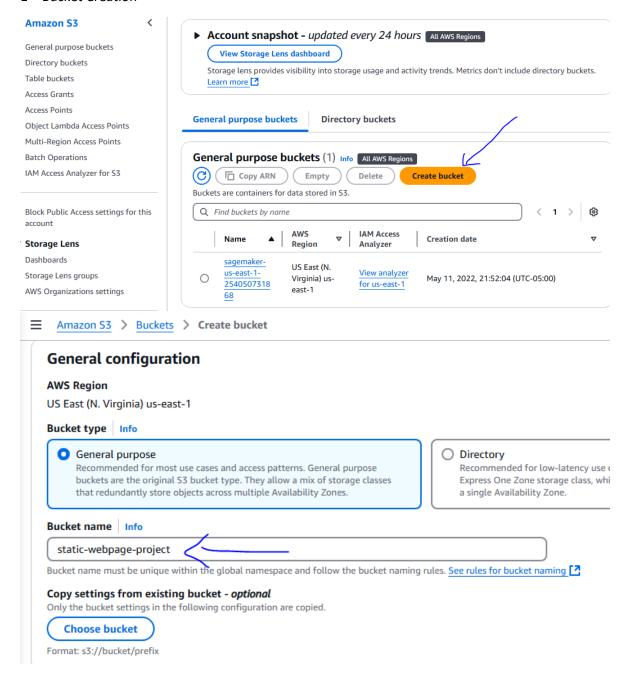
1 - Bucket Creation

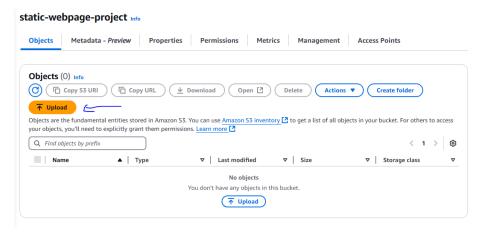


Block Public Access settings for this bucket

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

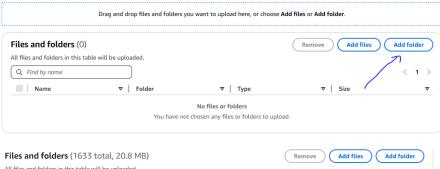
_	Block all public access Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
- (Block public access to buckets and objects granted through <i>new</i> access control lists (ACLs) S3 will block public access permissions 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.
- 1	Block public access to buckets and objects granted through <i>any</i> 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 <i>new</i> 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.
L	Block public and cross-account access to buckets and objects through <i>any</i> public bucket or access point policies 53 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.
	Atic-webpage-project Info Objects Metadata - Preview Properties Permissions Metrics Management Access Points
(
	Objects Metadata - Preview Properties Permissions Metrics Management Access Points Objects (0) Info □ Copy S3 URI □ Copy URL ▼ Download Open 🔁 Delete Actions ▼ Create folder
	Objects Metadata - Preview Properties Permissions Metrics Management Access Points Objects (O) Info ○ □ Copy S3 URI □ Copy URL ↓ Download Open 🗗 Delete Actions ▼ Create folder T Upload Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory 1 to get a list of all objects in your bucket. For others to access
	Objects Metadata - Preview Properties Permissions Metrics Management Access Points Objects (0) Info Copy S3 URI Copy URL Download Open [2] Delete Actions ▼ Create folder Tupload Upload Open [3] To get a list of all objects in your bucket. For others to access our objects, you'll need to explicitly grant them permissions. Learn more [2]
	Objects (O) Info Copy URL
	Objects (O) Info C Copy S3 URI Copy URL Download Open P Delete Actions ▼ Create folder T Upload Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory T to get a list of all objects in your bucket. For others to access our objects, you'll need to explicitly grant them permissions. Learn more P Q Find objects by prefix A Type ▼ Last modified ▼ Size ▼ Storage class ▼

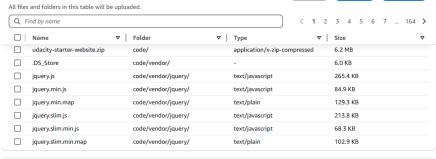
2 - Upload Files



Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. Learn more 🔼





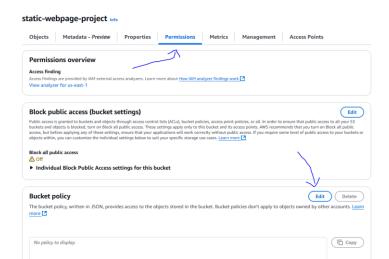


- ▶ Permissions
 Grant public access and access to other AWS accounts.
- ► Properties
 Specify storage class, encryption settings, tags, and more.



Cancel

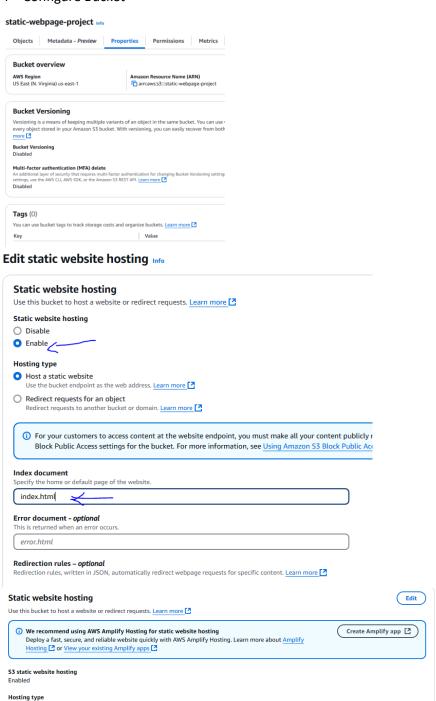
3 – Secure Bucket



Edit bucket policy Info

Bucket policy The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies do more Bucket ARN The arm:aws:s3:::static-webpage-project Policy

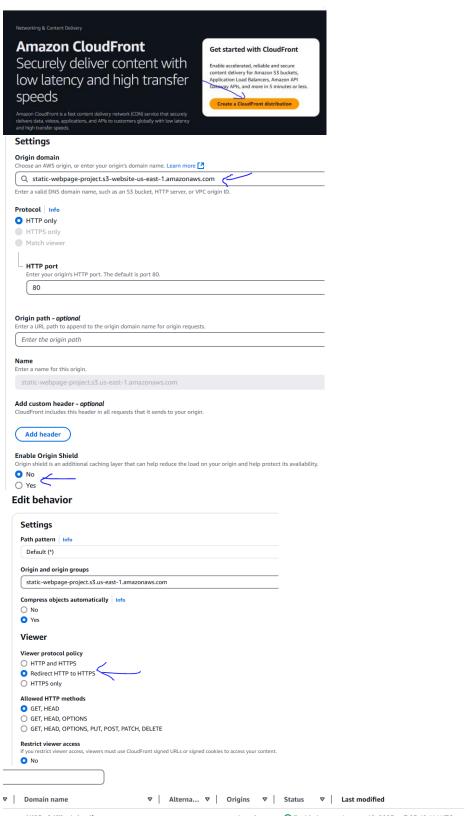
4 – Configure Bucket



Bucket website endpoint

When you configure your bucket as a static website, the website is available at the AMS degion-specific website endpoint of the bucket. Learn more Third http://static-webpage-project.s3-website-us-east-1.amazonaws.com

5 – Distribute Website



6 - Access Website

