

Static Hosting:

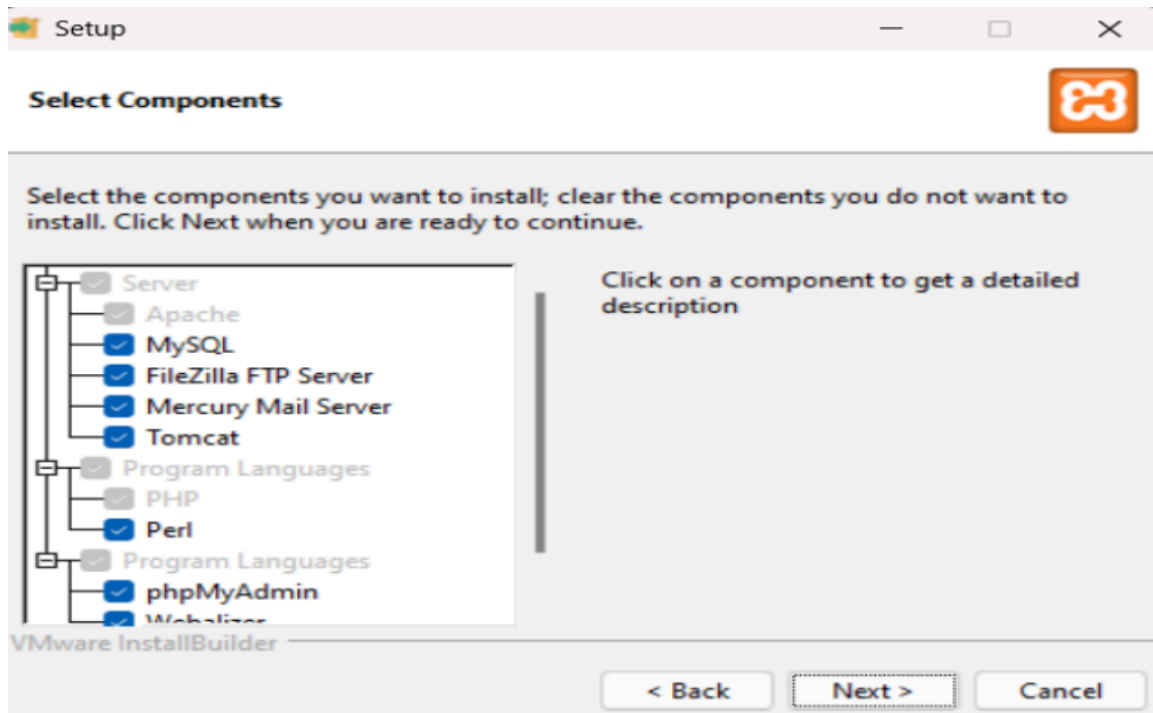
1) On local server (XAMPP)

Step 1: Install XAMPP from <https://www.apachefriends.org/>

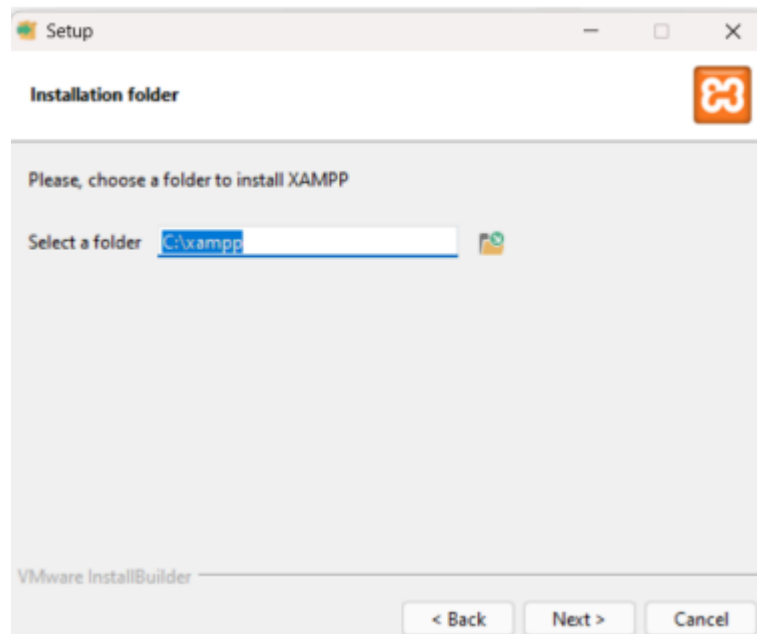
1) Select your OS. It will automatically start downloading.



