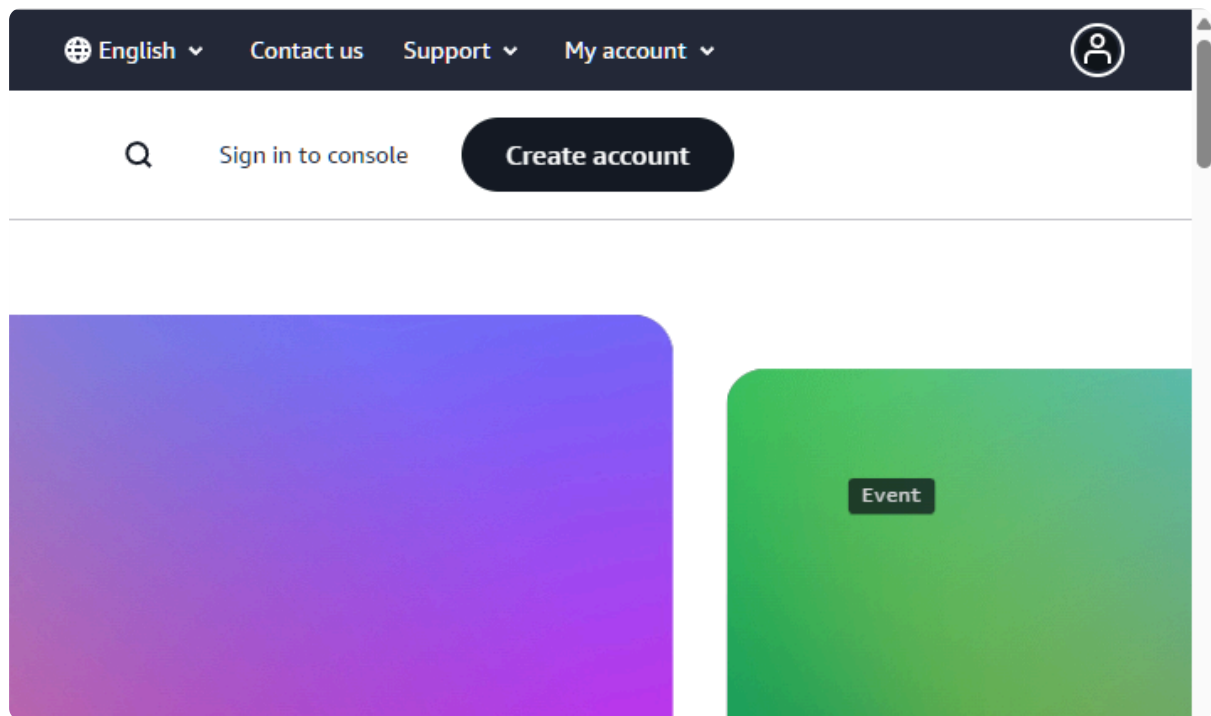


Expert Guide: Creating an Amazon S3 Static Site 8/20/2025

This guide use best practices to prevent 403 forbidden errors, duplicate content issues, and redirect problems.

We're going to start by going through all the steps necessary to set up, and configure your bucket, make the necessary changes to your site in Sparkzio, then upload your exported site to your Amazon S3 container.

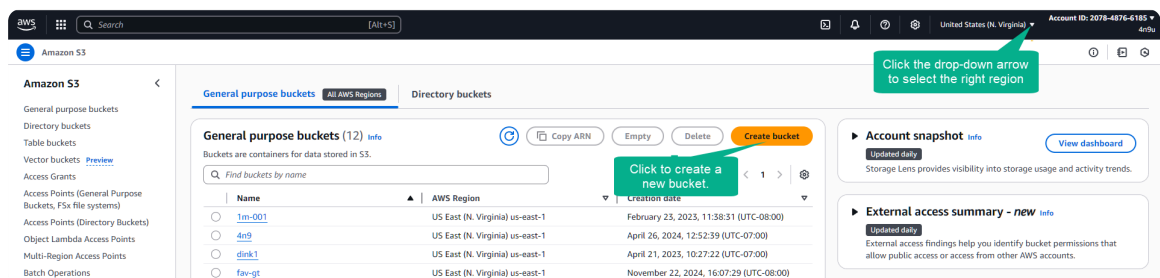
Requirements: You should have [7Zip](#) installed on your computer and you must have an Amazon AWS, Amazon Web Services, account, if you don't, [click here](#) to create an account for yourself.



