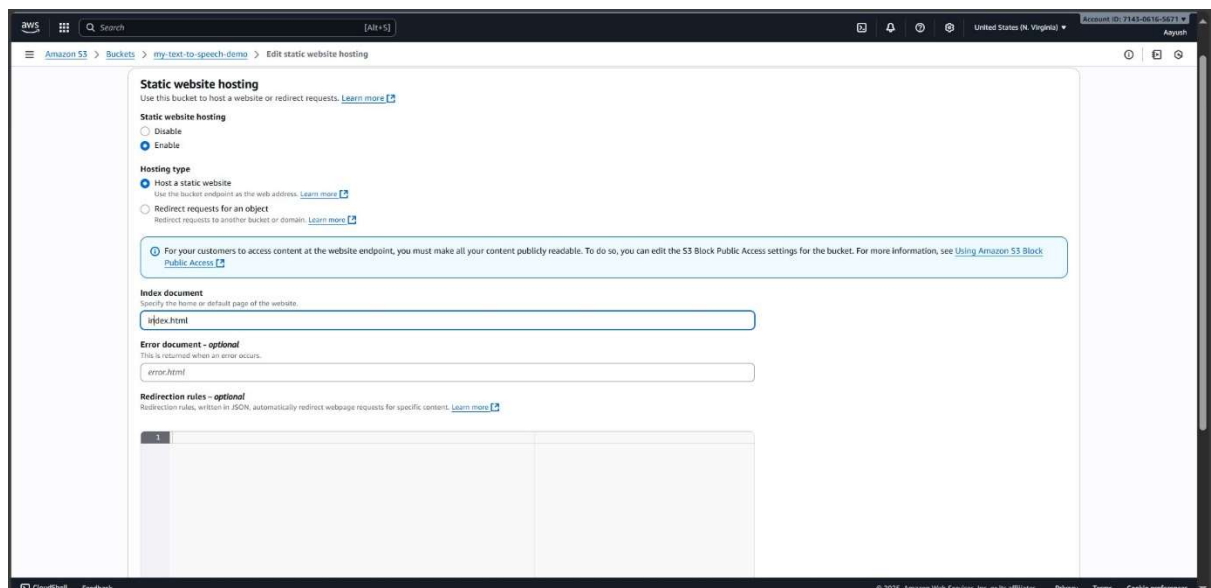
Name	AWS Region	Creation date
my-text-to-speech-demo	US East (N. Virginia) us-east-1	September 4, 2025, 23:51:54 (UTC+05:30)

The second screenshot shows the 'my-text-to-speech-demo' bucket page. It displays the 'Objects' tab, which is currently empty. The page includes a search bar and a table with columns for Name, Type, Last modified, Size, and Storage class.

The third screenshot shows the 'Upload' page for the bucket. It includes a section for 'Files and folders' with a search bar and a table with columns for Name, Folder, Type, and Size. Below this, there is a 'Destination' section with a link to the bucket and a 'Permissions' section with a link to the bucket's permissions.

Step 3. Enable Static Website Hosting

- Go to the Properties tab of the bucket.
 - Scroll down to Static website hosting.
 - Select Enable.
 - Choose Host a static website.
 - Enter: Index document → index.html
 - Save changes.
- 👉 You'll now get a bucket website endpoint URL (something like <http://my-portfolio-site.s3-website-us-east-1.amazonaws.com>).

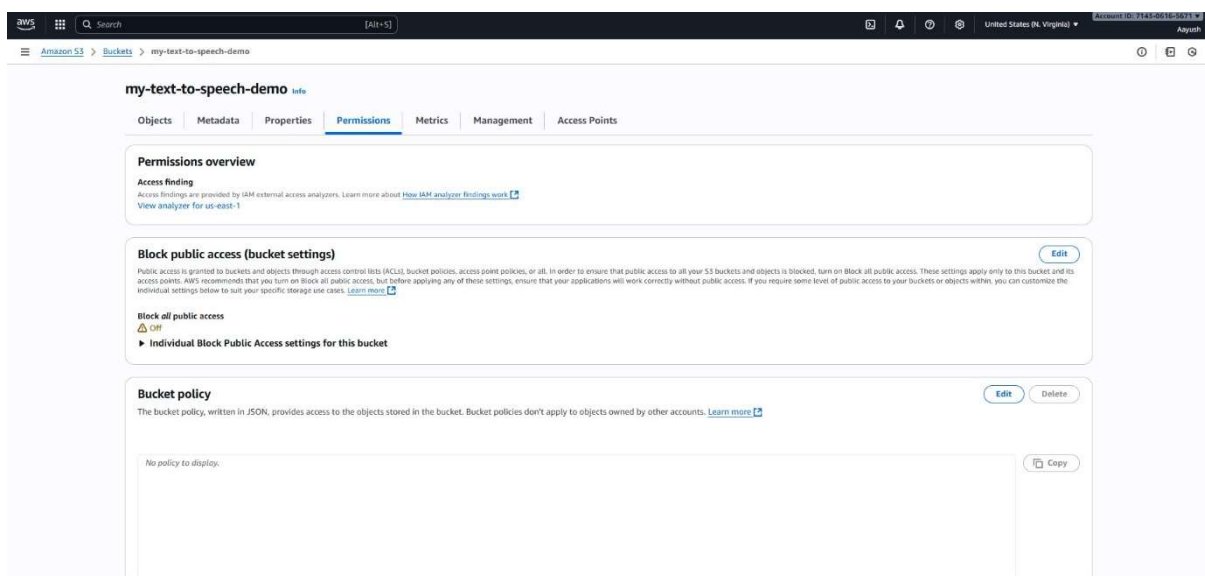


Step 4. Set Bucket Policy (Make Files Public)

- Go to the Permissions tab → Bucket policy.
- Add a policy like this (replace my-portfolio-site with your bucket name):

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

- Save changes.



Step 5. Test Your Website

- Copy the Website Endpoint URL from the Static website hosting section.
- Paste it in a browser → Your site should load 🎉.