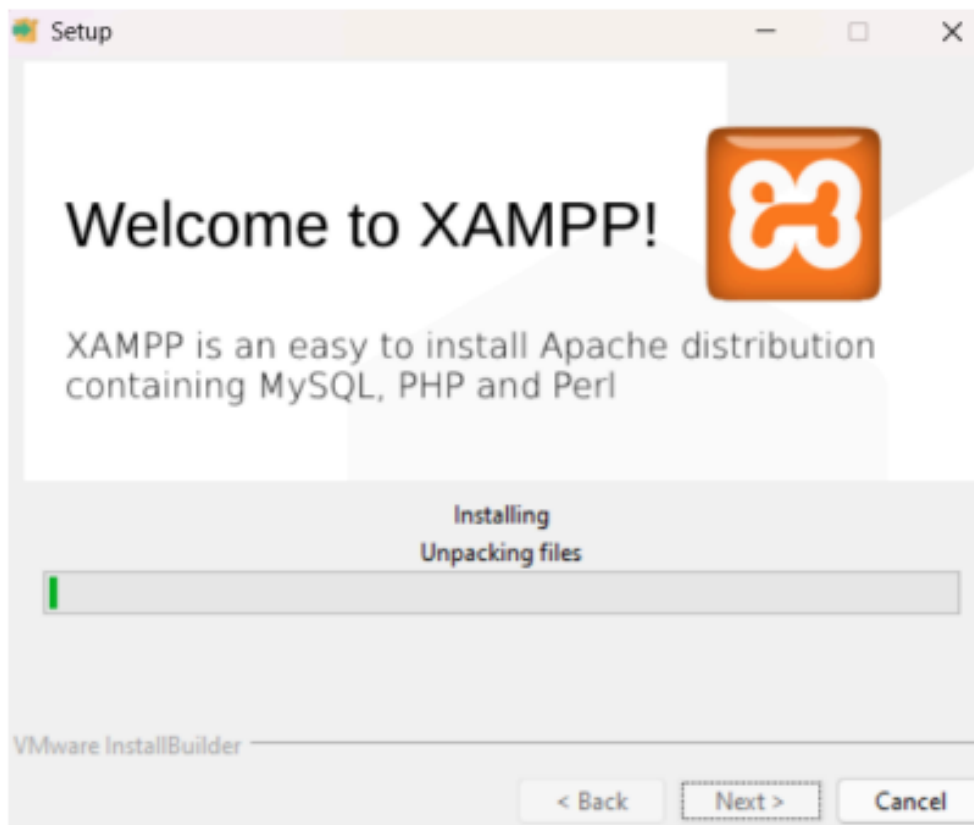
2) Open the setup file. Select all the required components and click next



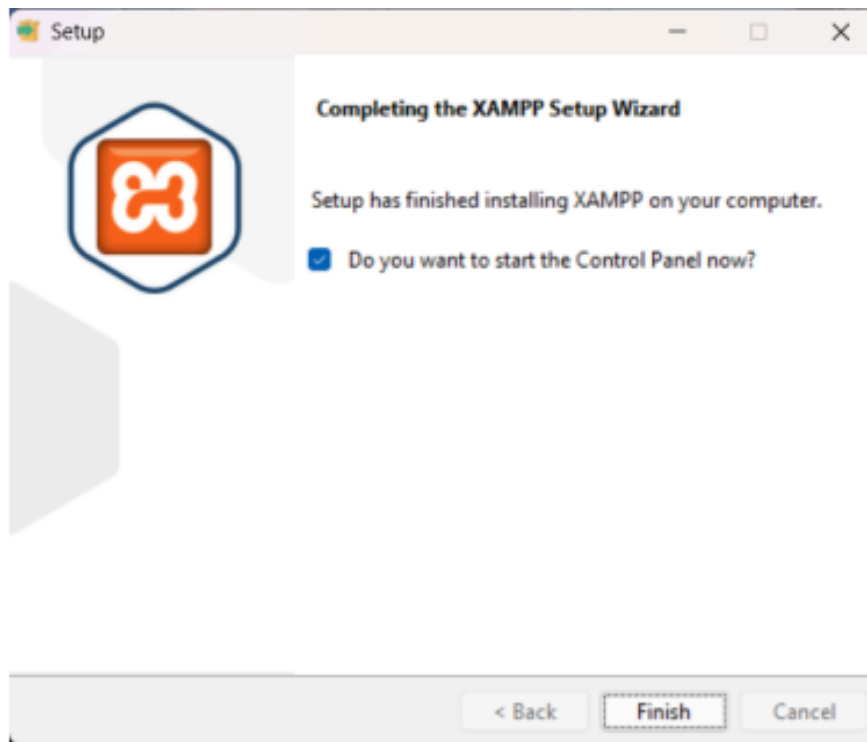
3) Choose the folder to install XAMPP in. Make sure the folder is empty. Click next