This process will be easily accomplished if you have logged into your Amazon AWS account in one tab of your browser, and in another tab, your site opened in Sparkzio .

Step 1: Create the S3 Bucket in N. Virginia

1. Go to the Amazon S3 console and make sure that the region, shown at the top, has been changed to United States (N. Virginia) us-east-1 and then click **Create bucket**.



The screenshot shows the 'Create bucket' page in the AWS Management Console. The page is divided into several sections: General configuration, Object Ownership, Block Public Access settings, Bucket Versioning, Tags, and Default encryption. Annotations with green arrows point to specific elements: 'Name your bucket' points to the bucket name input field; 'Leave disabled' points to the 'ACLs disabled (recommended)' radio button; 'Nothing should be checked' points to the 'Block all public access' checkbox; 'You must check' points to the 'I acknowledge that the current settings might result in this bucket and the objects within becoming public' checkbox; and 'Click to Create bucket' points to the 'Create bucket' button at the bottom right.

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](#)

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 the 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 objects. 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 and its objects, turn off Block all public access and configure the individual settings below to suit your specific storage use cases. [Learn more](#)

☐ **Block all public access**
Turning this setting on blocks all public access to this bucket and its objects 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 ignore new 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

☒ **Enable**

☐ **Disable**

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](#)

☒ **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)**
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](#).

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.](#)

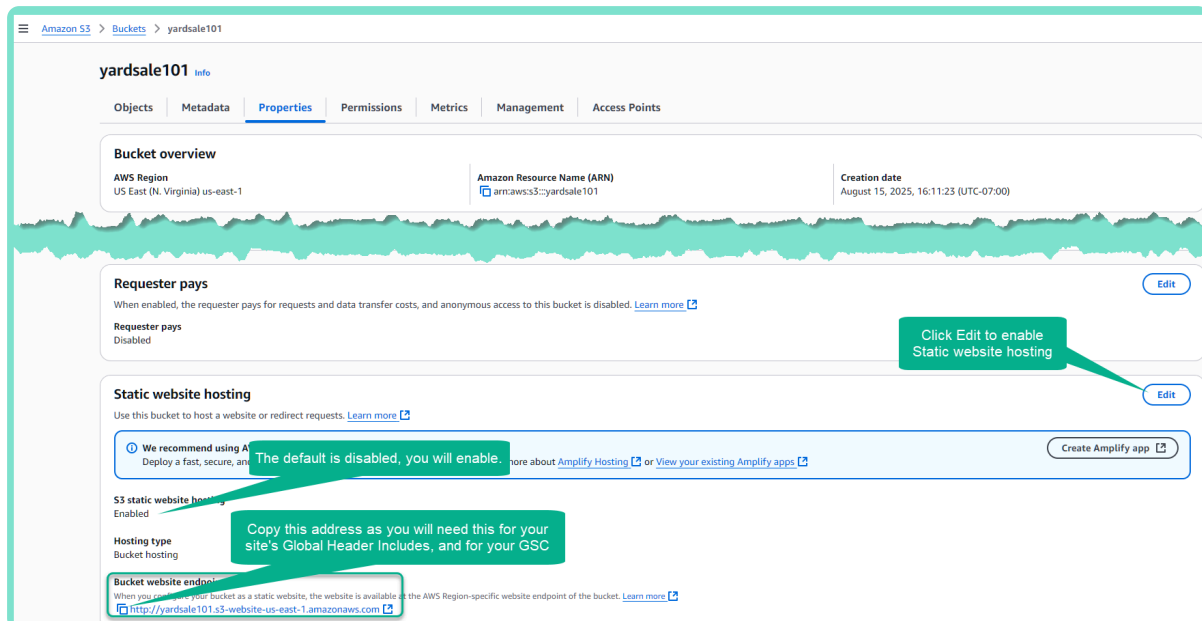
[Cancel](#) [Create bucket](#)

