



Creating & Hosting an static website using AWS S3 service

Step 1: Create an S3 Bucket

1. **Log in to AWS Management Console:** Go to [AWS Console](#).
2. **Navigate to S3:** Search for "S3" in the AWS search bar and select the **S3 service**.
3. **Click "Create Bucket":**
 - Enter a **unique bucket name** (e.g., **my-static-website**).
 - Choose the appropriate **AWS region**.
4. **Configure Bucket Options:**
 - Uncheck the **"Block all public access"** option & save changes.
 - Confirm the warning and allow public access.

aws [Search] [Alt+S] N. Virginia voclabs/user3312069-Ruturaj_Sonone @ 5256-2052-5649

Amazon S3 > Buckets > aws-made-easy-2543 > Edit Block public access (bucket settings)

Amazon S3 <

General purpose buckets

Directory buckets

Table buckets [New](#)

Access Grants

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

▼ Storage Lens

Dashboards

Storage Lens groups

AWS Organizations settings

Edit Block public access (bucket settings) Info

Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets 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.

[Cancel](#) [Save changes](#)

5. **Create the Bucket:** Click the **"Create bucket"** button.



Step 2: Upload Website Files

1. **Open Your Bucket:** Click on the bucket you just created.
2. **Upload Files:**
 - Click **"Upload"** and select your website files (e.g., [index.html](#) and [error.html](#)).
 - Ensure you include all necessary files (e.g., CSS, JS, images, etc.).

The screenshot shows the AWS S3 console interface. The left sidebar lists navigation options under 'Amazon S3', including 'General purpose buckets', 'Directory buckets', 'Table buckets', 'Access Grants', 'Access Points', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', and 'IAM Access Analyzer for S3'. The main content area displays the bucket 'aws-made-easy-2543' with tabs for 'Objects', 'Metadata - Preview', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Objects' tab is active, showing a list of three objects: 'Amazon-Web-Services-AWS-Logo-700x394.png' (70.1 KB), 'index.html' (801.0 B), and 'style.css' (849.0 B). Above the list are buttons for 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload'. A search bar is also present.

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	Amazon-Web-Services-AWS-Logo-700x394.png	png	December 28, 2024, 13:25:05 (UTC+05:30)	70.1 KB	Standard
<input type="checkbox"/>	index.html	html	December 28, 2024, 13:22:07 (UTC+05:30)	801.0 B	Standard
<input type="checkbox"/>	style.css	css	December 28, 2024, 13:25:03 (UTC+05:30)	849.0 B	Standard

3. Set Permissions:

- Under the permissions tab during upload, ensure files are publicly accessible.

Step 3: Enable Static Website Hosting

1. **Go to Properties:** In the bucket dashboard, select the **"Properties"** tab.
2. **Enable Static Website Hosting:**
 - Scroll to the **"Static Website Hosting"** section.



- Click **"Edit"** and enable the option.
- Specify:
 - **Index document:** `index.html`
 - **Error document:** `error.html` (optional)
- Save your changes.

Static website hosting

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

We recommend using AWS Amplify Hosting for static website hosting
Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about [Amplify Hosting](#) or [View your existing Amplify apps](#)

Create Amplify app

S3 static website hosting
Enabled

Hosting type
Bucket hosting

Bucket website endpoint
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)
<http://aws-made-easy-2543.s3-website-us-east-1.amazonaws.com>

Activate Windows

3. **Copy the Endpoint URL:** Note the provided **bucket website endpoint URL**. This is your website URL.

Step 4: Set Permissions for Public Access

1. Add a Bucket Policy:

- Go to the **"Permissions"** tab and select **"Bucket Policy"**.

Paste the following policy (replace `BUCKET_NAME` with your bucket's name):

json



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


Edit bucket policy [Info](#)

Bucket policy

[Policy examples](#)[Policy generator](#)

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:::aws-made-easy-2543`

Policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "PublicReadGetObject",
6       "Effect": "Allow",
7       "Principal": "*",
8       "Action": "s3:GetObject",
9       "Resource": "arn:aws:s3:::aws-made-easy-2543/*"
10    }
11  ]
12 }
```

Edit statement

Select a statement

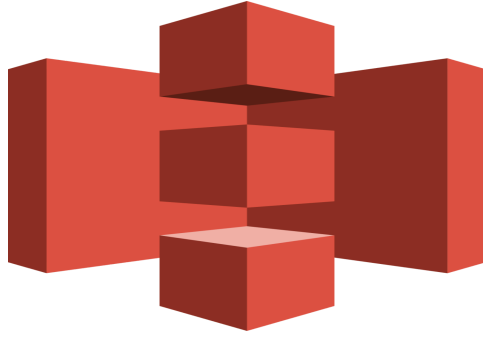
Select an existing statement in the policy or add a new statement.

[+ Add new statement](#)

- Save the policy.

Step 5: Test Your Website

1. Open the **S3 Bucket Endpoint URL** in your browser.



2. You should see your static website load.

Welcome to AWS Made Easy



About Us

This is a simple static website. It's lightweight and easy to customize!

Our Services

We offer a variety of services tailored to your needs. Contact us for more information.

© 2024 AWS Made Easy. All rights reserved.