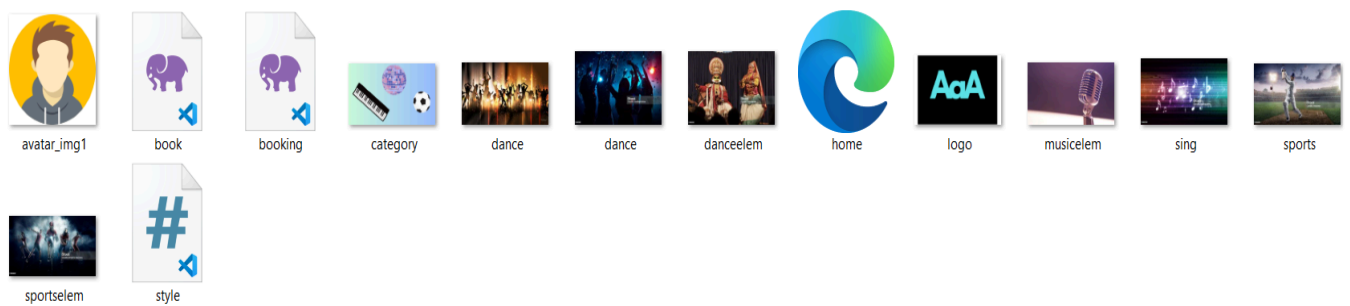
4) Select the language, click next. XAMPP starts to install



5) The installation is complete. Click Finish



Step 2: Setup a file that is to be hosted on the server. Make sure the file has extension .php



Step 3: Go to the directory where XAMPP was installed. Go to htdocs folder. Place your folder in this directory.

dashboard	05-08-2024 00:16	File folder	
file	07-01-2024 23:08	File folder	
img	05-08-2024 00:16	File folder	
webalizer	05-08-2024 00:16	File folder	
xampp	05-08-2024 00:16	File folder	
applications	15-06-2022 21:37	Microsoft Edge HT...	4 KB
bitnami	15-06-2022 21:37	CSS Source File	1 KB
favicon	16-07-2015 21:02	ICO File	31 KB
index	16-07-2015 21:02	PHP Source File	1 KB

Step 4: Open XAMPP Control Panel, start the Apache service (Required) and mySQL service (if needed)

XAMPP Control Panel v3.3.0 [Compiled: Apr 6th 2021]

XAMPP Control Panel v3.3.0

[Config](#)
[Netstat](#)
[Shell](#)
[Explorer](#)
[Services](#)
[Help](#)
[Quit](#)

Service	Module	PID(s)	Port(s)	Actions
	Apache	19328 16548	80, 443	<div>Stop</div> <div>Admin</div> <div>Config</div> <div>Logs</div>
	MySQL			<div>Start</div> <div>Admin</div> <div>Config</div> <div>Logs</div>
	FileZilla			<div>Start</div> <div>Admin</div> <div>Config</div> <div>Logs</div>
	Mercury			<div>Start</div> <div>Admin</div> <div>Config</div> <div>Logs</div>
	Tomcat	8196	8080	<div>Stop</div> <div>Admin</div> <div>Config</div> <div>Logs</div>