- Bucket name:** Enter a unique name (e.g., `my-project-site-2025`).
- Object Ownership:** Ensure **ACLs are disabled (recommended)** is selected.
- Block Public Access settings:** The box for **Block all public access** must be **unchecked**. Unchecking this setting is the same as Unchecking on all four settings below, which is what we want.
- Click **Create bucket**.
 - If the bucket isn't created, just scroll back up to the bucket name and change it to something else as someone has already claimed the name you tried to use. After

changing the name, click **Create bucket**. Do this as many times as needed until you successfully acquire a name

Step 2: Locate your newly created bucket name under General purpose buckets and click on it

1. Find the **Properties tab**, for this bucket, and click it.
2. Scroll to the bottom to **Static website hosting** and click **Edit**.
3. Select **Enable** and set the **Index document** to `index.html`.
4. Click **Save changes**.
5. Scroll back down to **Static website hosting** and copy the **Bucket website endpoint URL**. It will look like this: `http://your-bucket-name.s3-website-us-east-1.amazonaws.com` Save this endpoint in your notes, you will need to paste this URL into the the Global Site Header Includes, when you add the "canonical" tag to your site, in Sparkzio.
6. Click **Save changes**.



Step 3: Add the Bucket Policy

1. Go to the **Permissions** tab for your bucket.
2. Locate the **Bucket policy** section and click **Edit**.
3. Paste the following JSON code into this section. This policy grants the public read-only access to view your website files.
 - Remember to replace `your-bucket-name` with your actual S3 bucket name.

4. JSON

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

- This policy grants the `s3:GetObject` action to all principals (`*`), allowing them to retrieve any object in the bucket. This is the **correct and most secure way** to allow public read access for a static website. It gives access to your `index.html` , `robots.txt` , and `sitemap.xml` files without allowing public listing of the bucket's contents, which the `s3:ListBucket` action would permit.

5. Click **Save changes**.

Step 4: Open your site in Sparkzio

1. Review your site completely. Making changes, or corrections now, will save you time and avoids frustration.
2. Make sure that the copyright notice, at the footer of the page, has the company name and the current year, or previous year - current year. Example: ©2025 or ©2024-2025

Step 5: Add the "Official Address (URL)" Tag to Your Site.

To prevent search engines from seeing duplicate content, you must add a "canonical" tag to your site.

1. Go to the Site Settings for your site, and in the Site details `Global Header Includes` section, add the following line, exactly as shown:
2. `<link rel="canonical" href="PASTE_YOUR_S3_WEBSITE_URL_HERE">`
3. Replace `PASTE_YOUR_S3_WEBSITE_URL_HERE` with the actual S3 website URL you copied in Step 2, Item 5.
4. Apply changes and be sure to save any changes you may have made to your site

Step 6: Exporting & Uploading Your Site to Your Amazon S3 Bucket

Follow the steps shown in the video:

1. Export your site to a folder you have created on your computer, which will be a zip file.

2. Right click on the zip file and select extract here, using 7Zip.
3. As shown in the video, drag and drop these extracted files into your Amazon S3 bucket/container. This finalizes the entire process.

Your website is now fully configured and live. You can access it using the S3 website URL from Step 2 Item 5. Any 403 errors will be gone, no redirection errors, and the canonical tag added to your site, will prevent duplicate content issues.

The S3 website URL from Step 2 Item 5 will be used to add this site as a property in your GSC, Google Search Console.