00:32:18 [mysql] Press the Logs button to view error logs and check the Windows Event Viewer for more clues

00:32:18 [mysql] If you need more help, copy and post this entire log window on the forums

00:32:18 [mysql]

00:32:40 [Apache] Attempting to stop Apache (PID: 2636)

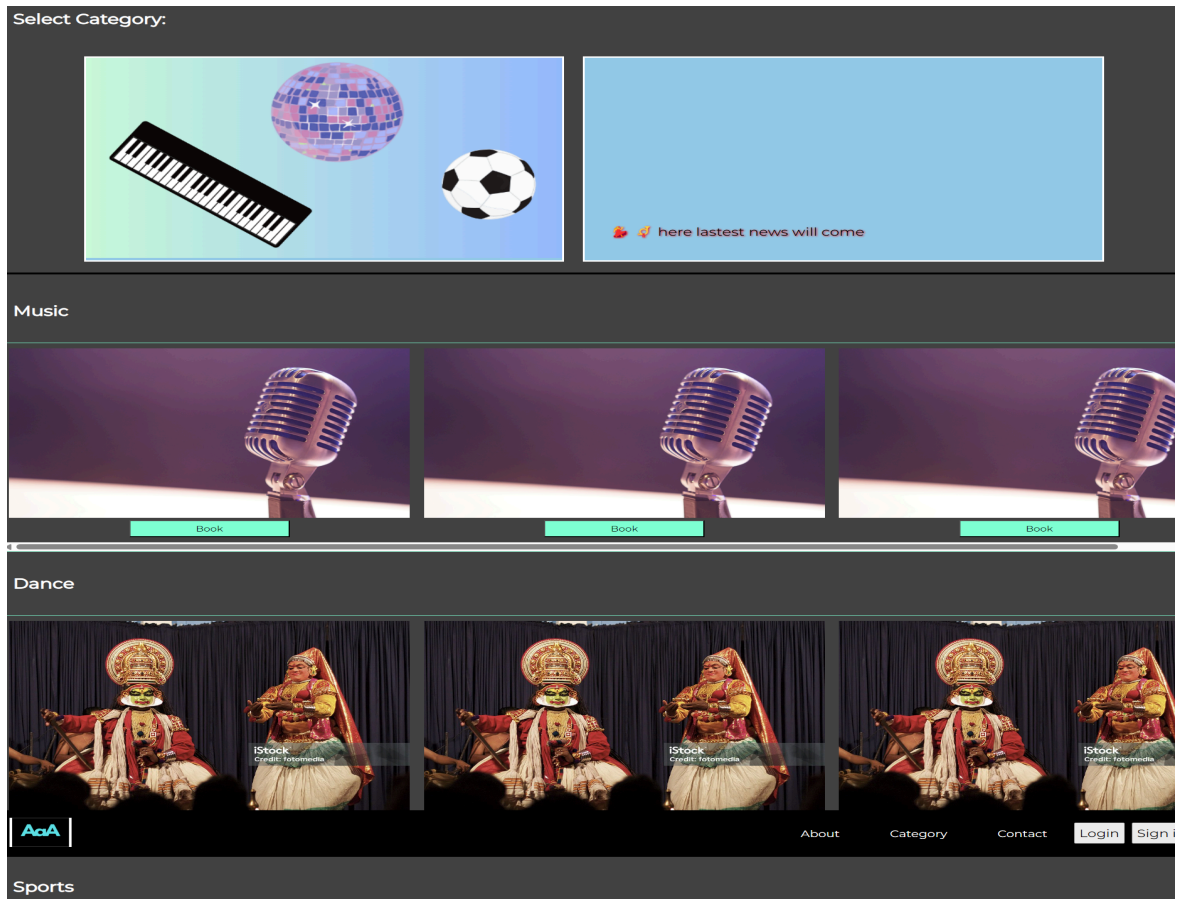
00:32:40 [Apache] Attempting to stop Apache (PID: 13212)

00:32:41 [Apache] Status change detected: stopped

00:32:42 [Apache] Attempting to start Apache app...

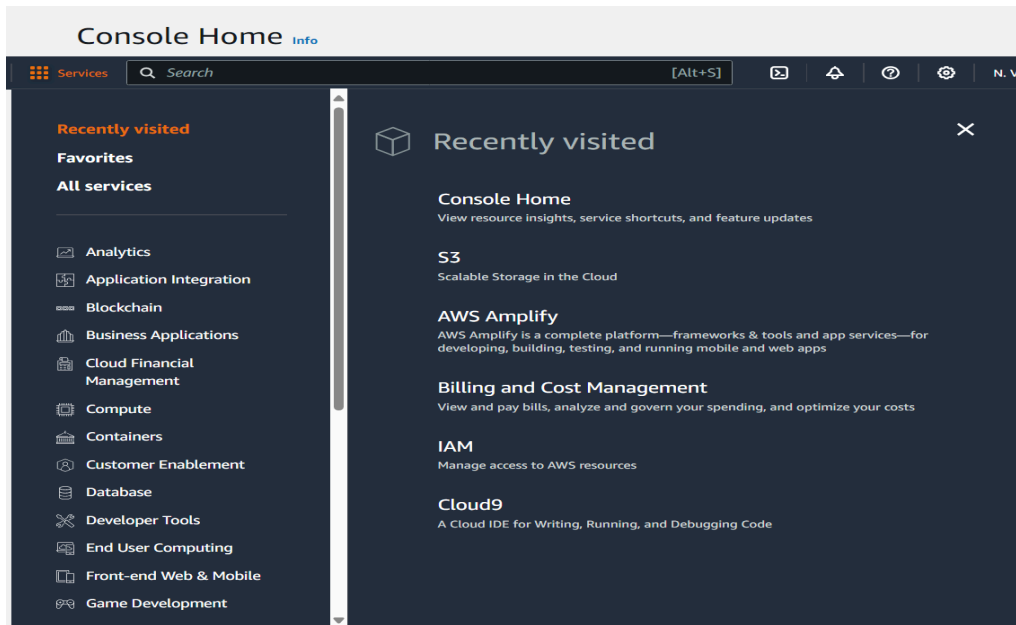
00:32:42 [Apache] Status change detected: running

Step 5: Open your web browser. Type localhost/YOUR_FILENAME.php. This will open your website on your browser.

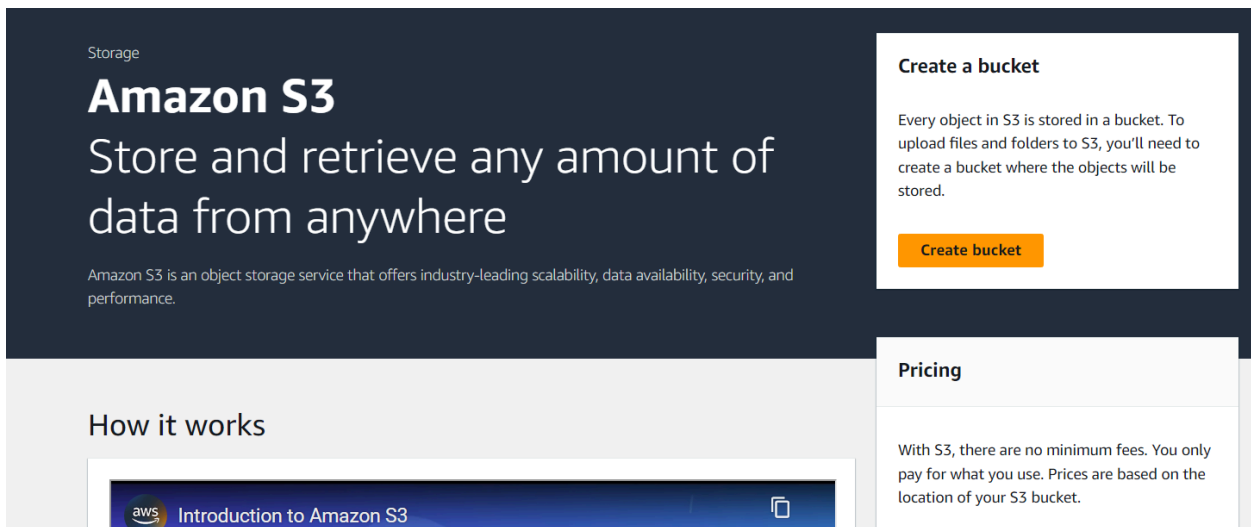


2) AWS S3

Step 1: Login to your AWS account. Go to services and open S3.



Step 2: Click on Create Bucket



Step 3: Give a name to your bucket, keeping other options default, scroll down and click on Create Bucket

[Amazon S3](#) / [BUCKETS](#) / Create bucket

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 - New**
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 name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

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

Choose bucket

Format: s3://bucket/prefix

Step 4: Click on the name of your bucket and goto Properties

► **Account snapshot** - updated every 24 hours [All AWS Regions](#)

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

[View Storage Lens dashboard](#)

General purpose buckets | Directory buckets

General purpose buckets (1) [Info](#) [All AWS Regions](#)

Buckets are containers for data stored in S3.

< 1 > ⚙

	Name	AWS Region	IAM Access Analyzer	Creation date
<input type="radio"/>	bucket-aws34	US East (N. Virginia) us-east-1	View analyzer for us-east-1	August 5, 2024, 01:15:15 (UTC+05:30)

Objects | **Properties** | Permissions | Metrics | Management | Access Points

Bucket overview

AWS Region US East (N. Virginia) us-east-1	Amazon Resource Name (ARN) arn:aws:s3:::bucket-aws34	Creation date August 5, 2024, 01:15:15 (UTC+05:30)
--	--	--

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

Disabled

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API.

Step 5: Scroll down till you find Static website hosting, click on edit

Requester pays
Edit

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)

Requester pays
Disabled

Static website hosting
Edit

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

Static website hosting
Disabled

Step 6: Enable static website hosting, in Index document, write the name of your document and in error document, give name as 404.html. Save your changes.

Edit static website hosting
Info

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](#)

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.
home.html

Error document - optional
This is returned when an error occurs.
404.html

Redirection rules - optional
Redirection rules, written in JSON, automatically redirect web browser requests for specific content. [Learn more](#)

Step 7: Go to Objects tab and click on upload file.

Objects
Properties
Permissions
Metrics
Management
Access Points

Objects (0)
Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload

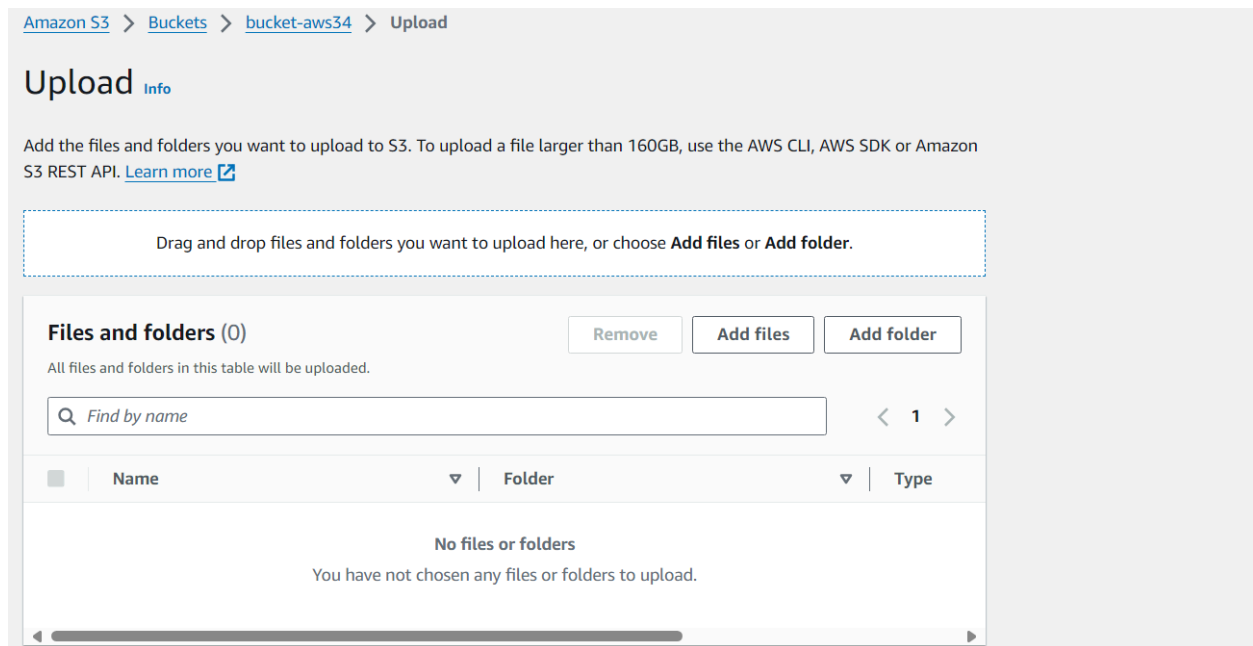
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix
1

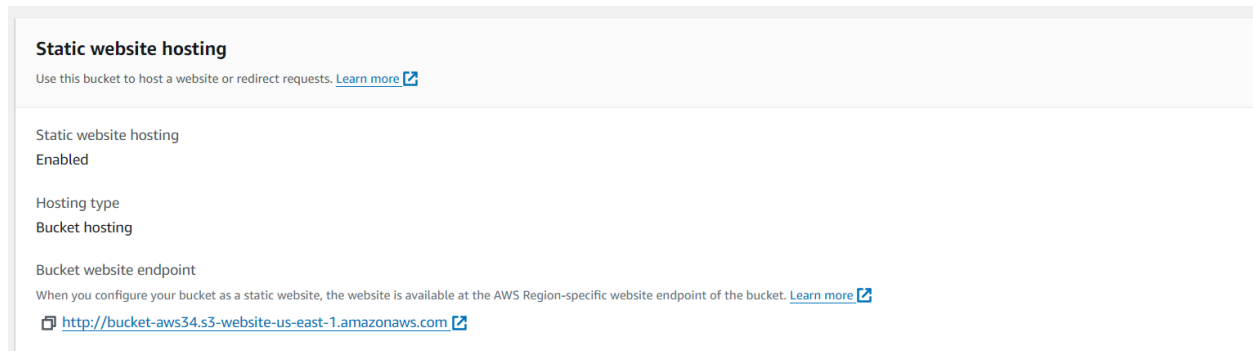
Name
Type
Last modified
Size
Storage class

No objects
You don't have any objects in this bucket.
Upload

Step 8: Click on Add files. Add all the files you want to upload. Then scroll down and click on Upload



Step 9: This will take you to the Objects screen. Switch to Properties, scroll down to Static web hosting. There you would find the link (Bucket website endpoint) to your website.



Step 10: Open the link. It will show a 403 forbidden error screen as the contents of the bucket are not available for the public users. To change this, go to Permissions tab, go to Block public access and click on edit

403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: DMNXJYFFWHMDVKEX
- HostId: shEGRFa01y+WK3nJfA/qRrcJSIS/sWWEf6VVQfy1P4v8Kz4WkLrdYN8rUtXgFzVtzbXZkziVxo=

An Error Occurred While Attempting to Retrieve a Custom Error Document

- Code: AccessDenied
- Message: Access Denied

Step 11: Uncheck the Block all public access checkbox and click on save changes

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.

Step 12: Scroll down to bucket policy and click edit

Bucket policy

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](#)

Edit

Delete

No policy to display.

Copy

Step 13:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
"Sid": "PublicReadGetObject",
"Effect": "Allow",
"Principal": {
  "AWS": "*"
},
"Action": "s3:GetObject",
"Resource": "arn:aws:s3:::YOUR-BUCKET-NAME-HERE/*"
}
]
}
```

Paste this code snippet in the policy textarea. Replace YOUR-BUCKET-NAME-HERE with the name you have given to your bucket. Save the changes.

Policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "PublicReadGetObject",
6       "Effect": "Allow",
7       "Principal": {
8         "AWS": "*"
9       },
10      "Action": "s3:GetObject",
11      "Resource": "arn:aws:s3:::bucket-aws34/*"
12    }
13  ]
14 }
15
```

Edit

Save

Step 14: Now reload the website. You can see your website

- [About](#)
- [Features](#)
- [Contact](#)

 logo

Login

Sign in




Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod

< >

Select Category:

 Category

 here latest news will come

Music



Book



Book



Book